msp

Algebra & Number Theory

msp.org/ant

K3 surfaces and equations for Hilbert modular surfaces

Noam Elkies and Abhinav Kumar

We outline a method to compute rational models for the Hilbert modular surfaces $Y_-(D)$, which are coarse moduli spaces for principally polarized abelian surfaces with real multiplication by the ring of integers in $\mathbb{Q}(\sqrt{D})$, via moduli spaces of elliptic K3 surfaces with a Shioda–Inose structure. In particular, we compute equations for all thirty fundamental discriminants D with $1 < D < 100$, and analyze rational points and curves on these Hilbert modular surfaces, producing examples of genus-2 curves over $\mathbb{Q}$ whose Jacobians have real multiplication over $\mathbb{Q}$.

1. Introduction

Hilbert modular surfaces have been objects of extensive investigation in complex and algebraic geometry, and more recently in number theory. Since Hilbert modular varieties are moduli spaces for abelian varieties with real multiplication by an order in a totally real field, they have intrinsic arithmetic content. Their geometry is enriched by the presence of modular subvarieties.

In [Hirzebruch 1973; Hirzebruch and van de Ven 1974; Hirzebruch and Zagier 1977] the geometric invariants of many of these surfaces were computed, and they were placed within the Enriques–Kodaira classification. A chief aim of the present work is to compute equations for birational models of some of these surfaces over the field of rational numbers.

More precisely, let D be a positive fundamental discriminant, i.e., the discriminant of the ring of integers $\mathcal{O}_D$ of the real quadratic field $\mathbb{Q}(\sqrt{D})$. The quotient $\mathrm{PSL}_2(O_D)\backslash(\mathcal{H}^+ \times \mathcal{H}^-)$ (where $\mathcal{H}^+$ and $\mathcal{H}^-$ are the complex upper and lower half-planes) parametrizes abelian surfaces with an action of $\mathcal{O}_D$. It has a natural

compactification $Y_-(D)$, obtained by adding finitely many points and desingularizing these cusps.

These surfaces $Y_-(D)$ have models defined over $\mathbb{Q}$, and the main goal of this paper is to describe a method to compute explicit equations for these models, as well as to carry out this method for all fundamental discriminants D with $1 < D < 100$. This felt like a good place to stop for now, though these calculations may be extended to some higher D, as well as to non-fundamental discriminants.

We briefly summarize the method, which we describe in more detail in later sections. The method relies on being able to explicitly parametrize K3 surfaces that are related by Shioda–Inose structure to abelian surfaces with real multiplication by some $\mathcal{O}_D$. The K3 surface corresponding to such an abelian surface has Néron–Severi lattice containing L_D, a specific indefinite lattice of signature $(1, 17)$ and discriminant $-D$. In all our examples, we obtain the moduli space $\mathcal{M}_D$ of L_D-polarized K3 surfaces as a family of elliptic surfaces with a specific configuration of reducible fibers and sections.

We then use the 2- and 3-neighbor method to transform to another elliptic fibration, with two reducible fibers of types II* and III* respectively. This lets us read off the map (generically one-to-one) of moduli spaces from $\mathcal{M}_D$ into the 3-dimensional moduli space $\mathcal{A}_2$ of principally polarized abelian surfaces, using the formulae from [Kumar 2008]. The image of $\mathcal{M}_D$ is the Humbert surface corresponding to discriminant D. The Hilbert modular surface $Y_-(D)$ itself is a double cover of the Humbert surface, branched along a union of modular curves. We use simple lattice arguments to obtain the branch locus, and pin down the exact twist for the double cover by counting points on reductions of the related abelian surfaces modulo several primes. In all our examples, the Humbert surface happens to be a rational surface (i.e., birational to $\mathbb{P}^2$ over $\mathbb{Q}$), and we display the equation of $Y_-(D)$ as a double cover of $\mathbb{P}^2$ branched over a curve of small degree. We analyze these equations in some detail, attempting to produce rational or elliptic curves on them, with the intent of producing several (possibly infinitely many) examples of genus-2 curves whose Jacobians have real multiplication. When $Y_-(D)$ is a K3 surface, it often has very high Picard number (19 or 20), and we attempt to compute generators for the Picard group. When $Y_-(D)$ is an honestly elliptic surface, we analyze the singular fibers and the Mordell–Weil group, and attempt to compute a basis for the sections.

To our knowledge, this is the first algebraic description of most of these surfaces by explicit equations. We outline some related work in the literature. Wilson [1998; 2000] obtained equations for the Hilbert modular surface $Y_-(5)$ corresponding to the smallest fundamental discriminant $D > 1$. Van der Geer [1988] gives a few examples of algebraic equations for Hilbert modular surfaces corresponding to a congruence subgroup of the full modular group (in other words, abelian surfaces

with some level structure). Humbert surfaces have also been well-studied in the literature, and Runge [1999] and Gruenewald [2008] have obtained equations for some of these. However, these equations are quite complicated, and do not shed as much light on the geometry of Hilbert modular surfaces. While the methods are simpler, involving theta functions and q-expansions, the result is analogous to exhibiting the modular polynomial whose zero locus in $\mathbb{A}^1 \times \mathbb{A}^1$ is a singular model of the complement of the cusps in the modular curve $X_0(N)$. The coefficients of these polynomials can quickly become enormous. We believe that our approach, giving simpler equations for these surfaces together with their maps to $\mathcal{A}_2$, is more conducive to an investigation of arithmetic properties.

It is our hope that these equations will be of much help in subsequent arithmetic investigation of these surfaces. For instance, they should provide a testing ground for many conjectures in Diophantine geometry, because of the abundance of rational curves and points. Another direction of future investigation is to use these equations to investigate modularity of the corresponding abelian surfaces. Modularity of abelian varieties with real multiplication over $\mathbb{Q}$ is now proven, by combining results of Ribet [2004] with the recent proof of Serre's conjecture by Khare and Wintenberger [2009a; 2009b]. However, unlike the case of dimension 1, where one has modular parametrizations and very good control of the moduli spaces, the situation in dimensions 2 and above is much less clear. For instance, it is not at all clear how to find a modular form corresponding to a given abelian surface with real multiplication.[1] We hope that the abundance of examples provided by these equations will help pave the path for a better understanding of the 2-dimensional case. For example, in [Dembélé and Kumar 2013], our formulas are combined with efficient computation of Hilbert modular forms to find examples of simple abelian surfaces over real quadratic fields, with everywhere good reduction. An example of such an abelian surface is the Jacobian of the genus-2 curve

$$2y^2 = x^6 - \tau x^5 + 74x^4 - 14\tau x^3 + 267x^2 - 13\tau x + 46$$
$$= \left(x^3 - \frac{1+\tau}{2}x^2 + 13x + \frac{3-\tau}{2}\right)\left(x^3 + \frac{1-\tau}{2}x^2 + 13x - \frac{3+\tau}{2}\right),$$

where $\tau = \sqrt{193}$ (the curve and its Jacobian can in fact be defined over $\mathbb{Q}$, but the Jacobian attains everywhere good reduction and real multiplication by $\mathcal{O}_{17}$ only over $\mathbb{Q}(\tau)$).

---

[1] Suppose $A/\mathbb{Q}$ is an abelian surface with $\mathbb{Q}$-endomorphisms by $\mathcal{O}_D$, and let $\varphi = \sum_n a_n q^n$ be an eigenform with every $a_n \in \mathcal{O}_D$. If φ corresponds to A then counting points over $\mathbb{F}_p$ and $\mathbb{F}_{p^2}$ determines each a_p up to Galois conjugation. But conceivably there might be some eigenform $\varphi' = \sum_n a'_n q^n$, different from both φ and its Galois conjugate, such that each a'_p equals either a_p or the Galois conjugate of a_p; if that happens, we do not know how to decide which eigenform corresponds to A. Likewise for abelian varieties of dimension 3 and higher.

The outline for the rest of the paper is as follows. In Section 2, we describe the relevant background on K3 surfaces and their moduli spaces, and their connection to moduli spaces of abelian surfaces via Shioda–Inose structures. In Section 3, we describe the Hilbert modular surfaces and the corresponding moduli spaces of K3 surfaces. In Section 4, we precisely describe our methods to compute their equations. Section 5 describes the 2- and 3-neighbor method in more detail. The rest of the paper consists of detailed examples of Hilbert modular surfaces for the discriminants less than 100, as well as an arithmetic investigation of these surfaces.

An accompanying online supplement contain formulas for the Igusa–Clebsch invariants, as well as a description of the parametrizations exhibited for the moduli spaces of K3 surfaces in the paper, and the details of the neighbor steps to transform to a fibration with II* and III* fibers. The online supplement can be obtained from this article's publication page. The files are also available as part of the source package for the arXiv version of this article (arXiv 1209.3527). See the file README.txt for an overview.

2. Moduli spaces of abelian surfaces and lattice polarized K3 surfaces

Throughout this section, we work with K3 surfaces over a field k of characteristic 0. When convenient, we will suppose $k \subseteq \mathbb{C}$, and use transcendental methods.

2.1. *K3 surfaces.* A K3 surface X over k is a projective algebraic nonsingular surface with $h^1(X, \mathcal{O}_X) = 0$ and $K_X \cong \mathcal{O}_X$. For such a surface, $H^2(X, \mathbb{Z})$ is torsion-free, and when endowed with the cup-product form becomes a 22-dimensional lattice, abstractly isomorphic with $\Lambda := E_8(-1)^2 \oplus U^3$. Here E_8 is the even unimodular lattice in eight dimensions, U is the hyperbolic plane with Gram matrix $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, and for any lattice Λ and real number α, the lattice $\Lambda(\alpha)$ consists of the same underlying abelian group with the form multiplied by α. The Néron–Severi group $NS(X)$ of algebraic divisors defined over $\bar{k}$ modulo algebraic equivalence, which for a K3 surface is the same as linear or numerical equivalence, is a primitive sublattice of Λ of signature $(1, \rho - 1)$, where $\rho \in \{1, \dots, 20\}$ is the Picard number of X. The orthogonal complement of $NS(X)$ is the transcendental lattice T_X. There is a Torelli theorem for K3 surfaces, due to Piatetski-Shapiro and Shafarevich [1971] and Friedman [1984], which describes the moduli space of K3 surfaces with a fixed polarization. More generally, let L be an even nondegenerate lattice of signature $(1, r - 1)$, with $r \in \{1, \dots, 20\}$. Assume that L has a unique primitive embedding in Λ, up to isometries of Λ. Then there is a coarse moduli space $\mathcal{F}_L$ of L-polarized K3 surfaces (X, j), where $j : L \to NS(X)$ is a primitive lattice embedding such that $j(L)$ contains a pseudo-ample class on X. The space $\mathcal{F}_L$ is isomorphic to the quotient of an appropriate fundamental

domain

$$\Omega_L = \mathbb{P}\big(\{\omega \in L^\perp \otimes \mathbb{C} \mid \langle \omega, \omega \rangle = 0, \langle \omega, \bar{\omega} \rangle > 0\}\big)$$

by an arithmetic subgroup Γ_L, which is the image of

$$\Gamma(L) = \{\sigma \in O(\Lambda) \mid \forall x \in L, \sigma(x) = x\}$$

in $O(\Lambda^\perp)$. (Here, we have fixed an embedding $i : L \to \Lambda$, so we may use its orthogonal complement $L^\perp$.) Therefore $\mathcal{F}_L$ is a quasiprojective variety.

In fact, there is a fine moduli space $\mathcal{K}_L$ of marked pseudo-ample L-polarized K3 surfaces, i.e., (X, ϕ), where $\phi : H^2(X, \mathbb{Z}) \to \Lambda$ is an isomorphism (a *marking*) such that $\phi^{-1}(L) \subseteq \mathrm{NS}(X)$. There is a period map which associates to such a marked K3 surface the class of the global algebraic 2-form up to scaling, giving a point $[\omega] \in \mathbb{P}(L^\perp \otimes \mathbb{C})$. Furthermore, $\omega \cup \omega = 0$ and $\omega \cup \bar{\omega} > 0$. This domain Ω_L consists of two copies of a bounded Hermitian domain of type IV_{20-r}. The period map $(X, \phi) \to [\omega_X]$ sets up an isomorphism between the moduli space $\mathcal{K}_L$ and the period domain Ω_L, using the Torelli theorem and the surjectivity of the period map [Kulikov 1977; Persson and Pinkham 1981]. The quotient $\Gamma_L \backslash \mathcal{K}_L \cong \Gamma_L \backslash \Omega_L$ forgets the marking, and describes a coarse moduli space of L-polarized K3 surfaces. For details, the reader may consult [Nikulin 1979a; Dolgachev 1996].

2.2. *Elliptic K3 surfaces.* We shall be especially interested in moduli spaces of elliptic K3 surfaces. In this paper, an elliptic K3 surface will be a K3 surface X with a relatively minimal genus-1 fibration $\pi : X \to \mathbb{P}^1$, together with a section. In other words, we may write a Weierstrass equation of X over $\mathbb{P}^1_t$ as

$$y^2 + a_1(t)xy + a_3(t)y = x^3 + a_2(t)x^2 + a_4(t)x + a_6(t), \tag{1}$$

with $a_i(t)$ a polynomial in t of degree at most $2i$. (More canonically, each a_i is a homogeneous polynomial of degree $2i$ in the two homogeneous coordinates of $\mathbb{P}^1_t$.) Of course, this Weierstrass equation describes the generic fiber of X; to understand the reducible special fibers, one can use Tate's algorithm [1975] to blow up the singular points and describe the minimal proper model. (This will also detect when a Weierstrass equation (1) is equivalent to one with each a_i vanishing to order at least i at some t_0, that is, when the equation gives not a K3 elliptic surface but a rational or constant one.) The singular fibers are classified by Kodaira and Néron, and the non-identity components of any reducible fiber $\pi^{-1}(v)$ contribute an irreducible root lattice (scaled by -1), say L_v, to the Néron–Severi lattice. The *trivial lattice* is defined to be

$$T = \mathbb{Z}O \oplus \mathbb{Z}F \oplus \left(\bigoplus_v L_v\right)$$

(note that O and F span a copy of the hyperbolic plane U).

A theorem of Shioda and Tate [Shioda 1972; 1990; Tate 1966b] shows that as long as the elliptic fibration is nontrivial (equivalently, it has at least one singular fiber), the Mordell–Weil group of X over $\mathbb{P}^1$ is isomorphic to $\mathrm{NS}(X)/T$. In particular, we have the Shioda–Tate formula

$$\rho(X) = 2 + \operatorname{rank} \mathrm{MW}(X/\mathbb{P}^1) + \sum_v \operatorname{rank} L_v.$$

One may also compute the discriminant of the Néron–Severi lattice:

$$|\mathrm{disc}(\mathrm{NS}(X))| = \frac{\det(H(X/\mathbb{P}^1)) \cdot \prod_v \mathrm{disc}(L_v)}{|\mathrm{MW}(X/\mathbb{P}^1)_{\mathrm{tors}}|^2},$$

where $H(X/\mathbb{P}^1)$ is the height pairing matrix for a basis of the torsion-free part of the Mordell–Weil group of X over $\mathbb{P}^1$.

If F is the class of the fiber for an elliptic K3 surface X, then F is primitive and nef, with $F^2 = 0$. Conversely, suppose that $F \in \mathrm{NS}(X)$ is a nonzero divisor class which is primitive and nef with $F^2 = 0$. Then a simple application of the Riemann–Roch theorem shows that F or $-F$ must be effective, and since F is nef, it must be represented by an effective divisor. Then a theorem of Piatetski-Shapiro and Shafarevich [1971, p. 559] shows that F defines a genus-1 fibration.

Lemma 1. *Let $F = \sum a_i E_i$ be a positive linear combination of smooth rational curves on a K3 surface X such that $F \cdot E_i = 0$ for all i, and such that F is a primitive class in $\mathrm{NS}(X)$. Then F defines a genus-1 fibration.*

Proof. We have $F^2 = \sum a_i (F \cdot E_i) = 0$. By the above discussion, it is enough to show that F is nef. Let E' be an irreducible curve on X. If E' is distinct from the E_i, then $E_i \cdot E' \geq 0$ for every i, and so $F \cdot E' \geq 0$. On the other hand, if $E' = E_i$, say, then $F \cdot E' = F \cdot E_i = 0$. Therefore F is nef.   □

Let us define an *elliptic divisor* to be a divisor satisfying the conditions of Lemma 1. We will frequently use this lemma, displaying an elliptic divisor by finding a subdiagram of the set of roots of $\mathrm{NS}(X)$, represented by smooth rational curves, which is an extended Dynkin diagram for a root lattice. Then the class of the appropriate linear combination of roots F will define a genus-1 fibration. We need to know when such a fibration has a section.

Lemma 2. *Suppose F is an elliptic divisor defining a genus-1 fibration $\pi : X \to \mathbb{P}^1$. Suppose $D \in \mathrm{NS}(X)$ satisfies $D \cdot F = 1$. Then π has a section.*

Proof. Consider the divisor $D' = D + mF$, for some large integer m. Then $(D')^2 = D^2 + 2m$, while $K \equiv 0$, so the Riemann–Roch theorem implies

$$h^0(D') - h^1(D') + h^2(D') = \frac{(D')^2}{2} + \chi(\mathcal{O}_X) = D^2 + m + 2.$$

Also, $h^2(D') = h^0(K - D') = h^0(-D') = 0$ by Serre duality, and since $(-D') \cdot H = -D \cdot H - mF \cdot H < 0$ for any ample divisor H, as long as m is large enough. Therefore we see that for large m, the divisor class D' can be represented by an effective divisor, which we may call D', by abuse of notation. Note that we still have $D' \cdot F = 1$. Decompose D' as $D'_{\text{vert}} + D'_{\text{hor}}$, where the first term contains all the components which lie along fibers of the genus-1 fibration defined by F, and the second contains the other components. Then $D'_{\text{hor}} \cdot F = 1$. Therefore, D'_{hor} must be reduced and irreducible, and thus defines a section of the genus-1 fibration. $\square$

Corollary 3. *Let F be an elliptic divisor, and let D_1 and D_2 be two divisor classes such that $D_1 \cdot F$ and $D_2 \cdot F$ are coprime. Then the fibration has a section.*

Proof. There exist integers a_1, a_2 such that $(a_1 D_1 + a_2 D_2) \cdot F = 1$. Now take $D = a_1 D_1 + a_2 D_2$ in Lemma 1. $\square$

Finally, we note a lattice-theoretic result which allows us to deduce that in all of the cases studied in this paper, the genus-1 fibration defined by an elliptic divisor F has a section.

Proposition 4. *Let D be a fundamental discriminant, and let $L = U \oplus N(-1)$, where U is the hyperbolic plane and N a positive definite lattice of rank 16 and discriminant D. Suppose in addition that N contains a sublattice isomorphic to $E_8 \oplus E_7$. If $v \in L$ is a primitive vector with $v \cdot v = 0$, then there exists $w \in L$ such that $v \cdot w = 1$.*

Proof. Suppose not. Then $\{v \cdot w : w \in L\} = c\mathbb{Z}$ for some integer $c > 1$. Since v is primitive, we can take a basis $v_1 = v, \ldots, v_{16}$ of L. Then

$$L' = \mathbb{Z}(v/c) + \mathbb{Z}v_2 + \cdots + \mathbb{Z}v_{16}$$

is an integral lattice containing L with index $c > 1$. Since $L' \supset L \supset U$, we have $L' = U \oplus N'(-1)$ (since U is unimodular), with N' a positive definite lattice containing N with index c. Then N' must be generated by $E_8 \oplus E_7$ and a vector x whose projection $x^\perp$ to the orthogonal complement of $E_8 \oplus E_7$ has norm $D/(2c^2)$. The dual lattice of $E_8 \oplus E_7$ has norms congruent to 0 or $\frac{3}{2}$ modulo 2, so $x^\perp$ has norm 0 or $\frac{1}{2}$ mod 2. Therefore D/c^2 must be an integer congruent to 0 or 1 modulo 4. Since D is a fundamental discriminant, this is impossible. $\square$

For the examples in this paper, we will often draw a Dynkin-type diagram indicating some of the roots of $\mathrm{NS}(X)$ for an elliptic K3 surface X, which will always be nodal classes (i.e., classes of smooth rational curves on X). We will outline an elliptic divisor F by drawing a subdiagram in bold which cuts out an extended Dynkin diagram of an irreducible root lattice (the multiplicities will be omitted). Where convenient, we will also indicate the class of a divisor D such that $D \cdot F = 1$ (in some cases, there is an obvious node in the Dynkin diagram satisfying

this property), or the classes of two divisors D_1 and D_2 such that $D_1 \cdot F$ and $D_2 \cdot F$ are coprime. This is not strictly necessary, because Proposition 4 guarantees the existence of such a divisor D, but having an explicit divisor might be useful for further calculations. Then F defines another elliptic fibration with section on X, and we may proceed as in Section 5 to write down its Weierstrass equation.

2.3. *Kummer surfaces, Nikulin involutions and Shioda–Inose structures.* Let A be an abelian surface, and consider the involution ι on A defined by multiplication by -1 in the group law. The quotient of A by the group $\{1, \iota\}$ is a surface Y' with sixteen singularities, the images of the 2-torsion points of A. In fact, Y' may be realized as a quartic surface in $\mathbb{P}^3$ with sixteen ordinary double points (which is the maximum number of singularities possible for a quartic surface in $\mathbb{P}^3$ [Hudson 1990, p. 15]), by considering the linear system on A corresponding to twice the theta divisor. The corresponding map is two-to-one from A to Y'.

Taking the minimal desingularization of Y' gives a K3 surface Y, the Kummer surface of A, which contains sixteen disjoint nodal classes coming from the blowups of the sixteen singular points. Note that if A is defined over some number field k, then so is $Y = \text{Km}(A)$. The Néron–Severi lattice of the surface Y contains the saturation of the lattice spanned by the sixteen special nodal classes; this is a lattice Λ_{Km} of signature $(0, 16)$ and discriminant 2^6. Conversely, Nikulin showed that a K3 surface whose Néron–Severi lattice contains Λ_{Km} must be the Kummer surface of some complex torus. Of course, since A is an abelian variety, Y is a projective surface, so $\text{NS}(Y)$ contains an ample divisor as well.

We will be especially concerned with the case when $A = J(C)$ is the Jacobian of a curve of genus 2. Let $x_0, \dots, x_5$ be the Weierstrass points of C. The embedding $\eta_0 : C \to A$ given by $x \mapsto [x] - [x_0]$ gives a particular theta divisor on A, and the translates $\eta_0(C) + [x_i] - [x_j]$ with $0 \le i < j \le 5$ give fifteen more special divisors. The images of these sixteen divisors (tropes) on the Kummer surface of A are disjoint rational curves, and each intersects six rational curves coming from the blowups of the singular points (i.e., the nodes). This classical configuration of tropes and nodes on the Kummer surface is called the $(16, 6)$ configuration, and the intersection pairing describes a vertex- and edge-transitive bipartite graph of degree 6 on 32 vertices, isomorphic with the quotient of the 6-cube by central reflection.

Next, consider a K3 surface X with a symplectic involution ι, i.e., an involution ι that multiplies the algebraic 2-forms on X by $+1$ (such an involution of X is also known as a Nikulin involution). Then ι has eight fixed points on X, and the minimal desingularization Y of the quotient $X/\{1, \iota\}$ is again a K3 surface. If in addition Y is a Kummer surface $\text{Km}(A)$ and the quotient map $\pi : X \to Y$ induces a Hodge isometry $\pi_* : T_X(2) \cong T_Y$, we say that X and A are related by a Shioda–Inose

structure. We have a diagram
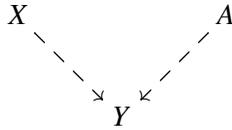
of rational maps of degree 2, and Hodge isometries $T_X(2) \cong T_Y \cong T_A(2)$, thus inducing a Hodge isometry $T_X \cong T_A$. (Note: A Hodge isometry is an isometry of cohomology lattices compatible with the Hodge decomposition.)

Conversely, a theorem of Morrison [1984] shows that any Hodge isometry between T_X and T_A for a K3 surface X and an abelian surface A is induced by a Shioda–Inose structure.

2.4. *Elliptic K3 surfaces with* II* *and* III* *fibers, and curves of genus* 2. We shall exploit such a Shioda–Inose correspondence between Jacobians of genus-2 curves and elliptic K3 surfaces with singular fibers of type II* and III*; equivalently, whose root lattices L_v are E_8 and E_7 respectively. Let C be a curve of genus 2 over k, and let

$$y^2 = f(x) = f_6 x^6 + \cdots + f_0 = f_6 \prod (x - \alpha_i)$$

be a Weierstrass equation for C, with $f_i \in k$ and $\alpha_i \in \bar{k}$ (though in general $\alpha_i \notin k$). There exist polynomial functions $I_2(f)$, $I_4(f)$, $I_6(f)$ and $I_{10}(f) = \mathrm{disc}(f)$ of degrees $2, 4, 6, 10$ in the coefficients of f (the Igusa–Clebsch invariants of f), giving a well-defined point $(I_2 : I_4 : I_6 : I_{10})$ in weighted projective space $\mathbb{P}^3_{1,2,3,5}$ which does not depend on the choice of Weierstrass equation. The complement of the hyperplane $z_4 = 0$ (where z_4 is the last coordinate on $\mathbb{P}^3_{1,2,3,5}$) yields a coarse moduli space $\mathcal{M}_2$ of curves of genus 2 [Igusa 1960]. Note that I_{10} is the discriminant of the sextic polynomial f, and therefore it cannot vanish. Also, the space $\mathcal{M}_2$ has a singular point at $(0:0:0:1)$, corresponding to the curve $y^2 = x^5 + 1$. Given $\alpha_1, \alpha_2, \alpha_3, \alpha_5 \in k$, with $\alpha_5 \neq 0$, it is not necessarily the case that one can construct a genus-2 curve over k with invariants $I_d = \alpha_{2d}$. There is an obstruction in $\mathrm{Br}_2(k)$: when it vanishes, the construction of C is made explicit by Mestre [1991]. In any case, C may always be defined over a quadratic extension of k. When k is a finite field, the Brauer obstruction vanishes, and we may define C over k. Also note that such a curve C is unique only up to $\bar{k}$-isomorphism, since $\mathcal{M}_2$ is only a coarse moduli space.

The main result of [Kumar 2008] is the following.

Theorem 5. *The elliptic* K3 *surface given by the Weierstrass equation*

$$y^2 = x^3 - t^3 \left(\frac{I_4}{12} t + 1 \right) x + t^5 \left(\frac{I_{10}}{4} t^2 + \frac{I_2 I_4 - 3 I_6}{108} t + \frac{I_2}{24} \right),$$

which has elliptic fibers of type E_8 and E_7 respectively at $t = \infty$ and $t = 0$, is related by a Shioda–Inose structure to the Jacobian of the genus-2 curve C whose Igusa–Clebsch invariants are $(I_2 : I_4 : I_6 : I_{10})$.

Let L be $U \oplus E_8(-1) \oplus E_7(-1)$. Then the above theorem gives an isomorphism

$$\psi : \mathcal{M}_2 \to \mathcal{E}_{E_8, E_7}$$

between the coarse moduli space $\mathcal{M}_2$ of genus-2 curves and the moduli space of elliptic K3 surfaces with an E_8 fiber at ∞ and an E_7 fiber at 0. Furthermore, this correspondence is Galois-invariant: the Igusa–Clebsch invariants of C and the Weierstrass coefficients of the K3 surface are defined over the same field. This is the key fact which leads to number-theoretic applications, such as computation of models of Shimura curves over $\mathbb{Q}$ in [Elkies 2008] or of Hilbert modular surfaces in this paper. However, note that C may not be itself defined over the ground field, even though its Igusa–Clebsch invariants are.

Now, let $\mathcal{A}_2$ be the moduli space of principally polarized abelian surfaces. Note that the space $\mathcal{M}_2$ is the complement of the divisor in $\mathcal{A}_2$ consisting of points corresponding to the product of two elliptic curves. On the other hand, the moduli space $\mathcal{E}_{E_8, E_7}$ is an open subset of the moduli space $\mathcal{F}_L$ of K3 surfaces polarized by $L = U \oplus E_8(-1) \oplus E_7(-1)$. We may write such a K3 surface in Weierstrass form

$$y^2 = x^3 + t^3(at + a')x + t^5(b''t^2 + bt + b').$$

It has an E_8 fiber at $t = \infty$ and at least an E_7 fiber at $t = 0$. The discriminant of the cubic polynomial is

$$d = -t^9 \big(27b''^2 t^5 + 54bb''t^4 + (4a^3 + 27b^2 + 54b'b'')t^3$$
$$+ (12a^2 a' + 54bb')t^2 + (12aa'^2 + 27b'^2)t + 4a'^3 \big).$$

By Tate's algorithm, $b'' \neq 0$ (otherwise we would have a rational elliptic surface), and the fiber at $t = \infty$ must be of type E_8, while the fiber at $t = 0$ is of type E_7 if and only if $a' \neq 0$, in which case one may set $a' = -1$ by scaling (x, y, t) appropriately. If on the other hand $a' = 0$, then the E_7 fiber gets promoted to an E_8 fiber (and no further, since b' cannot vanish, else we would have a rational elliptic surface). Therefore, the moduli space $\mathcal{E}_{E_8, E_7}$ is the complement in $\mathcal{F}_L$ of the hypersurface $a' = 0$ that corresponds to polarization by $U \oplus E_8(-1) \oplus E_8(-1)$.

When we do have $a' = 0$, it was shown by Inose that the K3 surface

$$y^2 = x^3 + at^4 x + t^5(b''t^2 + bt + b')$$

has a Shioda–Inose structure, making it 2-isogenous with a product of two elliptic curves [Inose 1978; Shioda 2006; Kuwata and Shioda 2008; Clingher and Doran 2007; Elkies ≥ 2015]. Recall that $b'b'' \neq 0$, and it follows from the formulas in

[Inose 1978; Shioda 2006; Kumar 2008] that the j-invariants j_1, j_2 of the two elliptic curves are determined by

$$\frac{j_1}{1728}\frac{j_2}{1728} = \frac{-a^3}{27b'b''}, \quad \left(1 - \frac{j_1}{1728}\right)\left(1 - \frac{j_2}{1728}\right) = \frac{b^2}{4b'b''}.$$

Note that again the map is Galois invariant and invertible, since a is only defined up to a cube root of unity (one may scale x by a cube root of unity), and b is only defined up to sign (one may scale t by -1).

Putting everything together, we have the following proposition.

Proposition 6. *There is a Galois invariant isomorphism $\phi : \mathcal{F}_L \to \mathcal{A}_2$, which on the open subset $\mathcal{E}_{E_8,E_7}$ restricts to the inverse of the explicit isomorphism $\psi : \mathcal{M}_2 \to \mathcal{E}_{E_8,E_7}$ given by Theorem 5.*

For a Hodge-theoretic approach to this isomorphism of moduli spaces, see [Gritsenko and Nikulin 1997, pp. 186–188].

3. Humbert surfaces and Hilbert modular surfaces

We next discuss moduli spaces of abelian surfaces with real multiplication. As above, let $D > 0$ be a fundamental discriminant, i.e., $D = d$ for $d \equiv 1 \pmod 4$ or $D = 4d$ for $d \equiv 2, 3 \pmod 4$, where $d > 1$ is squarefree in both cases. Then D is the discriminant of the ring of integers $\mathcal{O}_D = \mathbb{Z} + \mathbb{Z}(D + \sqrt{D})/2$ of the real quadratic field $K = \mathbb{Q}(\sqrt{D})$. Let σ_1, σ_2 be the two embeddings of K into $\mathbb{C}$. Then $\mathrm{SL}_2(\mathcal{O}_D)/\{\pm 1\}$ acts on $\mathcal{H}^+ \times \mathcal{H}^-$ by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} : (z_1, z_2) \mapsto \left(\frac{\sigma_1(a)z + \sigma_1(b)}{\sigma_1(c)z + \sigma_1(d)}, \frac{\sigma_2(a)z + \sigma_2(b)}{\sigma_2(c)z + \sigma_2(d)}\right),$$

where $\mathcal{H}^+ = \{z \in \mathbb{C} \mid \mathrm{Im}\, z > 0\}$ is the complex upper half-plane and $\mathcal{H}^- = -\mathcal{H}^+$ is the lower half-plane.

Let

$$\mathrm{SL}_2(\mathcal{O}_D, \mathcal{O}_D^*) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(K) \,\middle|\, a, d \in \mathcal{O}_D, c \in \mathcal{O}_D^*, b \in (\mathcal{O}_D^*)^{-1} \right\}.$$

We claim that this action is equivalent to the action of $\mathrm{SL}_2(\mathcal{O}_D, \mathcal{O}_D^*)$ on $\mathcal{H}^+ \times \mathcal{H}^+$. Here $\mathcal{O}_D^*$ is the dual of $\mathcal{O}_D$ with respect to the trace form on K (that is, $\mathcal{O}_D^*$ is the inverse different of K). It is an invertible $\mathcal{O}_D$-module of rank 1; in fact, it is easily checked to be $(1/\sqrt{D})\mathcal{O}_D$. Assume, without loss of generality, that $\sigma_1(\sqrt{D}) > 0$ and $\sigma_2(\sqrt{D}) < 0$. Then if we let

$$\psi : \mathcal{H}^+ \times \mathcal{H}^- \to \mathcal{H}^+ \times \mathcal{H}^+$$

be the biholomorphic map $(z_1, z_2) \mapsto (z_1\sigma_1(\sqrt{D}), z_2\sigma_2(\sqrt{D}))$, and

$$\phi : \mathrm{SL}_2(\mathcal{O}_D) \to \mathrm{SL}_2(\mathcal{O}_D, \mathcal{O}_D^*)$$

be the group isomorphism given by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} a & b\sqrt{D} \\ c/\sqrt{D} & d \end{pmatrix},$$

an easy check shows that the following diagram commutes.

$$
\begin{array}{ccc}
\mathrm{SL}_2(\mathcal{O}_D) \times \mathcal{H}^+ \times \mathcal{H}^- & \longrightarrow & \mathcal{H}^+ \times \mathcal{H}^- \\
\downarrow{\scriptstyle \phi \times \psi} & & \downarrow{\scriptstyle \psi} \\
\mathrm{SL}_2(\mathcal{O}_D, \mathcal{O}_D^*) \times \mathcal{H}^+ \times \mathcal{H}^+ & \longrightarrow & \mathcal{H}^+ \times \mathcal{H}^+
\end{array}
$$

Therefore, ψ induces an isomorphism on the quotients, as desired.

Next, we outline the proof that $\mathrm{SL}_2(\mathcal{O}_D, \mathcal{O}_D^*)$ is the coarse moduli space of principally polarized abelian surfaces with real multiplication by $\mathcal{O}_D$, closely following [Hirzebruch and van der Geer 1981]. Let $M = \mathcal{O}_D \oplus \mathcal{O}_D^*$, and define an alternating $\mathbb{Z}$-valued form on M by

$$E_M((\alpha_1, \beta_1), (\alpha_2, \beta_2)) = \mathrm{Tr}_{K/\mathbb{Q}}(\alpha_1 \beta_2 - \alpha_2 \beta_1).$$

Now, for $z = (z_1, z_2) \in \mathcal{H}^2$, consider the embedding

$$L_z : K \oplus K \to V = \mathbb{C}^2,$$
$$(\alpha, \beta) \mapsto \alpha z + \beta = \big(\sigma_1(\alpha)z + \sigma_1(\beta), \sigma_2(\alpha)z + \sigma_2(\beta)\big),$$

which gives us a lattice $L_z(M)$ in V. We use this to transfer E_M to $L_z(M)$ and extend the form $\mathbb{R}$-linearly. This gives an alternating form

$$E_{M,z} : V \times V \to \mathbb{R},$$

which can be described in coordinates on $\mathbb{C}^2$ as

$$E_{M,z}((\zeta_1, \zeta_2), (\eta_1, \eta_2)) = \frac{\mathrm{Im}\, \zeta_1 \overline{\eta_1}}{\mathrm{Im}\, z_1} + \frac{\mathrm{Im}\, \zeta_2 \overline{\eta_2}}{\mathrm{Im}\, z_2}.$$

This gives a Riemann form on the resulting complex torus $V/L_z(M)$, and since the form E_M on the lattice $L_z(M)$ is unimodular, we obtain an abelian variety with principal polarization. The action of $\mathcal{O}_D$ is as follows:

$$\iota(\alpha)(\zeta_1, \zeta_2) \mapsto (\sigma_1(\alpha)\zeta_1, \sigma_2(\alpha)\zeta_2).$$

Conversely, it is not hard to show that any principally polarized abelian surface with real multiplication by $\mathcal{O}_D$ can be identified with some $V/L_z(M)$. Finally, we note that the abelian surfaces corresponding to two different $z \in \mathcal{H}^+ \times \mathcal{H}^+$ are isomorphic (with an $\mathcal{O}_D$-equivariant isomorphism) exactly when these two points differ by an element of $\mathrm{SL}_2(\mathcal{O}_D, \mathcal{O}_D^*)$. Therefore, it follows that the moduli space

of abelian surfaces with real multiplication is $\mathrm{SL}_2(\mathcal{O}_D, \mathcal{O}_D^*)\backslash(\mathcal{H}^+ \times \mathcal{H}^+)$, which as we have shown above, is biholomorphic with $\mathrm{SL}_2(\mathcal{O}_D)\backslash(\mathcal{H}^+ \times \mathcal{H}^-)$.

The construction above yields a map from $\mathrm{SL}_2(\mathcal{O}_D)\backslash(\mathcal{H}^+ \times \mathcal{H}^-)$ to the quotient of $\mathcal{S}_2$, the Siegel upper half-space of degree 2, by the arithmetic group $\mathrm{Sp}_4(\mathbb{Z})$. In other words, we get a holomorphic map to $\mathcal{A}_2$, the moduli space of principally polarized abelian surfaces. Its image (or its closure in $\mathcal{A}_2$) is the *Humbert surface* $\mathcal{H}_D$ for discriminant D. We next show that the map from the Hilbert modular surface $\mathrm{SL}_2(\mathcal{O}_D)\backslash(\mathcal{H}^+ \times \mathcal{H}^-)$ to the Humbert surface is generically two-to-one. We may compute this degree above a very general point on the Humbert surface. Such a point corresponds to a principally polarized abelian surface A, where one has forgotten the action of $\mathcal{O}_D$ by endomorphisms. Generically, there are exactly two ways to extend the obvious map $\mathbb{Z} \to \mathrm{End}(A) \cong \mathcal{O}_D$ to $\mathcal{O}_D$, corresponding to the choice of image of $(D + \sqrt{D})/2$.

Our approach to computing equations of Hilbert modular surfaces begins as follows. Fix a discriminant D, which we assume to be a fundamental discriminant. First, we need to compute a model of the Humbert surface, i.e., the subvariety of $\mathcal{A}_2$ corresponding to abelian surfaces with real multiplication by $\mathcal{O}_D$. Via the inverse of the isomorphism $\phi : \mathcal{F}_L \to \mathcal{A}_2$ of Section 2.4 above, the Humbert surface corresponds to a surface inside the 3-dimensional moduli space of L-polarized K3 surfaces.

Define a pairing on $\mathcal{O}_D$ by $(\alpha, \beta) \mapsto \mathrm{tr}(\alpha\beta^*)$, where β^* is the Galois conjugate of β. This gives $\mathcal{O}_D$ the structure of an indefinite lattice, which we next identify with the Néron–Severi lattice of A.

Proposition 7. *Let A be a principally polarized abelian surface with $\mathrm{End}(A) \cong \mathcal{O}_D$. Then $\mathrm{NS}(A) \cong \mathrm{End}(A)$. The lattice $\mathrm{NS}(A)$ has a basis with Gram matrix*

$$\begin{pmatrix} 2 & D \\ D & (D^2-D)/2 \end{pmatrix} \tag{2}$$

of signature $(1, 1)$ and discriminant $-D$.

Proof. For a principally polarized abelian surface A, there is an isomorphism

$$\mathrm{NS}(A) \to (\mathrm{End}(A))^\dagger$$

induced naturally by the polarization, where $\dagger$ is the Rosati involution (also arising from the polarization). Note that for a general polarization one only gets a weaker isomorphism, between the $\mathbb{Q}$-spans of both sides. For the proof of both assertions, see Proposition 5.2.1 in [Birkenhake and Lange 2004]. Now, the Rosati involution is a positive involution of the real quadratic field $\mathrm{End}(A) \otimes \mathbb{Q}$, and hence cannot be the nontrivial element of the Galois group. It must therefore be the identity, whence the subring of $\mathrm{End}(A)$ fixed by $\dagger$ is $\mathrm{End}(A)$ itself, proving the first statement. The

isomorphism of groups $NS(A) \to End(A)$ is an isometry, taking the intersection form on $NS(A)$ to the form $(\phi, \psi) \mapsto tr(\phi \psi^\vee)$ on $End(A)$, which becomes $(\alpha, \beta) \mapsto tr(\alpha\beta^*)$ on $\mathcal{O}_D$. Computing the matrix of this form on the basis $(1, (D + \sqrt{D})/2)$ of $\mathcal{O}_D$, we obtain the claimed Gram matrix (2). $\square$

We henceforth use $\mathcal{O}_D$ also to denote the lattice with underlying group $\mathcal{O}_D \cong \mathbb{Z}^2$ and form $(\alpha, \beta) \mapsto tr(\alpha\beta^*)$, with Gram matrix (2).

Proposition 8. *There is a primitive embedding*, *unique up to isomorphism*, *of the lattice $\mathcal{O}_D$ into U^3. Let T_D be the orthogonal complement of $\mathcal{O}_D$ in U^3. Then there is a primitive embedding*, *unique up to isomorphism*, *of T_D into the K3 lattice Λ.*

Remark. In the present paper we analyze only fundamental discriminants D, for which every embedding into an even lattice of $\mathcal{O}_D$ and T_D (and of the lattice L_D, to be introduced before the next theorem) is automatically primitive. But the condition of primitivity is necessary to extend our theoretical analysis also to non-fundamental D.

Proof. Since $\mathcal{O}_D$ is 2-dimensional, the number of generators $\ell(\mathcal{O}_D^*/\mathcal{O}_D)$ of the discriminant group is at most 2. In fact, the discriminant group is cyclic of order D if D is odd, and isomorphic to $(\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/(\frac{D}{2}\mathbb{Z}))$ if D is even. Therefore, by [Nikulin 1979b, Theorem 1.14.4], $\mathcal{O}_D$ has a unique embedding into the even unimodular lattice U^3. Let the orthogonal complement be T_D; it has signature $(2, 2)$ and the same discriminant group. By another application of [Nikulin 1979b, Theorem 1.14.4], we see that T_D has a unique embedding into Λ_{K3}. $\square$

Let q_D be the discriminant form of $\mathcal{O}_D$, and let L_D be the orthogonal complement of T_D in Λ. Then L_D has signature $(1, 17)$ and discriminant form q_D. By [Nikulin 1979b, Theorem 1.13.2], L_D is characterized uniquely by its signature and discriminant form. Since $\Lambda \cong U^3 \oplus E_8(-1)^2$, it is clear that $L_D \cong E_8(-1)^2 \oplus \mathcal{O}_D$. Finally, L_D has a primitive embedding in Λ, which (again by [Nikulin 1979b, Theorem 1.14.4]) is unique up to isomorphism.

Theorem 9. *Let $\mathcal{F}_{L_D}$ be the moduli space of K3 surfaces that are lattice polarized by L_D. Then the isomorphism $\phi : \mathcal{F}_L \to \mathcal{A}_2$ of Section 2.4 induces a birational surjective morphism $\mathcal{F}_{L_D} \to \mathcal{H}_D$.*

Proof. First, we note that $\mathbb{Z} \subset \mathcal{O}_D$ induces an embedding of lattices $\langle 2 \rangle \subset \mathcal{O}_D$, and therefore an embedding $T_D \subset U^2 \oplus \langle -2 \rangle$ of orthogonal complements. Taking orthogonal complements once more in Λ_{K3}, we deduce $L \subset L_D$.

Fix embeddings $L \subset L_D \subset \Lambda_{K3}$. Then we have $L_D^\perp \hookrightarrow L^\perp$, which induces a map $\Omega_{L_D} \hookrightarrow \Omega_L$ of period domains. We also have a map $\Gamma_{L_D} \subset \Gamma_L$. These induce a map $\mathcal{F}_{L_D} = \Gamma_{L_D} \backslash \Omega_{L_D} \xrightarrow{\beta_D} \Gamma_L \backslash \Omega_L = \mathcal{F}_L$. We will use the fact that this morphism has degree 1 onto the image (i.e., it is an embedding on the generic point of $\mathcal{F}_{L_D}$). We postpone the proof of this fact until the conclusion of the present argument.

Let $\phi_D : \mathcal{F}_{L_D} \xrightarrow{\beta_D} \mathcal{F}_L \xrightarrow{\phi} \mathcal{A}_2$ be the composition of the maps above. Now suppose X is a K3 surface corresponding to a point p in the image of β_D. Then we have $\mathrm{NS}(X) \supset L_D \cong E_8(-1)^2 \oplus \mathcal{O}_D$, and therefore $T_X \subset T_D$. If A (corresponding to $\phi(p)$) is the abelian surface connected to X through a Shioda–Inose structure, we have $T_A \cong T_X \subset T_D$. Therefore, $\mathrm{NS}(A) \supset \mathcal{O}_D$, the orthogonal complement of T_D in U^3. Therefore $\mathrm{End}(A)^\dagger \supset \mathcal{O}_D$, and $\phi(p)$ must lie on the Humbert surface $\mathcal{H}_D$. This proves that the image of $\mathcal{F}_{L_D}$ lands in $\mathcal{H}_D$.

Conversely, suppose q is a point on $\mathcal{H}_D$ corresponding to an abelian surface A with real multiplication by $\mathcal{O}_D$. Then $\mathrm{End}(A) \supset \mathcal{O}_D$, and since the Rosati involution (being positive) can only act as the trivial element of $\mathbb{Q}(\sqrt{D})$, we must have $\mathrm{End}(A)^\dagger \supset \mathcal{O}_D$. Retracing the argument in the previous paragraph, we see $p = \phi^{-1}(q)$ must have $\mathrm{NS}(X) \supset L_D$, and therefore is in the image of β_D. This proves that $\phi \circ \beta_D$ is surjective onto $\mathcal{H}_D$.

Since ϕ is an isomorphism and β_D has degree 1 onto its image, so does $\phi \circ \beta_D$. $\qquad\square$

We now prove that fact used above: β_D is generically an embedding.

Proposition 10. *The map $\mathcal{F}_{L_D} \to \mathcal{F}_L$ is generically an embedding.*

Proof. To see this, we claim that it is enough to show that there is an element $\gamma_0 \in O(\Lambda)$ such that γ_0 fixes L pointwise, preserves the sublattice L_D, and acts by -1 on $L^\perp$. For suppose we have $x = \gamma y$ with $x, y \in \Omega_{L_D}$ and $\gamma \in \Gamma_L$, with x and y very general. Then we would like to show that in fact we already have $x = \gamma' y$ with $\gamma' \in \Gamma_{L_D}$. Then $\Lambda_x^{1,1} := \{z \in x \mid \langle z, x \rangle = 0\}$ and $\Lambda_y^{1,1}$ both equal L_D, since x and y are very general, and therefore γ preserves L_D (though it might not fix this lattice pointwise). If γ acts trivially on L_D, we may take $\gamma' = \gamma$, and are done. If not, then γ must act by -1 on $L_D/L \cong \mathbb{Z}$. Then $\gamma' = \gamma_0 \gamma$ will suffice.

To prove the claim, we may consider specific embeddings $L \subset L_D \subset \Lambda$. If $D \equiv 0 \pmod 4$, then $L_D \cong E_7(-1) \oplus \langle -D/2 \rangle \oplus U \oplus E_8(-1)$. We may embed it inside $(E_8(-1) \oplus U \oplus U) \oplus (U \oplus E_8(-1))$ by embedding $E_7(-1)$ inside $E_8(-1)$ as the orthogonal complement of a root δ, and $\langle -D/2 \rangle$ primitively inside $U \oplus U$. Let γ_0 be the automorphism of Λ which acts on the first copy of $E_8(-1)$ as the reflection s_δ in the hyperplane orthogonal to δ, by -1 on $U \oplus U$, and as the identity on the part $U \oplus E_8(-1)$.

If $D \equiv 1 \pmod 4$, consider a system of simple roots in $E_8(-1)$ whose intersections give the standard Dynkin matrix. Let α be the simple root such that if we remove the corresponding vertex from the Dynkin diagram, we obtain the Dynkin diagram for $E_7(-1)$. The orthogonal complement of this copy of $E_7(-1)$ is some root δ. Let $\beta \in U$ be any element of norm $(1-D)/2$. It is easy to check that the copy of $E_7(-1)$ and $\alpha + \beta$ generate a negative definite lattice M of discriminant D, and that $U \oplus M \oplus E_8(-1)$ is isometric to L_D (since it is has the right signature and discriminant). In other words, the diagram of embeddings

$$E_7(-1) \hookrightarrow M \subset E_8(-1) \oplus U \hookrightarrow E_8(-1) \oplus U^2$$

extends on adding a factor of $U \oplus E_8(-1)$ to

$$L = E_7(-1) \oplus U \oplus E_8(-1) \hookrightarrow M \oplus U \oplus E_8(-1) = L_D \subset E_8(-1) \oplus U^2 \oplus E_8(-1)$$
$$\rightarrow E_8(-1) \oplus U^3 \oplus E_8(-1) = \Lambda.$$

Now, consider the automorphism γ_0 of $\Lambda \cong E_8(-1) \oplus U^3 \oplus E_8(-1)$ given by $(s_\delta, -1|_U, -1|_U, 1_U, 1_{E_8(-1)})$. By construction, γ_0 fixes L pointwise, and acts by -1 on $L^\perp$. We need to show that γ_0 preserves L_D, or equivalently, that it preserves M. We know that M is spanned by $E_7(-1)$ (which is fixed by γ_0) and $\alpha + \beta$. Now, γ_0 takes β to $-\beta$, by construction. Also, $\alpha + \gamma_0(\alpha) = \alpha + s_\delta(\alpha) \in E_8(-1)$ is invariant by s_δ, and is therefore in the orthogonal complement $E_7(-1)$ of δ. Therefore $\gamma_0(\alpha) \in -\alpha + E_7(-1)$ and $\gamma_0(\alpha + \beta) \equiv -(\alpha + \beta) \mod E_7(-1)$. So γ_0 preserves the lattice M.   □

Next, we want to understand the Hilbert modular surface $Y_-(D)$, which is a double cover of $\mathcal{H}_D$. First, we must identify the branch locus. Since the map $Y_-(D) \rightarrow \mathcal{H}_D$ is obtained by simply forgetting the action of $e_D = (D + \sqrt{D})/2$ on the abelian surface, the branch locus is the subvariety W of $\mathcal{H}_D$ corresponding to abelian surfaces A such that $e_D = (D + \sqrt{D})/2$ and $e'_D = (D - \sqrt{D})/2$ are conjugate in the endomorphism ring, say by $\iota \in \operatorname{End}(A)$. It follows that ι^2 fixes $\mathcal{O}_D$ pointwise. Generically this implies $\iota^2 = \pm 1$, and $\iota e_D = e'_D \iota$. This shows that $\operatorname{End}(A)$ for such A is generically an order in a quaternion algebra B.

In fact, the branch locus corresponds to the case when we have a split quaternion algebra, i.e., $\iota^2 = 1$. Then A is isogenous over $\overline{\mathbb{Q}}$ to the square of an elliptic curve. To see this fact, observe that the map $\Gamma \backslash \mathcal{H}^2 \rightarrow \operatorname{Sp}_4(\mathbb{Z}) \backslash \mathcal{S}_2$ (where $\Gamma = \operatorname{SL}_2(\mathcal{O}_D, \mathcal{O}_D^*)$) factors through the quotient $(\Gamma \cup \Gamma\sigma) \backslash \mathcal{H}^2$, where σ is the involution $(z_1, z_2) \mapsto (z_2, z_1)$ exchanging the two factors of $\mathcal{H}^2$, and the induced map on this quotient is generically one-to-one [Hirzebruch and van der Geer 1981, p. 158]. Therefore, to understand the branch locus, we need to understand the 1-dimensional part of the fixed point set of σ on $\Gamma \backslash \mathcal{H}^2$. This (and more) was done by Hausmann [1982, p. 35]. The result is that the fixed point set consists of a small number of explicit modular curves F_w for $w \in \{1, 4, D, D/4\}$ (some of these may be empty, and when they are nonempty, these curves are irreducible). A simple explicit analysis of the condition relating z_1 and z_2 on these curves reveals that the generic point on each of these corresponds to an abelian surface whose ring of endomorphisms contains zero divisors, and is therefore a split quaternion algebra. For instance, the image of the diagonal of $\mathcal{H}^2$ (given by $z_1 = z_2$) in $\Gamma \backslash \mathcal{H}^2$ is an obvious component of the branch locus. For the corresponding abelian surface, as constructed earlier in this section, the map $(\zeta_1, \zeta_2) \mapsto (\zeta_2, \zeta_1)$ is a holomorphic involution, showing that the endomorphism algebra is split. For completeness, we prove this next.

Proposition 11. *Let* $\Gamma = \mathrm{SL}_2(\mathcal{O}_D, \mathcal{O}_D^*)$ *and let C be one of the curves F_w for $w \in \{1, D\}$ if D is odd, $w \in \{1, 4, D/4, D\}$ if D is even. The generic point on C corresponds to an abelian surface whose algebra of endomorphisms is a split quaternion algebra.*

Proof. We use the notation of [van der Geer 1988, Chapter V]. The ideal $\mathfrak{a} = \mathcal{O}_D^*$ has norm $A = 1/D$. In the reference, it is assumed that $\mathfrak{a}$ is an integral ideal, but we may for instance replace $\mathcal{O}_D^*$ by the integral $D\mathcal{O}_D^* = \sqrt{D}\mathcal{O}_D$ without loss of generality in Hausmann's proof. This would replace A by $D^2A = D$, and would not affect any of the arguments below, which depend only on the square class of A. Proposition V.1.5 of [van der Geer 1988] states that a point on F_N corresponds to an abelian surface whose endomorphism algebra is isomorphic to the indefinite quaternion algebra

$$Q_N = \left(\frac{D, -N/(AD)}{\mathbb{Q}}\right),$$

while Lemma V.1.4 in the book says that F_N is nonempty if and only if for each prime q dividing D and not dividing N, we have $\chi_{D(q)}(N) = (A, D)_q$. For an explanation of the notation, see [van der Geer 1988, pp. 2–3]. In our situation, we have $AD = 1$. If $N = D$, we get the algebra $\left(\frac{D,-D}{\mathbb{Q}}\right)$, which is obviously split. This argument also takes care of $N = D/4$ when D is even. Next, suppose $N = 1$. Then F_1 is nonempty if and only if for every prime dividing D, we have $(D, D)_q = 1$. So

$$1 = (D, D)_q = (D, -D)_q \cdot (D, -1)_q = (D, -1)_q.$$

It follows that the quaternion algebra $Q_1 = \left(\frac{D,-1}{\mathbb{Q}}\right)$ is split. The proof for $N = 4$ is similar. $\square$

Remark 12. A further analysis of the proof above reveals the number of components of the branch locus, which is corroborated by the calculations in this paper.

Coming back to our analysis of the endomorphisms of the abelian surfaces corresponding to points on the branch locus, we note that the Rosati involution must fix $\mathcal{O}_D$ and ι, by positivity. Consider the form $(x, y) \mapsto \mathrm{Tr}(x\bar{y})$, where $\bar{\ } : B \to B$ is the natural involution taking $\sqrt{D}$ to its negative and ι to its negative, and Tr is the reduced trace. The matrix of this form acting on $\mathcal{O}_D + \mathbb{Z}\iota$ is

$$\begin{pmatrix} 2 & D & 0 \\ D & (D^2-D)/2 & 0 \\ 0 & 0 & -2 \end{pmatrix},$$

which therefore gives an even lattice of signature $(1, 2)$ and discriminant $2D$. We claim that when D is fundamental, the index, call it c, of $\mathcal{O}_D \oplus \mathbb{Z}\iota$ as a sublattice of $\mathrm{End}(A)$ is 1 or 2, with $c = 2$ possible only if $4 \mid D$. Indeed $\mathrm{End}(A)$ is an even

lattice of rank 3 and discriminant $2D/c^2$. But the discriminant is an even integer because the rank is odd, and D has no repeated prime factors except possibly 2^2 or 2^3. Thus as claimed the index c must be either 1 or 2, with $c = 2 \Rightarrow 4 \mid D$. Therefore, the only possibilities for the discriminant of the resulting Néron–Severi group for a point corresponding to the branch locus are $2D$ and $D/2$. This is also the discriminant of the transcendental lattice of the abelian surface, and by the Shioda–Inose structure, the corresponding K3 surface also has a Néron–Severi lattice of rank 19 and discriminant $2D$ or $D/2$, and contains $L_D \cong E_8(-1)^2 \oplus \mathcal{O}_D$.

Finally, we mention that a group of involutions acts naturally on the Hilbert modular surface $Y_-(D)$. This group is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^{t-1}$, where t is the number of distinct primes dividing D. These extra involutions arise from the Hurwitz–Maass extension of $\mathrm{PSL}_2(\mathcal{O}_D, \mathcal{O}_D^*)$. For more details see [van der Geer 1988, Section I.4].

4. Method of computation

We now outline our method to obtain equations for the Hilbert modular surfaces $Y_-(D)$ for fundamental discriminants D.

Step 1. We compute the unique lattice L_D, writing it in the form $U \oplus N$ (we know L_D contains a copy of U, since $L = U \oplus E_8(-1) \oplus E_7(-1)$ does, and $L \supset L_D$). Note that N is not uniquely determined, and it turns out to be useful to choose N such that its root lattice R has small codimension in N, and such that N/R has a basis consisting of vectors of small (fractional) norm. One may then attempt to realize L_D as the Néron–Severi lattice of an elliptic K3 surface with reducible fibers corresponding to the irreducible root lattices in R. The remaining generators of the Néron–Severi lattice should then arise as sections (of small height) in the Mordell–Weil group of the elliptic fibration. Of course, we need to make sure that N contains $E_8 \oplus E_7$, but this is easily achieved by showing that the dual lattice N^* contains a vector of norm $2/D$.

For most of the examples in this paper, we were able to describe a family of elliptic K3 surfaces with Néron–Severi lattice L_D and with Mordell–Weil rank 0 or 1. This construction gives us a Zariski-open subset of $\mathcal{F}_{L_D}$, with some possible missing curves corresponding to jumps in the Mordell–Weil ranks or the ranks of the reducible fibers, or to denominators introduced in the parametrization process.

For all the examples we considered, the moduli space $\mathcal{F}_{L_D}$ turns out to be rational (i.e., birational with $\mathbb{P}^2$ over $\mathbb{Q}$). This property will fail to hold once D is large enough, but there is still some hope of writing down usable equations for $\mathcal{F}_{L_D}$ if it is not too complicated.

Suppose that we have exhibited a Zariski open subset of $\mathcal{F}_{L_D}$ as a Zariski open subset $U = \mathbb{P}^2_{r,s} \setminus V$ of the projective plane.

Step 2. We find a different elliptic fibration on the generic member of the family of K3 surfaces in Step 1, with reducible fibers of types E_8 at $t = \infty$ and E_7 at $t = 0$. This is accomplished by 2- and 3-neighbor steps, which we shall describe in the next section.

Once we obtain the alternate elliptic fibration, we may compute the map from U to $\mathcal{A}_2$ by the explicit formulas of Section 2.4. This gives us the Igusa–Clebsch invariants of the associated genus-2 curve, in terms of the two parameters r and s.

Step 3. Consider the base change diagram

$$
\begin{array}{ccc}
\widetilde{Y}_-(D) & \xrightarrow{\ \widetilde{\eta}\ } & \mathcal{F}_{L_D} \\[4pt]
\widetilde{\phi}\big\downarrow & & \big\downarrow \phi \\[4pt]
Y_-(D) & \xrightarrow{\ \eta\ } & \mathcal{H}_D
\end{array}
$$

Since ϕ is a birational map, so is $\widetilde{\phi}$. We want to describe the degree-2 map $\widetilde{\eta}$. In the current situation, we must have a model for $\widetilde{Y}_-(D)$ (which is birational to $Y_-(D)$) of the form

$$
z^2 = f(r, s),
$$

where $f(r, s) = 0$ describes the branch locus of $\widetilde{\eta}$. As we have seen, this locus $f(r, s) = 0$ must be the union of some irreducible curves, which are either components of the excluded locus V above, or belong to the sublocus of U where the Picard number jumps by 1, the discriminant changing to $2D$ or $D/2$. There are finitely many possibilities for how this may happen. For instance, the elliptic fibration may have an extra A_1 fiber, or a D_6 fiber may get promoted to an E_7 fiber, or the surface may have a new section that raises the Mordell–Weil rank. Similarly, in any instance, we may easily list the allowed changes in the reducible fibers, or the allowed heights and intersections with components of reducible fibers of a new section of the fibration. Hence we get a list of polynomials $f_1(r, s), f_2(r, s), \ldots, f_k(r, s) \in \mathbb{Z}[r, s]$ whose zero loci are the possible components of the branch locus. We may assume that each $f_i(r, s)$ has content 1.

We therefore have the following model for $\widetilde{Y}_-(D)$ as a double cover of $\mathbb{P}^2_{r,s}$:

$$
z^2 = f(r, s) = C f_{i_1}(r, s) f_{i_2}(r, s) \ldots f_{i_m}(r, s)
$$

for some subset $\{i_1, \ldots, i_m\} \subseteq \{1, \ldots, k\}$ and some squarefree integer C.

Step 4. In the final step, we show how to compute the subset $I = \{i_1, \ldots, i_m\}$ and the twist C. First, we note that the Hilbert modular surface $Y_-(D)$ has good reduction outside primes dividing D, by [Rapoport 1978; Deligne and Pappas 1994]. Therefore, there are only finitely many choices for C as well. Now we check each of these choices by computer, using the method described in the next paragraph, and rule out all but one.

So suppose we have a putative choice of C and I. We proceed to check whether this choice of twist is correct by reduction modulo several odd primes p that do not divide the discriminant D. We specialize r, s to elements of $\mathbb{F}_p$, and by the formulas of Step 2, obtain Igusa–Clebsch invariants for in weighted projective space over $\mathbb{F}_p$. Since the Brauer obstruction vanishes for finite fields, we can construct a curve $C_{r,s}$ over $\mathbb{F}_p$.

We may use the following lemma to detect whether the Jacobian of $C_{r,s}$ has real multiplication defined over $\mathbb{F}_p$ or not.

Lemma 13. *Let A be an abelian surface over $\mathbb{F}_p$, and let ϕ be the Frobenius endomorphism of A relative to $\mathbb{F}_p$. Suppose that the characteristic polynomial $P(T)$ of ϕ is irreducible over $\mathbb{Q}$. Let Q be the symmetric characteristic polynomial of $\phi + p\phi^{-1}$, defined by $P(T) = T^2 Q(T + pT^{-1})$.*

(1) *If A has real multiplication by an order in $\mathcal{O}_D$ defined over $\mathbb{F}_p$, then Q is a quadratic polynomial of discriminant $c^2 D$ for some integer c.*

(2) *If A has real multiplication by an order in $\mathcal{O}_D$, defined over $\mathbb{F}_{p^2}$, but not over $\mathbb{F}_p$, then we have $Q(X) = X^2 - n$ for some $n \in \mathbb{Z}$ not of the form $c^2 D$ for any integer c.*

(3) *If $Q(X)$ is a quadratic polynomial of discriminant D (resp. $c^2 D$ for some positive integer c), then A has real multiplication by $\mathcal{O}_D$ (resp. an order in $\mathcal{O}_D$ of conductor dividing c), defined over $\mathbb{F}_p$.*

Note that A might simultaneously have real multiplication $\iota : \mathcal{O} \hookrightarrow \text{End}(A)$ and $\iota' : \mathcal{O}' \hookrightarrow \text{End}(A)$ by two orders of $\mathcal{O}_D$, if its ring of endomorphisms is a quaternion algebra. Furthermore, if one of these is defined over $\mathbb{F}_p$ and the other only over $\mathbb{F}_p^2$, then by parts (1) and (2) of the lemma, $Q(X)$ must be of the form $X^2 - c^2 D$ for some integer c.

We will give the proof of the lemma below, but first we indicate how to use it to find the correct twist. We choose a suitable prime $p \nmid D$, and for some r, s in $\mathbb{F}_p$, we calculate the number of points mod p and p^2 of the resulting curve $C_{r,s}$. This is enough to describe the polynomial $Q(X)$ for the abelian surface $A = J(C)$, by the Lefschetz–Grothendieck trace formula. Suppose $P(T) = T^2 Q(T + pT^{-1})$ is irreducible. Then the first hypothesis of the lemma is satisfied. If in addition $Q(X) = X^2 + aX + b$ has discriminant D and nonzero linear term a, then A must have real multiplication defined over $\mathbb{F}_p$, by part (3) of the lemma (and the comments following it). In fact, most of the time we can even make do with the weaker assumption that $Q(X)$ has discriminant in the square class of D, since (3) guarantees that A has real multiplication by an order in $\mathbb{Q}(\sqrt{D})$. We can compute the discriminant of $\text{NS}(A)$ by computing that of $\text{NS}(Y)$, where Y is the elliptic K3 surface related to A by a Shioda–Inose structure. If this discriminant is D, it follows that A must have real multiplication by the full ring of integers $\mathcal{O}_D$.

Now, by the property of a coarse moduli space, A gives rise to an $\mathbb{F}_p$-point (r, s) of the Hilbert modular surface $Y_-(D)$, i.e., the corresponding point on the Humbert surface must actually lift to the double cover. Therefore, if $Cf_{i_1}(r, s) \ldots f_{i_m}(r, s)$ is not a square, we must have the wrong quadratic twist. We can run this test for many such $(r, s) \in \mathbb{F}_p \times \mathbb{F}_p$. Note that a single large prime is usually enough to pin down the correct choice of $\{i_1, \ldots, i_m\}$, by eliminating all but one possibility. However, to pin down the correct choice of C, we may need to use several primes, until we find one for which C/C' is not a quadratic residue, where C' is the correct twist. However, in any case, this procedure is guaranteed to terminate, and in practice, it terminates fairly quickly.

At the end of Step 4 of the algorithm, we have determined a birational model of $Y_-(D)$ over $\mathbb{Q}$. We now give the proof of the lemma above.

Proof of Lemma 13. We will use [Tate 1966a, Theorem 2]. Since $P(T)$ is irreducible, it follows that $F = \mathbb{Q}[\phi]$ is simple, and also that $F = E := \text{End}_{\mathbb{F}_p}(A) \otimes \mathbb{Q}$ is a quartic number field. First, assume that real multiplication by an order $\mathcal{O} \subset \mathcal{O}_D$ is defined over $\mathbb{F}_{p^2}$ but not over $\mathbb{F}_p$. Say $\mathcal{O}$ contains $f\sqrt{D}$ for some positive integer f. Then consider the base change of A to $\mathbb{F}_{p^2}$. The Frobenius over the new field is ϕ^2, and therefore, ϕ^2 commutes with $f\sqrt{D}$, but ϕ must anticommute with $f\sqrt{D}$. Therefore $\mathbb{Q}(\phi^2)$ is a strict subfield of $\mathbb{Q}(\phi)$, and must be quadratic. Hence ϕ^2 satisfies a quadratic equation $\phi^4 + a\phi^2 + b = 0$, and since this must be the characteristic polynomial of ϕ, we must have $b = p^2$. Therefore

$$\phi^2 + p^2\phi^{-2} + a = (\phi + p\phi^{-1})^2 + a - 2p = 0,$$

proving the assertion (1).

Now, assume that A has real multiplication by $\mathcal{O} \subset \mathcal{O}_D$, defined over $\mathbb{F}_p$, and let $f\sqrt{D} \subset \mathcal{O}$, as before. Then $\mathbb{Q}(\phi + p\phi^{-1})$ is a quadratic subfield of $\mathbb{Q}(\phi)$. Also, $f\sqrt{D} \in \mathbb{Q}(\phi)$, so we have $f\sqrt{D} = g(\phi)$ for some polynomial $g \in \mathbb{Q}[T]$. Then $f\sqrt{D}$ is its own dual isogeny, and so $f\sqrt{D} = g(p\phi^{-1})$ as well. Therefore, $f\sqrt{D} = \frac{1}{2}(g(\phi) + g(p\phi^{-1}))$ can be expressed as $h(\phi + p\phi^{-1})$ for some $h \in \mathbb{Q}(T)$. It follows that $\mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\phi + p\phi^{-1})$ and therefore the minimal polynomial $Q(T)$ of $\phi + p\phi^{-1}$ has discriminant equal to D times a square. This proves (2).

Finally, if Q is a quadratic polynomial of discriminant $c^2 D$, then $\eta = \phi + p\phi^{-1}$ is an endomorphism of A satisfying $Q(\eta) = 0$. Therefore $\mathbb{Z}[\eta] \cong \mathcal{O} := \mathbb{Z} + c\,\mathcal{O}_D$, and we conclude that A has real multiplication by $\mathcal{O}$ defined over $\mathbb{F}_p$, proving (3). $\qquad\square$

We conclude this section with a few comments on the models of Hilbert modular surfaces computed in this paper. We first give formulas for the family of elliptic K3 surfaces over $\mathcal{F}_{L_D}$, and then describe the 2- and 3-neighbor steps necessary to reach the alternate fibration of Step 2. The details of the parametrization will not be included in the paper, but they are available in the online supplement. Steps

3 and 4 are relatively easy to automate. We simply write down the result, which is the equation of $Y_-(D)$ as a double cover of the Humbert surface. We give a table of points of small height for which the Brauer obstruction vanishes, and the associated curves of genus 2. We also analyze the Hilbert modular surface further in the cases that we can describe it as a K3 or honestly elliptic surface. In particular, we determine the (geometric) Picard number and generators for the Mordell-Weil group of sections in most of the cases. We also analyze the branch locus of Step 3, identifying it with a union of quotients of classical modular curves in several cases, with the help of explicit formulas given in [Elkies 1998] or obtained by the methods of that paper. Finally, for many discriminants, we are able to exhibit curves of low genus on the surface, possessing infinitely many rational points.

We found the method of [van Luijk 2007] quite useful in determining the ranks of the Néron–Severi lattices of these surfaces. Briefly, the method is as follows. Let X be a smooth projective surface over $\mathbb{Q}$. For a prime p of good reduction, let X_p be the reduction of a good model of X at p. By counting points on $X_p(\mathbb{F}_q)$ for a small number of prime powers $q = p^e$, we obtain the characteristic polynomial of the Frobenius ϕ_p on some ℓ-adic étale cohomology group $H^2(X \times \bar{\mathbb{F}}_p, \mathbb{Q}_l)$. The number of roots $\rho_0(p)$ of this polynomial which are p times a root of unity is an upper bound on the geometric Picard number of X_p. Therefore $\rho(X) \le \rho_0(p)$ for such primes. If we have $\rho_0(p_1) = \rho_0(p_2) = \rho_0$, but the (expected) square classes of the discriminant of the Néron–Severi groups modulo these primes (as predicted by the Artin–Tate formula [Tate 1966b]) are distinct, we may even deduce $\rho(X) < \rho_0$. For if X_p does not satisfy the Tate conjecture for some $p \in \{p_1, p_2\}$, then $\rho(X) \le \rho(X_p) < \rho_0$. On the other hand, if both these reductions satisfy the Tate conjecture, then they also satisfy the Artin–Tate conjecture [Milne 1975a, 1975b], and since the size of the Brauer group of X_p is a square [Milne 1975a; Liu et al. 2005], the Néron–Severi groups must have discriminants in the same square class.

5. Neighbor method

Finally, we describe how to transform from one elliptic fibration to another, using 2- and 3-neighbor steps. We start with an elliptic K3 surface over a field k, which we assume has characteristic different from 2 or 3. Let F be the class of the fiber, and O be the class of the zero section. The surface X is a minimal proper model of a given Weierstrass equation

$$y^2 = x^3 + a_2(t)x^2 + a_4(t)x + a_6(t).$$

Here the elliptic fibration is $\pi : X \to \mathbb{P}^1_t$. Now, let F' be an elliptic divisor (i.e., F' is effective, $F'^2 = 0$, the components of F' are smooth rational curves, and F' is primitive).

We would like to write down the Weierstrass equation for this new elliptic fibration on X. The space of global sections $H^0(X, \mathcal{O}_X(F'))$ has dimension 2 over k. The ratio of any two linearly independent sections gives us the new elliptic parameter u. To compute the space of global sections, we proceed as follows. Any global section gives a section of the generic fiber $E = \pi^{-1}(\eta)$, which is an elliptic curve over $k(t) = k(\eta)$. Therefore, if we have a basis of global sections of $D = F'_{\text{hor},\eta}$ over $k(t)$, say $\{s_1, \ldots, s_r\}$ (where $r = h^0(\mathcal{O}_E(D)) = \deg(D) = F'_{\text{hor}} \cdot F = F' \cdot F$), we can assume that any global section of $\mathcal{O}_X(F')$ is of the form

$$b_1(t)s_1 + \cdots + b_r(t)s_r.$$

We can now use the information from F_{ver}, which gives us conditions about the zeroes and poles of the functions b_i, to find the linear conditions cutting out $H^0(X, \mathcal{O}_X(F'))$, which will be 2-dimensional.

When $F \cdot F' = r$, we say that going between these elliptic fibrations is an r-neighbor step. We will explain the reason for this terminology shortly. In this paper we use only 2- and 3-neighbor steps. First, we describe how to convert to a genus-1 curve in the case when $E = F_{\text{hor},\eta} = 2O$ or $3O$. These are the most familiar cases of the 2- and 3-neighbor steps, and the other cases of the 2-neighbor step that are needed are more exhaustively described in [Kumar 2014].

Suppose $D = 2O$. Then $\{1, x\}$ is a basis of global sections of $\mathcal{O}_E(D)$. Therefore, on X we obtain two global sections, 1 and $c(t) + d(t)x$ for some $c(t), d(t) \in k(t)$. The ratio between the two gives the elliptic parameter u. We set $x = (u - c(t))/d(t)$, and substitute into the Weierstrass equation to obtain an equation

$$y^2 = g(t, u).$$

Because F' is an elliptic divisor, the generic fiber of this surface over $\mathbb{P}^1_u$ is a curve of genus 1. Thus, once we absorb square factors into y^2 we obtain an equivalent g that is a polynomial of degree 3 or 4 in t. Then $y^2 = g(t, u)$ is standard form of the equation of a genus-1 curve as a branched double cover of $\mathbb{P}^1$.

Suppose $D = 3O$. Then $\{1, x, y\}$ is a basis of global sections of $\mathcal{O}_E(D)$. On X we obtain two global sections, 1 and $c(t) + d(t)x + e(t)y$. We set the ratio equal to u, solve for y, and substitute into the Weierstrass equation to obtain

$$\left(u - c(t) + d(t)x\right)^2 = e(t)^2\left(x^3 + a_2(t)x^2 + a_4(t)x + a_6(t)\right).$$

This equation is of degree 3 in x, and after some simple algebra (scaling and shifting x), we may arrange it to have degree 3 in t as well. We end up with a plane cubic curve, which is the standard model of a genus-1 curve with a degree-3 line bundle.

Finally, if we also know that the elliptic fibration corresponding to F' has a section (which follows in each of our examples by Proposition 4), then it is isomorphic

to the Jacobian of the genus-1 curve we have computed. We may use standard formulas to write down the Weierstrass equation of the Jacobian (see [An et al. 2001] and the references cited therein), and this is the desired Weierstrass equation for the elliptic fibration with fiber F'.

This neighbor step from F to F' corresponds to computing an explicit isomorphism between two presentations $\mathbb{Z}O + \mathbb{Z}F + T$ and $\mathbb{Z}O' + \mathbb{Z}F' + T'$ of NS(X). Note that $T \cong F^\perp/\mathbb{Z}F$, where $^\perp$ refers to the orthogonal complement in NS(X). The sublattice $(\mathbb{Z}F + \mathbb{Z}F')^\perp$ projects to an index-r sublattice of both $F^\perp/\mathbb{Z}F$ and $F'^\perp/\mathbb{Z}F'$, where $r = F \cdot F'$. Therefore these lattices are r-neighbors.

6. Discriminant 5

6.1. *Parametrization.* This is the smallest fundamental discriminant for real multiplication, and it is small enough that we do not need any 2- or 3-neighbor steps: we can instead just start with a K3 surface with E_8 and E_7 fibers, and ask for the extra condition which allows a section of height $\frac{5}{2} = 4 - \frac{3}{2}$.

Proposition 14. *The moduli space of* K3 *surfaces lattice polarized by* L_5, *the unique even lattice of signature* $(1, 17)$ *and discriminant 5 containing*

$$U \oplus E_8(-1) \oplus E_7(-1),$$

is birational to the projective plane $\mathbb{P}^2_{g,h}$. *The family of* K3 *surfaces is given by the Weierstrass equation*

$$y^2 = x^3 + \tfrac{1}{4}t^3(-3g^2t + 4)x - \tfrac{1}{4}t^5\big(4h^2t^2 + (4h + g^3)t + (4g + 1)\big).$$

Proof. We start with a family of elliptic K3 surfaces with E_8 and E_7 fibers:

$$y^2 = x^3 + xt^3(a_0 + a_1t) + t^5(b_0 + b_1t + b_2t^2).$$

To have discriminant -5 for the Picard group, the elliptic K3 surfaces in this family must have a section of height $\frac{5}{2} = 4 - \frac{3}{2}$. The x-coordinate for such a section must have the form $t^2(x_0 + x_1t + h^2t^2)$. Substituting x into the right-hand side and completing the square, we may solve for b_0, b_1, b_2 and a_1 in terms of a_0, h, x_0 and x_1. We then set $x_1 = eh$ and $x_0 = g + e^2/4$ to simplify the expressions. Finally, we note that scaling x, y, t by $\lambda^2, \lambda^3, \mu/\lambda$ gives a_0, e, g, h weights $(1, 3)$, $(0, 1)$, $(0, 2)$ and $(-1, 2)$ respectively with respect to (λ, μ). Therefore, we may scale a_0 and e to equal 1 independently (at most removing hypersurfaces in the moduli space), and get the parametrization in the statement of the proposition. We note that the section P of height $\frac{5}{2}$ is given by

$$x(P) = \tfrac{1}{4}t^2((1 + 2ht)^2 + 4g), \quad y(P) = \tfrac{1}{8}t^3(1 + 2ht)((1 + 2ht)^2 + 6g). \quad \square$$

Corollary 15. *The Humbert surface $\mathcal{H}_5$ is birational to $\mathbb{P}^2_{g,h}$, with the map to $\mathcal{A}_2$ given by the Igusa–Clebsch invariants*

$$(I_2 : I_4 : I_6 : I_{10}) = \big(6(4g+1), 9g^2, 9(4h+9g^3+2g^2), 4h^2\big).$$

Proof. This follows immediately from Theorem 9. The Igusa–Clebsch invariants may be read out directly from the Weierstrass equation above. □

Theorem 16. *A birational model over $\mathbb{Q}$ of the Hilbert modular surface $Y_-(5)$ is given by the following double cover of $\mathbb{P}^2_{g,h}$:*

$$z^2 = 2\big(6250h^2 - 4500g^2h - 1350gh - 108h - 972g^5 - 324g^4 - 27g^3\big).$$

It is a rational surface (i.e., birational to $\mathbb{P}^2$).

Proof. We follow the method of Section 4. The possible factors of the branch locus are g, h, $8h - 9g^2$ (the zero locus of this polynomial defines a subvariety of the moduli space for which the corresponding elliptic K3 surfaces acquire an extra I_2 fiber), $64h^2 + 48g^2h + 48g^5 + 9g^4$ (extra II fiber), and $6250h^2 - 4500g^2h - 1350gh - 108h - 972g^5 - 324g^4 - 27g^3$ (extra I_2 fiber). By Step 4 of the method, we deduce that only the last factor occurs, and the correct quadratic twist is by 2. It was already well-known that the Hilbert modular surface is a rational surface, but we give an explicit parametrization in the following analysis. □

6.2. *Analysis.* This is a rational surface: to obtain a parametrization, we complete the square in h, writing $h = k + 9(250g^2 + 75g + 6)/6250$. Following this up with $k = 3m(10g + 3)(15g + 2)/6250$, and removing square factors by writing $z = 3n(10g+3)(15g+2)/25$, we obtain the equation $5n^2 - m^2 + 9 + 30g = 0$, which we can solve for g. This gives an explicit birational map between $Y_-(5)$ and $\mathbb{P}^2_{m,n}$.

The branch locus is the curve obtained by setting $z = 0$, or alternatively $n = 0$ in the above parametrization. It is parametrized by one variable m; we have

$$(g, h) = \left(\frac{(m^2 - 9)}{30}, \frac{(m - 2)^2(m + 3)^3}{12500} \right).$$

6.3. *Examples.* We list in Table 1 some points of small height and corresponding genus-2 curves. The second entry in the table is the modular curve $X_0(67)/\langle w \rangle$, where w is the Atkin–Lehner involution. We find several other modular curves with real multiplication by $\mathcal{O}_5$ (and also a few for discriminants other than 5) corresponding to points of larger height.

6.4. *Brumer's and Wilson's families of genus-2 curves.* Genus-2 curves whose Jacobians have real multiplication by $\mathcal{O}_5$ have been studied by Brumer [1995] and Wilson [1998; 2000]. Brumer describes a 3-dimensional family of genus-2 curves

Rational point (g, h)	Sextic polynomial $f_6(x)$ defining the genus-2 curve $y^2 = f_6(x)$
$\left(-\frac{8}{3}, \frac{47}{2}\right)$	$-x^5 + x^4 - x^3 - x^2 + 2x - 1$
$\left(-\frac{37}{6}, 67\right)$	$x^6 + 2x^5 + x^4 - 2x^3 + 2x^2 - 4x + 1$
$\left(0, \frac{27}{50}\right)$	$3x^5 + 5x^3 + 1$
$\left(-\frac{1}{24}, \frac{1}{100}\right)$	$4x^6 + 4x^5 + 5x^4 - 5x^2 - 2x - 2$
$\left(-\frac{25}{54}, \frac{59}{81}\right)$	$-x^6 - 2x^4 - 6x^3 - 5x^2 - 6x - 1$
$\left(-\frac{2}{3}, -\frac{14}{25}\right)$	$-7x^6 - 7x^5 - 5x^4 + 5x^2 - x - 1$
$\left(\frac{47}{54}, \frac{71}{81}\right)$	$3x^6 - 6x^5 + 7x^4 - 2x^3 - 2x^2 - 1$
$\left(-\frac{1}{6}, \frac{1}{25}\right)$	$x^6 - 4x^5 + 10x^4 - 10x^3 + 5x^2 + 2x - 3$
$\left(-\frac{4}{3}, \frac{16}{25}\right)$	$-x^6 - x^5 + 5x^2 - 7x - 12$
$\left(-\frac{4}{3}, \frac{49}{22}\right)$	$7x^5 + 5x^4 + 3x^3 - 9x^2 - 14x - 7$
$\left(0, -\frac{54}{11}\right)$	$2x^6 - 6x^5 - 6x^4 + 3x^3 - 18x^2 - 6x - 2$
$\left(\frac{11}{6}, \frac{53}{11}\right)$	$9x^6 - 14x^5 + 13x^4 - 2x^3 - 22x^2 - 8x - 7$
$\left(-\frac{5}{24}, \frac{1}{64}\right)$	$6x^6 - 2x^5 - 15x^4 - 16x^3 - 25x^2 - 8x - 4$
$\left(\frac{11}{6}, -\frac{89}{25}\right)$	$-x^6 + 2x^5 - 5x^4 + 30x^3 - 10x^2 + 8x - 1$
$\left(-\frac{2}{3}, \frac{68}{11}\right)$	$-2x^6 - 2x^5 - 11x^4 - 29x^3 - 31x^2 - 26x - 6$
$\left(-\frac{2}{3}, \frac{26}{25}\right)$	$-2x^6 + 36x^5 + 5x^4 + 35x^3 - 10x^2 - 21x - 17$

Table 1. Some points of height ≤ 100 on the surface of Theorem 16 and the corresponding genus-2 curves.

given by

$$y^2 + \left(1 + x + x^3 + c(x + x^2)\right)y$$
$$= -bdx^4 + (b - d - 2bd)x^3 + (1 - 3b - bd)x^2 + (1 + 3b)x + b.$$

In the online supplement, we give formulas for the corresponding values of our parameters g and h.

Wilson describes a family of genus-2 curves by their Igusa–Clebsch invariants. His moduli space is 2-dimensional, though he uses three coordinates z_6, s_2 and σ_5 of weights 1, 2, 5 respectively, in a weighted projective space. These coordinates are related to ours via

$$(g, h) = \left(-\frac{2z_6^2 + s_2}{12z_6^2}, \frac{\sigma_5}{64z_6^5}\right).$$

7. Discriminant 8

7.1. Parametrization. We start with an elliptic K3 surface with fibers of type D_9 and E_7. A Weierstrass equation for such a family is given by

$$y^2 = x^3 + t\left((2r + 1)t + r\right)x^2 + 2rst^4(t + 1)x + rs^2t^7.$$

We then identify a fiber of type E_8, and transform to it by a 2-neighbor step.
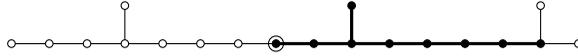
The resulting elliptic fibration has E_8 and E_7 fibers, and we may read out the Igusa–Clebsch invariants, and then compute the branch locus of the double cover that defines the Hilbert modular surface. It corresponds to elliptic K3 surfaces with an extra I_2 fiber. We obtain the following result for $Y_-(8)$.

Theorem 17. *The Humbert surface $\mathcal{H}_8$ is birational to $\mathbb{P}^2_{r,s}$, with the explicit map to $\mathcal{A}_2$ given by the Igusa–Clebsch invariants*

$$I_2 = -4(3s + 8r - 2),$$

$$I_4 = 4(9rs + 4r^2 + 4r + 1),$$

$$I_6 = -4(36rs^2 + 94r^2s - 35rs + 4s + 48r^3 + 40r^2 + 4r - 2),$$

$$I_{10} = -8s^2r^3.$$

A birational model over $\mathbb{Q}$ for the Hilbert modular surface $Y_-(8)$ as a double cover

Rational point (r, s)	Sextic polynomial $f_6(x)$ defining the genus-2 curve $y^2 = f_6(x)$
$\left(\frac{2}{25}, \frac{83}{50}\right)$	$x^6 - x^5 + 3x^4 + x^3 + x^2 + 2x + 1$
$\left(-\frac{34}{9}, \frac{50}{9}\right)$	$x^6 - 2x^5 - 2x^4 - 4x^3 + 2x^2 + 4x - 3$
$\left(-22, \frac{59}{2}\right)$	$x^6 + 2x^5 - 3x^4 + 5x^3 + x^2 - x - 1$
$\left(\frac{2}{49}, \frac{58}{49}\right)$	$-x^6 - 4x^5 - 6x^4 + 2x^2 + 2x - 1$
$\left(-52, \frac{83}{2}\right)$	$-4x^6 + 2x^5 + 5x^4 - 7x^3 - x + 1$
$\left(\frac{1}{8}, \frac{59}{32}\right)$	$-x^6 - x^5 - 7x^2 + 5x - 4$
$\left(-\frac{4}{9}, \frac{23}{8}\right)$	$-2x^6 + 6x^5 - x^4 - 7x^3 - x^2 - 3x$
$\left(80, \frac{83}{2}\right)$	$x^6 + 5x^5 + 8x^4 + 5x^3 + 5x^2 - 8x + 4$
$\left(\frac{19}{2}, 22\right)$	$-x^6 - 4x^5 - 8x^4 - 8x^3 - 8x^2 + 4x - 4$
$(94, -54)$	$-x^6 + 6x^4 - 8x^3 + 6x^2 + 6x - 9$
$\left(\frac{13}{8}, -\frac{2}{9}\right)$	$-x^6 + 6x^5 - 9x^4 + 3x^2 - 6x - 2$
$\left(\frac{86}{9}, -\frac{13}{2}\right)$	$x^6 - 7x^4 - 7x^3 - x^2 + 9x + 9$
$\left(-\frac{3}{8}, \frac{9}{4}\right)$	$-3x^6 - 9x^5 - 2x^4 + 10x^3 + x^2 + 3x$
$\left(\frac{1}{14}, \frac{10}{7}\right)$	$-x^6 - 2x^5 - 7x^4 + 4x^3 - 3x^2 + 10x - 5$
$\left(\frac{1}{18}, \frac{31}{18}\right)$	$-3x^6 - 10x^5 - 7x^4 - 5x^2 + 2x - 1$
$\left(\frac{1}{32}, \frac{19}{16}\right)$	$4x^6 - 7x^5 - 3x^4 - 2x^3 + 10x^2 + 5x + 1$

Table 2. Some points of small height on the surface of Theorem 17 and the corresponding genus-2 curves.

of $\mathbb{P}^2$ is given by the equation

$$z^2 = 2\,(16rs^2 + 32r^2s - 40rs - s + 16r^3 + 24r^2 + 12r + 2).$$

It is also a rational surface.

7.2. *Analysis.* This Hilbert modular surface is a rational surface. To see this, we may complete the square in s, setting $s = s_1 - r + 5/4 + 1/(32r)$. Then setting $s_1 = m(16r - 1)/(32r)$ and $z = n(16r - 1)$, we remove square factors from the equation, which becomes linear in r. We find $r = (m^2 - 1)/(32n^2 - 16)$, thus obtaining an explicit parametrization of $Y_-(8)$ by $\mathbb{P}^2_{m,n}$.

The branch locus is a genus-0 curve; we obtain a parametrization by setting $z = 0$:

$$(r, s) = \left(\frac{1 - t^2}{16}, \frac{(t + 3)^3}{16(t + 1)}\right).$$

7.3. *Examples.* Table 2 lists some points of small height and their genus-2 curves.

8. Discriminant 12

8.1. *Parametrization.* We start with an elliptic K3 surface with fibers of types E_8, D_6 and A_2. The Weierstrass equation for such a family is given by

$$y^2 = x^3 + \big((1 - f^2)(1 - t) + t\big)tx^2 + 2et^3(t - 1)x + e^2(t - 1)^2t^5.$$

We identify a fiber of type E_7, and move to the associated elliptic fibration by a 2-neighbor step.
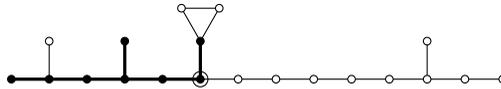
The new elliptic fibration has E_8 and E_7 fibers, and so we may read out the Igusa–Clebsch invariants, and determine the branch locus for the Hilbert modular surface.

Theorem 18. *A birational model over $\mathbb{Q}$ for the Hilbert modular surface $Y_-(12)$ as a double cover of $\mathbb{P}^2_{e,f}$ is given by the equation*

$$z^2 = (f - 1)(f + 1)(f^6 - f^4 - 18ef^2 + 27e^2 + 16e).$$

It is a rational surface.

8.2. *Analysis.* Note the extra involution $(e, f) \mapsto (e, -f)$ arising from the Hurwitz–Maass extension (as described at the end of Section 3), since 12 is not a prime power. In fact, there are two independent involutions evident in the diagram above, but one of them has been used up to fix the Weierstrass scaling of x (namely, the coefficient of x^2 evaluates to 1 at $t = 1$). The other involution is reflected in the

Weierstrass equation for the universal family of elliptic K3 surfaces as $f \mapsto -f$. It preserves the branch locus of the map $Y_-(12) \to \mathcal{H}_{12}$, and therefore lifts to $Y_-(12)$.

The branch locus has three components; the two simple components $f = \pm 1$ correspond to the D_6 fiber getting promoted to an E_7 fiber, while the remaining component corresponds to having an extra I_2 fiber. This last component is a rational curve; completing the square with respect to e, we find after some easy algebraic manipulation the parametrization

$$(e, f) = \left(\frac{16(h^2 - 1)}{(h^2 + 3)^3}, \frac{-4h}{h^2 + 3} \right).$$

This Hilbert modular surface is rational as well. To obtain an explicit parametrization, note that the right-hand side of the above equation is quadratic in e, and $e = 0$ makes it a square. Therefore the conic bundle over $\mathbb{P}^1_f$ has a section. Setting $z = ge + f^2(f^2 - 1)$, we may solve for e, obtaining a birational parametrization by $\mathbb{P}^2_{f,g}$.

We will not list the Igusa–Clebsch invariants for this (and higher) discriminants, as they are complicated expressions. They are available in the online supplement.

8.3. Examples. Table 3 lists some points of small height and their genus-2 curves.

Rational point (e, f)	Sextic polynomial $f_6(x)$ defining the genus-2 curve $y^2 = f_6(x)$
$\left(\frac{34}{27}, \frac{5}{3}\right)$	$-2x^6 - 2x^5 + x^4 - 3x^2 + 2x - 1$
$\left(\frac{34}{27}, -\frac{5}{3}\right)$	$x^5 - x^4 + x^3 - 3x^2 - x + 5$
$\left(\frac{51}{100}, 2\right)$	$-3x^6 + 6x^5 + 4x^4 - 2x^3 - 8x^2 - 6x - 6$
$\left(-\frac{11}{3}, -2\right)$	$-x^6 - 8x^3 + 12x - 12$
$\left(-\frac{11}{3}, 2\right)$	$-x^6 + 12x^4 + 8x^3 - 12x^2 + 12x - 4$
$\left(\frac{4}{3}, -2\right)$	$-8x^6 + 12x^4 + 8x^3 - 6x^2 - 12x - 3$
$\left(\frac{4}{3}, 2\right)$	$-5x^6 + 12x^5 - 6x^4 + 8x^3 - 12x^2 - 8$
$\left(-\frac{14}{27}, \frac{1}{3}\right)$	$-x^5 + 13x^4 - 6x^3 - 2x^2 + 3x - 7$
$\left(-\frac{29}{14}, -\frac{15}{14}\right)$	$x^6 + 2x^5 + 13x^4 - 16x^3 + 17x^2 + 4x + 8$
$\left(\frac{80}{81}, 2\right)$	$-8x^6 - 12x^5 + 15x^4 + 5x^3 - 21x^2 + 15x - 5$
$\left(\frac{51}{100}, -2\right)$	$-x^6 - 6x^5 - 11x^4 - 14x^3 - 23x^2 + 6x + 3$
$\left(-\frac{5}{2}, -\frac{3}{2}\right)$	$-5x^6 - 10x^5 - x^4 + 24x^3 - 5x^2 - 8x - 20$
$\left(-\frac{23}{54}, -\frac{1}{2}\right)$	$x^6 - 6x^5 - 3x^4 + 24x^3 - 3x^2 - 4$
$\left(\frac{25}{18}, -\frac{3}{2}\right)$	$4x^6 - 24x^5 + 27x^4 - 28x^3 + 21x^2 - 5$
$\left(-\frac{5}{54}, \frac{2}{3}\right)$	$3x^6 - 26x^5 + 31x^4 + 12x^3 - 3x^2 - 10x - 15$
$\left(\frac{13}{64}, -\frac{5}{4}\right)$	$-5x^6 + 3x^5 - 12x^4 + 28x^3 + 12x^2 - 36x$

Table 3. Some points of small height on the surface of Theorem 18 and the corresponding genus-2 curves.

We mention a few special curves on the Hilbert modular surface, which one may recognize by looking at a plot of the rational points. First, specializing f to some $f_0 \in \mathbb{Q}$ gives a conic in z and e, which always has a rational point (since, as we noted above, $e = 0$ makes the right-hand side a square). These may be used to produce many rational points and examples of genus-2 curves when the Brauer obstruction happens to vanish.

Another noticeable feature of the plot is the parabola $e = 4(f^2 - 1)/9$. We check that the Brauer obstruction vanishes identically on this locus, giving a family of genus-2 curves whose Jacobians have real multiplication by $\mathcal{O}_{12}$. Note that this is a non-modular curve: generically the endomorphism ring is no larger (i.e., not a quaternion algebra).

9. Discriminant 13

9.1. *Parametrization.* We start with an elliptic K3 surface with reducible fibers of types E_8, E_6 and A_1, and with a section of height $\frac{13}{6} = 4 - \frac{4}{3} - \frac{1}{2}$. A Weierstrass equation for such a family is given by

$$y^2 = x^3 + (4g+1)t^2x^2 - 4g(h-g-1)(t-1)t^3x + 4g^2(t-1)^2t^4(h^2t+1).$$

We identify an E_7 fiber below and move to it by a 2-neighbor step.

The resulting elliptic fibration has E_8 and E_7 fibers, so we may read out the Igusa–Clebsch invariants and work out the branch locus of the double cover defining the Hilbert modular surface. It corresponds to the elliptic K3 surface having an extra I_2 fiber.

Theorem 19. *A birational model over $\mathbb{Q}$ for the Hilbert modular surface $Y_-(13)$ as a double cover of $\mathbb{P}^2_{g,h}$ is given by the equation*

$$z^2 = 108gh^3 - (27g^2 + 468g - 4)h^2 + 8(82g^2 + 71g - 2)h - 16(2g-1)^3.$$

It is a rational surface.

9.2. *Analysis.* The surface $Y_-(13)$ is rational. To show this, we proceed as follows. The substitutions $g = g_1 - \frac{1}{54}$ and $h = h_1 + \frac{64}{27}$, followed by $h_1 = mg_1$, make the right-hand side quadratic in g_1, up to a square factor. Removing this factor by setting $z = z_1g_1/18$, and then setting $g_1 = g_2/54$, we get the conic bundle over $\mathbb{Q}(m)$

$$z_1^2 = 3m^2(4m-1)g_2^2 - 6(2m^3 - 301m^2 - 528m + 128)g_2 - 507(m^2 - 96m - 1024).$$

Furthermore, $g_2 = 1$ makes the resulting expression a square, giving us a rational point on the conic over $\mathbb{Q}(m)$. Therefore, we may set $z_1 = 36(m+20) + n(g_2 - 1)$ and solve for g_2. This gives us a birational parametrization of $Y_-(13)$ by $\mathbb{P}^2_{m,n}$.

We can also deduce that the branch locus is a rational curve, as follows. By setting $z_1 = 0$, we obtain a quadratic equation in g_2 whose discriminant, up to a square factor, is $m^2 - 44m + 16$. Setting it equal to n^2 and noting that $m = 0$ makes the expression a square, we obtain a parametrization of this conic, as

$$m = -4 \frac{2r + 11}{r^2 - 1}.$$

Working backwards, we obtain a parametrization of the branch locus as

$$(g, h) = \left(\frac{-2(r-2)^2(r+1)}{27(r+7)}, \frac{2(2r+5)^3}{27(r+1)(r+7)} \right).$$

9.3. Examples. Table 4 lists some points of small height and their genus-2 curves.

On a plot of rational points we observe the line $h = (g + 4)/3$, along which the Brauer obstruction vanishes, leading to a family of genus-2 curves whose Jacobians have "honest" real multiplication by $\mathcal{O}_{13}$.

Rational point (g, h)	Sextic polynomial $f_6(x)$ defining the genus-2 curve $y^2 = f_6(x)$
$\left(-17, \frac{1}{3}\right)$	$-3x^6 - 6x^5 + 4x^3 + 3x^2 + 6x - 5$
$\left(-\frac{13}{2}, -\frac{11}{2}\right)$	$x^5 + 5x^4 + 5x^3 - 5x^2 + 6x - 1$
$\left(-\frac{17}{2}, \frac{7}{2}\right)$	$-x^5 - 2x^4 - 3x^3 - 6x^2 - 7$
$\left(\frac{11}{5}, \frac{1}{5}\right)$	$x^6 + 4x^5 + 2x^4 - 8x^3 - 5x^2 - 5$
$\left(-\frac{1}{3}, \frac{11}{9}\right)$	$-x^6 + 3x^4 + 12x^3 + 6x^2 - 11$
$\left(-\frac{14}{11}, -\frac{2}{11}\right)$	$13x^6 + 12x^5 + 6x^4 + 10x^3 - 7x^2 - 2x + 1$
$\left(-\frac{2}{17}, \frac{2}{17}\right)$	$-x^6 - 2x^5 - x^4 + 14x^3 + 2x^2 - 8x - 9$
$\left(\frac{1}{5}, \frac{17}{15}\right)$	$3x^6 + 12x^5 + 6x^4 - 4x^3 - 15x^2 + 5$
$\left(-\frac{10}{3}, -\frac{10}{9}\right)$	$-x^6 + 18x^5 + 3x^4 - 6x^3 + 6x^2 - 5$
$(-10, 6)$	$-x^6 - 6x^4 - 10x^3 - 9x^2 - 30x + 11$
$\left(-\frac{18}{5}, \frac{14}{5}\right)$	$-x^6 - 2x^4 - 10x^3 + 7x^2 - 30x - 9$
$\left(-\frac{7}{13}, \frac{3}{13}\right)$	$-31x^6 + 12x^5 - 30x^4 + 4x^3 - 33x^2 - 12x - 1$
$\left(\frac{10}{3}, \frac{10}{3}\right)$	$7x^6 + 18x^5 - 9x^4 - 34x^3 + 18x^2 - 5$
$\left(-11, -\frac{11}{9}\right)$	$-5x^6 + 6x^5 + 3x^4 - 4x^3 + 18x^2 - 36x - 9$
$\left(-\frac{7}{8}, \frac{10}{3}\right)$	$-x^6 + 3x^4 - 20x^3 + 30x^2 - 36x + 9$
$\left(-\frac{13}{9}, \frac{13}{9}\right)$	$-x^6 - 9x^4 + 8x^3 - 30x^2 + 36x - 3$

Table 4. Some points of small height on the surface of Theorem 19 and the corresponding genus-2 curves.

10. Discriminant 17

10.1. *Parametrization*. We start with an elliptic K3 surface with a I_{17} fiber. A Weierstrass equation for such a family of surfaces is given by

$$y^2 = x^3$$
$$+ \left(1 + 2gt + (2h + (g+1)^2)t^2 + 2(gh + g + 2g^2 + h)t^3 + ((g+h)^2 + 2g^3)t^4\right)x^2$$
$$- 4h^2t^5\left(1 + gt + (h + 2g + 1)t^2 + (h + 2g^2 + g)t^3\right)x + 4h^4t^{10}\left((2g+1)t^2 + 1\right).$$

We first identify an E_7 fiber and go to the associated elliptic fibration via a 2-neighbor step.

The resulting elliptic fibration has E_7 and A_8 fibers, and a section P of height $\frac{17}{18} = 4 - \frac{3}{2} - \frac{14}{9}$. We next identify a fiber F' of type E_8 and perform a 3-neighbor step to move to the associated elliptic fibration.
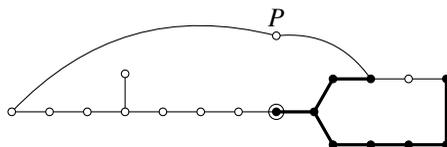
Since $P \cdot F' = 2$, while the remaining component of the A_8 fiber intersects F' with multiplicity 3, the new elliptic fibration has a section. We may therefore convert to the Jacobian; this has E_8 and E_7 fibers, and we may read out the Igusa–Clebsch invariants.

Theorem 20. *A birational model over $\mathbb{Q}$ for the Hilbert modular surface $Y_-(17)$ as a double cover of $\mathbb{P}^2$ is given by the equation*

$$z^2 = -256h^3 + (192g^2 + 464g + 185)h^2$$
$$- 2(2g+1)(12g^3 - 65g^2 - 54g - 9)h + (g+1)^4(2g+1)^2.$$

It is a rational surface.

10.2. *Analysis*. This is evidently a rational elliptic surface over $\mathbb{P}^1_g$. In fact, it is a rational surface over $\mathbb{Q}$. We exhibit a birational parametrization as follows: set $h = \left(4(2g+1) + m(2g+1)(27g+13)\right)/27$ and absorb square factors by setting $z = z_1(2g+1)(27g+13)/243$, to get (after scaling $g = g_1/3$) the equation

$$z_1^2 = -9(8m-1)^3g_1^2 - 2(16m+7)(424m^2 - 385m + 1)g_1$$
$$- 3(3328m^3 - 1923m^2 - 3138m - 803)$$

which is a conic bundle over $\mathbb{P}^1_m$. We see that $g_1 = -\frac{3}{2}$ makes the right hand side a

square, and so setting $z_1 = 9(2m + 11)/2 + n(g_1 + \frac{3}{2})$ and solving for g_1, we get a birational map from $\mathbb{P}^2_{m,n}$.

The branch locus is a curve of genus 0. To produce a parametrization, we set $z_1 = 0$ and note that the discriminant of the resulting quadratic equation in g_1 is a square times $64m^2 + 218m - 8$. Setting $64m^2 + 218m - 8 = (8m + r)^2$ and solving for m, we ultimately obtain:

$$(g, h) = \left(\frac{-(8r^3 - 111r^2 + 1212r - 8146)}{2(2r - 7)^3}, \frac{(r - 17)^2(r + 10)^4}{4(2r - 7)^6} \right).$$

10.3. Examples. Table 5 lists some points of small height and their genus-2 curves.

A plot of the rational points on $Y_-(17)$ reveals two special curves on the surface. First, there is the line $h = -g/2$. Substituting this into the equation for the Hilbert modular surface, we obtain a conic, which can be parametrized as

$$(g, h) = \left(-\frac{m^2 - 4}{2(m - 6)}, \frac{m^2 - 4}{4(m - 6)} \right).$$

The Brauer obstruction vanishes along this locus. However, this curve is modular: the endomorphism ring is a split quaternion algebra, strictly containing $\mathcal{O}_{17}$. The

Rational point (g, h)	Sextic polynomial $f_6(x)$ defining the genus-2 curve $y^2 = f_6(x)$
$(0, \frac{13}{32})$	$-2x^6 - x^5 - 6x^4 - 5x^3 - 4x^2 - 4x$
$(-\frac{5}{11}, \frac{1}{88})$	$3x^6 + 4x^5 + 4x^4 - 6x^3 - 5x^2 - 4x + 4$
$(6, 26)$	$-2x^6 + 2x^5 + x^4 + 8x^3 + 7x^2 + 4x$
$(\frac{9}{4}, \frac{77}{64})$	$-2x^6 - x^5 + 8x^4 - 5x^3 - 4x^2 + 4x - 4$
$(\frac{3}{5}, -\frac{11}{50})$	$-8x^6 + 8x^5 + 7x^4 + 2x^3 - x$
$(5, -11)$	$4x^5 + 9x^4 + 2x^3 - 8x^2 - 2x$
$(5, 22)$	$2x^6 - 4x^5 + 9x^4 - 10x^3 + 4x^2 - 4x$
$(\frac{1}{5}, \frac{28}{25})$	$-10x^6 - 10x^5 - 2x^4 - 7x^3 - x$
$(-\frac{1}{4}, -\frac{11}{64})$	$4x^5 + 3x^4 + 11x^3 - 7x^2 + x$
$(\frac{5}{4}, -\frac{35}{64})$	$x^5 - 7x^3 + 2x^2 - 8x + 12$
$(-\frac{5}{2}, -\frac{13}{8})$	$4x^5 - x^4 - 13x^3 - 3x^2 + 13x$
$(\frac{1}{5}, -\frac{7}{20})$	$3x^6 + 7x^5 + 6x^4 + 16x^3 + 14x^2 - 8x - 8$
$(-12, -\frac{23}{2})$	$-7x^6 - 19x^5 - 7x^4 + 14x^3 - x$
$(0, -\frac{1}{16})$	$-4x^6 + 19x^5 - 20x^4 + 11x^3 + 15x^2 - 8x - 4$
$(2, -\frac{35}{4})$	$-4x^5 + 20x^4 - 12x^3 - 15x^2 - 4x$
$(4, \frac{51}{8})$	$-4x^6 - 12x^5 - 27x^4 + 2x^3 + 12x^2 + 18x$

Table 5. Some points of small height on the surface of Theorem 20 and the corresponding genus-2 curves.

second curve is the parabola $h = -(6g^2 + g - 1)/8$. The Brauer obstruction vanishes along this curve too, giving a 1-parameter family of genus-2 curves whose Jacobians have real multiplication by $\mathcal{O}_{17}$.

11. Discriminant 21

11.1. *Parametrization.* We start with an elliptic K3 surface with fibers of type E_8, A_6 and A_2 at $t = \infty$, 0 and 1 respectively.
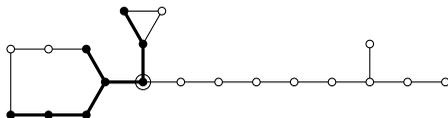
A Weierstrass equation for such a family is

$$y^2 = x^3 + (a_0 + a_1 t + a_2 t^2)x^2 + 2t^2(t-1)(b_0 + b_1 t)x + t^4(t-1)^2(c_0 + c_1 t)$$

with

$$a_0 = 1, \qquad a_1 = -r^2 + 2rs - 1, \qquad a_2 = (r-s)^2;$$
$$b_0 = (r^2 - 1)(s-r)^2, \quad b_1 = (r^2 - 1)(s-r)^2(rs - 1);$$
$$c_0 = (r^2 - 1)^2(s-r)^4, \quad c_1 = (r^2 - 1)^3(s-r)^4.$$

We identify a fiber of type E_7, and a 3-neighbor step gives us the desired $E_8 E_7$ fibration.

We read out the Igusa–Clebsch invariants, and the branch locus of $Y_-(21)$ as a double cover of $\mathbb{P}^2_{r,s}$ corresponds to the subvariety of the moduli space where the elliptic K3 surfaces have an extra I_2 fiber.

Theorem 21. *A birational model over $\mathbb{Q}$ for the Hilbert modular surface $Y_-(21)$ as a double cover of $\mathbb{P}^2_{r,s}$ is given by the equation*

$$z^2 = 16s^4 - 8r(27r^2 - 23)s^3 + (621r^4 - 954r^2 + 349)s^2$$
$$- 18(r^3 - r)(33r^2 - 29)s + (r^2 - 1)(189(r^4 - r^2) + 16).$$

It is a singular K3 surface (i.e., of Picard number 20).

11.2. *Analysis.* The extra involution (corresponding to $21 = 3 \cdot 7$) here is given by $(r, s) \mapsto (-r, -s)$.

The branch locus is a rational curve; a parametrization is given by

$$(r, s) = \left(\frac{h^4 + 72h^2 - 81}{18h(h^2 + 3)}, \frac{(h^2 - 9)(h^4 - 126h^2 + 189)}{432h(h^2 + 3)} \right).$$

The equation of $Y_-(21)$ above expresses it as a surface fibered by genus-1 curves over $\mathbb{P}^1_r$. In fact, since the coefficient of s^4 is a square, this fibration has a section,

and we may convert it to its Jacobian form, which after some simple Weierstrass transformations may be written as

$$z^2 = w^3 + (-27r^4 + 43)w^2 + 4(r^2 - 1)(8127r^4 - 18459r^2 + 9740)w$$
$$+ 4(r^2 - 1)^2 w(-186624r^6 + 1320813r^4 - 1817964r^2 + 705679).$$

This is a K3 surface with an elliptic fibration to $\mathbb{P}^1_r$. The discriminant of the cubic polynomial is

$$(r^2 - 1)^3(27r^2 - 25)^2(27r^4 + 342r^2 - 289)^3,$$

from which we deduce that we have three I_2 fibers (including $r = \infty$) and six I_3 fibers, which contribute 15 to the Picard number. We find the following sections.

$$P_0 = \left(6(r^2 - 1)(6r^2 - 7),\, 4(r - 1)(r + 1)(27r^4 + 342r^2 - 289)\right),$$
$$P_1 = \left(2(324r^4 - 1503r^2 + 1019)/21,\, 8(27r^2 - 25)(27r^4 + 342r^2 - 289)/(21\mu)\right),$$
$$P_2 = \left((-102 + 32\nu)(r^2 - 1),\, 32\nu r(r^2 - 1)(-27r^2 + 31 + 22\nu)\right),$$
$$P_3 = \left((-102 - 32\nu)(r^2 - 1),\, -32\nu r(r^2 - 1)(-27r^2 + 31 - 22\nu)\right).$$

Here $\mu = \sqrt{21}$ and $\nu = \sqrt{-1}$. Note that P_0 is a 3-torsion section, whereas the height matrix for P_1, P_2, P_3 is

$$\frac{1}{6} \begin{pmatrix} 2 & 0 & 0 \\ 0 & 13 & 1 \\ 0 & 1 & 13 \end{pmatrix}.$$

Therefore, the Picard number of the surface is 20, and the discriminant of the lattice spanned by these sections and the trivial lattice is $1008 = 2^4 3^2 7$. We showed that this is the entire Néron–Severi group by checking that the above subgroup of the Mordell–Weil group is 2- and 3-saturated.

Using P_0, we may rewrite the equation in the much simpler form

$$z^2 + (9r^2 - 13)wz + (r^2 - 1)(27r^4 + 342r^2 - 289)z = w^3.$$

The quotient of the Hilbert modular surface by the involution

$$(r, s, z) \mapsto (-r, -s, -z)$$

is the rational elliptic surface

$$z^2 = w^3 + (-27t^2 + 43)w^2 + 4(t - 1)(8127t^2 - 18459t + 9740)w$$
$$+ 4(t - 1)^2(-186624t^3 + 1320813t^2 - 1817964t + 705679).$$

It has three reducible fibers of type I_3 and one of type I_2, a 3-torsion section, and Mordell–Weil rank 1, generated by the following section of height $\frac{1}{6}$:

$$(z, w) = \left(2(324r^2 - 1503r + 1019)/21,\ 8(27r - 25)(27r^2 + 342r - 289)/(21\mu)\right).$$

11.3. *Examples.* Table 6 lists some points of small height and their genus-2 curves. The torsion section P_0 on the Jacobian model of $Y_-(21)$ pulls back to the curve

$$s = \frac{45r^3 + 9r^2 - 45r - 17}{2(27r^2 + 6r - 17)}.$$

The Brauer obstruction always vanishes for this family, and yields a family of genus-2 curves over $\mathbb{Q}(r)$, whose Jacobians have real multiplication by $\mathcal{O}_{21}$.

Another special curve which we observe from a plot of the rational points is the hyperbola $s^2 = (3r^2 + 1)/4$. It may be parametrized as

$$(r, s) = \left(\frac{4m}{4m^2 - 3},\ \frac{3 + 4m^2}{2(3 - 4m^2)}\right).$$

The Brauer obstruction also vanishes for this family.

Rational point (r, s)	Sextic polynomial $f_6(x)$ defining the genus-2 curve $y^2 = f_6(x)$
$\left(\frac{3}{2}, \frac{1}{44}\right)$	$-5x^6 - 8x^5 + 20x^4 + 5x^3 - 13x$
$\left(\frac{21}{34}, -\frac{43}{68}\right)$	$13x^6 + 26x^5 + 33x^4 + 9x^3 - 5x^2 - 11x$
$\left(-\frac{36}{13}, -\frac{49}{26}\right)$	$7x^6 - 42x^5 - 44x^4 - 12x^3 - 11x^2 - 14x - 7$
$\left(0, \frac{1}{2}\right)$	$13x^6 + 54x^5 + 32x^4 - 28x^3 - 25x^2 + 14x - 1$
$\left(0, -\frac{1}{2}\right)$	$-x^6 + 2x^5 + 4x^4 + 36x^3 + 25x^2 + 42x - 59$
$\left(\frac{45}{46}, -\frac{25}{92}\right)$	$9x^6 + 16x^5 + 12x^4 - 73x^3 - 41x^2 + 14x + 77$
$\left(-\frac{3}{2}, -\frac{1}{44}\right)$	$-13x^5 + 39x^4 + 31x^3 - 115x^2 - 50x - 125$
$\left(-\frac{21}{34}, \frac{43}{68}\right)$	$-13x^5 + 58x^4 - 83x^3 - 90x^2 + 100x + 125$
$\left(-\frac{45}{46}, \frac{25}{92}\right)$	$5x^5 + 30x^4 - 61x^3 - 122x^2 + 112x + 161$
$\left(3, -\frac{1}{28}\right)$	$28x^6 + 52x^5 - 149x^4 - 174x^3 + 235x^2 - 60x - 100$
$\left(\frac{55}{63}, -\frac{4}{63}\right)$	$8x^6 + 192x^5 + 237x^4 + 238x^3 - 15x^2 - 60x - 76$
$\left(-\frac{1}{3}, -\frac{11}{9}\right)$	$-56x^6 + 132x^5 + 102x^4 + 195x^3 - 240x^2 - 204x - 178$
$\left(-3, \frac{1}{28}\right)$	$4x^6 - 52x^5 + 133x^4 + 34x^3 - 171x^2 - 308x - 292$
$\left(\frac{1}{9}, \frac{11}{9}\right)$	$-2x^6 - 54x^5 + 135x^4 + 120x^3 - 135x^2 - 324x - 108$
$\left(-4, -\frac{7}{2}\right)$	$-15x^6 + 36x^5 + 5x^4 + 52x^3 + 50x^2 + 156x + 375$
$\left(-\frac{35}{69}, \frac{11}{69}\right)$	$4x^6 - 12x^5 - 219x^4 - 460x^3 + 15x^2 - 246x - 230$

Table 6. Some points of small height on the surface of Theorem 21 and the corresponding genus-2 curves.

12. Discriminant 24

12.1. *Parametrization.* We start with an elliptic K3 surface with fibers of type E_6, E_7 and A_3 at $t = \infty$, 0 and 1 respectively.

A Weierstrass equation for such a family is given by

$$y^2 = x^3 + t^2 x^2 + a(t-1)t^3 \big(2 + (d^2 - a + 1)(t-1)\big)x + a^2(t-1)^2 t^5 \big(1 + d^2(t-1)\big).$$

We identify a fiber of type E_8, and this leads us by a 3-neighbor step to an $E_8 E_7$ fibration.

From the new elliptic fibration we read out the Igusa–Clebsch invariants as usual, and then obtain the branch locus of $Y_-(24)$ as a double cover of $\mathbb{P}^2_{a,d}$, which is a union of two curves: one corresponding to an extra I_2 fiber, and one corresponding to the locus where the E_7 fiber promotes to an E_8 fiber.

Theorem 22. *A birational model over $\mathbb{Q}$ for the Hilbert modular surface $Y_-(24)$ as a double cover of $\mathbb{P}^2_{a,d}$ is given by the equation*

$$z^2 = (d^2 - a - 1)(16ad^4 - 8a^2d^2 - 20ad^2 + d^2 + a^3 - 3a^2 + 3a - 1).$$

It is a singular K3 surface.

12.2. *Analysis.* Note the extra involution $(a, d) \mapsto (a, -d)$.

The branch locus has two components. The first is the zero locus of $d^2 - a - 1$, and is obviously a rational curve (i.e., of genus 0) in the moduli space. It parametrizes the K3 surfaces in the family for which the E_7 fiber gets promoted to an E_8 fiber. The other component parametrizes elliptic K3 surfaces for which there is an extra I_2 fiber. It is also a genus-0 curve, though this fact is less obvious. A parametrization is given by

$$(a, d) = \left(\frac{1 - g^2}{2g^2 - 1}, \frac{g^3}{2g^2 - 1} \right).$$

The equation of the Hilbert modular surface describes it as a family of curves of genus 1 fibered over $\mathbb{P}^1_d$. In fact, we readily check that $(a, z) = (0, d^2 - 1)$ gives a section. So in fact, we have an elliptic surface, and by using the formula for the Jacobian, we can write it in Weierstrass form as

$$y^2 = x^3 - xd^2(144d^6 - 324d^4 + 235d^2 - 54)/48$$
$$- d^2(3456d^{10} - 22032d^8 + 50625d^6 - 54866d^4 + 28647d^2 - 5832)/1728.$$

This is an elliptic K3 surface E, and in fact, it is the base change (by $d \mapsto d^2$) of a rational elliptic surface with reducible fibers of types I_2, I_3 and I_4 (and therefore with Mordell–Weil rank 2). We can use this to readily compute one section

$$(x_0, y_0) = \left(11d^4 - 239d^2/12 + 9, (d^2 - 1)(9d^2 - 8)(32d^2 - 27)/8\right)$$

of height $\frac{1}{6}$. Translating x by x_0 and scaling to get rid of denominators, we get the following nicer form for E:

$$y^2 = x^3 + (132d^4 - 239d^2 + 108)x^2$$
$$+ 2(d^2 - 1)(9d^2 - 8)(32d^2 - 27)(10d^2 - 9)x + \left((d^2 - 1)(9d^2 - 8)(32d^2 - 27)\right)^2.$$

This has reducible fibers of type I_2 at $d = \infty$ and $d^2 = \frac{8}{9}$, type I_3 at $d^2 = \frac{27}{32}$, type IV at $d = 0$, and type I_4 at $d = \pm 1$. This gives a root system of type $A_1^3 \oplus A_2^3 \oplus A_3^2$, which has rank 15 and discriminant 1152.

In addition to the section $P_1 = \left(0, (d^2 - 1)(9d^2 - 8)(32d^2 - 27)\right)$, we also find the sections

$$P_2 = \left(-5(d^2 - 1)(9d^2 - 8), \sqrt{-1}(d^2 - 1)^2(9d^2 - 8)\right),$$
$$P_3 = \left(-(32d^2 - 27)(9d^2 - 8)/6, d(32d^2 - 27)(9d^2 - 8)/\sqrt{216}\right).$$

This shows that the elliptic K3 surface $Y_-(24)$ has geometric Picard number 20, i.e., is a singular K3 surface. The discriminant of the span of the algebraic divisors exhibited is 96. We showed that this is the entire Néron–Severi group by checking that our subgroup of the Mordell–Weil group is 2-saturated.

As mentioned, the quotient by the involution $d \mapsto -d$ is a rational elliptic surface

$$y^2 = x^3 + (132t^2 - 239t + 108)x^2$$
$$+ 2(t - 1)(9t - 8)(32t - 27)(10t - 9)x + \left((t - 1)(9t - 8)(32t - 27)\right)^2.$$

This surface has an I_2 fiber at $t = \frac{8}{9}$, an I_3 fiber at $t = \frac{27}{32}$ and an I_4 fiber at $t = 1$.

The Mordell–Weil group is generated by the sections

$$P_1 = \left(0, (t - 1)(9t - 8)(32t - 27)\right),$$
$$P_2 = \left(-5(t - 1)(9t - 8), \sqrt{-1}(t - 1)^2(9t - 8)\right),$$

with height matrix

$$\begin{pmatrix} \frac{1}{12} & 0 \\ 0 & \frac{1}{2} \end{pmatrix}.$$

12.3. Examples. Table 7 lists some points of small height and their genus-2 curves.

For instance, for the genus-2 curves corresponding to $\left(1, \frac{3}{2}\right)$ and $\left(1, -\frac{3}{2}\right)$, the point counts modulo p match the twist by $\mathbb{Q}(\sqrt{2})$ of a modular form of level 2592.

Rational point (a, d)	Sextic polynomial $f_6(x)$ defining the genus-2 curve $y^2 = f_6(x)$
$\left(\frac{77}{36}, -\frac{1}{6}\right)$	$-7x^6 - 18x^4 - 10x^3 + 3x^2 + 10x + 22$
$\left(\frac{21}{16}, \frac{1}{8}\right)$	$-12x^5 + 8x^4 + 24x^3 - 16x^2 - 21x + 14$
$\left(\frac{9}{4}, -\frac{1}{2}\right)$	$3x^6 - 12x^5 + 20x^4 - 79x^3 + 11x^2 - 84x + 60$
$\left(-\frac{7}{81}, -\frac{17}{18}\right)$	$27x^6 - 56x^5 - 21x^4 + 52x^3 + 57x^2 - 84x + 49$
$\left(\frac{77}{36}, \frac{1}{6}\right)$	$-32x^6 - 80x^5 + 94x^4 + 115x^3 - 91x^2 - 55x + 33$
$\left(\frac{9}{4}, -\frac{5}{4}\right)$	$-24x^6 + 48x^5 + 100x^4 + 120x^3 - 50x^2 - 72x - 41$
$\left(-\frac{3}{4}, -\frac{1}{4}\right)$	$25x^6 + 70x^4 + 24x^3 + 124x^2 + 48x + 72$
$\left(\frac{9}{4}, \frac{1}{2}\right)$	$-72x^6 + 84x^5 + 127x^4 - 123x^3 - 83x^2 + 51x + 25$
$\left(1, \frac{3}{2}\right)$	$9x^6 + 9x^4 - 60x^3 - 45x^2 + 132x - 53$
$\left(\frac{33}{50}, -\frac{1}{5}\right)$	$50x^5 - 50x^4 + 35x^3 - 35x^2 - 31x + 139$
$\left(-\frac{3}{4}, \frac{1}{4}\right)$	$33x^6 - 36x^5 + 110x^4 - 120x^3 + 140x^2 - 96x + 72$
$\left(\frac{21}{16}, -\frac{1}{8}\right)$	$7x^5 + 3x^4 + 78x^3 - 2x^2 + 63x + 147$
$\left(21, -\frac{5}{2}\right)$	$-8x^6 - 24x^5 + 80x^4 - 100x^3 + 170x^2 - 84x + 63$
$\left(-\frac{4}{9}, \frac{2}{3}\right)$	$-3x^6 + 14x^5 - 63x^4 + 96x^3 - 171x^2 - 48x - 188$
$\left(-\frac{7}{81}, \frac{17}{18}\right)$	$-7x^6 + 56x^5 - 95x^4 - 20x^3 - 205x^2 - 44x - 93$
$\left(21, \frac{5}{2}\right)$	$-24x^6 - 24x^5 - 280x^4 - 260x^3 + 170x^2 - 24x + 1$

Table 7. Some points of small height on the surface of Theorem 22 and the corresponding genus-2 curves.

We describe a few curves on the Hilbert modular surface, which can be used to produce rational points. Setting $a = -\frac{1}{9}$ gives a rational curve of genus 0, with infinitely many points. Sections of the fibration will also lead to curves birational to $\mathbb{P}^1$ over $\mathbb{Q}$. For instance, P_1 and $2P_1$ describe the rational curves given by $a = 4(d^2 - 1)/5$ and $a = (4d^2 - 5)/13$, respectively. The Brauer obstruction does not vanish identically on any of these.

13. Discriminant 28

13.1. *Parametrization.* We start with an elliptic K3 surface with fibers of type E_6, D_5 and A_4 at $t = \infty$, 0 and 1 respectively, and a section of height $\frac{28}{60} = \frac{7}{15} = 4 - \frac{6}{5} - 1 - \frac{4}{3}$.
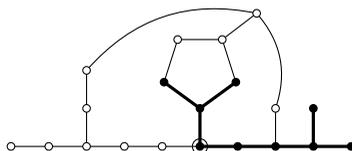
A Weierstrass equation for this family is given by

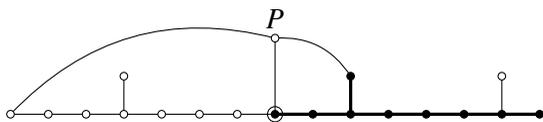$$y^2 = x^3 + atx^2 + bt^2(t - 1)^2 x + ct^3(t - 1)^4,$$

where

$$a = 2(f^2 - g^2)(t-1) + t,$$
$$b = (f^2 - g^2)^2(1-t) - 2(f^2 - g^2)(f+1)t,$$
$$c = (f+1)^2(f^2 - g^2)t.$$

We identify the class of a D_8 fiber and carry out a 2-neighbor step to convert to an elliptic fibration with D_8 and E_7 fibers, and a section of height $\frac{7}{2} = 4 + 2 \cdot 1 - 1 - \frac{3}{2}$.

Then we identify the class of an E_8 fiber, and carry out a 2-neighbor step to get the desired $E_8 E_7$ fibration.

The new elliptic fibration has a section, since $P \cdot F' = 5$, while the remaining component of the D_8 fiber has intersection number 2 with F'. We now read out the Igusa–Clebsch invariants.

Theorem 23. *A birational model over $\mathbb{Q}$ for the Hilbert modular surface $Y_-(28)$ as a double cover of $\mathbb{P}^2_{g,h}$ is given by the equation*

$$z^2 = -(g - f - 2)(g + f + 2)$$
$$\times (8g^4 + 92f^2g^2 + 180fg^2 + 71g^2 - 100f^4 - 180f^3 - 71f^2 + 4f + 4).$$

It is a singular K3 *surface.*

13.2. Analysis. It has a second involution $(f, g) \mapsto (f, -g)$. The branch locus consists of three components. The factors $g \pm (f + 2)$ correspond to the locus where the Picard number of the K3 surface jumps to 19, due to the presence of an I_2 fiber, but the discriminant decreases to 14, because the nontrivial section of height $\frac{7}{15}$ becomes divisible by 2. The more complicated factor corresponds to just the presence of an extra I_2 factor, which makes the discriminant 56. This component of the branch locus is also a genus 0 curve; a parametrization is given by

$$(f, g) = \left(-\frac{2m^4 + 17m^3 + 57m^2 + 85m + 47}{2(m+1)(m+2)(m^2 + 6m + 11)}, \; -\frac{(m^2 + 6m + 7)(2m^2 + 7m + 7)}{2(m+1)(m+2)(m^2 + 6m + 11)} \right).$$

Rational point (f, g)	Sextic polynomial $f_6(x)$ defining the genus-2 curve $y^2 = f_6(x)$
$\left(-\frac{31}{16}, -\frac{9}{16}\right)$	$9x^6 - 15x^5 + 39x^4 - 25x^3 + 36x^2 + 11$
$\left(-\frac{56}{65}, -\frac{61}{65}\right)$	$-37x^6 + 42x^5 + 17x^4 - 33x^3 - 7x^2 - 3x - 3$
$\left(-\frac{31}{16}, \frac{9}{16}\right)$	$15x^5 - 39x^4 - 11x^3 + 45x^2 + 27x$
$\left(-\frac{35}{24}, -\frac{31}{24}\right)$	$-27x^6 + 54x^5 - 36x^4 + 30x^3 - 24x^2 - 6x - 2$
$\left(-\frac{12}{11}, -\frac{1}{11}\right)$	$x^6 + 14x^5 + 61x^4 + 73x^3 - 49x^2 + 3x + 1$
$\left(-\frac{14}{9}, -\frac{5}{9}\right)$	$37x^6 + 69x^5 + 75x^4 + 79x^3 + 69x^2 + 12x + 20$
$\left(-\frac{2}{5}, -\frac{7}{5}\right)$	$-4x^6 + 12x^5 - x^4 + 87x^3 + 68x^2 + 48x + 3$
$\left(-\frac{13}{8}, -\frac{7}{8}\right)$	$3x^6 - 6x^5 + 5x^4 - 10x^3 + 41x^2 + 30x + 87$
$\left(-\frac{42}{41}, 1\right)$	$-92x^6 - 76x^5 + 21x^4 + 9x^3 + 9x^2 - x - 1$
$\left(-\frac{13}{8}, \frac{7}{8}\right)$	$18x^6 + 78x^5 + 44x^4 - 94x^3 - 76x^2 + 30x + 25$
$\left(\frac{5}{16}, -\frac{19}{16}\right)$	$-48x^6 + 45x^5 + 11x^4 + 87x^3 - 97x^2 - 63x + 56$
$\left(-\frac{30}{41}, -\frac{36}{41}\right)$	$-27x^6 + 57x^5 - 100x^4 - 68x^3 - 76x^2 + 36x$
$\left(-\frac{11}{3}, \frac{7}{3}\right)$	$16x^6 - 24x^5 - 111x^4 + 9x^3 + 102x^2 - 27x - 33$
$\left(\frac{26}{31}, -\frac{64}{31}\right)$	$-9x^6 - 6x^5 + 32x^4 + 32x^3 - 112x^2 - 6x + 99$
$\left(\frac{13}{80}, -\frac{15}{16}\right)$	$-9x^6 - 15x^5 + 85x^3 - 135x + 54$
$\left(\frac{26}{31}, \frac{64}{31}\right)$	$-25x^6 + 30x^5 - 64x^4 + 72x^3 - 136x^2 + 102x - 69$

Table 8. Some points of small height on the surface of Theorem 23 and the corresponding genus-2 curves.

Since the double cover is branched along a sextic, the Hilbert modular surface is itself a K3 surface. Setting $f = h - 2$ and then using the invertible substitution $h = t(1 + 1/x)$, $g = t(1 - 1/x)$ (and absorbing square factors) converts it to an elliptic fibration over $\mathbb{P}^1_t$, which we can write in Weierstrass form as

$$y^2 = x^3 - t(108t^3 - 176t^2 + 63t + 4)x^2$$
$$+ 32(t-1)^2 t^3 (135t^2 - 36t - 106)x - 64(t-1)^4 t^4 (6075t^2 - 6075t - 196).$$

This has fibers of type I_2 at $t = \infty$, $\frac{4}{5}$ and $\frac{28}{27}$, I_1^* at $t = 0$, I_5 at $t = 1$, and I_3 at $t = (19 \pm 7\sqrt{7})/36$, giving a contribution of $D_5 \oplus A_4 \oplus A_1^3 \oplus A_2^2$ to the Néron–Severi lattice. Therefore the Picard number is at least 18. We identify the sections

$$P_1 = \left(12t^2(t-1)(36t - 37), 4t^2(t-1)(27t - 28)(72t^2 - 76t + 1)\right),$$
$$P_2 = \big(t(1080t^3 - 2064t^2 + 953t + 28)/7,$$
$$2t^2(5t - 4)(27t - 28)(72t^2 - 76t + 1)/7^{3/2}\big),$$

with height matrix

$$\begin{pmatrix} \frac{7}{60} & 0 \\ 0 & \frac{2}{3} \end{pmatrix}.$$

Therefore the Picard number is 20. An easy lattice-theoretic argument (see the online supplement) shows that these sections must generate the Mordell–Weil group, and therefore the Néron–Severi lattice has discriminant 112.

The quotient by the involution $g \mapsto -g$ has equation

$$y^2 = x^3 - (84f^2 + 148f + 39)x^2/4 - (96f^4 + 364f^3 + 615f^2 + 500f + 140)x$$
$$- (f+2)^2(5f+2)^2(4f^2 + 4f - 1).$$

This is a rational elliptic surface with an I_4 fiber at $f = -1$, an I_3 fiber at $f = -\frac{17}{18}$, and I_2 fibers at $t = -\frac{26}{27}$ and $t = \infty$. The Mordell–Weil group is generated by the 2-torsion section $(-2(f+2)^2, 0)$ and the non-torsion section $\left(-2(f^2 + 3f + 3), (f+1)(18f + 17)\right)$ of height $\frac{1}{12}$.

13.3. *Examples.* Table 8 lists some points of small height and their genus-2 curves.

Next, we describe some special curves on the surface, which may be used to produce rational points. First, $f = -\frac{17}{18}$ gives a rational curve, which can be parametrized as $g = -19(h^2 - 2)/(18(h^2 + 2))$. The Brauer obstruction vanishes identically for this family, giving a family of genus-2 curves with real multiplication by $\mathcal{O}_{28}$. Next, the specialization $f = -\frac{26}{27}$ gives another rational curve, which can be parametrized as

$$g = -2\,\frac{13h^2 + 729h - 75816}{27(h^2 + 5832)}.$$

The Brauer obstruction does not vanish identically for this family. Finally, the section P_1 on the Jacobian of $Y_-(28)$ can be described as

$$(f, g) = \left(\frac{4t^2 - 8t + 1}{4t - 1}, \frac{4t^2 - 2t + 1}{4t - 1}\right).$$

The Brauer obstruction vanishes identically on this family as well.

From a plot of the rational points, we observe many rational points on the lines $g = \pm(5f + 2)/3$. However, the Brauer obstruction does not vanish identically along these lines.

14. Discriminant 29

14.1. *Parametrization.* We start with an elliptic K3 surface with fibers of type E_7 and A_8, and a section P of height $\frac{29}{18} = 4 - \frac{3}{2} - \frac{8}{9}$. A Weierstrass equation for this family is given by

$$y^2 = x^3 + \left(-(4f - 1)t^2 + (g - 2)t + 1\right)x^2$$
$$- 2gt^3\left(2f^2t^2 + (-g + 2f + 1)t - 1\right)x + g^2t^6\left((g - 4f)t + 1\right).$$

We identify a fiber F of type E_8, and go to the associated elliptic fibration by a 3-neighbor step. Note that $P \cdot F = 4$, while the remaining component of the A_8 fiber intersects F with multiplicity 3. Therefore the new fibration has a section.
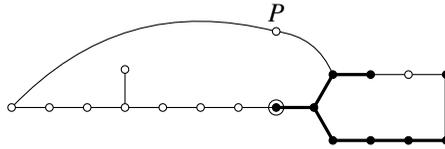
The new elliptic fibration has E_8 and E_7 fibers, and we may read out the Igusa–Clebsch invariants. The branch locus for the double cover of $\mathbb{P}^2_{f,g}$ corresponds to elliptic K3 surfaces having an extra I_2 fiber.

Theorem 24. *A birational model over $\mathbb{Q}$ for the Hilbert modular surface $Y_-(29)$ as a double cover of $\mathbb{P}^2$ is given by the equation*

$$z^2 = -g^4 + (6f + 11)g^3 - (27f^4 - 18f^3 + 5f^2 + 102f - 1)g^2$$
$$+ 8f(36f^3 - 25f^2 + 35f - 1)g - 16f^2(4f - 1)^3.$$

It is a K3 surface of Picard number 19.

14.2. *Analysis.* The branch locus is a rational curve, and a parametrization is given by

$$(f, g) = \left(\frac{(m+2)^2(m^2+2m-4)}{m^2(m^2+6m+12)}, \frac{4(m+2)^2(m+4)^3}{m(m^2+6m+12)^2} \right).$$

The substitution $g = hf$ makes the right-hand side of the equation a quartic in f, after absorbing a factor of f^2 into z^2 on the left. Also, $f = 0$ makes the right-hand side a square (namely $(h-4)^2$), giving us a point on the genus-1 curve over $\mathbb{P}^1_h$. We may then replace the genus-1 curve by its Jacobian, which has the following equation after the change of parameter $h = 4 - t$, and some Weierstrass transformations:

$$y^2 = x^3 - (t^4 - 10t^3 - t^2 - t - 16)x^2$$
$$- t(20t^5 - 140t^4 - 3740t^3 + 14234t^2 + 3349t - 1120)x$$
$$- t^2(3475t^6 - 46300t^5 + 180355t^4 - 10362t^3 - 849193t^2 + 276269t - 19600).$$

This is an elliptic K3 surface, with bad fibers of type I_4 at $t = \infty$, I_3 at $t = 0$ and at the roots of the polynomial $15t^3 + 12t^2 + 160t - 64$ (which gives the cubic field of discriminant -87), and I_2 at the roots of $2t^3 - 38t^2 + 255t - 28$ (which gives the cubic field of discriminant -116). The trivial lattice therefore has rank 16, leaving room for Mordell–Weil rank at most 4. We find the linearly independent sections

$$P_1 = \big(t(125t^3 - 700t^2 + 800t - 76)/4,$$

$$t(1375t^5 - 11450t^4 + 29240t^3 - 23616t^2 + 7296t - 512)/8),$$

$$P_2 = \big((30t^4 - 306t^3 + 636t^2 + 1833t - 448)/29,$$
$$(2t^3 - 38t^2 + 255t - 28)(15t^3 + 12t^2 + 160t - 64)/(29b)\big),$$

$$P_3 = \big(2(3a - 5)t^2 - 3(8a - 23)t,$$
$$at\big(-99t^3 + 18(a + 37)t^2 - 144(3a + 7)t + 416a - 288\big)/3\big).$$

Here $a = \sqrt{-3}$ and $b = \sqrt{29}$. Therefore, the Picard number of the Hilbert modular surface is at least 19. We showed by counting points modulo 11 and 13 that the Picard number must be exactly 19. This agrees with the calculations in [Oda 1982, p. 109]. The height matrix of the sections above is

$$\frac{1}{6}\begin{pmatrix} 20 & 0 & -10 \\ 0 & 3 & 0 \\ -10 & 0 & 14 \end{pmatrix}.$$

Therefore, the sublattice of the Néron–Severi lattice spanned by the sections above together with the trivial lattice has discriminant $2^4 \cdot 3^4 \cdot 5 = 6480$. By checking that it is 2- and 3-saturated, we showed that it is the entire Néron–Severi lattice, and therefore the sections P_1, P_2, P_3 generate the Mordell-Weil group.

14.3. *Examples.* Table 9 lists some points of small height and their genus-2 curves. The section P_1 corresponds to the rational curve given by $g = \frac{4}{5}uf$, with

$$f = \frac{22u^5 - 321u^4 + 1651u^3 - 3377u^2 + 1980u + 50}{25u^6 - 400u^5 + 2375u^4 - 6050u^3 + 4813u^2 + 2325u + 225}.$$

The Brauer obstruction vanishes identically, yielding a 1-parameter family of genus-2 curves with real multiplication by $\mathcal{O}_{29}$.
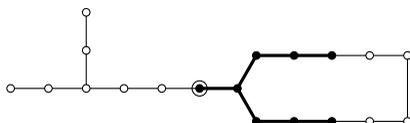
15. Discriminant 33

15.1. *Parametrization.* We start with an elliptic K3 surface with fibers of type A_{10} and E_6 at $t = \infty$ and $t = 0$ respectively. A Weierstrass equation for such a family is given by

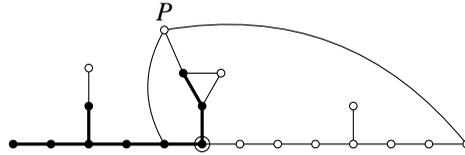$$y^2 = x^3 + (c + 2d + 1)t^2x^2 + 2(c + d)t^4x + ct^4,$$

with

$$c = (s^2 - r^2)^2t^2 - (s^2 - r^2)(s^2 - r^2 + 2r)t + s^2, \quad d = (s^2 - r^2)(1 - t) + r.$$

We identify the class of an E_7 fiber below, and perform a 2-neighbor step.

The new elliptic fibration has fibers of type E_6, E_7 and A_2, as well as a section P of height $\frac{33}{18} = \frac{11}{6} = 4 - 0 - \frac{3}{2} - \frac{2}{3}$. We then identify the class of an E_8 fiber and carry out a 3-neighbor step to an $E_8 E_7$ elliptic fibration.

The new elliptic fibration has a section, since $P \cdot F' = 5$, while the intersection number of the remaining component of the E_6 fiber with F' is 3, and these are coprime.

From the Weierstrass equation of the $E_8 E_7$ fibration, we determine the Igusa–Clebsch invariants, and then the equation of the branch locus.

Theorem 25. *A birational model over $\mathbb{Q}$ for the Hilbert modular surface $Y_-(33)$ as a double cover of $\mathbb{P}^2$ is given by the equation*

$$z^2 = 9s^6 - (26r^2 - 80r + 104)s^4 + (25r^4 - 152r^3 + 400r^2 - 408r + 432)s^2$$
$$- (8r^6 - 72r^5 + 280r^4 - 472r^3 + 336r^2 - 64r - 16).$$

Rational point (f, g)	Sextic polynomial $f_6(x)$ defining the genus-2 curve $y^2 = f_6(x)$
$\left(-37, -\frac{37}{2}\right)$	$-98x^5 - 56x^4 - 131x^3 - 114x^2 + 10x - 68$
$\left(\frac{20}{67}, \frac{16}{67}\right)$	$264x^6 + 760x^5 + 183x^4 - 630x^3 - 53x^2 - 20x - 4$
$\left(\frac{6}{7}, \frac{48}{7}\right)$	$12x^6 - 12x^5 - 409x^4 + 1062x^3 + 287x^2 - 588x - 252$
$(-40, 40)$	$-53x^6 + 227x^5 + 374x^4 + 1191x^3 + 669x^2 + 680x + 900$
$\left(-1, -\frac{29}{10}\right)$	$1210x^5 - 110x^4 + 511x^3 - 17x^2 + 53x + 1$
$\left(-4, -\frac{16}{5}\right)$	$-200x^6 + 1360x^5 - 995x^4 + 242x^3 - 191x^2 - 4x - 12$
$\left(-\frac{1}{7}, -\frac{37}{98}\right)$	$-1588x^6 + 986x^5 - 122x^4 + 221x^3 - 68x^2 - 2x - 8$
$(-6, 8)$	$540x^6 + 2052x^5 - 1149x^4 + 1724x^3 - 39x^2 - 894x - 506$
$\left(\frac{5}{43}, \frac{19}{43}\right)$	$-2x^6 + 80x^5 - 786x^4 + 2265x^3 + 74x^2 + 80x - 2$
$\left(\frac{8}{9}, \frac{16}{9}\right)$	$-4x^6 + 204x^5 - 837x^4 - 160x^3 + 2451x^2 + 1620x - 228$
$\left(-\frac{6}{13}, -\frac{16}{13}\right)$	$236x^6 - 796x^5 + 2293x^4 - 2178x^3 + 1525x^2 + 2492x - 764$
$\left(-\frac{4}{9}, \frac{16}{9}\right)$	$552x^6 - 2232x^5 + 3183x^4 + 562x^3 - 4713x^2 - 1248x - 88$
$\left(-3, \frac{36}{5}\right)$	$1024x^6 - 1920x^5 - 2252x^4 + 1065x^3 - 2288x^2 - 6195x + 66$
$\left(\frac{18}{19}, \frac{48}{19}\right)$	$-768x^6 - 2560x^5 + 1571x^4 + 7838x^3 - 2133x^2 - 6912x + 2376$
$\left(-\frac{4}{5}, -\frac{32}{25}\right)$	$-1412x^6 - 1372x^5 + 2149x^4 + 8226x^3 + 4889x^2 - 896x - 4096$
$\left(\frac{2}{9}, \frac{7}{9}\right)$	$3189x^6 + 4599x^5 - 6897x^4 - 9331x^3 + 5424x^2 + 5040x - 1968$

Table 9. Some points of small height on the surface of Theorem 24 and the corresponding genus-2 curves.

It is a singular K3 *surface.*

15.2. Analysis. This is a double cover of the (r, s)-plane branched along a sextic, and is therefore a K3 surface. The extra involution is given by $(r, s) \mapsto (r, -s)$. The equation of the branch locus may be transformed as follows: setting $t = s^2$, we have

$$-8r^6 + 72r^5 + (25t - 280)r^4 + (-152t + 472)r^3 + (-26t^2 + 400t - 336)r^2$$
$$+ (80t^2 - 408t + 64)r + (9t^3 - 104t^2 + 432t + 16) = 0$$

which, after resolution of singularities, becomes a genus-0 curve, parametrized by

$$r = \frac{m^3 + 4m^2 + 4m + 4}{m^2(m + 1)}, \qquad t = \frac{8(m^3 + 4m^2 + 4m + 2)}{m^4(m + 1)^2}.$$

Then the branch locus can be written as a double cover

$$s^2 = 8(m^3 + 4m^2 + 4m + 2)/(m^4(m + 1)^2).$$

After removing square factors and performing a Weierstrass transformation, it is converted to the elliptic curve $y^2 + y = x^3 - x^2$. It is isomorphic to $X_1(11) \cong X_0(33)/\langle w_{33} \rangle$, where w_{33} is the Atkin–Lehner involution.

For the equation of the Hilbert modular surface, the transformation $s = r + t$ makes the right-hand side of the equation a quartic in r, with the coefficient of r^4 being a square. Converting to the Jacobian form, and applying a Weierstrass transformation as well as scaling t, we get an elliptic fibration

$$y^2 = x^3 + (t^4 + 24t^3 + 58t^2 + 84t + 1)x^2$$
$$+ (280t^5 + 5488t^4 + 1376t^3 + 2192t^2 + 72t)x$$
$$+ 4608t^7 + 95632t^6 + 32576t^5 + 26848t^4 + 14656t^3 + 1296t^2.$$

This has bad fibers of type I_5 at $t = \infty$, type II at $t = 1$, type I_3 at $t = 0$, $\frac{1}{2}$ and $(-17 \pm 3\sqrt{33})/2$, and type I_2 at $t = -\frac{21}{2} \pm \frac{11\sqrt{33}}{6}$. These contribute $A_1^3 \oplus A_2^4 \oplus A_4$ to the Néron–Severi lattice.

By finding sections modulo a small prime and attempting to lift them to $\mathbb{Q}$ or $\mathbb{Q}(\sqrt{33})$, we find the following sections of small height:

$$P_1 = \left(4t(3t^2 + 60t - 13), \ 4t(t^2 + 17t - 2)(3t^2 + 63t - 2) \right),$$

$$P_2 = \left(-4t(3t + 11), \ 4t(t - 1)(3t^2 + 63t - 2) \right),$$

$$P_3 = \big((4\sqrt{33} + 12)t^2 - (2\sqrt{33} + 34)t,$$
$$(\sqrt{33} + 3)t(2t - 1)(2t + 3\sqrt{33} + 17)(6t + 63 - 11\sqrt{33})/6 \big).$$

Rational point (r, s)	Sextic polynomial $f_6(x)$ defining the genus-2 curve $y^2 = f_6(x)$
$\left(\frac{11}{3}, \frac{8}{3}\right)$	$-9x^6 - 6x^5 - 7x^4 + 7x^3 + 2x^2 + 3x - 2$
$(1, 3)$	$-4x^6 + 15x^4 - x^3 - 9x^2 + 12x + 5$
$\left(-\frac{13}{5}, \frac{27}{5}\right)$	$-14x^5 + 20x^4 + 2x^3 - 15x^2 - 4x$
$\left(\frac{28}{3}, \frac{23}{3}\right)$	$-5x^6 + 6x^5 - 5x^4 + 27x^3 - 11x^2 + 12x - 24$
$\left(\frac{73}{19}, -\frac{41}{19}\right)$	$-7x^6 + 15x^5 + x^4 - 31x^3 - 2x^2 + 12x + 12$
$(1, -3)$	$-x^6 - 3x^5 + 9x^4 + 34x^3 - 30x^2 - 9x + 8$
$\left(\frac{41}{51}, \frac{7}{51}\right)$	$-9x^6 - 9x^5 - 35x^4 + 11x^3 - 8x^2 + 12x$
$\left(\frac{16}{15}, \frac{1}{15}\right)$	$2x^6 - 3x^5 + 7x^4 + 13x^3 - 20x^2 + 36x - 15$
$\left(-\frac{13}{5}, -\frac{27}{5}\right)$	$-5x^5 - 3x^4 + 13x^3 - 17x^2 - 40x$
$\left(\frac{46}{3}, \frac{41}{3}\right)$	$-8x^6 + 36x^5 - 23x^4 - 21x^3 - 47x^2 - 18x - 9$
$\left(-\frac{17}{10}, \frac{27}{10}\right)$	$-20x^5 + 28x^4 - 37x^3 + 60x^2 + 44x$
$\left(\frac{13}{3}, -\frac{11}{3}\right)$	$7x^6 - 48x^5 + 68x^4 - 2x^3 - 25x^2 + 24x - 36$
$\left(-\frac{38}{11}, \frac{61}{11}\right)$	$-9x^6 - 6x^5 + 69x^4 - 19x^3 - 39x^2 + 12x - 8$
$\left(-\frac{29}{3}, -11\right)$	$-31x^5 + 71x^4 - 32x^3 + 23x^2 - 40x - 8$
$\left(\frac{1}{33}, \frac{56}{33}\right)$	$3x^6 + 24x^5 + 8x^4 + 41x^3 + 32x^2 - 72x - 36$
$\left(\frac{13}{3}, \frac{11}{3}\right)$	$-12x^6 + 24x^5 - 31x^4 + 81x^3 - 67x^2 + 39x - 70$

Table 10. Some points of small height on the surface of Theorem 25 and the corresponding genus-2 curves.

These are linearly independent in the Mordell–Weil group, and the matrix of Néron–Tate heights is

$$\frac{1}{30}\begin{pmatrix} 6 & -2 & 3 \\ -2 & 19 & -1 \\ 3 & -1 & 9 \end{pmatrix}.$$

It has determinant $\frac{11}{360}$, and so the sublattice of the Néron–Severi group generated by these sections and the trivial lattice has rank 20 and discriminant $-\frac{11}{360} \cdot 2^3 \cdot 3^4 \cdot 5 = -99$. We show that this is the full Picard group by checking that our subgroup of the Mordell–Weil group is 3-saturated. We deduce that $Y_-(33)$ is a singular K3 surface with Picard lattice of discriminant -99.

The quotient of the $Y_-(33)$ by the involution $s \mapsto -s$ has Weierstrass equation

$$y^2 = x^3 - 2(13r^2 - 40r + 52)x^2 + 9(25r^4 - 152r^3 + 400r^2 - 408r + 432)x$$
$$- 648(r - 1)^3(r^3 - 6r^2 + 14r + 2).$$

It is a rational elliptic surface, with reducible fibers of types I_5, I_3 and I_2 at $r = \infty$, 19 and 23 respectively. The Mordell–Weil group is generated by the section $\left(3(3r^2 - 16t + 112), 12(r - 23)(r - 19)\right)$ of height $\frac{1}{30}$.

15.3. *Examples.* Table 10 on the previous page lists some points of small height and their genus-2 curves.

We may attempt to match up these examples with eigenforms in the tables of modular forms. For instance, for the points $(1, 3)$ and $(1, -3)$, the corresponding genus-2 curves (with isogenous Jacobians)

$$y^2 = -(x^3 - 3x - 1)(4x^3 - 3x + 5),$$
$$y^2 = -(x^3 - 3x^2 + 1)(x^3 + 6x^2 + 9x - 8)$$

have the property that their traces match those of a newform of weight $1296 = 2^4 \cdot 3^4$ in the modular forms database.

We also see some simple rational curves on the Hilbert modular surface: the specialization $r = 19$ gives a rational curve parametrized by $s = -(16m^2 + 41)/(3m)$, while $r = 23$ is also a rational curve, parametrized by $s = -(16m^2 + 7)/m$. The Brauer obstructions do not identically vanish for points on these curves.

We have slightly better luck with sections of the elliptic fibration: for instance, the sections $P_1, 2P_1, 3P_1$ give rise to rational curves with respective parametrizations

$$\left(-\frac{3t^2 - 112}{2(3t + 8)}, \frac{3t^2 + 16t + 112}{2(3t + 8)}\right), \quad \left(-\frac{t^2 - 12}{2(t + 2)}, \frac{t^2 + 4t + 12}{2(t + 2)}\right),$$
$$\left(-\frac{3t^2 - 20}{6(t + 2)}, \frac{3t^2 + 12t + 20}{6(t + 2)}\right).$$

The Brauer obstruction vanishes identically on each of these.

16. Discriminant 37

16.1. *Parametrization.* We start with an elliptic K3 surface with fibers of type E_6, D_5 and A_4 at $t = \infty$, 0 and 1 respectively, and a section of height $\frac{37}{60} = 4 - \frac{4}{3} - \frac{5}{4} - \frac{4}{5}$.

A Weierstrass equation for this family is

$$y^2 = x^3 + atx^2 + bt^2(t - 1)^2 x + ct^3(t - 1)^4,$$

with

$$a = (2g - f + 1)(t - 1) + g^2 t/4,$$
$$b = (f - g - 1)\big((f + g - 1)(t - 1) + (f - 2)gt/2\big),$$
$$c = (g - f + 1)^2\big(f^2(t - 1) + (f - 2)^2\big)/4.$$

We identify the class of an D_8 fiber and carry out a 2-neighbor step to convert to an elliptic fibration with D_8 and E_6 fibers.

This new elliptic fibration has Mordell–Weil rank 2. In fact, it is quite easy to exhibit one non-torsion section P (we do so in the online supplement) of height $\frac{2}{3} = 4 - \frac{4}{3} - 2$. Then we find an E_8 fiber as shown below, and proceed to it by a 2-neighbor step. The section P combined with most of the components of the E_6 fiber gives a disjoint E_7 configuration, and therefore the new elliptic fibration has reducible fibers of type E_8 and E_7. The fact that $(-P)$ intersects the multiplicity-1 component of the E_8 fiber shown below implies that the new fibration has a section.

We then read out the Igusa–Clebsch invariants and write down the equation of the Hilbert modular surface.

Theorem 26. *A birational model over $\mathbb{Q}$ for the Hilbert modular surface $Y_-(37)$ as a double cover of $\mathbb{P}^2$ is given by the equation*

$$z^2 = f^2 g^4 + 2f(14f - 1)g^3 - (126f^3 - 142f^2 + 44f - 1)g^2$$
$$+ (f - 1)(54f^3 - 34f^2 + 17f - 10)g - (f - 1)^2(27f^2 - 8f + 8).$$

It is a K3 *surface of Picard number* 19.

16.2. *Analysis.* The branch locus corresponds to the locus where the elliptic K3 surface acquires an extra I_2 fiber. The transformation

$$(f, g) = \left(\frac{2x^2 y + 4xy + y + x^4 + x^3 - 3x^2 - x}{x^3(x + 2)}, \frac{2y + x^2 - 2x - 1}{x^2} \right)$$

converts it to the elliptic curve

$$y^2 + y = x^3 - x,$$

which is 37a in Cremona's tables. This is an elliptic curve of rank 1, isomorphic to $X_0(37)/\langle w \rangle$, where w is the Atkin–Lehner involution.

To analyze this Hilbert modular surface, note that we have a genus-1 fibration over $\mathbb{P}^1_f$, which has a section because the coefficient of g^4 is a square. Hence $Y_-(37)$ is an elliptic K3 surface. Taking the Jacobian of this genus-1 curve over $\mathbb{Q}(f)$, and

Rational point (f, g)	Sextic polynomial $f_6(x)$ defining the genus-2 curve $y^2 = f_6(x)$
$\left(\frac{3}{2}, \frac{11}{7}\right)$	$17x^6 - 24x^5 - 66x^4 + 68x^3 + 81x^2 - 54x - 27$
$\left(\frac{3}{4}, \frac{11}{9}\right)$	$15x^6 - 6x^5 - 71x^4 + 35x^3 + 94x^2 - 48x - 21$
$\left(\frac{3}{2}, \frac{1}{3}\right)$	$11x^6 - 54x^5 - 125x^4 - 52x^3 - 32x^2 - 42x - 75$
$\left(\frac{3}{2}, \frac{59}{65}\right)$	$-135x^6 + 108x^5 + 45x^4 - 44x^3 + 130x^2 - 12x + 95$
$\left(\frac{1}{4}, \frac{17}{5}\right)$	$81x^5 - 135x^4 + 13x^3 - 9x^2 + 70x - 15$
$\left(-\frac{13}{3}, \frac{16}{13}\right)$	$-13x^6 + 156x^5 - 24x^4 - 132x^3 - 45x^2 + 108x - 27$
$\left(-\frac{4}{9}, -\frac{13}{6}\right)$	$36x^6 - 108x^5 + 165x^4 - 124x^3 + 21x^2 + 36x - 28$
$\left(\frac{5}{3}, \frac{13}{10}\right)$	$-54x^6 + 54x^5 - 9x^4 - 84x^3 + 141x^2 - 180x + 100$
$\left(\frac{3}{16}, \frac{13}{8}\right)$	$52x^6 + 156x^5 - 39x^4 - 180x^3 + 9x^2 + 72x - 16$
$\left(-\frac{1}{2}, \frac{15}{13}\right)$	$-31x^6 + 156x^5 - 195x^4 - 260x^3 + 210x^2 + 156x + 23$
$\left(3, \frac{81}{11}\right)$	$-18x^6 + 122x^5 - 135x^4 - 268x^3 - 25x^2 + 144x + 176$
$\left(\frac{1}{4}, 3\right)$	$x^6 + 72x^5 - 18x^4 - 189x^3 - 117x^2 + 270x + 45$
$\left(\frac{31}{15}, \frac{16}{31}\right)$	$-53x^6 + 6x^5 - 21x^4 + 208x^3 - 258x^2 - 276x + 259$
$\left(\frac{34}{27}, \frac{14}{51}\right)$	$-2x^6 + 36x^5 - 138x^4 + 105x^3 - 33x^2 - 153x - 289$
$\left(3, \frac{7}{2}\right)$	$-108x^6 - 324x^5 - 207x^4 - 116x^3 + 105x^2 - 12x - 12$
$\left(\frac{22}{3}, \frac{38}{11}\right)$	$-22x^6 + 72x^5 + 84x^4 - 341x^3 - 441x^2 + 417x + 473$

Table 11. Some points of small height on the surface of Theorem 26 and the corresponding genus-2 curves.

reparametrizing $f = t/(t+1)$, we get, after some Weierstrass transformations, the equation

$$y^2 = x^3 - (t+1)(27t^3 + 21t^2 - 19t - 1)x^2 - 8t^2(t+1)^2(30t^2 - 235t - 1)x$$
$$- 16t^3(t+1)^2(3136t^4 + 5484t^3 + 1024t^2 - 2161t - 108).$$

This surface has reducible fibers of type IV at $t = -1$, type I_2 at $t = -\frac{1}{28}$, and type I_3 at $t = 0, \infty$ and the four roots of $(27t^4 + 45t^3 + 10t^2 + 22t + 3)$. This quartic polynomial describes a quadratic extension of $\mathbb{Q}(\sqrt{37})$. The bad fibers contribute $A_2^7 \oplus A_1$ to the trivial lattice. We also have a 3-torsion section

$$P_0 = \left(4t(t+1)(9t^2 + 7t - 3), 4t(t+1)(27t^4 + 45t^3 + 10t^2 + 22t + 3)\right)$$

and two non-torsion sections

$$P_1 = \left(4t(t+1)(49t^2 + 28t - 1), 4t(t+1)(637t^4 + 854t^3 + 276t^2 + 33t + 1)\right),$$
$$P_2 = \big(4(252t^4 + 457t^3 + 118t^2 - 177t - 9)/37,$$
$$4(t+3)(28t+1)(27t^4 + 45t^3 + 10t^2 + 22t + 3)/37^{3/2}\big).$$

These two sections have height $\frac{8}{3}$ and $\frac{5}{6}$ respectively and are orthogonal with respect

to the Néron–Tate height pairing. Therefore, the Néron–Severi lattice contains a sublattice of rank 19 and discriminant 1080. Counting points modulo 11 and 13 shows that the Picard number must be exactly 19. This is again confirmed by Oda's tables [1982, p. 109]. We checked that the Mordell–Weil subgroup generated by P_0, P_1 and P_2 is saturated at 2 and 3, and thus that we have the full Néron–Severi lattice.

16.3. *Examples.* Table 11 on the previous page lists some points of small height and their genus-2 curves.

Next, we describe some curves of small genus on the surface, which may be used to produce rational points. The specialization $f = -\frac{1}{27}$ gives a rational curve, with parametrization $g = 7(h^2 - 8h + 19)/(3(h^2 - 1))$. The Brauer obstruction does not vanish identically for this rational curve.

The sections P_1 and $-P_1$ give rational curves, parametrized by

$$g = \frac{13 f^2 - 7f + 3}{f(3f + 2)} \quad \text{and} \quad g = \frac{9 f^2 - 2f + 2}{7f + 1}$$

respectively. The Brauer obstruction vanishes on both these loci, yielding families of genus-2 curves whose Jacobians have real multiplication by $\mathcal{O}_{37}$.

17. Discriminant 40

17.1. *Parametrization.* We start with an elliptic K3 surface with fibers of type E_7, D_5 and A_4 at $t = \infty, 0$ and 1 respectively.

A Weierstrass equation for this family is given by

$$y^2 = x^3 + t\big(e^2 t + (4d + 1)(1 - t)\big)x^2$$
$$+ 2t^2(t - 1)^2\big(2det + 2d(d + 1)(1 - t)\big)x + 4d^2 t^3(t - 1)^4$$

with

$$d = (f - e + 1)(f + e - 1)/2.$$

We first identify the class of a D_8 fiber, and perform a 2-neighbor step to an elliptic fibration with D_8 and E_7 fibers.
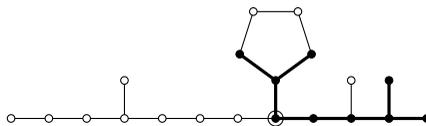
This fibration has a section P of height $5 = 4 + 2 - 1$. Next, we take a 2-neighbor step to go to a fibration with E_8 and E_7 fibers. We have $P \cdot F' = 9$, while the intersection number of the F' with the remaining component of the D_8 fiber is 2.

Since these are coprime, the new elliptic fibration has a section.
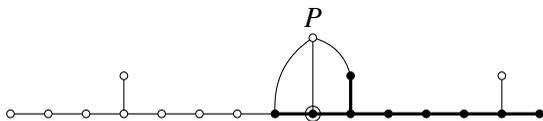
Finally, we read out the Igusa–Clebsch invariants, and compute the branch locus of the double cover, which is a union of two curves, one corresponding to an extra I_2 fiber, the other to a promotion of the fiber at $t = \infty$ from E_7 to E_8.

Theorem 27. *A birational model over $\mathbb{Q}$ for the Hilbert modular surface $Y_-(40)$ as a double cover of $\mathbb{P}^2_{e,f}$ is given by the equation*

$$z^2 = -(f^2 - e^2 + 1)\big(8f^4 + (-17e^2 + 12e - 8)f^2 + 9e^4 - 12e^3 + 7e^2 + 10e + 2\big).$$

It is a K3 *surface of Picard number* 19.

17.2. Analysis. The extra involution is $(e, f) \mapsto (e, -f)$. The branch locus is a union of two curves. The first, $f^2 - e^2 + 1 = 0$, is a rational curve, parametrized by say $(e, f) = \big((t^2 + 1)/(2t), (t^2 - 1)/(2t)\big)$. It corresponds to the subfamily of elliptic K3 surfaces for which the E_7 fiber is promoted to an E_8 fiber. The other component is also a rational curve, parametrized by

$$(e, f) = \left(-\frac{(m^2 - 2)^2}{m(m - 2)(m^2 - 4m + 2)}, \frac{2(m^2 - 2m + 2)(m^2 - m - 1)}{m(m - 2)(m^2 - 4m + 2)}\right).$$

It corresponds to elliptic K3 surfaces with an extra I_2 fiber.

The Hilbert modular surface is a double cover of a plane branched along a sextic, and is therefore a K3 surface. The transformation $f = e + t$ makes it a quartic in e, whose leading coefficient is a square. We thus get an elliptic K3 surface whose Weierstrass equation may be obtained by taking the Jacobian of this genus-1 curve. After some elementary algebra, we get the elliptic K3 surface

$$y^3 = x^3 + (t^4 + 24t^3 + 98t^2 + 16t + 1)x^2$$
$$+ (128t^5 + 2352t^4 + 1088t^3 + 64t^2)x - (512t^6 + 9216t^5 + 704t^4).$$

It has reducible fibers of types I_6 at $t = \infty$, I_4 at $t = 0$, I_3 at $t = -8 \pm \frac{5\sqrt{10}}{2}$, and I_2 at $t = \frac{1}{3}$ and $t = -9 \pm 4\sqrt{5}$, giving a contribution of $A_5 \oplus A_3 \oplus A_1^3 \oplus A_2^2$ to the Néron–Severi lattice. The trivial lattice thus has rank 17 and discriminant 1728.

We also have the two sections

$$P_1 = \big(4t(2t^2 + 36t + 3), -4t(t^2 + 18t + 1)(2t^2 + 32t + 3)\big),$$

$$P_2 = \big(-(6t^4 + 124t^3 + 303t^2 + 138t + 9)/10,$$
$$\sqrt{10}(2t + 3)(3t - 1)(t^2 + 18t + 1)(2t^2 + 32t + 3)/100\big).$$

These have heights $\frac{1}{12}$ and $\frac{7}{6}$ respectively, and are orthogonal with respect to the height pairing. Therefore, the Picard number is at least 19. Counting points modulo 7 and 11 proves that the Picard number is 19 (we thank Ronald van Luijk for carrying out such a calculation), in agreement with Oda's calculations [1982, p. 109]. The part of the Néron–Severi lattice spanned by the above sections with the trivial lattice has rank 19 and discriminant 168. We showed that this lattice is 2-saturated, so it is the full Néron–Severi lattice.

The quotient of the Hilbert modular surface by the involution $f \mapsto -f$ is the rational elliptic surface

$$y^2 = (x + 8e^2 - 8)\left(x^2 + (17e^2 - 12e + 8)x + 8(3e + 1)^2(e^2 - 2e + 2)\right).$$

It has reducible fibers of types I_6, I_3, I_2 at $e = \infty, 8, 9$, respectively, and the Mordell–Weil group is generated by the 6-torsion section

$$\left(-4(2e^2 + e - 11), \, 4(e - 9)(e - 8)\right);$$

indeed this is the universal elliptic curve over $X_1(6)$.

17.3. *Examples.* Table 12 lists some points of small height and their genus-2 curves.

Rational point (e, f)	Sextic polynomial $f_6(x)$ defining the genus-2 curve $y^2 = f_6(x)$
$\left(\frac{49}{8}, -\frac{47}{8}\right)$	$-12x^6 - 12x^5 - 21x^4 + 14x^3 + 39x^2 + 48x - 64$
$\left(\frac{31}{6}, 5\right)$	$108x^6 + 108x^5 - 81x^4 + x^3 + 63x^2 - 33x + 9$
$\left(-\frac{1}{12}, -\frac{5}{6}\right)$	$36x^5 + 78x^4 - 41x^3 - 129x^2 + 45x + 27$
$\left(-\frac{13}{10}, -\frac{4}{5}\right)$	$-72x^6 + 108x^5 + 135x^4 - 135x^3 - 219x^2 + 135x + 53$
$\left(\frac{49}{8}, \frac{47}{8}\right)$	$-72x^6 + 216x^5 - 315x^4 + 162x^3 + 21x^2 - 72x - 16$
$\left(-\frac{23}{14}, -\frac{13}{7}\right)$	$-8x^6 + 60x^5 - 87x^4 - 163x^3 + 288x^2 + 324x + 27$
$\left(-\frac{29}{12}, -\frac{25}{12}\right)$	$12x^6 + 132x^5 + 355x^4 - 90x^3 - 245x^2 + 36x - 44$
$\left(\frac{87}{55}, \frac{12}{55}\right)$	$44x^5 + 200x^4 - 422x^3 + 180x^2 - 81x$
$\left(-\frac{75}{28}, \frac{18}{7}\right)$	$-77x^6 + 147x^5 - 45x^4 - 335x^3 + 186x^2 - 180x - 432$
$\left(\frac{49}{23}, \frac{43}{23}\right)$	$46x^6 - 24x^5 + 252x^4 - 29x^3 + 468x^2 + 24x + 366$
$\left(-\frac{37}{36}, \frac{35}{36}\right)$	$-18x^6 - 258x^5 - 475x^4 + 220x^3 - 325x^2 + 72x - 48$
$\left(\frac{19}{8}, \frac{13}{8}\right)$	$432x^6 + 216x^5 - 27x^4 - 502x^3 - 87x^2 + 36x + 116$
$\left(\frac{55}{28}, -\frac{43}{28}\right)$	$-496x^6 + 48x^5 - 545x^4 + 90x^3 - 257x^2 + 120x - 80$
$\left(-\frac{1}{28}, \frac{15}{28}\right)$	$314x^6 + 426x^5 + 555x^4 + 140x^3 - 195x^2 - 264x - 176$
$\left(-\frac{23}{15}, \frac{22}{15}\right)$	$-586x^6 + 330x^5 - 512x^4 + 150x^3 - 110x^2 - 24x - 1$
$\left(-\frac{5}{4}, -\frac{1}{4}\right)$	$8x^6 - 168x^5 - 269x^4 + 466x^3 + 451x^2 - 624x - 376$

Table 12. Some points of small height on the surface of Theorem 27 and the corresponding genus-2 curves.

The section P_1 gives a rational curve

$$(e, f) = \left(-\frac{2g^2 + 11}{4g - 1}, \frac{2g^2 - g - 11}{4g - 1} \right).$$

However, the Brauer obstruction does not vanish identically on this locus. The section $2P_1$ gives a rational curve

$$(e, f) = \left(-\frac{2g^2 + 3}{4g}, \frac{2g^2 - 3}{4g} \right)$$

on the surface. Here, the Brauer obstruction does vanish identically, yielding a family of genus-2 curves with real multiplication by $\mathcal{O}_{40}$.

18. Discriminant 41

18.1. *Parametrization.*
We start with an elliptic K3 surface with fibers of type A_5 at $t = 0$ and A_{10} at $t = \infty$, with a section of height $\frac{41}{66} = 4 - \frac{4 \cdot 7}{11} - \frac{5}{6}$.

A Weierstrass equation for this family is given by

$$y^2 = x^3 + (t^2 + 2dft + cf^2)x^2 + 2t^2(dt + cf)x + ct^4,$$

with

$$c = r^2 s^2 \left(16t^2 - 8(4rs - 16s - r)t + (4rs - 16s + r)^2 \right),$$
$$d = rs(4t - 12rs + 16s + r),$$
$$f = (t + 4s)/(4rs).$$

We identify the class of an E_8 fiber, and perform a 3-neighbor step to an elliptic fibration with E_8 and A_7 fibers.
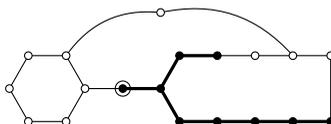
This fibration has a section P of height $\frac{41}{8} = 4 + 2 - \frac{7}{8}$. Next, we take a 2-neighbor step to go to a fibration with E_8 and E_7 fibers.
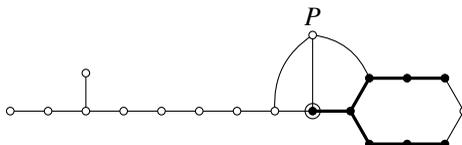
The intersection number of the new fiber F' with the remaining component of the A_7 fiber is 2 and with the section P is 5. Since these number are coprime, the new genus-1 fibration defined by F' has a section.

Reading out the map to $\mathcal{M}_2$ from the $E_8 E_7$ fibration, we obtain the following result.

Theorem 28. *A birational model over $\mathbb{Q}$ for the Hilbert modular surface $Y_-(41)$ as a double cover of $\mathbb{P}^2_{r,s}$ is given by the equation*

$$z^2 = (4s+1)^4 r^4 - 16(8s^2 + 42s - 1)(4s+1)^2 r^3$$
$$+ 32(128s^4 + 4672s^3 + 1976s^2 + 248s + 3)r^2$$
$$- 256(2688s^3 + 872s^2 + 82s - 1)r + 256(16s+1)^3.$$

It is a K3 *surface of Picard number* 19.

18.2. *Analysis.* The branch locus is a rational curve, with a parametrization given by

$$(r, s) = \left(-\frac{4(u-1)(u+1)^3}{(u^2 - u - 1)^2}, \ -\frac{1}{4u^2(u-1)^2} \right).$$

The Hilbert modular surface has a genus-1 fibration to $\mathbb{P}^1_r$, which is in fact an elliptic fibration, since the coefficient of r^4 is a perfect square. Converting to the Jacobian form, we get the Weierstrass equation

$$y^2 = x^3 + (t-1)(t^3 + 23t^2 + 96t - 32)x^2$$
$$+ 16(t-1)(4t^4 + 53t^3 - 217t^2 + 112t - 16)x.$$

This is an elliptic K3 surface, with bad fibers of type I_6 at $t = \infty$, I_4 at $t = 0$, III at $t = 1$, I_3 at $t = -15$, and I_2 at the four roots of $q(t) = 4t^4 + 53t^3 - 217t^2 + 112t - 16$. This quartic $q(t)$ describes a dihedral Galois extension K of $\mathbb{Q}$, quadratic over $\mathbb{Q}(\sqrt{41})$. Thus we get a trivial lattice of rank 17 and discriminant 2304. We also have a 2-torsion point $(0, 0)$ and the two non-torsion sections

$$P_1 = \left(-164(t-1), 4\mu(t-1)(t+15)(5t-6) \right),$$

$$P_2 = \left((5+\mu)(t-1)(8t^2 + 53t + 9t\mu - 185 - 29\mu)/16, \right.$$
$$\left. (5+\mu)(t-1)(t+15)(4t - 11 + \mu)(8t^2 + 53t + 9t\mu - 185 - 29\mu)/64 \right),$$

where $\mu = \sqrt{41}$. The height matrix for P_1 and P_2 is

$$\frac{1}{3} \begin{pmatrix} 4 & -2 \\ -2 & 1 \end{pmatrix}.$$

Therefore the Picard number is at least 19. Counting points modulo 7 and 11 shows that the Picard number must be 19, in agreement with [Oda 1982]. The sections above and the trivial lattice therefore generate a lattice of rank 19 and discriminant 512. We showed that it is 2-saturated, and is thus the full Néron–Severi lattice.

Rational point (r, s)	Sextic polynomial $f_6(x)$ defining the genus-2 curve $y^2 = f_6(x)$
$\left(\frac{52}{3}, -\frac{1}{5}\right)$	$-6x^6 + 3x^5 - 4x^4 + 3x^3 + 20x^2 - 36x + 20$
$\left(\frac{7}{2}, \frac{13}{12}\right)$	$-x^6 - 15x^5 - 65x^4 - 57x^3 + 40x^2 + 6x + 20$
$\left(\frac{56}{9}, -\frac{43}{40}\right)$	$-56x^6 - 42x^5 + 64x^4 - 78x^3 - 29x^2 + 36x - 28$
$\left(\frac{52}{7}, -\frac{2}{3}\right)$	$-24x^6 + 36x^5 - 34x^4 - 51x^3 + 86x^2 - 87x + 18$
$\left(13, -\frac{7}{12}\right)$	$-15x^6 + 33x^5 + 23x^4 + 73x^3 - 72x^2 - 54x - 108$
$\left(\frac{32}{5}, -\frac{47}{48}\right)$	$-18x^6 - 3x^5 + 46x^4 - 111x^3 + 22x^2 + 48x - 84$
$\left(\frac{92}{9}, -\frac{11}{14}\right)$	$-4x^6 + 24x^5 - 17x^4 + 3x^3 - 125x^2 - 72x - 95$
$\left(\frac{60}{13}, 3\right)$	$-10x^6 + 33x^5 + 40x^4 - 111x^3 - 152x^2 + 60x + 140$
$\left(\frac{76}{13}, -\frac{4}{3}\right)$	$-24x^6 - 12x^5 - 50x^4 + 111x^3 + 10x^2 + 129x - 153$
$\left(28, -\frac{23}{24}\right)$	$-46x^6 + 69x^5 - 14x^4 + 169x^3 - 134x^2 - 84x - 72$
$\left(\frac{68}{15}, -\frac{11}{4}\right)$	$48x^6 - 48x^5 - 119x^4 - 84x^3 + 145x^2 + 180x + 100$
$\left(\frac{23}{6}, \frac{21}{4}\right)$	$168x^5 + 85x^4 + 70x^3 + 229x^2 + 24x - 72$
$\left(\frac{40}{3}, -\frac{55}{56}\right)$	$-39x^6 + 36x^5 - 116x^4 + 186x^3 - 107x^2 + 240x - 200$
$\left(\frac{52}{25}, -\frac{1}{24}\right)$	$-112x^6 - 264x^5 + 25x^4 + 240x^3 - 125x^2 - 114x + 62$
$\left(\frac{4}{13}, -\frac{11}{96}\right)$	$16x^6 + 24x^5 - 223x^4 + 274x^3 - 7x^2 + 216x - 120$
$\left(\frac{27}{2}, \frac{11}{76}\right)$	$12x^6 - 132x^5 - 219x^4 + 286x^3 + 201x^2 - 264x - 56$

Table 13. Some points of small height on the surface of Theorem 28 and the corresponding genus-2 curves.

18.3. *Examples.* Table 13 lists some points of small height and their genus-2 curves.

Next, we describe some curves which are a source of many rational points. The specialization $s = -4$ gives a curve of genus 0, with a parametrization $r = -2(m^2 + 343)/(9(m - 13))$. The specialization $r = \frac{108}{25}$ also gives a rational curve, parametrized by $s = -(4m - 169)(4m + 169)/(16(108m - 10813))$. The Brauer obstruction vanishes on both these loci, giving families of curves whose Jacobians have real multiplication by $\mathcal{O}_{41}$.

Finally, sections of the elliptic fibration also give rational curves on the surface. For instance, the section P_0 is parametrized by

$$r = \frac{4(256s^3 - 48s^2 - 16s - 1)}{(4s + 1)^2(16s - 7)}.$$

The Brauer obstruction vanishes here as well.

19. Discriminant 44

19.1. *Parametrization.* We start with an elliptic K3 surface with fibers of type A_{10} at $t = 0$ and D_6 at $t = \infty$. This has Néron–Severi lattice of discriminant $11 \cdot 4 = 44$
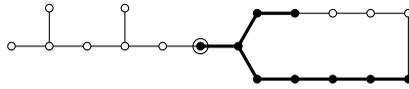
and rank $2 + 10 + 6 = 18$. The Weierstrass equation for this universal family can be written as

$$y^2 = x^3 + ax^2 + 2bt^4 x + ct^8,$$

with

$$a = s(r^2 s^2 - s^2 + 2s + 2)t^3 - s(2r^2 s - 3s + 2)t^2 + s(r^2 - 3)t + 1,$$
$$b = s^2 \big((2r^2 s^2 - 2s^2 + 4s + 1)/2t^2 - (r^2 s - 2s + 1)t - 1\big),$$
$$c = s^4 ((r^2 s - s + 2)t + 1).$$

We identify the class of an E_8 fiber and move to this fibration via a 3-neighbor step.

The new elliptic fibration has E_8, D_6 and A_1 fibers, and a section P of height $\frac{11}{2} = 4 + 2 \cdot 1 - \frac{1}{2}$. We identify an E_7 fiber F' below. Note that $P \cdot F' = 5$, while the excluded component of the D_6 fiber intersects F' in 2. Since 2 and 5 are coprime, we see that the fibration defined by F' has a section. We move to it by a 2-neighbor step.
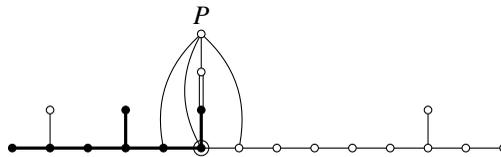
Calculating the Igusa–Clebsch invariants and following the rest of the algorithm in Section 4, we obtain the following result.

Theorem 29. *A birational model over $\mathbb{Q}$ for the Hilbert modular surface $Y_-(44)$ as a double cover of $\mathbb{P}^2_{r,s}$ is given by the equation*

$$z^2 = (rs + s - 1)(rs - s + 1)(r^6 s^2 - r^4 s^2 + 18r^2 s - 16s + 27).$$

It is an honestly elliptic surface, with arithmetic genus 2 and Picard number 29.

19.2. *Analysis.* The extra involution is $\iota : (r, s) \mapsto (-r, s)$. The branch locus has three components. The two simpler components $rs \pm (s - 1) = 0$ are obviously rational curves, and a simple calculation shows that they correspond to elliptic K3 surfaces for which the D_6 fiber gets promoted to an E_7 fiber. The more complicated component of the branch locus, corresponding to elliptic fibrations with an extra I_2 fiber, is also a rational curve; a parametrization is given by

$$(r, s) = \left(\frac{4m}{m^2 + 3}, -\frac{(m^2 + 3)^3}{16(m^2 - 1)} \right).$$

The right-hand side of the equation defining the Hilbert modular surface is quartic in s, whence the surface $Y_-(44)$ is elliptically fibered over $\mathbb{P}^1_r$. The two linear factors (or the fact that the coefficient of s^4 is a square) imply that there are sections, so we may convert to the Jacobian form:

$$y^2 = x^3 + 2(r^6 - r^4 - 9r^2 + 11)x^2 + (r^2 - 1)^3(r^6 + r^4 + 91r^2 - 121)x.$$

This is an honestly elliptic surface, with $\chi = 3$. It has reducible fibers of type I_2 at $r = 0$, I_6 at $r = \pm 1$, I_4 at $r = \infty$, I_3 at $r = \pm\frac{2}{\sqrt{3}}$, and type I_2 at the six roots of $(r^3 - 3r^2 + 5r + 11)(r^3 + 3r^2 + 5r - 11)$ (both factors generate the cubic field k_{-44} of discriminant -44). The trivial lattice has rank 26, leaving room for Mordell–Weil rank at most 4. We find the following sections, of which P_0 is 2-torsion, while P_1, P_2 and P_3 are linearly independent non-torsion sections, orthogonal with respect to the height pairing and of heights $\frac{7}{6}$, $\frac{3}{2}$ and $\frac{11}{6}$ respectively:

$P_0 = (0, 0),$
$P_1 = \left(11(r^2 - 1), 4\sqrt{11}\, r(r^2 - 1)^3(3r^2 - 4)\right),$
$P_2 = \left(-(r + 1)^3(r^3 - 3r^2 + 5r + 11), 6\sqrt{-3}\, r(r + 1)^3(r^3 - 3r^2 + 5r + 11)\right),$
$P_3 = \left((r - 1)(r + 1)^2(r^3 - 3r^2 + 5r + 11), 2r^3(r - 1)(r + 1)^2(r^3 - 3r^2 + 5r + 11)\right).$

Therefore, the Picard number is at least 29. Analysis of the associated quotient elliptic K3 surface and its twist (see below) shows that the Mordell–Weil rank is exactly 3 and therefore the Picard number is exactly 29. The sections above together with the trivial lattice generate a lattice of discriminant $133056 = 2^6 \cdot 3^3 \cdot 7 \cdot 11$. We checked that it is 2- and 3-saturated, and so it is the entire Néron–Severi lattice. Therefore these sections generate the Mordell–Weil group.

We next analyze the quotient of $Y_-(44)$ by the involution ι. Taking $t = r^2$, we find the equation

$$z^2 = s^4 t^4 - s^2(2s^2 - 2s + 1)t^3 + s^2(s^2 + 16s + 1)t^2$$
$$- s(2s - 3)(17s - 6)t + (s - 1)^2(16s - 27).$$

This has an elliptic fibration over $\mathbb{P}^1_s$, and since the coefficient of t^4 is a square, we may convert to the Jacobian, which is

$$y^2 = x^3 + s^2(s + 2)(s + 8)x^2 + 2s^3(6s^2 + 47s + 9)x + s^4(36s^2 + 268s - 27).$$

This is an elliptic K3 surface, with reducible fibers of type E_6 at $s = 0$, I_7 at $s = \infty$, I_3 at $s = -\frac{27}{4}$, and I_2 at the roots of $2s^3 + 14s^2 - 6s + 1$, which generates the cubic field k_{-44}. The trivial lattice has rank 19. We find a non-torsion section

$$P = (1 - 4s, 2s^3 + 14s^2 - 6s + 1)$$

of height $4 - \frac{12}{7} - \frac{3}{2} = \frac{11}{14}$. It is easy to show that P generates the Mordell–Weil group: the configuration of reducible fibers does not allow for either nontrivial torsion or a section of height $11/14n^2$ for any integer $n > 1$. Therefore the K3 surface is singular, with Néron–Severi lattice of discriminant $-396 = -4 \cdot 9 \cdot 11$.

We may also analyze the quotient by considering it as an elliptic surface over $\mathbb{P}^1_t$, and since the coefficient of s^4 is $t^2(t-1)^2$, which is a square, there is a section. Converting to the Jacobian, we get the elliptic K3 surface

$$y^2 = x^3 + 2(t^3 - t^2 - 9t + 11)x^2 + (t-1)^3(t^3 + t^2 + 91t - 121)x$$

which is also obtained by replacing r^2 by t in the Weierstrass equation of $Y_-(44)$. This elliptic fibration has bad fibers of type I_6^*, I_6 and I_3 at $t = \infty$, 1 and $\frac{4}{3}$ respectively, and of type I_2 at the roots of $t^3 + t^2 + 91t - 121$, which generates k_{-44}. Therefore, the root lattice has rank 18. We find the sections

$P_0 = (0, 0)$,

$P_1 = \left((1-t)(t-3\sqrt{-3})^2, 2(3-\sqrt{-3})(t-1)(t-3\sqrt{-3})(9t-6-2\sqrt{-3})/3\right)$

$P_2 = \left((1-t)(t+3\sqrt{-3})^2, 2(3+\sqrt{-3})(t-1)(t+3\sqrt{-3})(9t-6+2\sqrt{-3})/3\right)$,

with P_0 being 2-torsion, and P_1 and P_2 having height pairing matrix

$$\begin{pmatrix} \frac{5}{3} & \frac{1}{6} \\ \frac{1}{6} & \frac{5}{3} \end{pmatrix}.$$

These sections, along with the trivial lattice, generate a lattice of rank 20 and discriminant -396, which must therefore be the entire Néron–Severi lattice. The Mordell–Weil rank of this elliptic surface is 2.

Finally, we consider the quadratic twist of the above elliptic K3 surface, which is the quotient of $Y_-(44)$ by the involution $\iota' : (r, s, z) \mapsto (-r, s, -z)$. It is given by the equation

$$y^2 = x^3 + 2t(t^3 - t^2 - 9t + 11)x^2 + t^2(t-1)^3(t^3 + t^2 + 91t - 121)x.$$

This is an elliptic K3 surface with reducible fibers of type I_1^*, I_6, I_3 and I_2 at $t = 0$, 1, $\frac{4}{3}$ and ∞ respectively, and I_2 at the roots of $t^3 + t^2 + 91t - 121$. The trivial lattice has rank 18. We find the sections

$$P_0 = (0, 0),$$
$$P_1 = \left(11t(t-1)^3, 4\sqrt{11}t^2(t-1)^3(3t-4)\right),$$

the first being 2-torsion, and the second of height $\frac{7}{12}$. The Picard number is therefore at least 19. Counting points modulo 5 and 7 shows that it is exactly 19; therefore the Mordell–Weil rank is exactly 1. These sections and the trivial lattice span

a sublattice of discriminant 168 of the Néron–Severi lattice. This sublattice is 2-saturated, since the configuration of fibers does not allow for a section of height $\frac{7}{48}$, and we can easily check that the elliptic surface does not have 4-torsion or other 2-torsion sections. Therefore, we have the entire Néron–Severi lattice, and P_0 and P_1 generate the Mordell–Weil group.

The calculation of the Mordell–Weil ranks of the quotient elliptic surface and its quadratic twist allows us to conclude that the Mordell–Weil rank of the original (honestly) elliptic surface is $1 + 2 = 3$.

19.3. *Examples.* Table 14 lists some points of small height and their genus-2 curves.

The specializations $r = \pm 1$ give rational curves on the surface, but points on these correspond to decomposable abelian surfaces, which therefore have an endomorphism ring strictly larger than $\mathcal{O}_{44}$. The section P_0 is a rational curve, given by $s = (r^4 + 27)/(2(r^2 - 1)(r^2 - 8))$. However, the Brauer obstruction does not vanish identically on it.

(r, s)	Sextic polynomial $f_6(x)$ defining the genus-2 curve $y^2 = f_6(x)$
$\left(-2, -\frac{7}{6}\right)$	$101x^6 - 60x^5 + 2x^4 + 92x^2 + 48x + 24$
$\left(2, -\frac{7}{6}\right)$	$15x^6 - 168x^5 + 170x^4 - 112x^3 + 20x^2 - 8$
$\left(4, -\frac{7}{15}\right)$	$-24x^6 + 48x^5 + 52x^4 + 144x^3 + 238x^2 + 588x - 161$
$\left(-4, -\frac{7}{15}\right)$	$56x^6 + 196x^4 - 320x^3 + 250x^2 - 480x + 723$
$\left(-5, -\frac{13}{12}\right)$	$-144x^6 + 120x^5 + 265x^4 + 700x^3 - 425x^2 - 750x - 1750$
$\left(2, \frac{7}{12}\right)$	$696x^6 - 2112x^5 + 7492x^4 - 7032x^3 + 10234x^2 - 756x + 5103$
$\left(5, -\frac{13}{12}\right)$	$12x^6 - 60x^5 - 145x^4 + 400x^3 - 1225x^2 - 1500x + 11500$
$\left(2, \frac{13}{36}\right)$	$-5193x^6 - 5124x^5 - 16906x^4 - 11576x^3 - 17212x^2 - 6240x - 5304$
$\left(-\frac{3}{4}, \frac{36}{7}\right)$	$-4744x^6 - 15552x^5 + 7596x^4 + 42048x^3 - 20310x^2 - 32112x + 33553$
$\left(-2, \frac{13}{36}\right)$	$-18261x^6 + 13668x^5 + 65210x^4 - 41512x^3 - 74284x^2 + 18816x + 24696$
$\left(\frac{3}{4}, \frac{36}{7}\right)$	$-6504x^6 + 22608x^5 + 28428x^4 - 94288x^3 - 66510x^2 + 103092x + 73009$
$\left(-2, \frac{7}{12}\right)$	$25389x^6 - 97062x^5 - 511x^4 + 240860x^3 - 5989x^2 - 127758x - 83849$
$\left(-5, -\frac{9}{32}\right)$	$-691156x^6 + 20220x^5 - 232521x^4 + 19406x^3 - 22521x^2 + 2484x - 564$
$\left(2, -\frac{61}{42}\right)$	$-629624x^6 + 272400x^5 - 383596x^4 - 704000x^3 - 60778x^2$ $- 194100x - 32193$
$\left(-2, -\frac{61}{42}\right)$	$-550872x^6 + 1549296x^5 - 1810124x^4 - 2005984x^3$ $+ 3719134x^2 - 1321788x - 4862401$
$\left(5, -\frac{9}{32}\right)$	$1781676x^6 - 5240052x^5 + 5462991x^4 - 5705734x^3$ $+ 1769571x^2 + 1002576x - 1011776$

Table 14. Some rational points (r, s) of small height on the surface of Theorem 29 and the corresponding genus-2 curves.

20. Discriminant 53

20.1. *Parametrization.* We start with an elliptic K3 surface with A_8, A_6 and A_1 fibers, and a section of height $\frac{53}{126} = 4 - \frac{1}{2} - \frac{6}{7} - \frac{20}{9}$. A Weierstrass equation for this family is given by
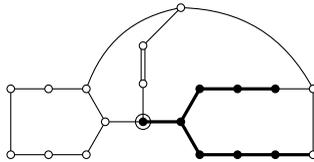
$$y^2 = x^3 + ax^2 + 2bt(t-h)x + ct^2(t-h)^2,$$

with

$$a = g^2t^4 + (4(h+1)^2 - 2g)t^3 + (4h^2 + 4gh + 6g - 3)t^2$$
$$+2(8h^2 - 4gh + 8h + 1)t + (2h+1)^2,$$
$$b = -4(h-g+1)\big(g(2h+1)t^2 + (6h^2 - 2gh + 6h + 1)t + (2h+1)^2\big),$$
$$c = 16(h-g+1)^2(2h+1)^2.$$

To transform to a fibration with E_8 and E_7 fibers, we first identify an E_7 fiber, and move to the associated elliptic fibration via a 2-neighbor step.

The resulting elliptic fibration has E_7 and A_8 fibers, and a section P of height $\frac{53}{18} = 4 + 2 \cdot 1 - \frac{3}{2} - 4 \cdot \frac{5}{9}$. We identify a fiber F of type E_8 and perform a 3-neighbor step to move to the associated elliptic fibration. Note that $P \cdot F = 4$, while the remaining component of the A_8 fiber intersects F with multiplicity 3. Therefore the new elliptic fibration has a section.
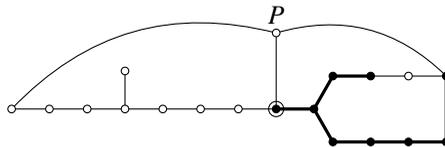
The new elliptic fibration has the requisite E_8 and E_7 fibers, and therefore we may read out the Igusa–Clebsch invariants, and describe the branch locus, which corresponds to elliptic K3 surfaces having an extra I_2 fiber.

Theorem 30. *A birational model over $\mathbb{Q}$ for the Hilbert modular surface $Y_-(53)$ as a double cover of $\mathbb{P}^2_{g,h}$ is given by the equation*

$$z^2 = -27h^4g^4 - 2h^3(13h^2 + 9h + 9)g^3$$
$$- (11h^6 + 138h^5 + 383h^4 + 506h^3 + 353h^2 + 120h + 16)g^2$$
$$-2(h+1)^2(52h^4 + 99h^3 + 65h^2 + 19h + 2)g - (h+1)^4(44h^3 + 76h^2 + 40h + 7).$$

It is an honestly elliptic surface, *with arithmetic genus* 2 *and Picard number* 28.

20.2. Analysis. The branch locus is a curve of genus 1, and the change of coordinates

$$g = -\frac{(x^2 - x + 1)(x^2 + 3x + 3)}{(x + 1)(2x + 1)y + x^4 + 3x^3 + 5x^2 + 3},$$

$$h = \frac{(x^5 - x^4 + 4x^3 - 4x^2 + x + 1)y + x^2(x^6 - x^5 + 2x^4 + 2x^3 - x + 1)}{(x^2 - x + 1)^2((x + 1)(2x + 1)y + x^4 + 3x^3 + 5x^2 + 3)}$$

transforms it to the elliptic curve $y^2 + xy + y = x^3 - x^2$ of conductor 53, which is isomorphic to $X_0(53)/\langle w \rangle$, where w is the Atkin–Lehner involution.

This surface has a genus-1 fibration over $\mathbb{P}^1_h$, making it honestly elliptic with $\chi = 3$. We could find no sections over $\mathbb{Q}$, although there certainly exist sections over $\overline{\mathbb{Q}}$, since the coefficient of g^4 is a square in $\mathbb{Q}(\sqrt{-3})$. The Jacobian of this fibration has the following equation (after making the linear fractional transformation $h = -t/(t + 1)$ on the base, and some Weierstrass transformations):

$$y^2 = x^3 + (t^6 - 18t^5 + 55t^4 + 106t^3 - 179t^2 + 24t - 16)x^2$$
$$-8(t - 1)t^2(37t^5 - 471t^4 - 140t^3 + 1121t^2 - 309t + 248)x$$
$$-16(t - 1)^2 t^4(196t^5 - 2797t^4 + 2712t^3 + 8606t^2 - 3084t + 3115).$$

This surface has reducible fibers of type I_7, I_4 and I_3 at $t = \infty, 0, 1$ respectively, type I_2 at the roots of $7t^3 - 99t^2 + 104t - 32$ (which generates the cubic field of discriminant $-2^2 \cdot 53$), and I_3 at the roots of $t^5 - 11t^4 - 11t^3 + 6t^2 - 3t - 9$ (which generates the quintic field of discriminant $-3^2 \cdot 53^2$, and whose roots generate a dihedral D_{10} extension unramified over its quadratic subfield $\mathbb{Q}(\sqrt{-3 \cdot 53})$). The trivial lattice has rank 26, leaving room for Mordell–Weil rank at most 4. We find the sections

$$P_1 = \left(-4(7t^6 - 106t^5 + 189t^4 + 202t^3 - 778t^2 + 342t - 216)/53, \right.$$
$$\left. 4(5t - 3)(7t^3 - 99t^2 + 104t - 32)(t^5 - 11t^4 - 11t^3 + 6t^2 - 3t - 9)/(53\sqrt{53})\right)$$
$$P_2 = \left(-4(49t^6 - 63t^5 + 99t^4 + 162t^3 - 351t^2 + 162t - 108)/27, \right.$$
$$(637t^8 - 378t^7 - 1485t^6 + 3186t^5 - 1755t^4 - 1782t^3 + 3942t^2 - 243t - 972)$$
$$\times 4t/(81\sqrt{-3})\big)$$

of heights $\frac{7}{6}$ and $\frac{21}{4}$ respectively, orthogonal with respect to the height pairing. Therefore, the Mordell–Weil rank is least 2. By Oda's calculations [1982], we deduce that the Mordell–Weil rank is exactly 2. The sections P_1 and P_2 and the trivial lattice span a lattice of discriminant $1000188 = 2^2 \cdot 3^6 \cdot 7^3$. Checking that it is saturated at 2, 3 and 7, we deduce that it must be the full Néron–Severi lattice.

(g, h)	Sextic polynomial $f_6(x)$ defining the genus-2 curve $y^2 = f_6(x)$
$\left(\frac{11}{152}, -\frac{16}{19}\right)$	$-2332x^6 - 902x^5 - 5060x^4 - 17111x^3 - 5995x^2 - 17545x - 27951$
$\left(\frac{8}{21}, -\frac{2}{3}\right)$	$-8788x^6 + 34200x^5 - 22425x^4 - 11907x^3 - 16230x^2 - 35604x + 34024$
$\left(\frac{72}{49}, -\frac{13}{7}\right)$	$816x^6 - 1944x^5 - 13459x^4 + 24712x^3 + 37733x^2 + 7596x - 2300$
$\left(\frac{75}{26}, -\frac{19}{4}\right)$	$-106605x^6 - 62661x^5 + 467345x^4 + 193313x^3 - 691816x^2$ $- 149592x + 346546$
$\left(\frac{12}{5}, -10\right)$	$139968x^6 + 471744x^5 - 1301409x^4 - 77363x^3 + 671633x^2$ $+ 236496x + 18756$
$\left(-\frac{72}{31}, -4\right)$	$-138482x^6 + 1643417x^5 + 2645029x^4 - 1507309x^3 - 2429567x^2$ $+ 1188320x + 36288$
$\left(\frac{2}{135}, -\frac{10}{11}\right)$	$2175200x^6 - 2750760x^5 + 2725545x^4 + 7678368x^3 - 5205621x^2$ $+ 3781674x + 9014158$
$\left(\frac{16}{63}, -5\right)$	$3829988x^6 + 11621820x^5 - 19617225x^4 - 25097450x^3 + 29201451x^2$ $+ 14626080x - 14560512$
$\left(\frac{18}{103}, -\frac{8}{11}\right)$	$-4788022x^6 - 21151494x^5 - 18288935x^4 - 20340320x^3 - 61042325x^2$ $+ 10128456x - 40124160$
$\left(-\frac{39}{76}, -\frac{29}{16}\right)$	$394632000x^6 - 1964113200x^5 - 1523778060x^4 + 4757784967x^3$ $+ 148400811x^2 - 3811137819x + 540964447$
$\left(\frac{55}{117}, -\frac{79}{144}\right)$	$-5511986931x^6 + 20881501795x^5 + 17115817125x^4 + 19864594645x^3$ $+ 1353729618x^2 - 16117938900x + 5833685448$
$\left(\frac{49}{135}, -\frac{61}{75}\right)$	$-26148549648x^6 - 278797809744x^5 - 748507062651x^4 + 329438683288x^3$ $+ 1420002530997x^2 - 1751808944796x + 1934174962804$
$\left(-\frac{50}{117}, -\frac{13}{9}\right)$	$-159682912000x^6 - 1077016472800x^5 - 2039981245815x^4$ $- 762577047304x^3 + 6811301171385x^2 - 4055008902300x + 449504680500$
$\left(\frac{81}{91}, -\frac{13}{7}\right)$	$134236157214x^6 + 962817170858x^5 - 12198892111873x^4 + 23659009829816x^3$ $+ 9649525790385x^2 - 12776814846900x - 8264106337500$
$\left(\frac{59}{153}, -\frac{17}{27}\right)$	$-687158622928816x^6 + 23483931596064x^5 - 14038441316573x^4$ $- 893569395800x^3 - 20141231607x^2 - 200112822x - 748062$

Table 15. Some rational points (g, h) of small height on the surface of Theorem 30 and the corresponding genus-2 curves.

20.3. *Examples.* Table 15 lists some points of small height and their genus-2 curves.

We could not find any curves of genus 0 which were not contained in the "bad locus" where the abelian surfaces have a strictly larger ring of endomorphisms.

21. Discriminant 56

21.1. *Parametrization.* We start with a K3 elliptic surface with D_6, A_8 and A_1 fibers, and a section P of height $\frac{56}{72} = \frac{7}{9} = 4 - 1 - \frac{20}{9}$. The Weierstrass equation of this family is

$$y^2 = x^3 + ax^2 + 2bt^2(\lambda t - \mu)x + ct^4(\lambda t - \mu)^2,$$

with

$$\lambda = (2h - g^2 + 1), \quad \mu = -2h,$$
$$c = -(g^2 - 1)^2\big(4(g^2 - 1)t - (h + 2)^2\big),$$
$$b = (g^2 - 1)\big(2(g^2 - 1)t^2 - (h^2 + 4h - 4g^2 + 8)t - (h + 2)^2\big),$$
$$a = (g^2 - 1)^2 t^3 + (h + 2)(h - 2g^2 + 4)t^2 + 2(h^2 + 4h - 2g^2 + 6)t + (h + 2)^2.$$

To find an $E_8 E_7$ fibration on such a K3 surface, we first identify the class of an E_7 fiber below.

This converts it to an $A_8 E_7$ fibration. Note that this fibration has a section, because the section P intersects F' in 3, whereas (for instance) the non-identity component of the A_1 fiber intersects F' in 2, and these two numbers are coprime.

The new fibration has a section of height $\frac{56}{18} = \frac{28}{9} = 4 - \frac{8}{9}$, which intersects the identity component of the E_7 fiber and component 1 of the A_8 fiber. We then do a 3-neighbor step to get an $E_8 E_7$ fibration.

The new fiber F'' satisfies $P' \cdot F'' = 2$, while the excluded component of the A_8 fiber intersects F'' in 3. Since these are coprime, the fibration defined by F'' has a section.

Now we can read out the Igusa–Clebsch invariants, and describe the branch locus of $Y_-(56)$ as a double over of $\mathbb{P}^2_{g,h}$.

Theorem 31. *A birational model over $\mathbb{Q}$ for the Hilbert modular surface $Y_-(56)$ as a double cover of $\mathbb{P}^2_{g,h}$ is given by the equation*

$$z^2 = (2h - g^2 + 1)\big(2h^5 + 27g^2 h^4 - 11h^4 + 72g^2 h^3 - 24h^3 - 40g^2 h^2$$
$$+ 104h^2 - 160g^2 h + 192h + 64g^4 - 144g^2 + 80\big).$$

It is a surface of general type.

21.2. *Analysis.* The extra involution is $g \mapsto -g$. The branch locus has two components. Points on the simpler component $2h - g^2 + 1 = 0$ (which is clearly a rational curve) correspond to elliptic K3 surfaces for which the A_1 and D_6 fibers merge and get promoted to a D_8 fiber. The other component corresponds to elliptic K3 surfaces with an extra I_2 fiber. It is also of genus 0, and a parametrization is given by

$$(g, h) = \left(\frac{s(s^4 + 22s^2 - 7)}{(3s^2 + 1)^2}, -\frac{(s^2 - 1)(s^2 - 5)}{2(3s^2 + 1)} \right).$$

The Hilbert modular surface $Y_-(56)$ is of general type.

We now analyze the quotient of the Hilbert modular surface by the involution $(g, h, z) \mapsto (-g, h, z)$. Setting $f = g^2$, the right-hand side becomes a cubic in f. After some elementary Weierstrass transformations, we get the equation

$$y^2 = x^3 - (27h^4 + 72h^3 - 40h^2 + 96h - 16)x^2 + 512h^3(7h^2 + 20h - 4)x.$$

This is an elliptic K3 surface, with reducible fibers of type I_6, I_6, I_4, I_3 at $h = 0, \infty, -2, \frac{2}{9}$ respectively, and I_2 fibers at $h = (-10 \pm 8\sqrt{2})/7$. The trivial lattice has rank 19 and discriminant 1728. There is an obvious 2-torsion section $P_0 = (0, 0)$, and we find a non-torsion section

$$P_1 = (128h, 128h(h + 2)^2)$$

of height $\frac{2}{3}$. We checked that the group generated by P_0 and P_1 is saturated at 2 and 3. Therefore, this is a singular K3 surface, with Néron–Severi lattice of rank 20 and discriminant -288.

Next, we analyze the twist of the elliptic K3 surface above, obtained by substituting $z = wg$ in the equation of the Hilbert modular surface, and then setting $f = g^2$ (it is the quotient of $Y_-(56)$ by the involution $(g, h, z) \mapsto (-g, h, -z)$). This twist is an honestly elliptic surface, with $\chi = 3$. After some simple algebra, the Weierstrass equation can be written as

$$y^2 = x^3 + (58h^5 + 149h^4 - 56h^3 - 152h^2 - 64h + 16)x^2$$
$$+ 8h^3(2h + 5)(h^2 - 4h - 4)^2(7h^2 + 20h - 4)x.$$

It has reducible fibers of type $I_0^*, I_6, I_4, I_3, I_2, I_2$ at $h = \infty, 0, -2, \frac{2}{9}, -\frac{1}{2}, -\frac{5}{2}$ respectively, I_4 fibers at $h = (-10 \pm 8\sqrt{2})/7$ and I_2 fibers at $h = 2 \pm 2\sqrt{2}$. The trivial lattice has rank 26. In addition to the 2-torsion section $P_0 = (0, 0)$, we find the sections

$$P_1 = \left(-56h^3(h^2 - 4h - 4), 16\sqrt{14}h^3(2h + 1)(9h - 2)(h^2 - 4h - 4) \right),$$
$$P_2 = \left(-8h^3(7h^2 + 20h - 4), 64\sqrt{-1}h^3(2h + 1)(7h^2 + 20h - 4) \right),$$
$$P_3 = \left(4h^2(7h^2 + 20h - 4), 4h^2(h + 2)^2(2h + 1)(7h^2 + 20h - 4) \right)$$

of heights $\frac{5}{6}$, 2 and $\frac{7}{6}$ respectively, orthogonal with respect to the height pairing. On the other hand, counting points on the reductions modulo 11 and 29 shows that the Picard number is at most 29. Therefore, it is exactly 29. The lattice spanned by these sections and the trivial lattice has discriminant $35840 = 2^{10} \cdot 5 \cdot 7$. We checked that it is 2-saturated, and therefore it must equal the entire Néron–Severi lattice.

21.3. *Examples.* Table 16 lists some points of small height and their genus-2 curves.

Next, we analyze curves of low genus on the Hilbert modular surface. The specialization $h = \frac{2}{9}$ gives a rational curve, parametrized by $g = (m^2 - 4m - 9)/(m^2 + 9)$. The Brauer obstruction vanishes identically for rational points on this curve, giving a 1-parameter family of genus-2 curves whose Jacobians have real multiplication by $\mathcal{O}_{56}$.

The specializations $h = -\frac{1}{2}$ and $h = -\frac{5}{2}$ give genus-1 curves with rational points, both of whose Jacobians have rank 1. The Brauer obstruction does not vanish identically on either of these loci.

We also obtain some genus-1 curves by pulling back some sections from the quotient K3 surface. For instance, the section $P_0 + P_1$ gives the genus-1 curve $g^2 = -(7h^4 + 20h^3 - 4h^2 - 32h - 16)/16$ which has rational points (such as

(g, h)	Sextic polynomial $f_6(x)$ defining the genus-2 curve $y^2 = f_6(x)$
$\left(-\frac{79}{61}, \frac{28}{61}\right)$	$-2000x^6 + 2040x^5 - 565x^4 + 628x^3 - 349x^2 - 36x - 68$
$\left(\frac{23}{19}, \frac{24}{95}\right)$	$480x^6 + 1200x^5 + 2657x^4 + 1264x^3 + 497x^2 - 2220x + 660$
$\left(\frac{2}{13}, -\frac{6}{13}\right)$	$-600x^6 - 360x^5 + 2660x^4 + 256x^3 - 2698x^2 - 222x + 639$
$\left(-\frac{2}{13}, -\frac{6}{13}\right)$	$1096x^6 - 24x^5 - 3388x^4 + 608x^3 + 2750x^2 - 930x - 225$
$\left(\frac{79}{61}, \frac{28}{61}\right)$	$1350x^6 + 270x^5 + 3375x^4 - 3944x^3 + 1669x^2 - 5328x + 3392$
$\left(-\frac{3}{7}, -\frac{8}{7}\right)$	$-1340x^6 + 5900x^5 - 2227x^4 + 5096x^3 + 2707x^2 + 10x + 1950$
$\left(\frac{3}{7}, -\frac{8}{7}\right)$	$1440x^6 - 4720x^5 - 13227x^4 + 20x^3 + 7389x^2 - 1080x - 432$
$\left(-\frac{1}{7}, \frac{24}{7}\right)$	$-12600x^6 - 3192x^5 - 16975x^4 - 4442x^3 + 5717x^2 - 516x + 4$
$\left(\frac{1}{91}, -\frac{40}{91}\right)$	$3740x^6 - 6420x^5 - 11789x^4 + 18160x^3 + 7315x^2 - 13356x + 2268$
$\left(-\frac{11}{7}, \frac{9}{7}\right)$	$35220x^6 + 10548x^5 + 43345x^4 - 10038x^3 + 3313x^2 - 228x + 52$
$\left(-\frac{23}{19}, \frac{24}{95}\right)$	$47824x^6 + 45048x^5 + 13973x^4 - 11016x^3 + 9341x^2 - 2040x + 400$
$\left(\frac{2}{3}, \frac{2}{9}\right)$	$-6883x^6 + 10038x^5 + 62514x^4 + 31744x^3 - 21780x^2 + 3720x - 200$
$\left(\frac{37}{31}, \frac{9}{31}\right)$	$-1548x^6 - 7732x^5 - 33547x^4 - 51202x^3 - 71163x^2 + 65988x - 11772$
$\left(-\frac{4}{17}, -\frac{3}{8}\right)$	$-316x^6 + 4764x^5 + 21121x^4 - 11666x^3 - 75071x^2 + 20364x + 49716$
$\left(\frac{11}{7}, \frac{9}{7}\right)$	$25092x^6 + 70500x^5 + 71881x^4 - 29834x^3 - 80543x^2 - 25908x + 38700$
$\left(\frac{55}{13}, \frac{28}{3}\right)$	$-94x^6 - 114x^5 - 2497x^4 - 660x^3 - 29263x^2 - 10920x - 170352$

Table 16. Some rational points (g, h) of small height on the surface of Theorem 31 and the corresponding genus-2 curves.

$(h, g) = (1, \pm 1)$), with a Jacobian of conductor $2^4\, 211$ and Mordell–Weil group $\cong \mathbb{Z}^2$. The section $2P_1$ gives the genus-1 curve $g^2 = -(49h^4 - 112h^3 + 64h^2 - 32h - 16)/16$ which also has rational points $(h, g) = (1, \pm 1)$, with Jacobian of conductor $2^6\, 7 \cdot 23$ and Mordell–Weil group $\cong (\mathbb{Z}/2\mathbb{Z}) \oplus \mathbb{Z}$. The Brauer obstruction does not vanish identically on either of these loci.

22. Discriminant 57

22.1. *Parametrization.* We start with an elliptic K3 surface with fibers of type E_6, A_7 and A_2 at $t = \infty, 0, 1$ respectively, and a section of height $\frac{57}{72} = \frac{19}{24} = 4 - \frac{4}{3} - \frac{3 \cdot 5}{8}$.

The Weierstrass equation for this family is

$$y^2 = x^3 + ax^2 + 2bt^2(t - 1)x + ct^4(t - 1)^2,$$

with

$$a = t(t - 1)\big((g^2 - \tfrac{1}{4})(h^2 - 3) + 2gh\big) + \big((g^2 + \tfrac{1}{4})h - g\big)^2 t^2 - t + 1,$$

$$b = -\big(g^2 - \tfrac{1}{4}\big)^2 (h^2 - 1)$$
$$\big((1 - t) - \big((g^2 - \tfrac{1}{4})(h^2 - 2) + 2gh\big)t(1 - t) - \big(g - \tfrac{1}{2}h\big)\big((g^2 + \tfrac{1}{4})h - g\big)t^2\big),$$

$$c = \big(g^2 - \tfrac{1}{4}\big)^4 (h^2 - 1)^2 \big((1 - t) + \big(g - \tfrac{1}{2}h\big)^2 t^2 + t(1 - t)\big(\big(g - \tfrac{1}{2}h\big)^2 - \big(gh + \tfrac{1}{2}\big)^2\big)\big).$$

We identify an E_8 fiber below, and the resulting 3-neighbor step takes us to an elliptic fibration with E_8 and A_7 fibers.
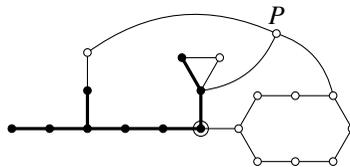
Since $P \cdot F' = 2$ for the new fiber F', while the intersection number of the remaining component of the E_6 fiber with F' is 3, we deduce that the new fibration has a section.

The new fibration has a section of height $\frac{57}{8} = 4 + 2 \cdot 2 - \frac{1 \cdot 7}{8}$. Now we can identify an E_7 fiber F'' and move to the $E_8 E_7$ fibration by a 2-neighbor step. Note that since $Q \cdot F'' = 7$, while the remaining component of the A_7 fiber intersects F'' in 2, the new fibration will have a section.
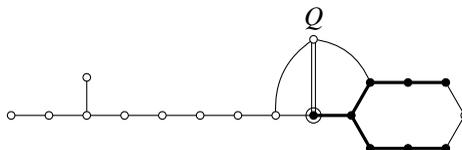
Now we can read out the Igusa–Clebsch invariants and compute the branch locus, which is the subfamily with an extra I_2 fiber.

Theorem 32. *A birational model over $\mathbb{Q}$ for the Hilbert modular surface $Y_-(57)$ as a double cover of $\mathbb{P}^2_{g,h}$ is given by the equation*

$$z^2 = (256g^6 - 176g^4 + 40g^2 - 3)h^4 + (2176g^5 - 960g^3 + 104g)h^3$$
$$+(4320g^4 - 688g^2 - 34)h^2 + (-3456g^5 + 576g^3 + 328g)h - 2160g^4 - 648g^2 + 361.$$

It is an honestly elliptic surface, with arithmetic genus 2 and Picard number 29.

22.2. *Analysis.* The extra involution is $(g, h) \mapsto (-g, -h)$. The branch locus has genus 2; the transformation

$$(g, h) = \left(\frac{y + x^2 + 1}{4x^3}, \frac{x(4y - x^4 - 14x^2 - 1)}{(x^2 - 1)^2} \right)$$

converts it to Weierstrass form

$$y^2 = 3x^6 + 11x^4 + x^2 + 1.$$

It is isomorphic to the quotient of $X_0(57)$ by the Atkin–Lehner involution w_{57}.

The Hilbert modular surface $Y_-(57)$ is an honestly elliptic surface, with a genus-1 fibration over $\mathbb{P}^1_g$, and in fact, setting $h = 1$ gives a section. Therefore, we may use the Jacobian form, which has the Weierstrass equation

$$y^2 = x^3 + 4(12g^2 - 1)(28g^2 - 5)x^2$$
$$-4(2g-1)^3(2g+1)^3(12g^2-5)(108g^2-19)x + (2g-1)^6(2g+1)^6(108g^2-19)^2.$$

It has reducible fibers of type I_7 at $g = \pm\frac{1}{2}$, IV at $g = \infty$, I_2 at $g = \pm\frac{\sqrt{57}}{18}$, and I_3 at the four roots of $432g^4 + 216g^2 - 49$ (which generate a dihedral extension containing $\mathbb{Q}(\sqrt{57})$). The trivial lattice contributes 26 to the rank of the Néron–Severi lattice, leaving room for Mordell–Weil rank at most 4. We find the sections

$$P_1 = \left(0, (2g-1)^3(2g+1)^3(108g^2-19)\right),$$
$$P_2 = \left((2g-1)^2(2g+1)^2(6g-1)(6g+1),\right.$$
$$\left. 2g(2g-1)^2(2g+1)^2(432g^4+216g^2-49)\right),$$
$$P_3 = \left((\mu+3)(18g-\mu)(2g-1)(2g+1)^3/3,\right.$$
$$\left. (36g^2+9-2\mu)(2g+6+\mu)(18g-\mu)(2g-1)(2g+1)^3/3\right)$$

(where $\mu = \sqrt{57}$), with nondegenerate height pairing matrix

$$\frac{1}{42}\begin{pmatrix} 38 & 0 & -19 \\ 0 & 20 & -10 \\ -19 & -10 & 39 \end{pmatrix}.$$

Therefore, the Picard number is at least 29. In fact, counting points modulo 7 and 11 shows that the Picard number must be exactly 29. Alternatively, analysis of the quotients below gives another proof. The sections above together with the trivial lattice span a lattice of discriminant $11970 = 2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 19$. We checked that it is 3-saturated, and thus it is all of the Néron–Severi lattice. Therefore, these sections generate the Mordell–Weil group.

Next, we analyze the quotient by the involution $(g, h, z) \mapsto (-g, -h, z)$. This turns out to have a genus-1 fibration with section over the t-line, where $t = g^2$. The Weierstrass equation may be written (after a linear change of the base parameter and a Weierstrass transformation)

$$y^2 = x^3 + 4(t+1)(3t+2)(7t+2)x^2$$
$$- 4t^3(t+1)^2(3t-2)(27t+8)x + t^6(t+1)^3(27t+8)^2.$$

This is an elliptic K3 surface with fibers of type I_7 at $t = 0$, I_0^* at $t = -1$, I_2 at $t = -\frac{8}{27}$, II at $t = \infty$, and I_3 at $t = -2 \pm \frac{2\sqrt{57}}{9}$. Thus the trivial lattice has rank 17, leaving room for at most three independent sections.

We find the independent sections

$$P_1 = \left(t^2(t+1)(9t+8),\, t^2(t+1)^2(27t^2 + 108t + 32)\right),$$
$$P_2 = \big((t+1)(27t+8)(3t^2 - 64t - 64)/57,$$
$$(t+1)^2(t+40)(27t+8)(27t^2 + 108t + 32)/57^{3/2}\big)$$

of heights $\frac{5}{21}$ and $\frac{7}{6}$ respectively, and orthogonal with respect to the height pairing. Therefore the Picard number is at least 19. Counting points modulo 11 and 13 shows that the Picard number cannot be 20. These sections together with the trivial lattice generate a lattice of discriminant 140. We check that it is 2-saturated and must therefore be the full Néron–Severi lattice.

Replacing g^2 by t in the Weierstrass equation for $Y_-(57)$ gives a quadratic twist of the above quotient K3 surface, given by the Weierstrass equation

$$y^2 = x^3 + 4(12t - 1)(28t - 5)x^2$$
$$- 4(4t - 1)^3(12t - 5)(108t - 19)x + (4t - 1)^6(108t - 19)^2.$$

This is an elliptic K3 surface with fibers of type I_7 at $t = \frac{1}{4}$, I_2 at $t = \frac{19}{108}$, I_3 at $t = -\frac{1}{4} \pm \frac{\sqrt{57}}{18}$ and IV^* at $t = \infty$. The section $P = (0, (4t - 1)^3(108t - 19))$ has height $\frac{19}{42}$. Therefore, this K3 surface is singular. Together with the trivial lattice, the section P spans a lattice of discriminant $171 = 3^2 \cdot 19$. Since there is no 3-torsion section, and we cannot have a section of height $19/(3^2 \cdot 42)$ due to the configuration of fibers, this must be the full Néron–Severi lattice.

Therefore, the Mordell–Weil rank of the original surface must be $2 + 1 = 3$.

(g, h)	Sextic polynomial $f_6(x)$ defining the genus-2 curve $y^2 = f_6(x)$
$\left(-\frac{1}{10}, -\frac{5}{3}\right)$	$-2x^6 + 15x^5 + 131x^4 + 240x^3 - 61x^2 - 8$
$\left(\frac{7}{10}, -\frac{29}{3}\right)$	$81x^6 + 54x^5 - 286x^4 - 186x^3 + 323x^2 + 120x - 130$
$\left(\frac{7}{18}, 9\right)$	$-108x^6 + 324x^5 - 243x^4 + 186x^3 - 279x^2 - 80$
$\left(-\frac{7}{6}, \frac{21}{5}\right)$	$-100x^6 - 390x^5 - 204x^4 + 74x^3 - 69x^2 - 12x + 8$
$\left(-\frac{1}{18}, -3\right)$	$-220x^6 + 420x^5 - 111x^4 + 238x^3 + 381x^2 + 168x + 24$
$\left(-\frac{1}{4}, -\frac{16}{3}\right)$	$95x^6 - 114x^5 + 325x^4 + 35x^3 + 10x^2 - 429x - 234$
$\left(\frac{5}{14}, \frac{35}{3}\right)$	$120x^6 - 192x^5 + 122x^4 + 286x^3 - 448x^2 + 357x - 63$
$\left(\frac{19}{18}, -\frac{3}{5}\right)$	$58x^6 + 39x^5 - 129x^4 + 132x^3 + 519x^2 + 240x - 40$
$\left(-\frac{7}{10}, \frac{29}{3}\right)$	$-390x^6 + 451x^5 - 230x^4 - 593x^3 + 682x^2 + 220x - 200$
$\left(\frac{4}{9}, 18\right)$	$-540x^6 + 729x^5 - 135x^4 + 255x^3 - 225x^2 - 36x - 52$
$\left(-\frac{5}{2}, -\frac{10}{3}\right)$	$-60x^6 - 156x^5 + 137x^4 + 310x^3 - 351x^2 + 108x + 756$
$\left(-\frac{17}{10}, -\frac{47}{33}\right)$	$60x^5 + 839x^4 + 278x^3 - 652x^2 - 36x - 489$
$\left(\frac{1}{18}, 3\right)$	$-60x^6 + 60x^5 - 3x^4 + 184x^3 + 669x^2 + 132x + 868$
$\left(\frac{5}{2}, \frac{10}{3}\right)$	$-819x^5 - 1042x^4 + 61x^3 + 248x^2 - 48x$
$\left(-\frac{1}{18}, \frac{9}{5}\right)$	$-40x^6 - 72x^5 - 45x^4 - 534x^3 - 297x^2 - 324x - 1188$
$\left(-\frac{5}{2}, \frac{5}{3}\right)$	$-36x^6 + 84x^5 + 491x^4 - 750x^3 - 337x^2 - 912x - 1200$

Table 17. Some rational points (g, h) of small height on the surface of Theorem 32 and the corresponding genus-2 curves.

22.3. *Examples.*

Table 17 lists some points of small height and their genus-2 curves.

The specialization $h = 0$ gives a genus-1 curve with rational points, whose Jacobian has rank 1. Of course, there is a large supply of genus-1 curves, simply by specializing g, since we have an elliptic surface.

The sections P_1 and P_2 give rational curves $h = -16g/(4g^2 - 1)$ and $h = (72g^3 - 36g^2 + 78g - 7)/((4g^2 - 1)(6g - 7))$ respectively. The Brauer obstruction vanishes on these curves.

23. Discriminant 60

23.1. *Parametrization.*

We start with a K3 elliptic surface with E_6, D_6, A_4 fibers at ∞, 0, 1 respectively. The Weierstrass equation for this family is

$$y^2 = x^3 + atx^2 + 2bt^3(t - 1)x + ct^5(t - 1)^2,$$

with

$$a = (h^2 - g^2 - 1)^2 - 4(2h^2 - 3g^2 + 6)(t - 1),$$
$$b = 4\big(-4(h^2 - g^2 - 1)^2 + 16(h^2 - 2g^2 + 1)(t - 1)\big),$$
$$c = 256\big((h^2 - g^2 - 1)^2 + 4g^2(t - 1)\big).$$

We identify an E_8 fiber below, and move to this elliptic fibration by a 3-neighbor step.
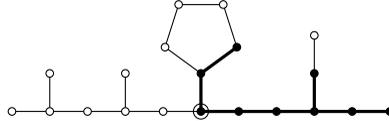
The new elliptic fibration has fibers of type E_8, D_6 and A_1, and a section P of height $\frac{60}{8} = \frac{15}{2} = 4 + 2 \cdot 2 - \frac{1}{2}$. We now identify an E_7 fiber F' and perform a 2-neighbor step to go to the new fibration. Note that it has a section, since $P \cdot F' = 7$, while the remaining component of the D_6 fiber has intersection number 2 with F'.
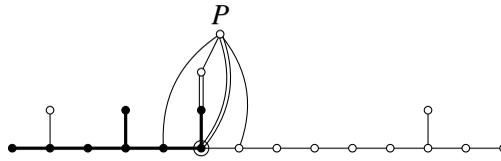
From the resulting $E_8 E_7$ fibration, we can read out the map to $\mathcal{A}_2$.

Theorem 33. *A birational model over $\mathbb{Q}$ for the Hilbert modular surface $Y_-(60)$ as a double cover of $\mathbb{P}^2_{g,h}$ is given by the equation*

$$z^2 = -(h^2 - 2h - g^2 + 5)(h^2 + 2h - g^2 + 5)$$
$$\times (8h^6 - 25g^2h^4 + 24h^4 + 26g^4h^2 - 86g^2h^2 + 24h^2 - 9g^6 + 66g^4 + 47g^2 + 8).$$

It is a surface of general type.

23.2. Analysis. The surface $Y_-(60)$ has two extra commuting involutions, $\iota_1 : (g, h) \mapsto (-g, h)$ and $\iota_2 : (g, h) \mapsto (g, -h)$. The two simpler components

$$h^2 \pm 2h - g^2 + 5 = 0$$

of the branch locus correspond to the subfamily of elliptic K3 surfaces where the D_6 fiber gets promoted to an E_7 fiber, while the more complicated component corresponds to an extra I_2 fiber. The simpler components are easily seen to be rational curves, as they define conics in the (g, h)-plane, with rational points. The last component is also a rational curve; a parametrization is given by

$$(g, h) = \left(\frac{(t^2 + 1)^3}{t(t^2 - 1)(t^2 - 2t - 1)}, \frac{(t^2 + 2t - 1)(t^4 - t^3 + 2t^2 + t + 1)}{t(t^2 - 1)(t^2 - 2t - 1)} \right).$$

This Hilbert modular surface is of general type.

We now analyze some of the quotients of this surface by the involutions. The quotient under both involutions is given by

$$z^2 = -(h^2 - 2gh + 6h + g^2 - 10g + 25)$$
$$(8h^3 - 25gh^2 + 24h^2 + 26g^2h - 86gh + 24h - 9g^3 + 66g^2 + 47g + 8),$$

and this is actually a rational surface; the transformation

$$(g, h) = (h' + g'^2 + 2g' + 5, h' + g'^2)$$

converts the above equation into a conic bundle over $\mathbb{P}^1_{h'}$ with a section.

The quotient by the involution ι_1 turns out to be an elliptic K3 surface, with Weierstrass equation given by

$$y^2 = x^3 + 2t^2(215t^2 + 356t + 140)x^2 - t^3(t + 2)^3(5t^2 + 874t + 864)x/3$$
$$-8t^4(t + 2)^6(163t^2 - 54t - 216)/27.$$

It has reducible fibers of type E_6 at $t = 0$, I_6 at $t = -2$, I_2 at $t = -1$ and $t = -\frac{2}{9}$, and I_3 at $t = (-7 \pm 5\sqrt{5})/19$. The trivial lattice therefore has rank 19. We find a 3-torsion section with x-coordinate $11t^2(t + 2)^2/3$ and a non-torsion section with $x = -t^2(t + 2)^2/3$. Therefore the K3 surface is singular. These sections, together with the trivial lattice, generate a lattice of rank 20 and discriminant 60. It must be the full Néron–Severi lattice, since otherwise there would have to be a 6-torsion section or section of height $\frac{5}{24}$, neither of which is possible with our configuration of reducible fibers.

The quotient by the involution ι_2 is also an elliptic K3 surface, with Weierstrass equation

$$y^2 = x^3 - (11t^4 - 20t^2 + 8)x^2 + 16(t - 1)^3(t + 1)^3(4t^2 - 5)x.$$

This has bad fibers of type I_6 at $t = \pm 1$, I_2 at $t = \pm\frac{\sqrt{5}}{2}$, and I_3 at $t = \pm\frac{2}{\sqrt{3}}$. Therefore the trivial lattice has rank 18, leaving room for at most two independent sections. We find the following sections, of which the first is 6-torsion.

$$P_0 = \left(2(t^2 - 1)(4t^2 - 5), 4(t^2 - 1)(3t^2 - 4)(4t^2 - 5)\right),$$
$$P_1 = \left((11 - 3\mu)t^2(t^2 - 1)/2, (3 + 5\mu)t(t^2 - 1)/12(18t^2 - 15 + \mu)\right),$$
$$P_2 = \left((11 + 3\mu)t^2(t^2 - 1)/2, (3 - 5\mu)t(t^2 - 1)/12(18t^2 - 15 - \mu)\right),$$

where $\mu = \sqrt{-15}$. The height pairing matrix of P_1 and P_2 is

$$\frac{1}{3}\begin{pmatrix} 7 & -2 \\ -2 & 7 \end{pmatrix}.$$

(g, h)	Sextic polynomial $f_6(x)$ defining the genus-2 curve $y^2 = f_6(x)$
$\left(\frac{17}{6}, -\frac{13}{6}\right)$	$468x^6 + 1332x^5 + 1345x^4 - 20x^3 + 1051x^2 - 150x + 186$
$\left(-\frac{17}{6}, \frac{13}{6}\right)$	$-12x^6 + 132x^5 + 371x^4 + 1506x^3 + 1391x^2 - 528x - 1872$
$\left(\frac{17}{6}, \frac{13}{6}\right)$	$-942x^6 + 3150x^5 - 869x^4 - 4220x^3 + 745x^2 + 2244x + 468$
$\left(-\frac{17}{6}, -\frac{7}{6}\right)$	$48x^6 - 360x^5 + 1907x^4 - 4000x^3 + 5195x^2 + 828x + 2556$
$\left(-\frac{17}{6}, -\frac{13}{6}\right)$	$-4500x^6 - 9300x^5 - 5365x^4 + 4106x^3 + 3335x^2 - 2112x - 2648$
$\left(-\frac{17}{6}, \frac{7}{6}\right)$	$-4116x^6 - 6468x^5 + 8617x^4 + 11086x^3 - 12239x^2 - 3708x + 4212$
$\left(\frac{17}{6}, \frac{7}{6}\right)$	$72x^6 - 2136x^5 + 15869x^4 - 258x^3 - 1759x^2 + 108x - 4$
$\left(\frac{17}{6}, -\frac{7}{6}\right)$	$12x^6 - 36x^5 + 929x^4 - 1458x^3 + 16361x^2 - 4452x + 1476$
$\left(\frac{51}{5}, -\frac{54}{5}\right)$	$9248x^6 - 2312x^5 + 12427x^4 - 29852x^3 - 21811x^2 + 26690x + 21270$
$\left(\frac{57}{10}, \frac{43}{10}\right)$	$2272x^6 + 35064x^5 + 12877x^4 - 24234x^3 - 37079x^2 + 29700x - 3500$
$\left(-\frac{51}{5}, -\frac{54}{5}\right)$	$-6368x^6 - 20760x^5 + 11991x^4 + 29560x^3 - 61443x^2 + 39870x - 12150$
$\left(-\frac{46}{15}, -\frac{49}{15}\right)$	$-575x^6 - 3075x^5 - 12269x^4 - 16401x^3 - 56024x^2 - 21792x - 73242$
$\left(-\frac{61}{10}, \frac{49}{10}\right)$	$-36450x^6 - 10530x^5 + 6327x^4 + 78760x^3 - 29879x^2 - 17700x + 2612$
$\left(\frac{61}{10}, \frac{49}{10}\right)$	$8612x^6 - 4020x^5 - 52381x^4 - 4290x^3 + 91787x^2 + 47220x - 11540$
$\left(\frac{61}{10}, -\frac{49}{10}\right)$	$-17092x^6 + 13812x^5 - 101885x^4 + 63210x^3 - 89229x^2 + 69580x - 15092$
$\left(-\frac{51}{5}, \frac{54}{5}\right)$	$-100572x^6 - 102884x^5 - 147679x^4 - 25432x^3 + 27727x^2 + 35870x - 11890$

Table 18. Some rational points (g, h) of small height on the surface of Theorem 33 and the corresponding genus-2 curves.

Therefore the Picard number of this K3 surface is 20. The discriminant of the sublattice of $\mathrm{NS}(X)$ generated by the trivial lattice and these sections is 180. We checked that this lattice is 2- and 3-saturated, which proves that it is the entire Picard group.

23.3. *Examples*. Table 18 lists some points of small height and their genus-2 curves.

We now describe some curves of genus 1, possessing infinitely many rational points, on the Hilbert modular surface. These were obtained by pulling back rational curves on the quotients by ι_1 and ι_2 obtained as sections of the elliptic fibrations. In each case we give the curve as a double cover of $\mathbb{P}^1$, exhibit a coordinate of a point on $\mathbb{P}^1$ that lifts to a rational point, and give the conductor and Mordell–Weil group.

- $v = \infty$, conductor $2^4 \, 3^2 \, 11 \cdot 97$, Mordell–Weil group $(\mathbb{Z}/2\mathbb{Z}) \oplus \mathbb{Z}$, equation

$$g^2 = \frac{v^4 + 132v^3 + 11784v^2 + 566280v + 20175732}{36(v+9)^2}, \qquad h = \frac{v^2 + 72v + 4560}{6(v+9)}.$$

- $v = 1$, conductor $2 \cdot 3 \cdot 7 \cdot 17 \cdot 19$, Mordell–Weil group $(\mathbb{Z}/2\mathbb{Z})^2 \oplus \mathbb{Z}$, equation

$$g^2 = \frac{4913v^4 + 1990v^2 + 153}{36(v^2 - 1)^2}, \quad h = -\frac{25v^2 + 3}{2(v^2 - 1)}.$$

- $t = -1$, conductor $5^2 \, 11 \cdot 17 \cdot 47$, Mordell–Weil group $\mathbb{Z}^2$, equation

$$g^2 = \frac{14049t^4 - 57248t^3 + 87462t^2 - 59840t + 15657}{(t+1)^2(9t-11)^2}, \quad h = -\frac{2(t-1)(54t-67)}{(t+1)(9t-11)}.$$

- $v = 0$, conductor $238 = 2 \cdot 7 \cdot 17$, Mordell–Weil group $(\mathbb{Z}/2\mathbb{Z}) \oplus \mathbb{Z}$, equation

$$h^2 = \frac{833v^4 + 190v^2 + 1}{4(v^2 - 1)^2}, \quad g = \frac{27v^2 + 5}{2(v^2 - 1)}.$$

We can obtain a few more such curves from these, by applying the involution ι_2 to the first three curves, and the involution ι_1 to the last. If two genus-2 curves are parametrized by points related by such an involution, then the curves' Jacobians are isogenous.

24. Discriminant 61

24.1. *Parametrization.* Start with an elliptic surface with D_7, A_6 and A_2 fibers and a section of height $\frac{61}{84} = 4 - \frac{2}{3} - \frac{6}{7} - \frac{7}{4}$.

The Weierstrass equation for this family can be written as

$$y^2 = x^3 + ax^2 + 2bt(1-1)x + ct^2(t-1)^2,$$

where

$$
\begin{aligned}
a = {}& 4h^3(h-g)^3t^3 + (h-g)^2(g^2h^2 - 4gh^2 - 8h^2 - 2g^2h + g^2 + 12g + 12)t^2 \\
& - 2(g+1)(h-g)(g^2h + 4h - g^2 - 6g)t + g^2(g+1)^2, \\
b = {}& -4(g+1)(h-g)^2\big((h-g)^2(2gh^2 + 4h^2 + g^2h - g^2 - 6g - 6)t^2 \\
& + (g+1)(h-g)(g^2h + 2h - 2g^2 - 6g)t - g^2(g+1)^2\big), \\
c = {}& 16(g+1)^2(h-g)^4\big((g+2)(h-g)t + g(g+1)\big)^2.
\end{aligned}
$$

We first perform a 2-neighbor step to move to an elliptic fibration with E_7 and A_7 fibers, by locating an E_7 fiber, as follows.
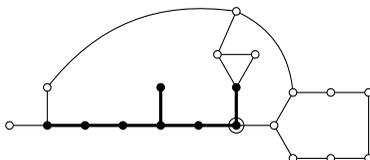
This elliptic fibration has Mordell–Weil rank 2, and we can in fact write down two generators of the Mordell–Weil group, which intersect the components of reducible fibers as shown below. Next, we identify the class of an E_8 fiber, and use it to perform 2-neighbor step to an elliptic fibration with E_8, A_5 and A_1 fibers, and Mordell–Weil rank 2.
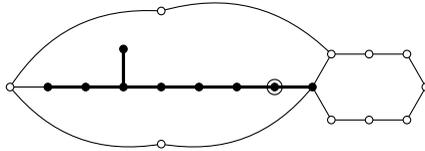
We show one of the generators P of the Mordell–Weil lattice, which has height $4 - 2 \cdot \frac{4}{6} - \frac{1}{2}$. Next, we go to a fibration with E_8 and E_6 fibers using the fiber class F' of E_6 below. Since $P \cdot F' = 1$, the new elliptic fibration has a section.
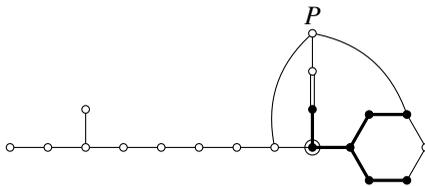
We can find a section P' of this elliptic fibration with E_8 and E_6 fibers, of height $\frac{8}{3} = 4 - \frac{4}{3}$. We use it to go to a fibration with E_8 and E_7 fibers as shown.
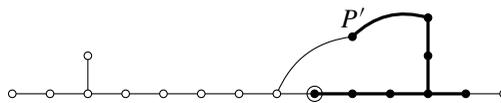
From the resulting $E_8 E_7$ fibration we read out the Igusa–Clebsch invariants and calculate the equation of $Y_-(61)$ as a double cover of $\mathbb{P}^2_{g,h}$.

Theorem 34. *A birational model over $\mathbb{Q}$ for the Hilbert modular surface $Y_-(61)$ as a double cover of $\mathbb{P}^2_{g,h}$ is given by the equation*

$$z^2 = (h-1)^4 g^4 - 2(h-1)h(h^3 - 14h^2 - 20h - 21)g^3$$
$$+ h(h^5 - 46h^4 - 19h^3 + 42h^2 + 39h - 44)g^2$$
$$+ 2h^2(10h^4 + 5h^3 - 13h^2 - h + 12)g - h^2(8h^4 - 13h^2 + 16).$$

It is an honestly elliptic surface, with arithmetic genus 2 and Picard number 28.

24.2. *Analysis*. The branch locus has genus 1. The transformation

$$g = -\frac{8x^3y - 34x^2y + 37xy - 14y + x^6 - 10x^5 + 44x^4 - 89x^3 + 98x^2 - 58x + 14}{x^2(x-1)^3(x-7)},$$

$$h = \frac{12x^2y - 35xy + 26y + 3x^4 + 11x^3 - 61x^2 + 74x - 26}{x^2(9x^2 - 24x + 13)}$$

converts it to the Weierstrass form

$$y^2 + xy = x^3 - 2x + 1,$$

an elliptic curve of conductor 61. It is isomorphic to $X_0(61)/\langle w \rangle$, where w is the Atkin–Lehner involution.

The Hilbert modular surface $Y_-(61)$ is an honestly elliptic surface, since we have an evident genus-1 fibration over $\mathbb{P}_h^1$. Since the coefficient of g^4 is a square, we convert to the Jacobian. In Weierstrass form, we obtain

$$\begin{aligned}
y^2 = x^3 &+ h(h^5 + 14h^4 + 23h^3 - 102h^2 + 88)x^2 \\
&- h^2(110h^6 + 908h^5 - 2854h^4 - 1028h^3 + 4795h^2 + 120h - 2000)x \\
&+ h^4\big(1728h^7 + 16849h^6 - 24666h^5 - 50145h^4 \\
&\qquad\qquad\qquad + 52138h^3 + 50406h^2 - 29200h - 20000\big).
\end{aligned}$$

This elliptic surface S has $\chi(\mathcal{O}_S) = 3$, with bad fibers of type I_0^* at $h = 0$, I_7 at $h = \infty$, I_2 at $h = 1$ and at the roots of $h^3 + 13h^2 + 24h + 16$ (which generates the cubic field of discriminant -244), and I_3 at $h = -1$ and at the roots of $3h^4 + 23h^3 - 64h^2 + 22h + 25$ (which generates the quartic field of discriminant $-3 \cdot 61^2$, a quadratic extension of $\mathbb{Q}(\sqrt{61})$). The trivial lattice therefore has rank 26, leaving room for at most 4 independent sections. We find the two sections

$$P_1 = \big(h^2(-36h + 55), \ 12h^2(3h^4 + 23h^3 - 64h^2 + 22h + 25)\big),$$

$$\begin{aligned}
P_2 = \big(&-(36h^6 + 444h^5 + 472h^4 - 1492h^3 - 799h^2 + 1048h - 400)/61, \\
&4(15h^2 - 2h - 5)(h^3 + 13h^2 + 24h + 16)(3h^4 + 23h^3 - 64h^2 + 22h + 25)/61^{3/2}\big)
\end{aligned}$$

of heights $\frac{13}{21}$ and $\frac{11}{6}$ respectively, and orthogonal to each other under the height pairing. By Oda's calculations, the Picard number is 28, and therefore the Mordell–Weil rank is exactly 2. The sublattice of the Picard group generated by the above sections and the trivial lattice has discriminant $41184 = 2^5 \cdot 3^2 \cdot 11 \cdot 13$. We checked that it is 2- and 3-saturated, and therefore it must be the entire Néron–Severi lattice. Therefore the Mordell–Weil group is generated by P_1 and P_2.

24.3. *Examples*. Table 19 lists some points of small height and their genus-2 curves.

(g, h)	Sextic polynomial $f_6(x)$ defining the genus-2 curve $y^2 = f_6(x)$
$\left(-\frac{3}{2}, \frac{1}{2}\right)$	$-32x^6 - 144x^5 - 229x^4 - 24x^3 - 157x^2 - 84x + 92$
$\left(\frac{47}{72}, -\frac{1}{8}\right)$	$-10x^6 - 42x^5 + 39x^4 + 728x^3 + 489x^2 + 1260x - 1068$
$\left(-\frac{47}{12}, -\frac{11}{4}\right)$	$756x^6 - 756x^5 + 1953x^4 - 282x^3 - 327x^2 + 1404x - 1444$
$\left(-\frac{86}{9}, -8\right)$	$-348x^6 - 972x^5 - 2661x^4 - 2326x^3 - 2205x^2 + 1260x - 140$
$\left(-\frac{17}{18}, -\frac{1}{2}\right)$	$467x^6 + 1551x^5 + 3906x^4 + 3027x^3 - 495x^2 - 1800x + 400$
$\left(\frac{15}{4}, 5\right)$	$-325x^6 + 1410x^5 + 1045x^4 - 3993x^3 - 2636x^2 + 3456x + 2143$
$\left(-\frac{69}{58}, -\frac{20}{29}\right)$	$-128x^6 + 96x^5 - 2519x^4 + 4362x^3 + 1321x^2 + 456x + 32$
$\left(\frac{31}{45}, \frac{14}{5}\right)$	$-204x^6 - 108x^5 + 2553x^4 - 946x^3 - 4683x^2 - 360x + 1200$
$\left(1, \frac{4}{3}\right)$	$-188x^6 - 1812x^5 - 4707x^4 - 130x^3 + 6189x^2 - 1620x + 108$
$\left(\frac{13}{18}, -\frac{1}{2}\right)$	$-612x^6 + 3708x^5 - 6501x^4 + 5656x^3 + 693x^2 - 318x - 1126$
$\left(-\frac{29}{6}, -\frac{29}{8}\right)$	$-148x^6 + 2472x^5 - 1481x^4 + 5001x^3 - 6980x^2 + 1425x - 6625$
$\left(-\frac{37}{18}, -\frac{1}{2}\right)$	$-16x^6 - 264x^5 + 477x^4 - 2268x^3 + 4029x^2 - 6156x + 10372$
$\left(\frac{23}{84}, -\frac{1}{3}\right)$	$-4671x^6 - 6660x^5 - 10362x^4 + 11195x^3 + 1287x^2 + 1590x + 7621$
$\left(\frac{5}{6}, \frac{5}{3}\right)$	$821x^6 - 1896x^5 - 4922x^4 + 8588x^3 + 11341x^2 - 7674x - 8247$
$\left(-\frac{23}{2}, -10\right)$	$2716x^6 + 84x^5 + 7107x^4 + 10642x^3 + 4803x^2 + 13764x + 10204$
$\left(\frac{65}{18}, \frac{5}{2}\right)$	$-3756x^6 - 12012x^5 + 9297x^4 + 18116x^3 - 10335x^2 - 7560x + 3600$

Table 19. Some rational points (g, h) of small height on the surface of Theorem 34 and the corresponding genus-2 curves.

Next, we list some rational curves on the surface. The specialization $h = -1$ gives a rational curve, but the curves of genus 2 corresponding to the points on this curve have Jacobians with endomorphism ring larger than just $\mathcal{O}_{61}$ (they are isogenous to the symmetric squares of elliptic curves). The section P_1 gives the rational curve $g = (3h^2 - 7h + 5)/(3(h - 1))$, for which the Brauer obstruction vanishes identically, yielding a 1-parameter family of genus-2 curves whose Jacobian have real multiplication by $\mathcal{O}_{61}$.

25. Discriminant 65

25.1. *Parametrization.* We start with an elliptic surface with E_7, A_4 and A_4 fibers at $t = \infty, 0, 1$ respectively, and a section of height $\frac{65}{50} = \frac{13}{10} = 4 - \frac{3}{2} - \frac{2 \cdot 3}{5}$. The Weierstrass equation of such a family is

$$y^2 = x^3 + \left(a_0(1 - t) + a_1 t(1 - t) + t^2\right)x^2$$
$$+ 2t^2(t - 1)e\left(b_0(1 - t) + b_1 t(1 - t) + t^2\right)x + e^2 t^4(t - 1)^2(c_0(1 - t) + t),$$

with

$$a_0 = (s^2 - 5)^2(2rs^2 + s + 2r)^2/4,$$

$$a_1 = 4(5s^6 - 8s^4 - 7s^2 - 6)r^2 + 4s(5s^4 - 13s^2 - 4)r + 5s^4 - 18s^2 + 5,$$
$$b_0 = (s^2 - 5)(2rs^2 + s + 2r)(2rs^4 + s^3 + 4rs^2 + s - 6r)/4,$$
$$b_1 = 8(s^2 - 1)(s^2 + 1)^2 r^2 + 8s(s^4 - 1)r + 2s^4 - 2s^2 + 1,$$
$$c_0 = (2rs^4 + s^3 + 4rs^2 + s - 6r)^2/4,$$
$$e = -(s - 1)(s + 1)(2rs^2 - 4rs + s + 2r - 2)(2rs^2 + 4rs + s + 2r + 2).$$

To describe an elliptic fibration with E_8 and E_7 fibers, we identify the class of an E_8 fiber and move by a 2-neighbor step to an $E_8 A_4 A_2$ fibration.
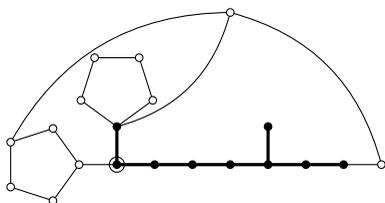
The new elliptic fibration has Mordell–Weil rank 2, and we compute two generators P and Q, each of height $\frac{32}{15} = 4 - \frac{2}{3} - \frac{6}{5}$, with intersection pairing $\frac{7}{15}$. We draw P in the figure below, as well as the class of an A_7 fiber F'. Because $Q \cdot F' = 1$, the new fibration has a section.
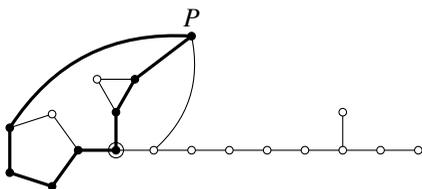
The new elliptic fibration has A_7 and E_8 fibers, and a section P' of height $\frac{65}{8} = 4 + 2 \cdot 3 - 3 \cdot \frac{5}{8}$. We now go to $E_8 E_7$ via a 2-neighbor step. Note that the section P' intersects the new E_7 fiber F'' in 7, while the remaining component of the A_7 fiber intersects F'' in 2. Since these are coprime, the genus-1 fibration defined by F'' has a section.
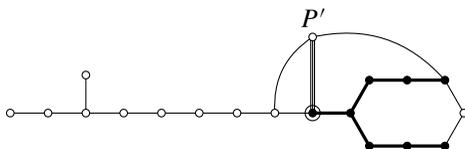
We now read out the Igusa–Clebsch invariants, and compute the equation of $Y_-(65)$ as a double cover of $\mathbb{P}^2_{r,s}$. It is branched over the locus where the K3 surfaces acquire an extra I_2 fiber.

Theorem 35. *A birational model over $\mathbb{Q}$ for the Hilbert modular surface $Y_-(65)$ as a double cover of $\mathbb{P}^2_{r,s}$ is given by the equation*

$$z^2 = -16(s^4 + 2s^2 + 13)^2(4s^6 + 3s^4 - 10s^2 - 13)r^4$$
$$- 32s(4s^{12} + 15s^{10} + 127s^8 - 10s^6 - 494s^4 - 1253s^2 - 949)r^3$$
$$- 8(12s^{12} + 33s^{10} + 408s^8 - 898s^6 - 2672s^4 - 2023s^2 + 404)r^2$$
$$- 8s(4s^{10} + 7s^8 + 149s^6 - 627s^4 - 641s^2 + 148)r$$
$$- (4s^{10} + 3s^8 + 166s^6 - 997s^4 + 328s^2 - 80).$$

It is an honestly elliptic surface, with arithmetic genus 2 and Picard number 28.

25.2. Analysis. This is an honestly elliptic surface, with the extra involution $\iota :$ $(r, s, z) \mapsto (-r, -s, z)$ corresponding to the factorization $65 = 5 \cdot 13$.

The branch locus is a curve of genus 1, isomorphic to the elliptic curve

$$y^2 + xy = x^3 - x$$

of conductor 65. For lack of space we do not write down the explicit isomorphism here, relegating the relevant formulae to the online supplement. This elliptic curve is isomorphic to the quotient of $X_0(65)$ by the Atkin–Lehner involution w_{65}.

We were unable to find a section of this genus-1 fibration. However, for purposes of analyzing the Picard number, we study the Jacobian of this elliptic curve over $\mathbb{Q}(s)$, given by

$$y^2 = x^3 + (8s^6 + 13s^4 - 106s^2 + 101)x^2$$
$$+ (16s^{12} + 52s^{10} - 564s^8 + 1416s^6 - 1624s^4 + 900s^2 - 196)x.$$

This has reducible fibers of type I_8 at $s = \pm 1$, I_4 at $s = \infty$, I_3 at $s = \pm\frac{\sqrt{13}}{3}$, and I_2 at the four roots of $4s^4 + 29s^2 - 49$ (a dihedral extension containing $\sqrt{65}$). The trivial lattice therefore has rank 27, leaving room for Mordell–Weil rank at most 3. There is the obvious 2-torsion section $(0, 0)$, and we find a non-torsion section of height $\frac{2}{3}$:

$$P = \big((73 + 9\mu)/2(s^2 - 1)^2(s^2 + (29/8 - 5/8\mu)),$$
$$(657 + 81\mu)/2s(s^2 - 1)^2(s^2 - 13/9)(s^2 + (29/8 - 5/8\mu))\big)$$

with $\mu = \sqrt{65}$. Analysis of the quotient by ι, and its twist, shows that the Mordell–Weil rank is exactly 1. Therefore the Picard number of $Y_-(65)$ is 28. The discriminant of the sublattice of the Néron–Severi group generated by the trivial lattice and these two sections is $6144 = 2^{11} \cdot 3$. We checked that it is 2-saturated, and so it equals the entire Néron–Severi lattice. Therefore the sections above generate the Mordell–Weil group.

The quotient by the involution ι is given by the equation

$$
\begin{aligned}
w^2 = {} & -16t^2(t^2 + 2t + 13)^2(4t^3 + 3t^2 - 10t - 13)r^4 \\
& - 32t^2(4t^6 + 15t^5 + 127t^4 - 10t^3 - 494t^2 - 1253t - 949)r^3 \\
& - 8t(12t^6 + 33t^5 + 408t^4 - 898t^3 - 2672t^2 - 2023t + 404)r^2 \\
& - 8t(4t^5 + 7t^4 + 149t^3 - 627t^2 - 641t + 148)r \\
& - (4t^5 + 3t^4 + 166t^3 - 997t^2 + 328t - 80),
\end{aligned}
$$

where $t = s^2$. Once again we study the Jacobian elliptic fibration: it has the equation

$$
\begin{aligned}
y^2 = {} & x^3 + (8t^4 + 13t^3 - 106t^2 + 101t)x^2 \\
& + (16t^8 + 52t^7 - 564t^6 + 1416t^5 - 1624t^4 + 900t^3 - 196t^2)x.
\end{aligned}
$$

This is an elliptic K3 surface with bad fibers of type I_0^* at $t = 0$, I_8 at $t = 1$, I_3 at $t = \frac{13}{9}$, and I_2 at $t = \infty$ and $t = (-29 \pm 5\sqrt{65})/8$. Therefore the trivial lattice has rank 18, and the Mordell–Weil rank can be at most 2. As before we have a 2-torsion

(r, s)	Sextic polynomial $f_6(x)$ defining the genus-2 curve $y^2 = f_6(x)$
$\left(\frac{40}{41}, -\frac{1}{5}\right)$	$-396x^6 + 216x^5 + 281x^4 - 889x^3 + 50x^2 + 939x + 315$
$\left(-\frac{40}{41}, \frac{1}{5}\right)$	$-648x^5 + 3015x^4 - 422x^3 - 4369x^2 + 2216x - 752$
$\left(\frac{35}{136}, \frac{1}{5}\right)$	$-72x^6 + 969x^5 - 3509x^4 + 847x^3 + 9373x^2 + 816x - 3724$
$\left(-\frac{40}{143}, -\frac{2}{5}\right)$	$-240x^6 - 384x^5 + 695x^4 + 2724x^3 + 5543x^2 - 10992x - 2736$
$\left(\frac{2}{15}, -2\right)$	$-16200x^5 + 1125x^4 - 8972x^3 - 30493x^2 + 14186x - 18974$
$\left(\frac{40}{143}, \frac{2}{5}\right)$	$-4368x^6 + 420x^5 + 28144x^4 - 13235x^3 - 35846x^2 + 10080x + 14112$
$\left(-\frac{5}{64}, \frac{7}{5}\right)$	$800x^6 + 6480x^5 + 19405x^4 + 35306x^3 - 39491x^2 - 2688x - 48$
$\left(-\frac{49}{197}, \frac{1}{2}\right)$	$5088x^6 - 48648x^5 + 85307x^4 + 9352x^3 - 59071x^2 - 15690x + 730$
$\left(\frac{49}{197}, -\frac{1}{2}\right)$	$546x^6 + 9798x^5 + 24115x^4 - 25228x^3 - 98531x^2 + 58920x + 38880$
$\left(-\frac{35}{136}, -\frac{1}{5}\right)$	$2744x^6 - 22344x^5 - 45297x^4 - 16942x^3 + 100440x^2 + 89910x - 72900$
$\left(\frac{5}{64}, -\frac{7}{5}\right)$	$-332100x^6 + 344220x^5 - 54545x^4 + 106126x^3 - 68117x^2 + 3528x - 16464$
$\left(-\frac{2}{15}, 2\right)$	$-216000x^6 + 506400x^5 - 283195x^4 - 70483x^3 + 13883x^2 + 3456x + 300$
$\left(-\frac{1}{65}, \frac{1}{2}\right)$	$-366600x^6 - 2197788x^5 - 64538x^4 + 11447529x^3 + 133360x^2$ $- 19021554x + 9447840$
$\left(\frac{1}{65}, -\frac{1}{2}\right)$	$-412287975x^6 - 3236837061x^5 + 5479876697x^4 + 3156545763x^3$ $+ 1177706300x^2 - 7413585000x - 1103500000$

Table 20. Some rational points (r, s) of small height on the surface of Theorem 35 and the corresponding genus-2 curves.

point $P_1 = (0, 0)$. We also find a non-torsion point

$$P_2 = \big((73 - 9\mu)t(t - 1)^2(8t + 29 + 5\mu)/16,$$
$$(-73 + 9\mu)t^2(t - 1)^2(9t - 13)(8t + 29 + 5\mu)/16\big)$$

of height $\frac{1}{3}$, with $\mu = \sqrt{65}$ as before. Therefore, the Picard number is at least 19, and point counting modulo 11 and 23 shows that the Picard number must be 19. We verified by checking 2-saturation that the sections P_1 and P_2 and the trivial lattice span the Néron–Severi group, which has discriminant 64.

We next analyze the quotient by $\iota' : (r, s, z) \mapsto (-r, -s, -z)$, which is the quadratic twist of the elliptic K3 surface above by $\sqrt{t}$:

$$y^2 = x^3 + (8t^3 + 13t^2 - 106t + 101)x^2$$
$$+ (16t^6 + 52t^5 - 564t^4 + 1416t^3 - 1624t^2 + 900t - 196)x.$$

This is also an elliptic K3 surface, with reducible fibers of type I_2^* at $t = \infty$, I_8 at $t = 1$, I_3 at $t = \frac{13}{9}$, and I_2 at $t = (-29 \pm 5\sqrt{65})/8$. The trivial lattice has rank 19. Again, point counting modulo 11 and 23 shows that the Picard number is 19, and the Mordell–Weil group therefore has rank 0, with only the 2-torsion section $(0, 0)$.

25.3. *Examples.* Table 20 on the previous page lists some points of small height and their genus-2 curves.

26. Discriminant 69

26.1. *Parametrization.* Start with an elliptic K3 surface with fibers of type E_6, A_8 and A_1 and a section of height $\frac{69}{54} = \frac{23}{18} = 4 - \frac{1}{2} - \frac{20}{9}$. We can write down the Weierstrass equation of this family as

$$y^2 = x^3 + (a_0 + a_1 t + a_2 t^2)x^2 + t^3(b_0 + b_1 t + b_2 t^2)x + t^6(c_0 + c_1 t + c_2 t^2),$$

with

$$a_0 = \tfrac{1}{4}(\sigma_2 - \sigma_1 + 2)^2, \qquad\qquad a_1 = \tfrac{1}{2}(\sigma_2^2 - \sigma_2(\sigma_1 - 4) - 2(\sigma_1 - 1)),$$
$$a_2 = \tfrac{1}{4}(\sigma_2^2 + 4\sigma_2 - 8), \qquad\qquad b_0 = \tfrac{1}{2}\sigma_2(\sigma_2 - \sigma_1 + 2)^2,$$
$$b_1 = \tfrac{1}{2}(\sigma_2^3 - \sigma_2^2(\sigma_1 - 4) - \sigma_1^2 - \sigma_2\sigma_1 + 2\sigma_1)), \quad b_2 = \tfrac{1}{2}(\sigma_2(\sigma_1 - 6) + 2(\sigma_1 - 1)),$$
$$c_0 = \tfrac{1}{4}\sigma_2^2(\sigma_2 - \sigma_1 + 2)^2, \qquad c_1 = \tfrac{1}{2}\sigma_2(\sigma_1 - 2)(\sigma_2 - \sigma_1), \qquad c_2 = \tfrac{1}{4}(\sigma_1^2 - 4\sigma_2),$$
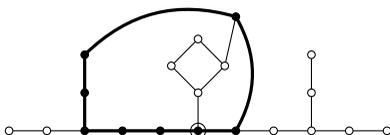
where

$$\sigma_1 = r + s, \qquad \sigma_2 = rs.$$

First we find the class of another E_6 fiber below and go to that elliptic fibration via a 2-neighbor step.
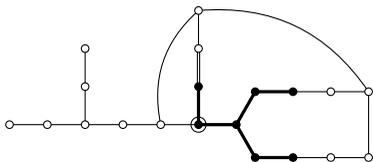

The resulting elliptic fibration has E_6, E_6 and A_3 fibers, and a section of height $\frac{23}{12} = 4 - \frac{4}{3} - \frac{3}{4}$. Now we find the class of an A_7 fiber in the diagram below.

The resulting fibration has A_7, A_5, A_2 and A_1 fibers, a 2-torsion section, and a non-torsion section P of height $\frac{69}{72} = \frac{23}{24} = 4 - \frac{2}{3} - \frac{3\cdot3}{6} - \frac{1\cdot7}{8}$. We next identify the class F' of an E_7 fiber, and go to it via a 2-neighbor step. Note that $P \cdot F' = 1$, so the new fibration has a section.
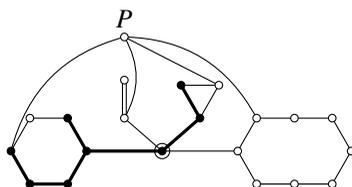
The new elliptic fibration has E_7, A_7 and A_1 fibers, a 2-torsion section Q', and a non-torsion section P' of height $\frac{69}{8} = 4 + 2 \cdot 3 - \frac{1}{2} - \frac{7}{8}$. We identify a fiber F'' of type E_7 below.
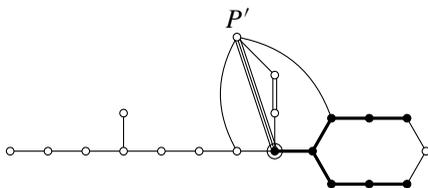
Note that $P' \cdot F'' = 2 \cdot 3 + 3 = 9$, while the remaining component of the A_7 fiber intersects F'' with multiplicity 2. Therefore the new elliptic fibration has a section. Converting to the Jacobian, we read out the Weierstrass coefficients of the $E_8 E_7$ form, which give us the Igusa–Clebsch invariants.

Theorem 36. *A birational model over $\mathbb{Q}$ for the Hilbert modular surface $Y_-(69)$ as a double cover of $\mathbb{P}^2_{r,s}$ is given by the equation*

$$z^2 = (r-1)^2 r^4 s^6 - 2(r-1)r^2(r^3 + 13r^2 - 37r + 22)s^5$$
$$+ (r^6 + 100r^5 - 439r^4 + 640r^3 - 357r^2 + 72r - 16)s^4$$
$$- 2(59r^5 - 320r^4 + 590r^3 - 436r^2 + 133r - 32)s^3$$
$$+ (44r^5 - 357r^4 + 872r^3 - 830r^2 + 314r - 83)s^2$$
$$+ 2(36r^4 - 133r^3 + 157r^2 - 65r + 19)s - 16r^4 + 64r^3 - 83r^2 + 38r - 11.$$

It is a surface of general type.

26.2. *Analysis.* This is a surface of general type, with an extra involution $(r, s, z) \mapsto (s, r, z)$, corresponding to $69 = 3 \cdot 23$.

The branch locus is a curve of genus 2; the transformation

$$r = -\frac{x^3 y + x^2 y - y - 3x^6 - 4x^5 + x^4 + 6x^3 - 2x^2 - 2x + 1}{2x^2(x^2 + x - 1)^2},$$

$$s = \frac{x^3 y + x^2 y - y + 3x^6 + 4x^5 - x^4 - 6x^3 + 2x^2 + 2x - 1}{2x^2(x^2 + x - 1)^2}$$

converts it into Weierstrass form

$$y^2 = (x^3 + x^2 - 1)(5x^3 - 7x^2 + 4x - 1).$$

It is isomorphic to $X_0(69)/\langle w \rangle$, where w is the Atkin–Lehner involution.

The quotient surface is (with $m = r + s, n = rs$)

$$z^2 = -16m^4 + 4(11n^2 + 18n + 16)m^3 + (n^4 - 118n^3 - 357n^2 - 202n - 83)m^2$$
$$- 2(n^5 - 50n^4 - 254n^3 - 328n^2 - 61n - 19)m$$
$$+ n^6 - 26n^5 - 203n^4 - 466n^3 - 330n^2 + 36n - 11.$$

The substitution $m = n + k$ makes the right-hand side quartic in n, with highest coefficient a square. Converting to the Jacobian, we get (after some Weierstrass transformations and change of the parameter on the base) the elliptic K3 surface

$$y^2 = x^3 - (88t^3 + 15t^2 + 6t - 1)x^2 + 8t^3(250t^3 + 57t^2 + 45t - 8)x$$
$$+ 16t^5(1125t^3 + 552t^2 + 208t - 36).$$

This has fibers of type I_5 at $t = 0$, I_0^* at $t = \infty$, I_2 at $t = (-3 \pm 2\sqrt{3})/4$, and I_3 at the roots of $25t^3 + 17t^2 + 2t - 1$ (which generates the cubic field of discriminant -23). The trivial lattice has rank 18, leaving room for at most two independent sections. We find the non-torsion section

$$P_1 = \left(4t(1-t), 4t(25t^3 + 17t^2 + 2t - 1)\right)$$

of height $\frac{1}{5}$. Counting points modulo 7 and 13 then shows that the Picard number must be exactly 19. Therefore, the discriminant of the sublattice spanned by P_1 and the trivial lattice is $432 = 2^4 \cdot 3^3$. Looking at the contributions to the Néron–Tate height from the fiber configuration, one easily sees that there cannot be any 2- or 3-torsion. Similarly, it is impossible to have a section of height $\frac{1}{20}$ or $\frac{1}{45}$. Therefore, this sublattice must be the entire Néron–Severi lattice, and P_1 is a generator of the Mordell–Weil group.

26.3. Examples. Table 21 lists some points of small height and their genus-2 curves.

(r, s)	Sextic polynomial $f_6(x)$ defining the genus-2 curve $y^2 = f_6(x)$
$\left(\frac{5}{6}, \frac{5}{2}\right)$	$-144x^6 - 336x^5 + 491x^4 - 274x^3 + 4919x^2 - 23076x - 6476$
$\left(\frac{5}{7}, \frac{10}{3}\right)$	$-108456x^6 + 89940x^5 + 3518x^4 + 11915x^3 + 29021x^2 - 40515x + 2841$
$\left(\frac{10}{3}, \frac{5}{7}\right)$	$-7146x^6 + 26076x^5 + 26698x^4 - 128487x^3 - 87881x^2 + 140967x + 106899$
$\left(\frac{9}{14}, 3\right)$	$-205648x^6 - 71112x^5 + 4931x^4 - 3219x^3 - 1369x^2 + 336x + 64$
$\left(3, \frac{9}{14}\right)$	$-47792x^6 + 212184x^5 - 134731x^4 - 131082x^3 + 58025x^2 + 39900x + 3500$
$\left(\frac{5}{2}, \frac{5}{6}\right)$	$111132x^6 + 308700x^5 + 150199x^4 - 166350x^3 - 85877x^2 + 37080x + 3208$
$\left(\frac{5}{4}, -\frac{25}{3}\right)$	$-203124x^6 + 537156x^5 - 1147529x^4 - 958036x^3$ $- 185681x^2 + 583356x - 97236$
$\left(\frac{31}{18}, 3\right)$	$-4138876x^6 - 12791196x^5 - 14043627x^4 - 2580588x^3$ $- 2332545x^2 - 7239150x - 962750$
$\left(\frac{97}{34}, 3\right)$	$-4774900x^6 + 11612125x^5 - 1487685x^4 - 13117009x^3$ $+ 29039993x^2 + 24527448x - 2106844$
$\left(3, -\frac{13}{9}\right)$	$-1749188x^6 + 9004404x^5 - 5544841x^4 - 13022828x^3$ $- 36459313x^2 + 31091676x + 62509084$
$\left(3, \frac{31}{18}\right)$	$1490720x^6 + 34810248x^5 + 203477725x^4 - 39952362x^3$ $- 392594159x^2 + 53751372x - 121943204$
$\left(\frac{31}{5}, \frac{5}{6}\right)$	$354444x^6 + 2968308x^5 - 37732823x^4 + 4713146x^3$ $+ 223323505x^2 + 714572220x - 955946700$
$\left(-\frac{25}{3}, \frac{5}{4}\right)$	$-28660432x^6 - 9277032x^5 - 367100597x^4 + 64181262x^3$ $- 1142233133x^2 + 827398968x - 146839168$
$\left(\frac{9}{8}, \frac{29}{13}\right)$	$953161100x^6 - 1709768900x^5 + 57159815x^4 - 997590336x^3$ $- 322970431x^2 - 72177962x + 2546122$
$\left(\frac{5}{6}, \frac{31}{5}\right)$	$6865596x^6 - 82041816x^5 + 58608103x^4 + 1250964773x^3$ $+ 921256891x^2 - 4495870224x - 3609058132$
$\left(-\frac{53}{7}, \frac{71}{57}\right)$	$-125838448x^6 + 33513120x^5 - 1068122125x^4 + 1220630640x^3$ $- 2407159591x^2 + 4627695870x - 2358802782$

Table 21. Some rational points (r, s) of small height on the surface of Theorem 36 and the corresponding genus-2 curves.

By pulling back some of the low-height sections of the quotient, we produce curves of low genus on $Y_-(69)$. Since $r + s = m$ and $rs = n$, the appropriate condition is that $m^2 - 4n = (r - s)^2$ be a square (then we can take a square root and solve for r, s). In other words, $(n + k)^2 - 4n$ must be a square. The section P_1 is given by $n = -(5k^2 - 17k + 15)/(k - 2)$; it gives rise to a genus-1 curve

$$y^2 = 16k^4 - 100k^3 + 237k^2 - 254k + 105,$$

which has rational points (for instance, at infinity). It is therefore an elliptic curve, and we calculate that it has conductor 1711 (prime) and Mordell–Weil group $\mathbb{Z}^2$.

Similarly, the section $-P_1$ is defined by $n = -(25k^2 - 92k + 89)/(10k - 21)$. It also gives rise to a genus-1 curve

$$y^2 = 225k^4 - 1130k^3 + 1931k^2 - 1350k + 445$$

with rational points (as at $k = \infty$). It is an elliptic curve of conductor $50435 = 5 \cdot 7 \cdot 11 \cdot 131$, with trivial torsion and rank 1.

27. Discriminant 73

27.1. Parametrization. Start with a K3 elliptic surface with fibers of type A_6, A_9 and a section of height $\frac{73}{70} = 4 - \frac{21}{10} - \frac{6}{7}$. The Weierstrass equation is

$$y^2 = x^3 + (a_0 + a_1t + a_2t^2 + a_3t^3 + a_4t^4)x^2$$
$$+ 2\mu t(b_0 + b_1t + b_2t^2 + b_3t^3)x + \mu^2 t^2(c_0 + c_1t + c_2t^2),$$

with

$$\mu = -2s^4(s + 2r)^2, \qquad a_0 = s^2(rs - 2r - 2)^2, \qquad a_4 = 16r^2(r + 1)^2,$$
$$b_0 = s(rs - 2r - 2)^2, \qquad b_3 = 4r(r + 1)^2(s + 2r + 2), \quad c_0 = (rs - 2r - 2)^2,$$
$$c_2 = (r + 1)^2(s + 2r + 2)^2,$$
$$a_3 = 8r(r + 1)\big((r + 1)s^2 + 2(4r + 1)s + 4r(r - 1)\big),$$
$$c_1 = -2(s + 2r + 2)\big(s^2 + (r + 2)(r - 1)s - 2(r^2 - 1)\big),$$
$$b_1 = -3s^4 - 2r(r + 5)s^3 - 2(r^3 + 4r^2 - 2r - 2)s^2 - 8(r + 1)s + 8r(r + 1)^2,$$
$$a_1 = -2s\big(3s^4 + r(r + 11)s^3 + 2(5r^2 - r - 1)s^2 + 4(r + 1)(r^2 + 1)s - 8r(r + 1)^2\big),$$
$$b_2 = (r + 1)^2s^3 + 2(r^3 + 7r^2 + 6r + 2)s^2$$
$$+ 4(4r^3 + 8r^2 + 7r + 1)s + 8(r - 1)r(r + 1)(r + 2),$$
$$a_2 = (r + 1)^2s^4 + 4(4r^2 + 3r + 1)s^3 + 4(4r^3 + 10r^2 + 10r + 1)s^2$$
$$+ 16r(r + 1)(r - 2)s + 16r^2(r + 1)^2.$$

We first identify the class of an E_8 fiber, and perform a 3-neighbor step to move to an elliptic fibration with E_8 and A_7 fibers.
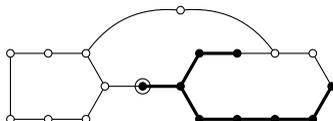
This fibration has a section of height $\frac{73}{8} = 4 + 2 \cdot 3 - \frac{7}{8}$. Next, we locate an E_7 fiber and compute a 2-neighbor step to go to a fibration with E_8 and E_7 fibers.
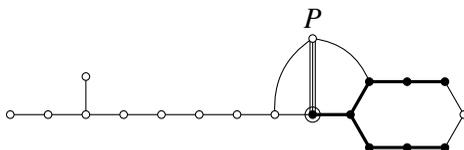
The intersection number of the new fiber F' with the remaining component of the A_7 fiber is 2 and with the section P is 9. Therefore, the new genus-1 fibration defined by F' has a section since 9 and 2 are coprime.

Theorem 37. *A birational model over $\mathbb{Q}$ for the Hilbert modular surface $Y_-(73)$ as a double cover of $\mathbb{P}^2_{r,s}$ is given by the equation*

$$z^2 = 16(s-2)^2 r^4 + 8(s-2)(17s^3 - 52s^2 + 36s - 8)r^3$$
$$+ (s^6 + 56s^5 - 384s^4 + 448s^3 + 432s^2 - 512s + 64)r^2$$
$$+ 2s(s+2)(s^4 - 34s^3 + 108s^2 - 64s + 16)r + s^2(s+2)^4.$$

It is an honestly elliptic surface, with arithmetic genus 2 and Picard number 28.

27.2. *Analysis.* The branch locus is a curve of genus 2; the transformation of coordinates

$$r = \frac{3x^3 y - 3xy + y - x^6 - 2x^5 - 4x^4 - 3x^2 + 4x - 1}{2x^2(x^2 + 2x - 1)^2},$$

$$s = -2\frac{(2xy - y - x^3 - 7x^2 + 3x)}{(x+1)^2(x^2 + 2x - 1)}$$

converts it to Weierstrass form

$$y^2 = x^6 + 4x^5 + 2x^4 - 6x^3 + x^2 - 2x + 1.$$

This is a genus-2 curve, isomorphic to the quotient of $X_0(73)$ by the Atkin–Lehner involution.

The Hilbert modular surface $Y_-(73)$ is an elliptic surface. Since the coefficient of r^4 is a square, this genus-1 curve over $\mathbb{P}^1_s$ has a section. Computing the Jacobian,

we get the following Weierstrass equation after a change of parameter on the base
and some simple Weierstrass transformations:

$$y^2 = x^3 - (83t^6 - 316t^5 + 390t^4 - 158t^3 - 21t^2 + 22t - 1)x^2$$
$$+ 8(t-1)^4 t^3 (287t^5 - 1040t^4 + 960t^3 - 73t^2 - 217t + 67)x$$
$$- 16(t-1)^7 t^6 (1323t^5 - 5887t^4 + 7110t^3 - 1426t^2 - 2201t + 1033).$$

This is an honestly elliptic surface with $\chi = 3$. It has reducible fibers of type
I_7 at $t = 1$, I_6 at $t = 0$, I_5 at $t = \infty$, I_3 at $t = (-5 \pm \sqrt{73})/4$, and I_2 at $t = -1$
and $(13 \pm \sqrt{73})/24$. The trivial lattice therefore has rank 24, leaving room for
Mordell–Weil rank at most 6.

We find the following four independent sections.

$$P_1 = \left(4t^3(t-1)^2(9t-7), \; 4t^3(t-1)^2(t+1)(3t-2)(2t^2+5t-6)\right),$$
$$P_2 = \left(4t^3(t-1)(7t^2-17t+8), \; 4t^3(t-1)(t+1)(9t^2-13t+5)\right),$$
$$P_3 = \left(4t^2(t-1)^3(19t-16), \; 4t^2(t-1)^3(7t^2-12t+8)(12t^2-13t+2)\right),$$
$$P_4 = \big(4t^3(7t^3-24t^2-2\mu t+42t-2\mu+9),$$
$$(-13+\mu)t^3(t+1)(-24t+13+\mu)(-17-16t+3\mu)(-4t-5+\mu)/192\big)$$

(where $\mu = \sqrt{73}$), with nondegenerate height pairing matrix

$$\begin{pmatrix} \frac{26}{21} & \frac{5}{7} & -\frac{1}{7} & -\frac{2}{3} \\ \frac{5}{7} & \frac{68}{35} & \frac{11}{7} & -\frac{1}{5} \\ -\frac{1}{7} & \frac{11}{7} & \frac{41}{21} & \frac{1}{2} \\ -\frac{2}{3} & -\frac{1}{5} & \frac{1}{2} & \frac{49}{30} \end{pmatrix}.$$

Therefore, the Mordell–Weil rank is at least 4. From Oda's calculations [1982,
p. 109], the Picard number is 28, so the Mordell–Weil rank is $28 - 24 = 4$ and
our sections generate a subgroup of finite index in the full Mordell–Weil group.
The sublattice of the Néron–Severi lattice generated by the trivial lattice and these
sections has discriminant $3916 = 2^2 \cdot 11 \cdot 89$. We checked that this sublattice is
2-saturated, and therefore it is the entire Néron–Severi lattice.

27.3. *Examples*. Table 22 lists some points of small height and their genus-2
curves.

We get many curves of genus 0 on the surface by taking sections of the elliptic
fibration. For instance, the Brauer obstruction vanishes for the two curves defined by
$r = -(s-4)(s+2)/(4(s-2))$ and $r = s(s+2)/((s-2)(3s-2))$, yielding families
of genus-2 curves parametrized by s, whose Jacobians have real multiplication
by $\mathcal{O}_{73}$.

(r, s)	Sextic polynomial $f_6(x)$ defining the genus-2 curve $y^2 = f_6(x)$
$\left(-\frac{10}{3}, \frac{4}{3}\right)$	$-4x^6 - 12x^5 - 23x^4 + 4x^3 + 31x^2 + 57x - 18$
$(-3, 1)$	$4x^6 - 3x^4 - 35x^3 + 12x + 76$
$(5, 3)$	$-4x^6 - 24x^5 + 7x^4 + 83x^3 + 25x^2 - 75x - 40$
$\left(\frac{9}{4}, 3\right)$	$-15x^5 + 73x^4 - 41x^3 - 158x^2 - 12x + 36$
$\left(-5, \frac{3}{2}\right)$	$-50x^6 + 45x^5 - 2x^4 - 159x^3 + 70x^2 + 12x - 120$
$\left(\frac{5}{6}, -2\right)$	$-48x^6 + 168x^5 - 149x^4 + 56x^3 - 53x^2 + 12x - 4$
$\left(-\frac{5}{12}, -1\right)$	$195x^6 + 82x^5 - 75x^4 - 186x^3 - 233x^2 - 96x - 87$
$\left(\frac{5}{3}, \frac{1}{2}\right)$	$-60x^6 - 105x^5 + 55x^4 + 49x^3 + 13x^2 + 252x + 116$
$\left(-\frac{2}{3}, -\frac{2}{5}\right)$	$-36x^6 + 39x^5 - 217x^4 + 129x^3 - 271x^2 - 108x + 84$
$\left(\frac{5}{4}, -6\right)$	$20x^6 + 84x^5 - 15x^4 - 162x^3 + 225x^2 + 324x - 180$
$\left(\frac{9}{5}, -8\right)$	$-204x^6 + 348x^5 + 27x^4 + 34x^3 + 3x^2 + 108x - 36$
$\left(-\frac{1}{3}, \frac{4}{5}\right)$	$-25x^6 + 135x^5 + 139x^4 - 383x^3 + 82x^2 + 252x - 162$
$\left(\frac{9}{14}, -2\right)$	$-48x^6 - 72x^5 - 219x^4 - 319x^3 - 159x^2 - 432x + 192$
$\left(-\frac{14}{5}, 12\right)$	$-440x^6 + 90x^5 + 324x^4 + 38x^3 - 9x^2 - 36x - 8$
$\left(-\frac{9}{4}, 1\right)$	$-455x^6 - 420x^5 + 66x^4 - 167x^3 - 15x^2 - 3x - 6$
$\left(\frac{6}{5}, 4\right)$	$-160x^6 + 450x^5 - 114x^4 - 474x^3 + 171x^2 + 162x - 27$

Table 22. Some rational points (r, s) of small height on the surface
of Theorem 37 and the corresponding genus-2 curves.

28. Discriminant 76

28.1. *Parametrization.* Start with a K3 elliptic surface with fibers of type A_6, A_2
and D_7, and a section of height $\frac{76}{84} = \frac{19}{21} = 4 - 1 - \frac{2}{3} - \frac{10}{7}$. The Weierstrass equation
of this family is

$$y^2 = x^3 + (a_0 + a_1 t + a_2 t^2 + a_3 t^3)x^2 + t^2(b_0 + b_1 t + b_2 t^2)x + t^4(c_0 + c_1 t + c_2 t^2),$$

with

$c_0 = (r^2 - 1)^2 s^4 (2s - r + 1)^2 (2s + r + 1)^2/16,$

$b_0 = (r^2 - 1)s^2 (2s - r + 1)(2s + r + 1)/2,$

$a_3 = (r^2 - 1)(s + 1)^6,$
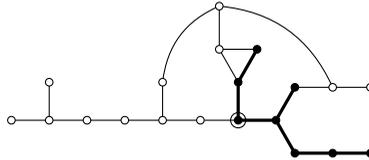
$a_1 = r^2 s^2 - 5s^2 + r^2 s - 7s + r^2 - 3,$

$c_2 = (r^2 - 1)^2 r^2 s^6 (s + 1)^6,$

$a_2 = (s + 1)^2 (r^2 s^2 + 3s^2 - 3r^2 s + 7s - 2r^2 + 3),$

$a_0 = 1,$

$b_2 = (r^2 - 1)s^2(s+1)^4(2r^2s^2 + 6s^2 - 2r^2s + 6s + r^4 - 2r^2 + 1)/2,$

$c_1 = (r^2 - 1)^2 s^4 (s+1)^2 (2s - r + 1)(2s + r + 1)$
$$\times (4r^2s^2 - 12s^2 - 8s - r^4 + 2r^2 - 1)/16,$$

$b_1 = -(r^2 - 1)s^2\big((2s^2 + 3s + 2)r^4 - 2(4s^4 + 8s^3 + 10s^2 + 8s + 3)r^2$
$$+ (2s + 1)(16s^3 + 32s^2 + 21s + 4)\big)/4.$$

We identify the class of an E_7 fiber:

The resulting 3-neighbor step gives us an elliptic fibration with D_8 and E_7 fibers, and also a section P of height $\frac{19}{2} = 4 + 2 \cdot 4 - \frac{3}{2} - 1$. Next we take a 2-neighbor step to go from D_8 to E_8, keeping the E_7 fiber intact.
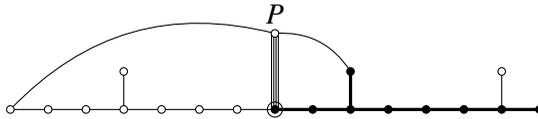
The intersection number of F' with the remaining component of the D_8 fiber is 2, whereas $P \cdot F' = 11$. Therefore the new fibration has a section.

Now we may read out the Igusa–Clebsch invariants from the Weierstrass equation of this $E_8 E_7$ fibration, and thence compute the equation of $Y_-(76)$ as a double cover of the r, s-plane, following our general method of Section 4.

Theorem 38. *A birational model over $\mathbb{Q}$ for the Hilbert modular surface $Y_-(76)$ as a double cover of $\mathbb{P}^2$ is given by the equation*

$$z^2 = -(rs - 3s - 2)(rs + 3s + 2)(32s^4 + 80s^3 - 13r^2s^2 + 85s^2 - 4r^2s + 32s + 4r^4).$$

It is a surface of general type.

28.2. Analysis. The branch locus has three components; the more complicated one is where the elliptic K3 surface has an extra I_2 fiber, while the two simpler components correspond to an extra I_2 fiber as well as the section becoming divisible by 2, giving a section of height $\frac{19}{84} = 4 - \frac{1}{2} - \frac{2}{3} - \frac{6}{7} - \frac{7}{4}$. The simpler components are easily seen to be curves of genus 0. The last component is a curve of genus 1; the transformation

$$(r, s) = \left(\frac{2y + x + 1}{x^2 + x + 2}, \frac{-2}{x^2 + x + 2} \right)$$

converts it to Weierstrass form

$$y^2 + xy + y = x^3 + x^2 + 1,$$

which is an elliptic curve of conductor 38. It is isomorphic to $X_0(76)/\langle w_4, w_{19} \rangle$.

The Hilbert modular surface $Y_-(76)$ is a surface of general type. The extra involution is $\iota : (r, s) \mapsto (-r, s)$. Next, we analyze the quotient of the surface by ι. This turns out to be an elliptic K3 surface, and after some Weierstrass transformations and linear shift of parameter on the base, its Weierstrass equation may be written as

$$y^2 = x^3 + (13t^4 - 48t^3 - 6t^2 + 8t + 1)x^2 + 64t^4(2t - 1)(t^3 - 5t^2 + 7t + 1)x.$$

It has fibers of type I_8 at $t = 0$, I_5 at $t = 1$, I_3 at $t = -\frac{1}{7}$, and I_2 at $t = \frac{1}{2}$ and at the roots of $t^3 - 5t^2 + 7t + 1$ (which generates the cubic field of discriminant -76). The trivial lattice has rank 19. In addition to the obvious 2-torsion section $P_0 = (0, 0)$, we find a section $P_1 = (16t^3(2t - 1), 16t^3(t - 1)(2t - 1)(7t + 1))$ of height $\frac{19}{120}$. Therefore the K3 surface is singular. These sections and the trivial lattice generate a sublattice of the Néron–Severi lattice of discriminant -76. It must be the entire Néron–Severi lattice, since otherwise, we would have either another 2-torsion section, a 4-torsion section, or a section of height $\frac{19}{480}$, none of which is possible with this configuration of reducible fibers.

The quotient of $Y_-(76)$ by the involution $(r, s, z) \mapsto (-r, s, -z)$ is an honestly elliptic surface with $\chi = 3$. Its Weierstrass equation may be written as follows:

$$y^2 = x^3 + (t - 1)(64t^5 - 160t^4 + 53t^3 + 33t^2 - 5t - 1)x^2$$
$$+ 16(t - 1)t^4(2t - 1)(t^3 - 5t^2 + 7t + 1)(32t^3 - 16t^2 + 21t - 5)x.$$

It has bad fibers of type I_8 at $t = 0$, I_4 at $t = \infty$ and $t = \frac{1}{3}$, III at $t = 1$, I_3 at $t = -\frac{1}{7}$, and I_2 at $t = \frac{1}{2}$, at the roots of $t^3 - 5t^2 + 7t + 1$ seen above, and at the roots of $32t^3 - 16t^2 + 21t - 5$ (which generates the cubic field of discriminant -152). Hence the trivial lattice has rank 25, leaving room for Mordell–Weil rank at most 5. Counting points on the reduction modulo 11 and 23 shows that the Picard number is at most 29. On the other hand, we find three independent sections in addition to the 2-torsion section $P_0 = (0, 0)$:

$$P_1 = \left(152(t - 1)t^4(2t - 1), \ 8\mu(t - 1)t^4(2t - 1)(3t - 1)(4t - 3)(7t + 1)\right),$$
$$P_2 = \left(4(t^3 - 5t^2 + 7t + 1)t^3, \ 4t^3(2t - 1)(3t - 1)^2(t^3 - 5t^2 + 7t + 1)\right),$$
$$P_3 = \left(-(t - 1)^3(32t^3 - 16t^2 + 21t - 5), \ 2\nu(t - 1)^2(3t - 1)^2(32t^3 - 16t^2 + 21t - 5)\right).$$

Here $\mu = \sqrt{19}$ and $\nu = \sqrt{-1}$. These sections have heights $\frac{23}{12}$, $\frac{9}{8}$ and $\frac{13}{8}$ respectively, and are orthogonal with respect to the height pairing. Therefore, the Mordell–Weil rank is either 3 or 4; we have not been able to determine it exactly.

(r, s)	Sextic polynomial $f_6(x)$ defining the genus-2 curve $y^2 = f_6(x)$
$\left(-\frac{4}{11}, -\frac{8}{11}\right)$	$-8x^6 + 48x^5 - 196x^4 + 324x^3 - 340x^2 - 330x - 65$
$(2, -4)$	$375x^6 + 300x^5 + 230x^4 - 224x^3 - 76x^2 - 48x + 72$
$\left(\frac{7}{3}, -\frac{1}{3}\right)$	$-80x^6 - 120x^5 - 109x^4 - 348x^3 - 469x^2 - 120x + 80$
$(-2, -4)$	$-225x^6 + 600x^5 + 650x^4 + 400x^3 + 20x^2 - 8$
$\left(\frac{13}{23}, -\frac{19}{23}\right)$	$-228x^6 + 684x^5 - 1029x^4 - 432x^3 + 525x^2 + 150x + 10$
$\left(-\frac{7}{3}, -\frac{1}{3}\right)$	$100x^6 - 220x^5 + 621x^4 - 528x^3 + 1699x^2 - 234x + 1478$
$\left(\frac{19}{33}, -\frac{9}{11}\right)$	$256x^6 - 1056x^5 - 2335x^4 + 1480x^3 + 1715x^2 - 1386x + 126$
$\left(\frac{19}{11}, \frac{1}{11}\right)$	$-2232x^6 - 2016x^5 + 2581x^4 + 2802x^3 - 983x^2 - 660x - 180$
$\left(\frac{47}{37}, -\frac{43}{37}\right)$	$3100x^6 - 540x^5 - 271x^4 - 1742x^3 + 161x^2 + 84x + 252$
$\left(\frac{43}{27}, \frac{29}{27}\right)$	$-592x^6 + 372x^5 + 1003x^4 + 1328x^3 - 1406x^2 - 132x - 3709$
$\left(-\frac{19}{33}, -\frac{9}{11}\right)$	$-4404x^6 - 540x^5 - 1697x^4 - 980x^3 - 257x^2 - 240x - 64$
$\left(\frac{22}{17}, -\frac{20}{17}\right)$	$600x^6 - 3360x^5 + 3604x^4 + 2256x^3 + 4546x^2 + 1440x + 775$
$\left(-\frac{22}{13}, -\frac{20}{13}\right)$	$-367x^6 - 618x^5 - 1539x^4 + 316x^3 + 1839x^2 + 4662x + 3507$
$\left(-\frac{1}{23}, -\frac{31}{46}\right)$	$-2245x^6 - 137x^5 - 5393x^4 - 1675x^3 - 3618x^2 - 1728x - 675$
$\left(\frac{22}{13}, -\frac{20}{13}\right)$	$1425x^6 - 2610x^5 + 6333x^4 - 4948x^3 + 8271x^2 - 4242x + 5971$
$\left(-\frac{1}{23}, -\frac{17}{23}\right)$	$24x^6 + 552x^5 + 2075x^4 - 1970x^3 - 9925x^2 + 9072x + 1216$

Table 23. Some rational points (r, s) of small height on the surface of Theorem 38 and the corresponding genus-2 curves.

28.3. *Examples*. Table 23 lists some points of small height and their genus-2 curves.

We now describe some curves on $Y_-(76)$, which are useful in producing rational points.

The specialization $s = -\frac{2}{3}$ gives a genus-1 curve $y^2 = -81r^4 + 63r^2 + 19$. It has rational points, such as $(r, y) = (1, 1)$. It is thus an elliptic curve; we find that it has conductor 760 and Mordell–Weil group $(\mathbb{Z}/2\mathbb{Z}) \oplus \mathbb{Z}$. The specialization $s = -\frac{8}{7}$ gives a rational curve, which we can parametrize as $r = -5(m^2 - 1)/(4(m^2 + 1))$.

The sections P_1, $P_1 + P_0$, $2P_1 + P_0$ and $3P_1 + P_0$ of the K3 quotient give the following genus-1 curves, which all have rational points.

Equation	conductor	Mordell–Weil group
$r^2 = -(8s^3 + 28s^2 + 27s + 8)/s$	$2 \cdot 29$	$\mathbb{Z}$
$r^2 = -(s^3 - s^2 - 11s - 8)/s$	$2^4 \, 11 \cdot 191$	$\mathbb{Z}^2$
$r^2 = -(8s^4 + 4s^3 - 33s^2 - 44s - 16)/(s + 2)^2$	$3^5 \, 19$	$\mathbb{Z}^2$
$r^2 = -(s^4 + s^3 - 3s^2 - s + 1)$	$2^2 \, 5 \cdot 29$	$(\mathbb{Z}/2\mathbb{Z}) \oplus \mathbb{Z}$

The section $2P_1$ gives a genus-0 curve $r^2 + s^2 + 6s + 4 = 0$, which we can parametrize as

$$(r, s) = \left(-\frac{m^2 + 4m - 1}{m^2 + 1}, -\frac{m^2 + 2m + 5}{m^2 + 1} \right).$$

The Brauer obstruction always vanishes on this locus, giving us a 1-parameter family of genus-2 curves whose Jacobians have real multiplication by $\mathcal{O}_{76}$.

29. Discriminant 77

29.1. *Parametrization*. We start with a family of K3 surfaces with fibers of type A_1, A_3, A_5 and D_5, a 2-torsion section T, and two orthogonal sections P, Q of height $\frac{11}{12} = 4 - 0 - \frac{2 \cdot 2}{4} - \frac{1 \cdot 5}{6} - (1 + \frac{1}{4})$ and $\frac{7}{4} = 4 - 0 - \frac{1 \cdot 3}{4} - \frac{3 \cdot 3}{6} - 0$. The orthogonality comes from $0 = 2 - 0 - \frac{1 \cdot 2}{4} - \frac{1 \cdot 3}{6} - 0 - 1$, where the last term comes from the intersection number $(P) \cdot (Q)$ on the surface. We can write the Weierstrass equation of this family as

$$\begin{aligned}
y^2 = x^3 &+ \big((rs - 1)^2 - (s^2 - 1)(rs - 4r^2 - 1)t \\
&+ r(s^2 - 1)(rs^2 + 8s - 57r)t^2/4 + 8r^2(s^2 - 1)t^3\big)x^2 \\
&+ r^2(s^2 - 1)^2 t^3 (t - 1)^2 \big(16r^2 t + (rs - 1)^2 - (s - 5r)^2\big)x.
\end{aligned}$$

We go to $E_8 E_7$ form in three steps, via $D_8 E_6$ and $E_8 E_6$.

First, we identify a D_8 fiber F' in the figure below (we omit drawing the node representing Q and the edges connecting it to the rest of the diagram, as it would clutter up the picture).
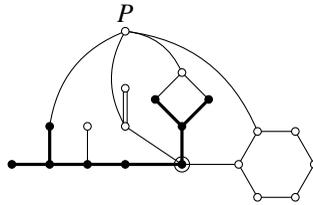
The section P intersects F' once, and so the new fibration has a section. It has D_8 and E_6 fibers and rank 2.

Next, we identify the class of an E_8 fiber below, and go to an elliptic fibration with E_8 and E_6 fibers, by a 2-neighbor step.

The resulting elliptic fibration has Mordell–Weil lattice of rank 2 and discriminant $\frac{77}{3}$. We can relatively easily describe a section P'' of height $\frac{8}{3}$, which intersects a non-identity component of the E_6 fiber.

Now the E_7 fiber F''' drawn below defines an elliptic fibration with a section and with E_8 and E_7 fibers.

We now read out the Igusa–Clebsch invariants and proceed as in Section 4 to compute the equation of $Y_-(77)$ as a double cover of the Humbert surface $\mathcal{H}_{77}$.

Theorem 39. *A birational model over $\mathbb{Q}$ for the Hilbert modular surface $Y_-(77)$ as a double cover of $\mathbb{P}^2$ is given by the equation*

$$z^2 = r^2(r-1)^2(r+1)^2 s^6 + 2r(r-1)(r+1)(21r^2 - 13)s^5$$
$$- (14r^6 - 433r^4 + 328r^2 + 27)s^4 - 4r(281r^4 - 522r^2 - 79)s^3$$
$$- (343r^6 + 6268r^4 + 1763r^2 - 54)s^2 + 2r(3997r^4 + 2446r^2 - 171)s$$
$$- (1372r^6 + 4531r^4 - 362r^2 + 27).$$

It is a surface of general type.

29.2. Analysis. It is a surface of general type. It has an extra involution $(r, s) \mapsto (-r, -s)$. The branch locus is a curve of genus 2. The change of coordinates

$$(r, s) = \left(\frac{4xy - 5x^4 - 22x^2 - 21}{x(x^2 + 7)^2}, \frac{-(2x^2 y + 2y - x^5 - 6x^3 - 9x)}{(x^2 - 1)^2} \right)$$

(r, s)	Sextic polynomial $f_6(x)$ defining the genus-2 curve $y^2 = f_6(x)$
$\left(-\frac{1}{2}, -\frac{23}{5}\right)$	$1581x^6 - 25965x^5 + 128199x^4 - 124655x^3 - 282240x^2 - 92400x - 9478$
$\left(-\frac{3}{5}, -\frac{47}{9}\right)$	$926711x^6 - 351913x^5 - 2531791x^4 + 699677x^3 + 2176646x^2$ $- 359536x - 579882$
$\left(\frac{1}{2}, \frac{23}{5}\right)$	$2038350x^6 + 1601640x^5 - 6288456x^4 + 116705x^3 - 5729115x^2$ $- 8845053x - 2931103$
$\left(-\frac{13}{2}, 6\right)$	$10433826x^6 - 16243110x^5 + 25749477x^4 - 25899800x^3 + 5297523x^2$ $- 6454140x - 9577876$
$\left(\frac{13}{2}, -6\right)$	$-749865564x^6 + 4317895148x^5 + 1178682897x^4 - 6739621816x^3$ $- 800208729x^2 + 2973824982x + 128797182$
$\left(-\frac{33}{65}, -\frac{239}{63}\right)$	$-5738303278944x^6 + 6551435295576x^5$ $+ 28045528925148x^4 - 5100723398753x^3 - 23656013198837x^2$ $+ 3333165270637x + 3904336668117$

Table 24. Some rational points (r, s) of small height on the surface of Theorem 39 and the corresponding genus-2 curves.

converts it to Weierstrass form

$$y^2 = x^6 + 5x^4 + 3x^2 + 7.$$

It is isomorphic to the quotient of $X_0(77)$ by the Atkin–Lehner involution w_{77}.

29.3. *Examples.* Table 24 on the previous page lists some points of small height and their genus-2 curves.

30. Discriminant 85

30.1. *Parametrization.* We start with a K3 elliptic surface with fibers of type E_6, D_5 and A_4, with a section of height $\frac{85}{60} = \frac{17}{12} = 4 - \frac{4}{3} - \frac{5}{4}$.
  The Weierstrass equation is

$$y^2 = x^3 + t(a_0 + a_1 t) x^2 + 2t^2(t-1)(b_0 + b_1 t) x + t^3(t-1)^4(c_0 + c_1 t),$$

with

$$a_0 = -4(e^2 - 1)(3ef^2 + 2e^2 f + 2f - 2e^2 + e + 2),$$
$$c_0 = -64e^2(e^2 - 1)^3(f^2 - 1)^2(f + 2e + 1)(ef - e + 2),$$
$$a_1 = 4(e^2 - 1)^2 f^2,$$
$$b_0 = 8e(e^2 - 1)^2(f^2 - 1)(3ef^2 + 4e^2 f + 4f - 4e^2 + 5e + 4),$$
$$b_1 = -8f(e^2 - 1)^2(f^2 - 1)(e^4 f + e^3 f - ef + f - e^4 + e^3 + e + 1),$$
$$c_1 = 16(e^2 - 1)^2(f^2 - 1)^2(e^4 f + e^3 f - ef + f - e^4 + e^3 + e + 1)^2.$$

We identify the class of a D_8 fiber below, and move to the new elliptic fibration via a 2-neighbor step.
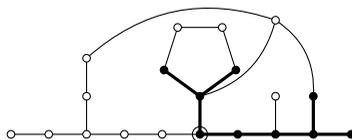
The new elliptic fibration has reducible fibers of type D_8 and E_6, and Mordell–Weil rank 2. Next, we move to an elliptic fibration with E_8 and E_6 fibers by another 2-neighbor step, using the E_8 fiber shown below.
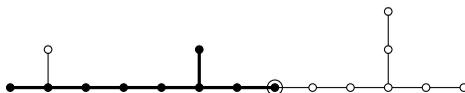
The new elliptic fibration has E_8 and E_6 fibers. We can find an explicit section P of the $E_8 E_6$ fibration which intersects a non-identity component of the E_6 fiber and does not intersect the zero section.

Let F be an E_7 fiber enclosed by the box in the picture below. We move to it by a 2-neighbor step, to recover an elliptic fibration with E_8 and E_7 fibers.
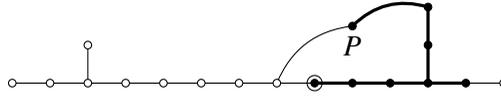
We may now read out the Igusa–Clebsch invariants, and work out the equation of $Y_-(85)$ as a double cover of $\mathbb{P}^2_{e,f}$.

Theorem 40. *A birational model over $\mathbb{Q}$ for the Hilbert modular surface $Y_-(85)$ as a double cover of $\mathbb{P}^2_{e,f}$ is given by the equation*

$$
\begin{aligned}
z^2 = {} & -(e^2 - e - 1)^2(8e^4 + 11e^2 + 8)f^4 \\
& + 4(e^4 - 1)(18e^4 - 11e^3 + 27e^2 + 11e + 18)f^3 \\
& - 2(82e^8 - 118e^7 - 9e^6 - 60e^5 - 173e^4 + 60e^3 - 9e^2 + 118e + 82)f^2 \\
& + 4(e^4 - 1)(4e^2 - 5e - 4)(9e^2 - 13e - 9)f \\
& - (2e^2 - e - 2)^2(11e^4 - 34e^3 + 5e^2 + 34e + 11).
\end{aligned}
$$

It is an honestly elliptic surface, of arithmetic genus 3 and Picard number 37 or 38.

30.2. Analysis. It is an honestly elliptic surface, with extra involution $\iota : (e, f, z) \mapsto (-1/e, -f, z/e^4)$.

The branch locus is a hyperelliptic curve of genus 3. The change of coordinates

$$
(e, f) = \left(\frac{y + x^4 + x^3 - x + 1}{2x^2 + 2x - 1}, \ \frac{(3x^4 + x^3 - 3x^2 - x + 3)y - (x^2 - 1)(x^2 + 1)^3}{(x^2 + x - 1)^2(2x^4 - x^2 + 2)} \right)
$$

converts it to Weierstrass form:

$$
y^2 = x^8 + 2x^7 - x^6 - 8x^5 + x^4 + 8x^3 - x^2 - 2x + 1.
$$

It is isomorphic to the quotient of $X_0(85)$ by the Atkin–Lehner involution w_{85}.

The equation of $Y_-(85)$ describes it as an elliptic surface over $\mathbb{P}^1_e$. So far, we are unable to find a section.

The Jacobian of this genus-1 curve over $\mathbb{Q}(e)$ can be written (after some Weierstrass transformations) as

$$
\begin{aligned}
y^2 = {} & x^3 + (e^8 - 10e^7 + 3e^6 + 84e^5 + 85e^4 - 84e^3 + 3e^2 + 10e + 1)x^2 \\
& - 8e^5(23e^6 - 133e^5 - 420e^4 - 64e^3 + 420e^2 - 133e - 23)x \\
& - 16e^9(108e^6 - 637e^5 - 1944e^4 - 26e^3 + 1944e^2 - 637e - 108).
\end{aligned}
$$

It has $\chi = 4$. There are bad fibers of type I_9 at $e = 0$ and $e = \infty$, I_3 at $e = \pm 1$, I_2 at the roots of $e = 4 \pm \sqrt{17}$, and I_3 at the roots of $3e^6 - 16e^5 - 54e^4 + 5e^3 + 54e^2 - 16e - 3$

(which generates the compositum of $\mathbb{Q}(\sqrt{85})$ and the cubic field of discriminant $-3 \cdot 5 \cdot 17$). The trivial lattice has rank 36, leaving room for at most four independent sections. So far, we can only say from the ensuing analysis that the rank is either 1 or 2.

Next, we analyze the quotient of this surface by the involution ι. In terms of $g = e - 1/e$ and $h = f/(e + 1/e)$ (which are invariant under ι), its equation is

$$z^2 = -(g-1)^2(g^2+4)^2(8g^2+27)h^4 + 4g(g^2+4)^2(18g^2-11g+63)h^3$$
$$- 2(g^2+4)(82g^4 - 118g^3 + 319g^2 - 414g - 27)h^2$$
$$+ 4g(4g-5)(9g-13)(g^2+4)h - (2g-1)^2(11g^2 - 34g + 27).$$

This is also an honestly elliptic surface, this time with $\chi = 3$. Its Jacobian is

$$y^2 = x^3 + (g^2+4)(g^4 - 10g^3 + 7g^2 + 66g - 27)x^2$$
$$+ 8g(g-8)(g^2+4)^2(g^3 - 12g^2 - 12g + 27)x + 16g^2(g-8)^2(g^2+4)^3(g^2 - 14g - 27).$$

It has bad fibers of type I_9 at $g = \infty$, I_3 at $g = 0$, I_2 at $g = 8$, I_0^* at $g = \pm 2\sqrt{-1}$, and I_3 at the roots of $3g^3 - 16g^2 - 45g - 27$ (which generates the cubic field of discriminant -255). The trivial lattice has rank 27, leaving room for Mordell–Weil rank at most 3. Counting points modulo 11 and 19 shows that the Picard number is at most 29. On the other hand, we are able to find the non-torsion section

$$P_1 = \Big(-4(g-8)(g^2+4)(9g^3 + 3g^2 + g + 72)/85,$$
$$4(g-8)(21g-4)(g^2+4)^2(3g^3 - 16g^2 - 45g - 27)/85^{3/2}\Big)$$

of height $\frac{3}{2}$. Therefore, the Mordell–Weil rank is either 1 or 2.

Next, we consider the quadratic twist of the quotient elliptic surface, which is obtained by simply removing the factors of $(g^2 + 4)$ in the Weierstrass equation above (recalling that $g^2 + 4 = (e + 1/e)^2$). We get a K3 surface with a genus-1 fibration, whose Jacobian has Weierstrass equation

$$y^2 = x^3 + (g^4 - 10g^3 + 7g^2 + 66g - 27)x^2$$
$$+ 8g(g-8)(g^3 - 12g^2 - 12g + 27)x + 16g^2(g-8)^2(g^2 - 14g - 27).$$

It has reducible fibers of type I_9 at $g = \infty$, I_2 at $g = 8$, and I_3 at $g = 0$ and at the roots of $3g^3 - 16g^2 - 45g - 27$. Therefore the trivial lattice has rank 19, and the Mordell–Weil rank can be 0 or 1. We find a 3-torsion section

$$P_0 = (8g + 36, 4(3g^3 - 16g^2 - 45g - 27)).$$

Counting points modulo 7 and 19 shows that the Picard number is exactly 19. The 3-torsion section and trivial lattice span a sublattice of discriminant $162 = 2 \cdot 3^4$ of the Néron–Severi lattice of discriminant. It is easy to check that this sublattice is 3-saturated, and therefore must form the entire Néron–Severi lattice.

(e, f)	Sextic polynomial $f_6(x)$ defining the genus-2 curve $y^2 = f_6(x)$
$\left(\frac{1}{2}, -\frac{29}{15}\right)$	$576x^6 + 432x^5 + 927x^4 + 81x^3 + 171x^2 - 72x - 208$
$\left(\frac{4}{3}, \frac{1}{7}\right)$	$-1344x^6 - 672x^5 - 2233x^4 - 3026x^3 - 997x^2 - 2196x - 548$
$\left(\frac{7}{2}, \frac{8}{17}\right)$	$-1566x^6 - 7704x^5 - 4056x^4 - 8581x^3 - 5841x^2 - 2055x - 2395$
$\left(-2, \frac{29}{15}\right)$	$-3500x^6 - 2100x^5 + 11205x^4 + 2422x^3 - 11295x^2 + 1080x + 2160$
$\left(-2, \frac{23}{21}\right)$	$-316x^6 + 3048x^5 + 14649x^4 + 10547x^3 - 13509x^2 - 1296x + 1728$
$\left(-\frac{6}{7}, -13\right)$	$-5028x^6 - 10620x^5 - 2605x^4 - 16750x^3 + 5255x^2 - 6600x + 2832$
$\left(-\frac{1}{2}, -7\right)$	$8964x^6 - 3132x^5 + 18927x^4 + 6286x^3 + 6655x^2 + 11300x - 500$
$\left(\frac{2}{5}, -\frac{7}{3}\right)$	$21006x^6 - 45414x^5 + 16263x^4 - 20048x^3 - 7227x^2 + 960x - 3200$
$\left(-\frac{3}{4}, -\frac{3}{5}\right)$	$5500x^6 + 30300x^5 + 19835x^4 + 20174x^3 - 46885x^2 + 2340x - 380$
$\left(\frac{5}{2}, \frac{7}{3}\right)$	$-12852x^6 - 15876x^5 + 40383x^4 + 49976x^3 - 30231x^2 - 43650x + 2250$
$\left(\frac{11}{20}, -\frac{71}{49}\right)$	$-66020x^6 + 43980x^5 + 10001x^4 + 1154x^3 - 5899x^2 - 1464x + 1096$
$\left(-\frac{2}{5}, -\frac{7}{3}\right)$	$-72620x^6 + 37884x^5 - 12135x^4 + 29302x^3 - 4107x^2 + 1848x - 2672$
$\left(-\frac{5}{2}, \frac{7}{3}\right)$	$20x^6 + 180x^5 - 3879x^4 - 34668x^3 + 44937x^2 + 62856x - 73296$
$\left(\frac{7}{6}, 13\right)$	$-5442x^6 + 3630x^5 - 7079x^4 - 93460x^3 + 35059x^2 - 420x + 9212$
$\left(-4, \frac{11}{9}\right)$	$-16964x^6 - 33804x^5 + 53325x^4 + 100170x^3 - 35163x^2 - 81540x - 1116$
$\left(\frac{11}{2}, \frac{9}{13}\right)$	$-102046x^6 + 130482x^5 + 61857x^4 + 9504x^3 - 74697x^2 - 38412x - 14036$

Table 25. Some rational points (e, f) of small height on the surface of Theorem 40 and the corresponding genus-2 curves.

30.3. *Examples.* Table 25 lists some points of small height and their genus-2 curves.

31. Discriminant 88

31.1. *Parametrization.* We start with an elliptic K3 surface with fibers of type A_9, D_4 and A_2, and a section of height $\frac{11}{15} = 4 - \frac{2}{3} - 1 - \frac{16}{10}$. The Weierstrass equation for this family is

$$y^2 = x^3 + (a_0 + a_1 t + a_2 t^2 + a_3 t^3)x^2$$
$$+ 2t^2(\lambda t - \mu)(b_0 + b_1 t + b_2 t^2 + b_3 t^3)x + t^4(\lambda t - \mu)^2(c_0 + c_1 t)^2,$$

with

$$a_0 = 1, \qquad \mu = rs + 2s + 1, \qquad \lambda = s(r + 2)^2(2s + 1)^2,$$
$$c_0 = -2, \qquad b_0 = 2, \qquad a_1 = -8s(rs + 2r + 1),$$
$$c_1 = 8(r + 2)s^2 + 8(r + 1)s + r^2,$$
$$b_3 = 2r(r + 2)s(2s + 1)(8s + r^2)(8s^2 + r),$$
$$b_2 = 32r(r + 2)s^4 + 32(3r^2 + 4r + 2)s^3 - 4(r^3 - 20r^2 - 24r - 8)s^2 + 4(r - 1)r^2 s,$$

$$b_1 = -16(r+1)s^2 - 8(3r+2)s - r^2,$$

$$a_3 = 4rs\big(64rs^4 + 16(r^3 + 3r^2 + 12r + 4)s^3$$
$$+ 2r(r^2 + 4)s^2 + r(r^3 + 12r^2 + 12r + 16)s + r^3\big),$$

$$a_2 = 4s\big(4r^2s^3 + 8r(2r-1)s^2 - 4(r^3 - 4r^2 - 4r - 1)s - r^2(r+4)\big).$$

First we identify an E_7 fiber, and make a 3-neighbor move to it.

This gives us an elliptic fibration with E_7, D_5 and A_3 fibers, and a section of height $\frac{88}{32} = \frac{11}{4} = 4 - \frac{5}{4}$. Then we can identify a D_8 fiber F' below, and move to the associated genus 1 fibration by a 2-neighbor step.

To see that the genus-1 fibration defined by this fiber F' has a section, note that $P \cdot F' = 3$, while F' intersects the near leaf of the D_5 fiber with multiplicity 2. Therefore we may replace the genus-1 fibration by its Jacobian.

Finally, we go by another 2-neighbor move to a fibration with E_8 and E_7 fibers. We identify the class of an E_8 fiber F'' below. The Mordell–Weil group is generated by a section P' of height $88/(2 \cdot 4) = 11 = 4 + 2 \cdot 4 - 1$, so the section must intersect the zero section with multiplicity 4, and it must intersect the near leaf of the D_8 fiber. Therefore $P' \cdot F'' = 2 \cdot 4 + 3 = 11$, whereas the omitted far leaf of the D_8 fiber intersects F'' with multiplicity 2. So the new fibration has a section.

We may now read out the Igusa–Clebsch invariants and compute the equation of the branch locus for $Y_-(88) \mapsto \mathbb{P}^2_{r,s}$.

Theorem 41. *A birational model over $\mathbb{Q}$ for the Hilbert modular surface $Y_-(88)$ as a double cover of $\mathbb{P}^2_{r,s}$ is given by the equation*

$$z^2 = (8rs^2 + 16s^2 + 8s + r^2)(8r^3s^4 + 16r^2s^4 + 96r^3s^3 + 472r^2s^3 + 544rs^3$$
$$- 27r^4s^2 - 120r^3s^2 + 64r^2s^2 + 472rs^2 + 16s^2 - 46r^3s - 120r^2s + 96rs + 8s - 27r^2).$$

It is a surface of general type.

31.2. Analysis. The branch locus has two components. Both correspond to elliptic K3 surfaces with an extra I_2 fiber, and the simpler component to having a 2-torsion section in addition. The simpler component of the branch locus has genus 1; the change of coordinates $r = 2y/x^2$, $s = -1/(2x)$ converts it to Weierstrass form

$$y^2 + y = x^3 - x^2,$$

which is an elliptic curve of conductor 11 (isomorphic to $X_1(11)$).

The other component has genus 2. The transformation

$$(r, s) = \left(\frac{-(x-1)y + (x+1)(x^3 - 3x^2 - 3x - 1)}{3x^2 + 2x + 1}, \right.$$

$$\left. \frac{(3x+1)y - (x+1)(3x^3 + 3x^2 + 3x + 1)}{4x(x^2 - 2x - 1)} \right)$$

converts it to Weierstrass form

$$y^2 = x^6 - 2x^5 + 11x^4 + 20x^3 + 15x^2 + 6x + 1.$$

The Hilbert modular surface $Y_-(88)$ is a surface of general type. We now analyze its quotient by the involution $\iota : (r, s, z) \mapsto (1/s, 1/r, z/(rs)^3)$. Writing $h = -(s + 1/r)$, $m = (s - 1/r)^2$, we find the equation

$$z^2 = (h^4 - 2h^3 - 2mh^2 + 2mh + m^2 + 1)(9h^6 - 30h^5 - 26mh^4 + 16h^4 + 58mh^3$$
$$+ 30h^3 + 25m^2h^2 - 8mh^2 - 25h^2 - 28m^2h - 30mh - 8m^3 - 8m^2 - 2m).$$

The invertible transformation $m = 2 + 1/t + 8/(nt) + 4/(nt)^2$, $h = -1 - 2/(nt)$ makes this a quartic in n,

$$z^2 = (4t - n - 4)(t(2t+1)(6t^2 - 13t + 8)n^3 + 4t(2t-3)^2n^2 - 4(2t-1)^2n + 16(t-1)),$$

with an obvious section $n = 4t - 4$. Converting to the Jacobian, we get an elliptic K3 surface with the following equation (after some Weierstrass transformations and a change of parameter $t \mapsto 1 - t$ on the base):

$$y^2 = x^3 + (28t^4 - 24t^3 - 8t^2 + 4t + 1)x^2$$
$$- 16t^3(t-1)^2(t^3 - 10t^2 + 4t + 1)x + 64t^6(t-1)^4(29t^2 - 10t - 3).$$

This has bad fibers of type I_6 at $t = 0$, I_5 at $t = 1$, I_2 at $t = \frac{1}{2}$ and $t = -\frac{1}{6}$, and I_3 at $t = \frac{1}{4} \pm \frac{\sqrt{33}}{12}$. The trivial lattice has rank 17. We find the independent sections

$$P_1 = \left(-4t(t-1)(7t^2 - 2t - 1), \ 4t(t-1)(t+1)(2t-1)(6t^2 - 3t - 1) \right),$$
$$P_2 = \left(4t(t-1)^2(5t+1), \ 4t(t-1)^2(6t+1)(6t^2 - 3t - 1) \right),$$

$$P_3 = \left(4t^3(6 - 13t),\ 12\sqrt{-3}\,t^4(2t - 1)(6t + 1)\right),$$

with height matrix

$$\begin{pmatrix} \frac{8}{15} & \frac{1}{10} & 0 \\ \frac{1}{10} & \frac{2}{15} & 0 \\ 0 & 0 & \frac{3}{2} \end{pmatrix}.$$

Therefore the K3 surface is singular, and an easy argument shows that these sections and the trivial lattice must span the Néron–Severi lattice, which therefore has rank 20 and discriminant -99.

31.3. *Examples.* Table 26 lists some points of small height and their genus-2 curves.

We describe some curves on the surface which are a source of rational points (some more may be produced by applying the involution ι). The specialization

(r, s)	Sextic polynomial $f_6(x)$ defining the genus-2 curve $y^2 = f_6(x)$
$\left(-\frac{2}{3}, -\frac{7}{10}\right)$	$25x^6 + 120x^5 - 291x^4 - 1292x^3 + 987x^2 + 588x - 497$
$\left(-4, \frac{3}{2}\right)$	$486x^6 - 810x^5 + 1323x^4 - 800x^3 + 585x^2 - 48x + 64$
$\left(-\frac{10}{7}, -\frac{3}{2}\right)$	$515x^6 + 1314x^5 - 3120x^4 - 1332x^3 + 2292x^2 + 720x - 200$
$\left(-\frac{4}{7}, -\frac{3}{10}\right)$	$20x^6 + 180x^5 - 159x^4 - 3276x^3 + 249x^2 + 1980x - 1100$
$\left(\frac{2}{3}, -\frac{1}{4}\right)$	$4608x^6 + 6048x^5 + 3771x^4 - 1026x^3 + 351x^2 - 36x + 4$
$\left(-\frac{20}{7}, -\frac{5}{6}\right)$	$356x^6 - 4980x^5 + 6373x^4 + 2580x^3 - 4409x^2 - 4170x - 790$
$\left(\frac{8}{21}, -\frac{2}{5}\right)$	$1664x^6 + 624x^5 + 3747x^4 - 5222x^3 + 5511x^2 - 1140x + 15020$
$\left(-\frac{6}{5}, -\frac{7}{20}\right)$	$6260x^6 - 21060x^5 + 7009x^4 - 1254x^3 - 239x^2 - 540x - 100$
$\left(-\frac{10}{3}, -\frac{7}{4}\right)$	$2x^6 + 54x^5 + 45x^4 + 1080x^3 - 2961x^2 - 44352$
$\left(-\frac{4}{3}, -\frac{13}{6}\right)$	$-14388x^6 - 86076x^5 - 115441x^4 + 70272x^3 + 86417x^2 - 10794x + 314$
$\left(-\frac{22}{21}, -\frac{13}{70}\right)$	$7865x^6 - 9750x^5 + 62049x^4 - 2788x^3 + 162759x^2 - 4350x + 119375$
$\left(-\frac{5}{2}, \frac{21}{8}\right)$	$363300x^6 - 50652x^5 + 128541x^4 + 2266x^3 + 19257x^2 + 1008x + 896$
$\left(\frac{38}{65}, -\frac{13}{40}\right)$	$-1106244x^6 + 336780x^5 + 23283x^4 + 248770x^3 - 101625x^2$ $- 33072x - 28736$
$\left(-\frac{8}{39}, -\frac{1}{42}\right)$	$-48600x^6 + 483840x^5 - 1386285x^4 - 264482x^3 - 282489x^2$ $+ 883404x - 1658988$
$\left(-\frac{70}{13}, -\frac{21}{22}\right)$	$599697x^6 - 445662x^5 + 824913x^4 - 838612x^3 + 2057823x^2$ $- 1620774x + 957519$
$\left(-\frac{10}{7}, -\frac{13}{36}\right)$	$-1112220x^6 + 2309556x^5 - 397465x^4 - 269262x^3 - 847153x^2$ $- 265908x + 612$

Table 26. Some rational points (r, s) of small height on the surface of Theorem 41 and the corresponding genus-2 curves.

$s = -\frac{5}{6}$ gives a genus-1 curve

$$y^2 = -(9r^2 + 50r + 40)(243r^2 + 670r - 40).$$

It has rational points, such as $(r, y) = (0, 40)$. It is thus an elliptic curve; we find that it has conductor $2 \cdot 3 \cdot 5^2 \cdot 29 \cdot 53$ and Mordell–Weil group $(\mathbb{Z}/2\mathbb{Z}) \oplus \mathbb{Z}^2$.

Pulling back sections of the elliptic fibration on the quotient surface gives us some more curves of genus 1, each with a rational point and rank 1:

Equation		point	conductor	group
$h =$	$g^2 =$			
$-\dfrac{4t^2 - 5t + 2}{2t(t-1)}$	$\dfrac{(2t-1)(14t^3 - 25t^2 + 16t - 4)}{4t^2(t-1)^2}$	$t = \frac{1}{2}$	53	$\mathbb{Z}$
$-\dfrac{12t^2 - 5t + 2}{2t(3t-2)}$	$\dfrac{252t^4 - 192t^3 + 73t^2 - 20t + 4}{4t^2(3t-2)^2}$	$t = 0$	$2 \cdot 3 \cdot 4391$	$\mathbb{Z}$
$-\dfrac{8t^2 - 15t + 8}{2t(t-1)}$	$\dfrac{92t^4 - 320t^3 + 433t^2 - 268t + 64}{4t^2(t-1)^2}$	$t = 0$	$7 \cdot 977$	$(\mathbb{Z}/2\mathbb{Z}) \oplus \mathbb{Z}$
$-\dfrac{3t^2 - 3t + 2}{3t(t-1)}$	$\dfrac{18t^4 - 27t^3 + 24t^2 - 15t + 4}{9t^2(t-1)^2}$	$t = 0$	$2^5 3^2 7$	$(\mathbb{Z}/2\mathbb{Z}) \oplus \mathbb{Z}$

32. Discriminant 89

32.1. *Parametrization.* We start with an elliptic K3 surface with fibers of type $A_8 A_7$, and a section of height $\frac{89}{72} = 4 - \frac{1 \cdot 8}{9} - \frac{3 \cdot 5}{8}$.

The Weierstrass equation for this family is

$$y^2 = x^3 + (a_0 + a_1 t + a_2 t^2 + a_3 t^3 + a_4 t^4)x^2$$
$$+ 2\mu t^2 (b_0 + b_1 t + b_2 t^2 + b_3 t^3)x + \mu^2 t^4 (c_0 + c_1 t + c_2 t^2),$$

with

$a_0 = (rs+1)^2,$ $\quad b_0 = -(rs+1)^2,$ $\qquad\qquad c_0 = (rs+1)^2,$

$\mu = 4rs(r+1)^2,$ $\quad b_3 = s(s^2 - rs - 2s + 1)^2,$ $\quad a_4 = s^2(s^2 - rs - 2s + 1)^2,$

$c_2 = (s^2 - rs - 2s + 1)^2,$

$c_1 = 2rs^3 - 2(r^2 + 4r + 1)s^2 + 4(r+1)^2 s - 2,$

$b_2 = (2r-1)s^4 - (3r^2 + 7r - 2)s^3 + (r^3 + 6r^2 + 7r - 1)s^2 - 2r(r+1)s + r,$

$a_1 = -2(r^2 - r)s^3 + 2(r^3 - 6r - 1)s^2 + 2(4r^2 + 6r + 1)s + 2r,$

$b_1 = r(r-2)s^3 - (r^3 - r^2 - 10r - 2)s^2 - (6r^2 + 10r + 3)s - r + 1,$

$a_3 = 2s\big((r-1)s^4 - (2r^2 + 3r - 3)s^3 + (r^3 + 4r^2 + 3r - 3)s^2 - (2r^2 + 2r - 1)s + r\big),$

$$a_2 = (r^2 - 4r + 1)s^4 - 2(r^3 - 2r^2 - 9r)s^3$$
$$+ (r^4 - 16r^2 - 22r - 3)s^2 - 2(r^3 - r - 1)s + r^2.$$

To obtain an $E_8 E_7$ elliptic fibration on these K3 surfaces, we first move by a 2-neighbor step to one with E_7 and A_8 fibers.
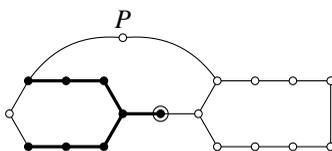
The elliptic fibration defined by this new fiber F' has a section, since $P \cdot F' = 1$. Also, the new elliptic fibration must have a section P' of height $\frac{89}{18} = 4 + 2 \cdot 2 - \frac{3}{2} - \frac{2 \cdot 7}{9}$.

Finally, we go to $E_8 E_7$ by a 3-neighbor step.
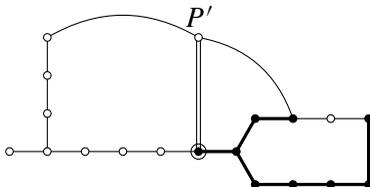
The new fiber F'' satisfies $P' \cdot F'' = 2 + 2 \cdot 3 = 8$, and the identity component of the E_7 fiber intersects F' in 3. Since these have greatest common divisor 1, the genus-1 fibration defined by F' has a section.

Theorem 42. *A birational model over $\mathbb{Q}$ for the Hilbert modular surface $Y_-(89)$ as a double cover of $\mathbb{P}^2_{r,s}$ is given by the equation*

$$z^2 = s^4 r^6 - 2s^3(2s^2 + 3s + 2)r^5 + s^2(6s^4 + 16s^3 - 49s^2 - 26s + 6)r^4$$
$$- 2s(2s^6 + 6s^5 - 50s^4 + 26s^3 + 73s^2 - 35s + 2)r^3$$
$$+ (s^8 - 36s^6 + 26s^5 + 273s^4 - 514s^3 + 271s^2 - 38s + 1)r^2$$
$$+ 2(s - 1)^2 s(s^5 - 4s^4 + 25s^3 - 107s^2 + 147s - 44)r + (s - 4)^3(s - 1)^4 s.$$

It is a surface of general type.

32.2. Analysis. The branch locus has genus 1; one can give an explicit isomorphism (see the online supplement) to the elliptic curve of conductor 89 given by the Weierstrass equation

$$y^2 + xy + y = x^3 + x^2 - x.$$

It is isomorphic to $X_0(89)/\langle w \rangle$, where w is the Atkin–Lehner involution.

The Hilbert modular surface $Y_-(89)$ is a surface of general type. Note that the change of coordinates $r = s + g$ simplifies the equation a bit further, making the

(r, s)	Sextic polynomial $f_6(x)$ defining the genus-2 curve $y^2 = f_6(x)$
$\left(-\frac{31}{3}, -\frac{1}{6}\right)$	$-334084x^6 + 65892x^5 + 847841x^4 - 156012x^3 - 1036555x^2 - 453867x - 525$
$\left(-\frac{49}{9}, -\frac{2}{3}\right)$	$632x^6 - 480x^5 + 43475x^4 - 97578x^3 - 1030393x^2 + 855708x - 1045044$
$(-19, -1)$	$126905x^6 + 2388081x^5 - 2600778x^4 - 3075787x^3 - 5448045x^2$ $- 3683352x - 709200$
$\left(-\frac{31}{10}, \frac{5}{2}\right)$	$-83300x^6 + 168420x^5 + 5079215x^4 - 6586832x^3 + 584735x^2$ $+ 70020x - 8100$
$\left(-\frac{5}{6}, \frac{11}{6}\right)$	$2185004x^6 - 12346980x^5 + 10798163x^4 + 732660x^3 + 47975267x^2$ $+ 21406020x + 27911916$
$\left(\frac{13}{9}, -\frac{5}{9}\right)$	$-14966100x^6 - 43598124x^5 + 25890735x^4 + 105396908x^3 - 44422995x^2$ $- 65750574x + 34674550$
$\left(-\frac{40}{7}, -\frac{1}{2}\right)$	$2754000x^6 + 86434200x^5 + 150411025x^4 - 14830346x^3 - 49970411x^2$ $+ 242599308x + 131021492$
$\left(\frac{16}{33}, \frac{11}{3}\right)$	$25329267x^6 - 96789717x^5 + 223774305x^4 - 449560367x^3 - 46904988x^2$ $- 772810308x + 413626230$

Table 27. Some rational points (r, s) of small height on the surface of Theorem 42 and the corresponding genus-2 curves.

degree of the right-hand side equal to 6 in each variable. However, it complicates the original defining Weierstrass equation of the family of K3 surfaces, so we have chosen the (r, s) coordinate system.

32.3. *Examples.* Table 27 lists some points of small height and their genus-2 curves.

We find two elliptic curves of positive rank on the surface. The specialization $s = \frac{25}{22}$ gives a curve of genus 1

$$y^2 = 1210000r^4 - 19157600r^3 - 17065736r^2 + 678600r - 8575$$

with rational points (as at infinity), conductor $3 \cdot 5 \cdot 11 \cdot 163 \cdot 191 \cdot 881$, and rank at least 2. The locus $s = r + \frac{101}{50}$ gives another curve of genus 1,

$$y^2 = -3739190000r^4 - 21451957600r^3 - 43018833576r^2$$
$$- 36551728152r - 11227811551,$$

with rational points (as at $(r, y) = (-1, \pm65^2)$), conductor $2^4 \cdot 5 \cdot 17 \cdot 19 \cdot 463 \cdot 58787$, and rank at least 3. We were not able to determine the exact rank of either curve, but the global root numbers indicate that the rank should be even for the former curve and odd for the latter, so one might guess that the lower bounds 2 and 3 on their ranks are sharp.

33. Discriminant 92

33.1. *Parametrization.* We start with an elliptic K3 surface with fibers of type A_8, A_1 and D_6, and a section of height $\frac{92}{72} = \frac{23}{18} = 4 - \frac{1 \cdot 1}{2} - \frac{4 \cdot 5}{9}$.

The Weierstrass equation may be written as

$$y^2 = x^3 + (a_0 + a_1 t + a_2 t^2 + a_3 t^3) x^2$$
$$+ 2t^2 (\lambda t - \mu)(b_0 + b_1 t + b_2 t^2) x + t^4 (\lambda t - \mu)^2 (c_0 + c_1 t),$$

with

$\lambda = (r+s)^2,$ $\qquad\qquad$ $\mu = r + 2s,$

$a_3 = -4rs(s + r^2 + r)(s^2 + rs - r),$ $\qquad$ $a_0 = (rs - r - 1)^2,$

$b_0 = -4rs^2(rs - r - 1)^2,$ $\qquad\qquad$ $c_0 = 16r^2 s^4 (rs - r - 1)^2,$

$a_1 = -2r((r+1)^2(s-1)^2 + s^2),$ $\qquad$ $b_1 = 4r^2 s^2 (rs + 2s - r - 1)^2,$

$c_1 = -64r^3(r+1)(s-1)s^5,$

$b_2 = -8r^2 s^3 \big((r+2)s^2 + (2r^2 + 2r - 1)s - 2r(r+1)\big),$

$a_2 = r(rs + 4s - r - 1)(4s^2 + r^2 s + 4rs - r^2 - r).$

As in the case of discriminant 56, we first go to an $E_7 A_8$ fibration using the E_7 fiber F' identified below. Note that $F' \cdot P = 3$, while the component of the D_6 fiber which is not included in F' intersects F' with multiplicity 2. Since $\gcd(2, 3) = 1$, the fibration defined by F' has a section.
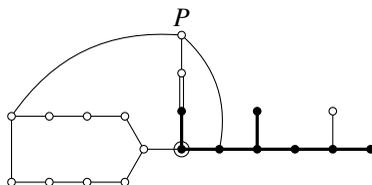
The new elliptic fibration has a section P' of height $\frac{92}{2 \cdot 9} = \frac{46}{9} = 4 + 2 \cdot 1 - \frac{8}{9}$, which must therefore intersect the zero section, the identity component of the E_7 fiber and component 1 of the A_8 fiber.

We identify an E_8 fiber and compute its Weierstrass equation by a 3-neighbor move. Note that it intersects P' in 7 and the excluded component of the A_8 fiber in 3. Therefore the fibration it defines has a section, and we may convert to the Jacobian.
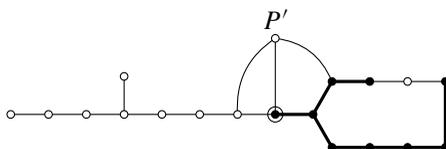
Now we read out the Igusa–Clebsch invariants and compute the branch locus.

Theorem 43. *A birational model over* $\mathbb{Q}$ *for the Hilbert modular surface* $Y_-(92)$ *as a double cover of* $\mathbb{P}^2_{r,s}$ *is given by the equation*

$$z^2 = (s + r^2 + r)(s^2 + rs - r)$$
$$\times \big((s-1)^3 r^5 + (s-1)^2(s^2 - 15s - 3)r^4 - (s-1)(42s^3 - 27s^2 - 31s - 3)r^3$$
$$-(27s^5 - 30s^4 - 77s^3 + 69s^2 + 17s + 1)r^2 + s(46s^3 - 30s^2 - 42s - 1)r - 27s^3\big).$$

It is a surface of general type.

33.2. Analysis. The branch locus has three components. Points of the two simpler components correspond to elliptic K3 surfaces where the D_6 fiber is promoted to an E_7 fiber, while the more complicated component corresponds to an extra I_2 fiber. All the three components are rational (genus 0). This is obvious from inspection for the simpler components, and for the last we have the parametrization

$$(r, s) = \left(\frac{t(t^2 + 2)(t+1)^2}{(t+2)(t^3 + 2t^2 + 2t + 2)}, \frac{-t(t+1)(t^3 + 2t^2 + 4t + 4)}{(t+2)^2(t^2 + 2)} \right).$$

The surface $Y_-(92)$ is a surface of general type. The extra involution is $(r, s, z) \mapsto (-1/s, -1/r, z/(rs)^4)$. We now analyze the quotient of the Hilbert modular surface by this involution. Because the involution fixes r/s, we obtain the quotient by setting $r = st$ and writing everything in terms of $m = s - 1/(ts)$. We find the equation

$$y^2 = \big(t^2(t+1)m - t^3 + t^2 + 2t + 1\big)\big(t^3(t+1)m^3 - t(3t^3 + 17t^2 + 42t + 27)m^2$$
$$+ t(3t^3 + 31t^2 + 72t + 30)m - (t^4 + 15t^3 + 30t^2 + 7t + 8)\big),$$

which expresses the quotient as a genus-1 curve over $\mathbb{Q}(t)$. Since there is an obvious section (where the first factor vanishes), we may convert to the Jacobian, which has the Weierstrass equation (after shifting t by 1 and performing some Weierstrass transformations)

$$y^2 = x^3 - (2t + 1)(8t^3 + 8t^2 - 6t - 1)x^2$$
$$- 8(t-1)t^4(t+1)(10t^2 - 32t - 5)x - 16(t-1)^2t^8(t+1)(47t + 7).$$

This is an elliptic K3 surface. It has reducible fibers of type I_8 at $t = 0$, I_3 at 1 and $(-7 \pm 3\sqrt{3})/11$, and I_2 at the roots of $11t^3 - 10t^2 + 5t + 1$ (which generates the cubic field of discriminant -23). Therefore the trivial lattice has rank 18. We easily identify a non-torsion section P of height $\frac{5}{8}$ with x-coordinate $4t^3(6t + 1)$. On the other hand, counting points modulo 13 and 17 shows that the Picard number cannot be 20. Therefore the Picard number of this quotient surface is 19. The sublattice of the Néron–Severi group spanned by P and the trivial lattice has discriminant $360 = 2^3 \cdot 3^2 \cdot 5$. It is easy to see from height calculations that there cannot be any 2-

(r, s)	Sextic polynomial $f_6(x)$ defining the genus-2 curve $y^2 = f_6(x)$
$\left(\frac{3}{10}, -\frac{39}{70}\right)$	$5981584x^6 - 4016376x^5 + 1699985x^4 + 313485x^3 - 168322x^2$ $+ 49665x + 21175$
$\left(\frac{70}{39}, -\frac{10}{3}\right)$	$2916x^6 + 591516x^5 + 6670933x^4 + 12740602x^3 - 44084051x^2$ $+ 8704740x + 16105100$

Table 28. Some rational points (r, s) of small height on the surface of Theorem 43 and the corresponding genus-2 curves.

or 3-torsion sections, and that P cannot be divisible by 2 or 3 in the Mordell–Weil group. Hence, this sublattice is the entire Néron–Severi lattice.

33.3. *Examples*. Table 28 lists some points of small height and their genus-2 curves.

Specializations of r or s, and pullbacks of sections of the quotient, do not seem to yield any genus 0 or 1 curves on the surface (at any rate, none corresponding to abelian surfaces with "honest" real multiplication by $\mathcal{O}_{92}$ and not a larger endomorphism ring).

34. Discriminant 93

34.1. *Parametrization*. Start with an elliptic K3 surface with fibers of type A_{10}, A_3 and A_2, with a section of height $\frac{31}{44} = 4 - \frac{3}{4} - \frac{28}{11}$. The extra involution comes from flipping the A_2 fiber.

This family has the Weierstrass equation

$$y^2 = x^3 + (a_0 + a_1 t + a_2 t^2 + a_3 t^3 + a_4 t^4)x^2$$
$$+ 2t(\lambda t - \mu)(b_0 + b_1 t + b_2 t^2 + b_3 t^3)x + t^2(\lambda t - \mu)^2(c_0 + c_1 t + c_2 t^2),$$

with

$$\lambda = -(n^2 - 1), \qquad \qquad \mu = (n^2 - mn - n - m)(n^2 + mn + n - m),$$

$$a_0 = (m + 1)^2 n^8, \qquad \qquad b_0 = m^4(m + 1)^2 n^8,$$

$$c_0 = m^8(m + 1)^2 n^8, \qquad \qquad a_4 = 1,$$

$$c_2 = m^8 n^4, \qquad \qquad b_3 = m^4 n^2,$$

$$a_3 = (m^2 + 2m + 4)n^2 - 3m^2, \qquad c_1 = m^8 n^4((m^2 + 2m + 2)n^2 - m^2),$$

$$b_2 = m^4 n^2\big((m^2 + 2m + 3)n^2 - 2m^2\big),$$

$$a_2 = 3(m^2 + 2m + 2)n^4 - 2m^2(m^2 + 3m + 3)n^2 + 3m^4,$$

$$b_1 = m^4 n^2\big((2m^2 + 4m + 3)n^4 - m^2(m + 1)(m + 2)n^2 + m^4\big),$$

$$a_1 = (3m^2 + 6m + 4)n^6 - 3m^2(m + 1)^2 n^4 + m^4(m + 1)(m + 3)n^2 - m^6.$$

We first identify the class of an E_8 fiber below, and move to it by a 3-neighbor step.
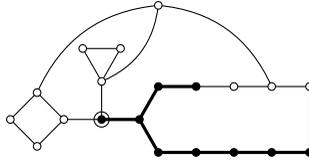
This gives us an elliptic fibration with E_8, A_5 and A_2 fibers, and a section P of height $\frac{93}{18} = \frac{31}{6} = 4 + 2 \cdot 1 - \frac{5}{6}$. We then identify an E_7 fiber and move to it by a 2-neighbor step. Since the new fiber intersects the section P in 7 and the excluded component of the A_5 fiber in 3, we see that the new fibration has a section.
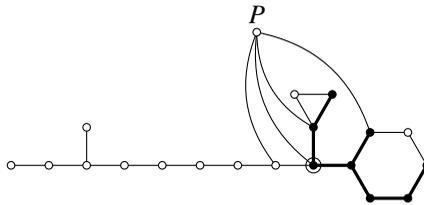
Theorem 44. *A birational model over $\mathbb{Q}$ for the Hilbert modular surface $Y_-(93)$ as a double cover of $\mathbb{P}^2_{m,n}$ is given by the equation*

$$z^2 = 16(n^2 - 1)^2 n^2 m^6 + 8(n^2 - 1)(21n^4 + 22n^2 - 27)m^5$$
$$- (27n^8 - 684n^6 - 1246n^4 + 1620n^2 + 27)m^4$$
$$- 8n^2(27n^6 - 109n^4 - 471n^2 + 41)m^3 - 8n^2(81n^6 + 135n^4 - 273n^2 - 7)m^2$$
$$- 96n^4(9n^2 - 1)(n^2 + 3)m - 16n^4(n^2 + 3)(27n^2 + 1).$$

It is a surface of general type.

34.2. *Analysis.* The extra involution is $\iota : (m, n) \mapsto (m, -n)$.

The branch locus is a curve of genus 4, isomorphic to $X_0(93)/\langle w_{93} \rangle$, where w_{93} is the Atkin–Lehner involution. We do not give the explicit isomorphism here, but the formulas are available in the online supplement. Setting $k = n^2$, we can write it as a double cover of a genus-2 curve, which can be transformed to the Weierstrass form

$$y^2 - (9x^3 + 11x - 3)y + x^2(69x^3 - 56x^2 + 81x - 22) = 0.$$

This Hilbert modular surface is a surface of general type. The quotient by this involution ι has the equation (with $k = n^2$)

$$z^2 = -27(m+2)^4 k^4 + 4(4m^6 + 42m^5 + 171m^4 + 218m^3 - 270m^2 - 624m - 328)k^3$$
$$- 2(16m^6 - 4m^5 - 623m^4 - 1884m^3 - 1092m^2 - 144m + 24)k^2$$
$$+ 4m^2(4m^4 - 98m^3 - 405m^2 - 82m + 14)k + 27m^4(8m - 1).$$

This has a genus-1 fibration over $\mathbb{Q}(m)$. The fibration has a section at infinity defined over $\mathbb{Q}(\sqrt{-3})$; we do not know whether there is a section defined over $\mathbb{Q}$. The Jacobian has the Weierstrass equation

$$y^2 = x^3 + (m^6 + 20m^5 + 118m^4 + 186m^3 + 33m^2 + 18m - 3)x^2$$
$$+ 8m^2(m + 10)(9m^4 + 39m^3 + 57m^2 - 1)x$$
$$+ 16m^4(m + 10)^2(4m^3 + 13m^2 + 18m - 3).$$

This is an honestly elliptic surface with $\chi = 3$. It has reducible fibers of type I_9 at $m = \infty$, I_4 at $m = 0$, I_2 at $m = -10$, and I_3 at the roots of

$$m^6 + 11m^5 + 16m^4 + 32m^3 + 17m^2 - 9m + 1$$

(whose splitting field is a dihedral extension of degree 12 containing $\sqrt{93}$). The trivial lattice has rank 26, leaving room for Mordell–Weil rank up to 4. Counting points modulo 13 and 17 shows that the Picard number is at most 29. On the other hand, we are (so far) able to produce the sections

$$P_0 = \left(-16(m^3 + m^2 + 6m - 1), 32(m^6 + 11m^5 + 16m^4 + 32m^3 + 17m^2 - 9m + 1)\right),$$
$$P_1 = \left(-16(m + 10)(m^5 + m^4 + 6m^3 + 3m^2 + 18m - 3)/31,\right.$$
$$\left. 288(m + 10)(3m^2 + 2m + 9)(m^6 + 11m^5 + 16m^4 + 32m^3 + 17m^2 - 9m + 1)/93^{3/2}\right),$$

of which P_0 is 3-torsion, while P_1 has height $\frac{3}{2}$. Therefore, the Mordell–Weil rank is between 1 and 3.

34.3. Examples. Table 29 lists some points of small height and their genus-2 curves.

(m, n)	Sextic polynomial $f_6(x)$ defining the genus-2 curve $y^2 = f_6(x)$
$\left(2, \frac{1}{3}\right)$	$-2112x^6 - 5184x^5 + 5451x^4 + 2593x^3 - 4596x^2 - 2223x - 101$
$\left(-10, \frac{5}{3}\right)$	$-7452x^6 - 4860x^5 - 24039x^4 - 4540x^3 - 17205x^2 + 4686x - 302$
$\left(\frac{1}{5}, \frac{1}{7}\right)$	$-24786x^6 + 25272x^5 + 90900x^4 - 73885x^3 - 107482x^2 + 54020x + 40286$
$(-10, 5)$	$-31752x^5 - 48825x^4 + 52868x^3 - 175537x^2 + 91124x - 80644$
$\left(2, -\frac{1}{3}\right)$	$-594x^6 + 10962x^5 - 154233x^4 + 391936x^3 + 265521x^2 + 330228x - 71068$
$(-10, -5)$	$43756x^6 + 110088x^5 + 463887x^4 - 609201x^3 + 208770x^2 - 6300x - 211000$
$\left(-10, -\frac{5}{3}\right)$	$-3008x^6 + 270048x^5 - 773739x^4 - 611989x^3 - 2150523x^2$ $+ 631152x - 342144$
$\left(\frac{1}{5}, -\frac{1}{7}\right)$	$-253800x^6 - 1186380x^5 - 1627302x^4 + 4611739x^3 + 1795017x^2$ $- 2139291x + 2480233$

Table 29. Some rational points (m, n) of small height on the surface of Theorem 44 and the corresponding genus-2 curves.

35. Discriminant 97

35.1. *Parametrization.* Start with an elliptic K3 surface with fibers of type D_5, A_4 and A_6, with a section of height $\frac{97}{140} = 4 - \left(1 + \frac{1}{4}\right) - \frac{6}{5} - \frac{6}{7}$.

We can write the Weierstrass equation as

$$y^2 = x^3 + (a_0 + a_1 t + a_2 t^2 + a_3 t^3)x^2 + 2t^2(t-1)^2(b_0 + b_1 t + b_2 t^2)x$$
$$+ t^4(t-1)^4(c_0 + c_1 t),$$

with

$a_0 = (r+1)^2(rs^2 + s^2 + r^2 s + r)^2,$

$a_1 = 2(r+1)\big((r+1)^2 s^5 + 2(r+1)(r^2 - r - 1)s^4 + r(r^3 - 4r^2 - 4r + 2)s^3$
$\qquad - r(2r^3 + r^2 + 2r + 5)s^2 - r^2(r^2 + 3r + 3)s - r^2(r+1)\big),$

$a_2 = (r+1)^2 s^6 + 2(r+1)(r^2 - 4r - 2)s^5 + (r^4 - 16r^3 - 6r^2 + 18r + 4)s^4$
$\qquad - 2r(4r^3 - 6r^2 - 4r + 11)s^3 + r(6r^3 - 6r^2 - 3r + 20)s^2$
$\qquad\qquad + 2r^2(r+3)(2r+3)s + r^2(r+1)^2,$

$a_3 = -4r(s-1)s(s+r)\big(s^3 + (r-2)s^2 - (r-2)s - 2r - 3\big),$

$b_0 = 4r(r+1)^2(s-1)^2 s(s+r)(rs^2 + s^2 + r^2 s + r)^2,$

$b_1 = 4r(r+1)(s-1)^2 s(s+r)$
$\qquad \times \big((r+1)^2 s^5 + 2(r+1)(r^2 - 2r - 1)s^4 + r(r^3 - 8r^2 - 6r + 4)s^3$
$\qquad\qquad - r(4r^3 + r^2 + 2r + 7)s^2 - r^2(r^2 + 5r + 5)s - r^2(r+1)\big),$

$b_2 = -8r^2(r+1)(s-1)^2 s^2(s+r)^2\big(2s^3 + 2(r-2)s^2 - 2(r-2)s - r - 3\big),$

$c_0 = 16r^2(r+1)^2(s-1)^4 s^2(s+r)^2(rs^2 + s^2 + r^2 s + r)^2,$

$c_1 = -64r^3(r+1)^2(s-1)^4 s^3(s+r)^3(s^2 + rs - s + 1).$

First we identify a D_8, and move to the associated elliptic fibration (which also has an A_6 fiber) by a 2-neighbor step.

This elliptic fibration has D_8 and A_6 fibers, and two independent sections P, Q with height matrix

$$\begin{pmatrix} \frac{8}{7} & -\frac{5}{14} \\ -\frac{5}{14} & \frac{22}{7} \end{pmatrix}.$$

We identify a fiber F' of type E_8 and move to the associated fibration by a 2-neighbor step. Note that $Q \cdot F' = 3$, while the remaining component of the D_8 fiber has intersection 2 with F'. Therefore the new genus-1 fibration has a section.
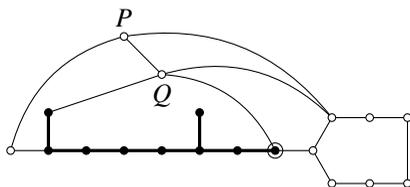
The new elliptic fibration has bad fibers of types E_8 and A_7, and a section P' of height $\frac{97}{8} = 2 + 2 \cdot 6 - 3 \cdot \frac{5}{8}$. We identify a fiber F'' of type E_7, and move to the associated elliptic fibration by a 2-neighbor step. Note that $P' \cdot F'' = 13$, while the remaining component of the A_7 fiber has intersection 2 with F''. Therefore the elliptic fibration associated to F'' has a section, and is the of the desired type $E_8 E_7$.
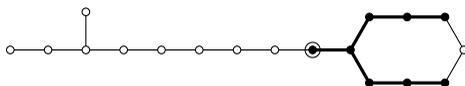
We now read out the Igusa–Clebsch invariants and work out the equation of the branch locus of $Y_-(97)$ as a double cover of $\mathcal{H}_{97}$.

Theorem 45. *A birational model over $\mathbb{Q}$ for the Hilbert modular surface $Y_-(97)$ as a double cover of $\mathbb{P}^2_{r,s}$ is given by the equation*

$$z^2 = s^2(s^2 + 14s + 1)r^6 + 2s(2s^4 + 27s^3 - 13s^2 + 15s + 1)r^5$$
$$+ (6s^6 + 80s^5 - 75s^4 + 128s^3 - 54s^2 + 18s + 1)r^4$$
$$+ 2(2s^7 + 28s^6 - 32s^5 + 84s^4 - 74s^3 + 48s^2 - 13s + 1)r^3$$
$$+ (s^8 + 18s^7 - 11s^6 + 68s^5 - 101s^4 + 112s^3 - 69s^2 + 22s + 1)r^2$$
$$+ 2s^2(s^6 + 3s^5 - 5s^4 + 7s^3 + 3s^2 - 16s + 12)r + (s-2)^4s^4.$$

It is a surface of general type.

35.2. Analysis. The branch locus is a genus-3 curve, isomorphic to the quotient of $X_0(97)$ by the Atkin–Lehner involution. We omit the formulas for the isomorphism, but they are available in the online supplement.

The Hilbert modular surface itself is of general type. The substitution $r = u - s$ simplifies the equation of the double cover somewhat, making it degree-6 in each variable. However, it complicates the original Weierstrass equation of the K3 family, so we have chosen the (r, s)-coordinates on the moduli space.

(r, s)	Sextic polynomial $f_6(x)$ defining the genus-2 curve $y^2 = f_6(x)$
$\left(\frac{5}{2}, -2\right)$	$-100x^6 + 180x^5 + 3x^4 + 12x^3 - 207x^2 + 54x + 54$
$\left(-\frac{5}{3}, \frac{2}{3}\right)$	$115x^6 - 120x^5 - 692x^4 - 42x^3 + 643x^2 + 36x - 156$
$\left(\frac{8}{15}, -\frac{6}{5}\right)$	$-418x^6 - 99x^5 + 700x^4 + 130x^3 - 401x^2 - 45x + 81$
$\left(-\frac{14}{3}, 6\right)$	$528x^6 - 792x^5 + 311x^4 - 26x^3 - 205x^2 + 60x - 20$
$\left(-\frac{20}{7}, \frac{5}{14}\right)$	$-72x^6 - 72x^5 + 669x^4 + 706x^3 - 1623x^2 - 60x + 500$
$\left(\frac{13}{6}, -\frac{3}{2}\right)$	$1236x^6 - 852x^5 - 1919x^4 + 1702x^3 + 1473x^2 - 940x - 700$
$\left(\frac{17}{6}, -\frac{1}{3}\right)$	$200x^6 - 420x^5 + 1918x^4 - 1455x^3 + 2968x^2 + 1740x - 1175$
$\left(-\frac{13}{7}, \frac{11}{21}\right)$	$-1872x^5 - 3540x^4 + 1021x^3 + 2331x^2 - 1185x + 145$
$\left(\frac{23}{35}, -\frac{5}{14}\right)$	$370x^6 + 1084x^5 - 2510x^4 - 683x^3 - 32x^2 - 752x - 3822$
$\left(-\frac{11}{30}, \frac{5}{6}\right)$	$-1225x^6 + 3570x^5 - 3266x^4 - 176x^3 + 3463x^2 + 1446x + 5868$
$\left(\frac{1}{2}, \frac{5}{2}\right)$	$-1938x^6 + 3132x^5 + 1730x^4 - 855x^3 + 609x^2 - 9065x + 5145$
$\left(-\frac{19}{30}, \frac{3}{10}\right)$	$4900x^6 + 5320x^5 - 11751x^4 - 4255x^3 + 2867x^2 + 4515x - 1596$
$\left(-\frac{29}{18}, \frac{10}{9}\right)$	$16048x^6 - 7524x^5 - 11096x^4 + 16107x^3 - 4244x^2 - 5652x - 864$
$\left(\frac{13}{4}, -\frac{1}{4}\right)$	$-1140x^6 + 4820x^5 - 3105x^4 + 3366x^3 - 16681x^2 - 6468x - 12348$
$\left(-\frac{7}{2}, 6\right)$	$14076x^6 - 20748x^5 + 11899x^4 + 1252x^3 - 125x^2 + 2676x + 380$
$\left(\frac{9}{10}, -\frac{2}{5}\right)$	$-6688x^6 + 9840x^5 - 8271x^4 + 24640x^3 - 5373x^2 + 12150x - 7290$

Table 30. Some rational points (r, s) of small height on the surface of Theorem 45 and the corresponding genus-2 curves.

35.3. *Examples.* Table 30 lists some points of small height and their genus-2 curves.

We find a few curves with infinitely many rational points. For instance, $r = 1 - s$ gives a rational curve, with parametrization

$$(r, s) = \left(\frac{(m+1)(m+3)}{m^2 + 7}, \frac{-4(m-1)}{m^2 + 7}\right).$$

The Brauer obstruction vanishes identically along this curve. However, it turns out to be a modular curve: the corresponding abelian surfaces have endomorphism ring a (split) quaternion algebra.

Another curve of genus 0 is given by $r = -(3s^2 + 8s + 4)/(3s)$. Again, the Brauer obstruction vanishes, and this time we get a family of abelian surfaces with "honest" real multiplication.

The locus $r = \frac{1}{2} - s$ gives a genus-1 curve

$$y^2 = (2s + 1)(2s^3 - 39s^2 + 28s + 36)$$

with conductor $5862 = 2 \cdot 3 \cdot 977$ and Mordell–Weil group $\mathbb{Z}^2$.

Acknowledgements

References

[An et al. 2001] S. Y. An, S. Y. Kim, D. C. Marshall, S. H. Marshall, W. G. McCallum, and A. R. Perlis, "Jacobians of genus one curves", *J. Number Theory* **90**:2 (2001), 304–315. MR 2002g:14040 Zbl 1066.14035

[Birkenhake and Lange 2004] C. Birkenhake and H. Lange, *Complex abelian varieties*, 2nd ed., Grundlehren der Mathematischen Wissenschaften **302**, Springer, Berlin, 2004. MR 2005c:14001 Zbl 1056.14063

[Brumer 1995] A. Brumer, "The rank of $J_0(N)$", pp. 3, 41–68 in *Columbia University Number Theory Seminar* (New York, 1992), Astérisque **228**, Soc. Math. France, Paris, 1995. MR 96f:11083 Zbl 0851.11035

[Clingher and Doran 2007] A. Clingher and C. F. Doran, "Modular invariants for lattice polarized $K3$ surfaces", *Michigan Math. J.* **55**:2 (2007), 355–393. MR 2009a:14049 Zbl 1132.14035

[Deligne and Pappas 1994] P. Deligne and G. Pappas, "Singularités des espaces de modules de Hilbert, en les caractéristiques divisant le discriminant", *Compositio Math.* **90**:1 (1994), 59–79. MR 95a:11041 Zbl 0826.14027

[Dembélé and Kumar 2013] L. Dembélé and A. Kumar, "Examples of abelian surfaces with everywhere good reduction", preprint, 2013. arXiv 1309.3821

[Dolgachev 1996] I. V. Dolgachev, "Mirror symmetry for lattice polarized $K3$ surfaces", *J. Math. Sci.* **81**:3 (1996), 2599–2630. MR 97i:14024 Zbl 0890.14024

[Elkies 1998] N. D. Elkies, "Elliptic and modular curves over finite fields and related computational issues", pp. 21–76 in *Computational perspectives on number theory* (Chicago, IL), edited by D. A. Buell and J. T. Teitelbaum, AMS/IP Stud. Adv. Math. **7**, Amer. Math. Soc., Providence, RI, 1998. MR 99a:11078 Zbl 0915.11036

[Elkies 2008] N. D. Elkies, "Shimura curve computations via $K3$ surfaces of Néron–Severi rank at least 19", pp. 196–211 in *Algorithmic number theory*, edited by A. J. van der Poorten and A. Stein, Lecture Notes in Comput. Sci. **5011**, Springer, Berlin, 2008. MR 2010e:11056 Zbl 1205.11069

[Elkies ≥ 2015] N. D. Elkies, "Elliptic curves of high rank over $\mathbb{Q}$ and $\mathbb{Q}(t)$", In preparation.

[Friedman 1984] R. Friedman, "A new proof of the global Torelli theorem for $K3$ surfaces", *Ann. of Math.* (2) **120**:2 (1984), 237–269. MR 86k:14028 Zbl 0559.14004

[van der Geer 1988] G. van der Geer, *Hilbert modular surfaces*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)] **16**, Springer, Berlin, 1988. MR 89c:11073 Zbl 0634.14022

[Gritsenko and Nikulin 1997] V. A. Gritsenko and V. V. Nikulin, "Siegel automorphic form corrections of some Lorentzian Kac–Moody Lie algebras", *Amer. J. Math.* **119**:1 (1997), 181–224. MR 98g:11056 Zbl 0914.11020

[Gruenewald 2008] D. Gruenewald, *Explicit Algorithms for Humbert Surfaces*, Ph.D. thesis, University of Sydney, 2008, Available at http://echidna.maths.usyd.edu.au/~davidg/thesis.pdf.

[Hausmann 1982] W. Hausmann, "The fixed points of the symmetric Hilbert modular group of a real quadratic field with arbitrary discriminant", *Math. Ann.* **260**:1 (1982), 31–50. MR 84j:10036 Zbl 0467.10020

[Hirzebruch 1973] F. E. P. Hirzebruch, "Hilbert modular surfaces", *Enseignement Math.* (2) **19** (1973), 183–281. MR 52 #13856 Zbl 0285.14007

[Hirzebruch and van de Ven 1974] F. Hirzebruch and A. van de Ven, "Hilbert modular surfaces and the classification of algebraic surfaces", *Invent. Math.* **23** (1974), 1–29. MR 51 #517 Zbl 0296.14020

[Hirzebruch and van der Geer 1981] F. Hirzebruch and G. van der Geer, *Lectures on Hilbert modular surfaces*, Séminaire de Mathématiques Supérieures **77**, Presses de l'Université de Montréal, 1981. MR 83i:10037 Zbl 0483.14009

[Hirzebruch and Zagier 1977] F. Hirzebruch and D. Zagier, "Classification of Hilbert modular surfaces", pp. 43–77 in *Complex analysis and algebraic geometry*, edited by J. W. L. Baily and T. Shioda, Iwanami Shoten, Tokyo, 1977. MR 58 #524 Zbl 0354.14011

[Hudson 1990] R. W. H. T. Hudson, *Kummer's quartic surface*, Cambridge University Press, 1990. MR 92e:14033 Zbl 0716.14025

[Igusa 1960] J.-i. Igusa, "Arithmetic variety of moduli for genus two", *Ann. of Math.* (2) **72** (1960), 612–649. MR 22 #5637 Zbl 0122.39002

[Inose 1978] H. Inose, "Defining equations of singular $K3$ surfaces and a notion of isogeny", pp. 495–502 in *Proceedings of the International Symposium on Algebraic Geometry* (Kyoto University, 1977), edited by M. Nagata, Kinokuniya Book Store, Tokyo, 1978. MR 81h:14021

[Khare and Wintenberger 2009a] C. Khare and J.-P. Wintenberger, "Serre's modularity conjecture, I", *Invent. Math.* **178**:3 (2009), 485–504. MR 2010k:11087 Zbl 05636295

[Khare and Wintenberger 2009b] C. Khare and J.-P. Wintenberger, "Serre's modularity conjecture, II", *Invent. Math.* **178**:3 (2009), 505–586. MR 2010k:11088 Zbl 05636296

[Kulikov 1977] V. S. Kulikov, "Degenerations of $K3$ surfaces and Enriques surfaces", *Izv. Akad. Nauk SSSR Ser. Mat.* **41**:5 (1977), 1008–1042, 1199. In Russian; translated in *Math. USSR-Izv.* **11**:5 (1977), 957–989. MR 58 #22087b Zbl 0367.14014

[Kumar 2008] A. Kumar, "$K3$ surfaces associated with curves of genus two", *Int. Math. Res. Not.* **2008**:6 (2008), Art. ID rnm165, 26. MR 2009d:14044 Zbl 1145.14029

[Kumar 2014] A. Kumar, "Elliptic fibrations on a generic Jacobian Kummer surface", *J. Algebraic Geom.* **23** (2014), 599–667.

[Kuwata and Shioda 2008] M. Kuwata and T. Shioda, "Elliptic parameters and defining equations for elliptic fibrations on a Kummer surface", pp. 177–215 in *Algebraic geometry in East Asia* (Hanoi, 2005), edited by K. Konno and V. Nguyen-Khac, Adv. Stud. Pure Math. **50**, Math. Soc. Japan, Tokyo, 2008. MR 2009g:14039 Zbl 1139.14032

[Liu et al. 2005] Q. Liu, D. Lorenzini, and M. Raynaud, "On the Brauer group of a surface", *Invent. Math.* **159**:3 (2005), 673–676. MR 2005k:14036 Zbl 1077.14023

[van Luijk 2007] R. van Luijk, "K3 surfaces with Picard number one and infinitely many rational points", *Algebra Number Theory* **1**:1 (2007), 1–15. MR 2008d:14058 Zbl 1123.14022

[Mestre 1991] J.-F. Mestre, "Construction de courbes de genre 2 à partir de leurs modules", pp. 313–334 in *Effective methods in algebraic geometry* (Castiglioncello, 1990), edited by T. Mora and C. Traverso, Progr. Math. **94**, Birkhäuser, Boston, 1991. MR 92g:14022 Zbl 0752.14027

[Milne 1975a] J. S. Milne, "On a conjecture of Artin and Tate", *Ann. of Math.* (2) **102**:3 (1975), 517–533. MR 54 #2659 Zbl 0343.14005

[Milne 1975b] J. S. Milne, "On the conjecture of Artin and Tate", 1975, Available at http://jmilne.org/math/articles/add/1975a.pdf. Notes on *Ann. of Math. (2)* **102**:3 (1975), 517–533. Zbl 0343.14005

[Morrison 1984] D. R. Morrison, "On $K3$ surfaces with large Picard number", *Invent. Math.* **75**:1 (1984), 105–121. MR 85j:14071 Zbl 0509.14034

[Nikulin 1979a] V. V. Nikulin, "Finite groups of automorphisms of Kählerian $K3$ surfaces", *Trudy Moskov. Mat. Obshch.* **38** (1979), 75–137. In Russian. MR 81e:32033 Zbl 0433.14024

[Nikulin 1979b] V. V. Nikulin, "Integer symmetric bilinear forms and some of their geometric applications", *Izv. Akad. Nauk SSSR Ser. Mat.* **43**:1 (1979), 111–177, 238. In Russian; translated in *Math. USSR-Izv.* **14**:1 (1980), 103–167. MR 80j:10031 Zbl 0408.10011

[Oda 1982] T. Oda, *Periods of Hilbert modular surfaces*, Progress in Mathematics **19**, Birkhäuser, Boston, 1982. MR 83k:10057 Zbl 0489.14014

[Persson and Pinkham 1981] U. Persson and H. Pinkham, "Degeneration of surfaces with trivial canonical bundle", *Ann. of Math.* (2) **113**:1 (1981), 45–66. MR 82f:14030 Zbl 0426.14015

[Piatetski-Shapiro and Shafarevich 1971] I. Piatetski-Shapiro and I. R. Shafarevich, "Torelli's theorem for algebraic surfaces of type K3", *Izv. Akad. Nauk SSSR Ser. Mat.* **35** (1971), 530–572. In Russian; translated in *Math. USSR-Izv.* **5**:3 (1971), 547–588. MR 44 #1666 Zbl 0219.14021

[Rapoport 1978] M. Rapoport, "Compactifications de l'espace de modules de Hilbert–Blumenthal", *Compositio Math.* **36**:3 (1978), 255–335. MR 80j:14009 Zbl 0386.14006

[Ribet 2004] K. A. Ribet, "Abelian varieties over $\mathbf{Q}$ and modular forms", pp. 241–261 in *Modular curves and abelian varieties*, edited by J. Cremona et al., Progr. Math. **224**, Birkhäuser, Basel, 2004. MR 2005k:11120 Zbl 1092.11029

[Runge 1999] B. Runge, "Endomorphism rings of abelian surfaces and projective models of their moduli spaces", *Tohoku Math. J.* (2) **51**:3 (1999), 283–303. MR 2000g:14056 Zbl 0972.14017

[Shioda 1972] T. Shioda, "On elliptic modular surfaces", *J. Math. Soc. Japan* **24** (1972), 20–59. MR 55 #2927 Zbl 0226.14013

[Shioda 1990] T. Shioda, "On the Mordell–Weil lattices", *Comment. Math. Univ. St. Paul.* **39**:2 (1990), 211–240. MR 91m:14056 Zbl 0725.14017

[Shioda 2006] T. Shioda, "Kummer sandwich theorem of certain elliptic $K3$ surfaces", *Proc. Japan Acad. Ser. A Math. Sci.* **82**:8 (2006), 137–140. MR 2008b:14064 Zbl 1112.14044

[Tate 1966a] J. Tate, "Endomorphisms of abelian varieties over finite fields", *Invent. Math.* **2** (1966), 134–144. MR 34 #5829 Zbl 0147.20303

[Tate 1966b] J. Tate, "On the conjectures of Birch and Swinnerton-Dyer and a geometric analog", in *Séminaire Bourbaki* 1965/1966 (Exposé 306), W. A. Benjamin, Amsterdam, 1966. Reprinted as pp. 415–440 in *Séminaire Bourbaki* **9**, Soc. Math. France, Paris, 1995. MR 1610977 Zbl 0199.55604

[Tate 1975] J. Tate, "Algorithm for determining the type of a singular fiber in an elliptic pencil", pp. 33–52 in *Modular functions of one variable, IV*, edited by B. J. Birch and W. Kuyk, Lecture Notes in Math. **476**, Springer, Berlin, 1975. MR 52 #13850 Zbl 1214.14020

[Wilson 1998] J. Wilson, *Curves of genus 2 with real multiplication by a square root of* 5, Ph.D. thesis, Oxford University, 1998, Available at http://eprints.maths.ox.ac.uk/32/1/wilson.pdf.

[Wilson 2000] J. Wilson, "Explicit moduli for curves of genus 2 with real multiplication by $\mathbf{Q}(\sqrt{5})$", *Acta Arith.* **93**:2 (2000), 121–138. MR 2001f:11099 Zbl 0966.11027

elkies@math.harvard.edu   *Department of Mathematics, Harvard University, Cambridge, MA 02138, United States*

abhinav@math.mit.edu   *Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139, United States*

msp

Intermediate co-*t*-structures, two-term silting objects, τ-tilting modules, and torsion classes

Osamu Iyama, Peter Jørgensen and Dong Yang

If (A, B) and (A′, B′) are co-*t*-structures of a triangulated category, then (A′, B′) is called intermediate if A ⊆ A′ ⊆ ΣA. Our main results show that intermediate co-*t*-structures are in bijection with two-term silting subcategories, and also with support τ-tilting subcategories under some assumptions. We also show that support τ-tilting subcategories are in bijection with certain finitely generated torsion classes. These results generalise work by Adachi, Iyama, and Reiten.

Introduction

The aim of this paper is to discuss the relationship between the following objects:

- Intermediate co-*t*-structures.
- Two-term silting subcategories.
- Support τ-tilting subcategories.
- Torsion classes.

The motivation is that if T is a triangulated category with suspension functor Σ and (X, Y) is a *t*-structure of T with heart H = X ∩ ΣY, then there is a bijection between "intermediate" *t*-structures (X′, Y′) with ΣX ⊆ X′ ⊆ X and torsion pairs of H. This is due to [Beligiannis and Reiten 2007, Theorem 3.1] and [Happel et al. 1996, Proposition 2.1]; see [Woolf 2010, Proposition 2.3].

We will study a co-*t*-structure analogue of this which also involves silting subcategories, that is, full subcategories S ⊆ T with thick closure equal to T which satisfy $\mathrm{Hom}_T(S, \Sigma^i S) = 0$ for $i \geq 1$. Silting subcategories are a useful generalisation of tilting subcategories.

The next theorem follows from the bijection between bounded co-*t*-structures and silting subcategories in [Mendoza Hernández et al. 2013, Corollary 5.9]. See [Pauksztello 2008] and [Aihara and Iyama 2012] for background on co-*t*-structures

and silting subcategories. Note that the *co-heart* of a co-t-structure (A, B) is $A \cap \Sigma^{-1}B$. If F, G are full subcategories of a triangulated category, then $F * G$ denotes the full subcategory of objects e which permit a distinguished triangle $f \to e \to g$ with $f \in F$, $g \in G$.

Theorem 0.1 (Theorem 2.2). *Let T be a triangulated category*, (A, B) *a bounded co-t-structure of T with co-heart S. Then we have a bijection between the following sets*:

(i) *Co-t-structures (A', B') of T with $A \subseteq A' \subseteq \Sigma A$.*

(ii) *Silting subcategories of T which are in $S * \Sigma S$.*

The co-t-structures in (i) are called *intermediate*. The silting subcategories in (ii) are called *two-term*, motivated by the existence of a distinguished triangle $s_1 \to s_0 \to s'$ with $s_i \in S$ for each $s' \in S'$. The theorem reduces the study of intermediate co-t-structures to the study of two-term silting subcategories.

Our main results on two-term silting subcategories and τ-tilting theory can be summed up as follows. We extend the notion of support τ-tilting modules for finite-dimensional algebras over fields given in [Adachi et al. 2014] to essentially small additive categories; see Definitions 1.3 and 1.5. For a commutative ring $\Bbbk$, we say that a $\Bbbk$-linear category is *Hom-finite* if each Hom-set is a finitely generated $\Bbbk$-module.

Theorem 0.2 (Theorems 3.4 and 4.6). *Let T be a triangulated category with a silting subcategory S. Assume that each object of $S * \Sigma S$ can be written as a direct sum of indecomposable objects unique up to isomorphism. Then there is a bijection between the following sets*:

(i) *Silting subcategories of T which are in $S * \Sigma S$.*

(ii) *Support τ-tilting pairs of $\mathrm{mod}\, S$.*

If T is Krull–Schmidt, $\Bbbk$-linear and Hom-finite over a commutative ring $\Bbbk$, and $S = \mathrm{add}\, s$ for a silting object s, then there is a bijection between the following sets:

(iii) *Basic silting objects of T which are in $S * \Sigma S$, modulo isomorphism.*

(iv) *Basic support τ-tilting modules of $\mathrm{mod}\, E$, modulo isomorphism, where $E = \mathrm{End}_T(s)$.*

Note that in this case, there is a bijection between (i) *and* (iii) *by* [Aihara and Iyama 2012, Proposition 2.20, Lemma 2.22(a)].

Note that Theorem 0.2 is a much stronger version of Theorem 3.2 of [Adachi et al. 2014], where T is assumed to be the homotopy category of bounded complexes of finitely generated projective modules over a finite-dimensional algebra Λ over a field, and s is assumed to be Λ.

Moreover, we give the following link between τ-tilting theory and torsion classes. Our main result shows that support τ-tilting pairs correspond bijectively with certain finitely generated torsion classes, which is a stronger version of [Adachi et al. 2014, Theorem 2.7]. Note that Fac M is the subcategory of Mod C consisting of factor objects of finite direct sums of objects of M, and P(T) denotes the Ext-projective objects of T; see Definition 1.7.

Theorem 0.3 (Theorem 5.1). *Let $\Bbbk$ be a commutative noetherian local ring and* C *an essentially small, Krull–Schmidt, $\Bbbk$-linear Hom-finite category. There is a bijection* M $\mapsto$ Fac M *from the first of the following sets to the second*:

(i) *Support τ-tilting pairs* (M, E) *of* mod C.

(ii) *Finitely generated torsion classes* T *of* Mod C *such that each finitely generated projective* C*-module has a left* P(T)*-approximation.*

1. Basic definitions

Let C be an additive category. When we say that U is a *subcategory* of C, we always assume U is full and closed under finite direct sums and direct summands. For a collection U of objects of C, we denote by add U the smallest subcategory of C containing U.

Let C be an essentially small additive category. We write Mod C for the abelian category of contravariant additive functors from C to the category of abelian groups, and mod C for the full subcategory of finitely presented functors; see [Auslander 1974, pp. 184, 204].

The suspension functor of a triangulated category is denoted by Σ.

We first recall the notions of co-*t*-structures and silting subcategories.

Definition 1.1. Let T be a triangulated category. A *co-t-structure* on T is a pair (A, B) of full subcategories of T such that:

(i) $\Sigma^{-1}A \subseteq A$ and $\Sigma B \subseteq B$.

(ii) $\text{Hom}_T(a, b) = 0$ for $a \in A$ and $b \in B$.

(iii) For each $t \in T$ there is a triangle $a \to t \to b \to \Sigma a$ in T with $a \in A$ and $b \in B$.

The *co-heart* is defined as the intersection $A \cap \Sigma^{-1}B$. See [Pauksztello 2008; Bondarko 2010].

Definition 1.2. Let T be a triangulated category.

(i) A subcategory U of T is called a *presilting subcategory* if $T(u, \Sigma^{\geq 1}u') = 0$ for any $u, u' \in U$.

(ii) A presilting subcategory $S \subseteq T$ is a *silting subcategory* if $\text{thick}(S) = T$; see [Aihara and Iyama 2012, Definition 2.1(a)]. Here $\text{thick}(S)$ denotes the smallest thick subcategory of T containing S.

(iii) An object $u \in \mathsf{T}$ is called a *presilting object* if it satisfies $\mathsf{T}(u, \Sigma^{\geq 1} u) = 0$, namely, if $\mathrm{add}(u)$ is a presilting subcategory. Similarly an object $u \in \mathsf{T}$ is called a *silting object* if $\mathrm{add}(u)$ is a silting subcategory.

Next we introduce the notion of support τ-tilting subcategories.

Definition 1.3. Let C be an essentially small additive category.

(i) Let M be a subcategory of $\mathrm{mod}\,\mathsf{C}$. A class $\left\{ P_1 \xrightarrow{\pi^m} P_0 \to m \to 0 \mid m \in \mathsf{M} \right\}$ of projective presentations in $\mathrm{mod}\,\mathsf{C}$ is said to have *property (S)* if

$$\mathrm{Hom}_{\mathrm{mod}\,\mathsf{C}}(\pi^m, m') : \mathrm{Hom}_{\mathrm{mod}\,\mathsf{C}}(P_0, m') \to \mathrm{Hom}_{\mathrm{mod}\,\mathsf{C}}(P_1, m')$$

is surjective for any $m, m' \in \mathsf{M}$.

(ii) A subcategory M of $\mathrm{mod}\,\mathsf{C}$ is said to be *τ-rigid* if there is a class of projective presentations $\{P_1 \to P_0 \to m \to 0 \mid m \in \mathsf{M}\}$ which has property (S).

(iii) A *τ-rigid pair* of $\mathrm{mod}\,\mathsf{C}$ is a pair (M, E), where M is a τ-rigid subcategory of $\mathrm{mod}\,\mathsf{C}$ and $\mathsf{E} \subseteq \mathsf{C}$ is a subcategory with $\mathsf{M}(\mathsf{E}) = 0$, that is, $m(e) = 0$ for each $m \in \mathsf{M}$ and $e \in \mathsf{E}$.

(iv) A τ-rigid pair (M, E) is *support τ-tilting* if $\mathsf{E} = \mathrm{Ker}(\mathsf{M})$ and for each $s \in \mathsf{C}$ there exists an exact sequence $\mathsf{C}(-, s) \xrightarrow{f} m^0 \to m^1 \to 0$ with $m^0, m^1 \in \mathsf{M}$ such that f is a left M-approximation.

It is useful to recall the notion of Krull–Schmidt categories:

Definition 1.4. An additive category C is called *Krull–Schmidt* if each of its objects is the direct sum of finitely many objects with local endomorphism rings. It follows that these finitely many objects are indecomposable and determined up to isomorphism; see [Bass 1968, Theorem I.3.6]. It also follows that C is *idempotent complete*; that is, for an object c of C and an idempotent $e \in \mathsf{C}(c, c)$, there exist objects c_1 and c_2 such that $c = c_1 \oplus c_2$ and $e = \mathrm{id}_{c_1}$; see [Keller 2013, 5.1].

(i) An object $c \in \mathsf{C}$ is *basic* if it has no repeated indecomposable direct summands.

(ii) For an object $c \in \mathsf{C}$, let $\#_{\mathsf{C}}(c)$ denote the number of pairwise nonisomorphic indecomposable direct summands of c.

The following is a version of Definition 1.3 for rings:

Definition 1.5. Let E be a ring such that $\mathrm{mod}\,E$ is Krull–Schmidt.

(i) A module $U \in \mathrm{mod}\,E$ is called *τ-rigid* if there is a projective presentation $P_1 \xrightarrow{\pi} P_0 \to U \to 0$ in $\mathrm{mod}\,E$ such that $\mathrm{Hom}_E(\pi, U)$ is surjective.

(ii) A τ-rigid module $U \in \mathrm{mod}\,E$ is called *support τ-tilting* if there is an idempotent $e \in E$ which satisfies $Ue = 0$ and $\#_{\mathrm{mod}\,E}(U) = \#_{\mathrm{prj}(E/EeE)}(E/EeE)$.

Remark 1.6. Part (ii) of the definition makes sense because $\mathsf{prj}(E/EeE)$ is Krull–Schmidt. Namely, since $\mathsf{mod}\, E$ is Krull–Schmidt, it follows that $\mathsf{prj}\, E$ is Krull–Schmidt with additive generator E_E. The same is hence true for $(\mathsf{prj}\, E)/[\mathsf{add}\, eE]$ for each idempotent $e \in E$, and it is not hard to check that the endomorphism ring of E_E in $(\mathsf{prj}\, E)/[\mathsf{add}\, eE]$ is E/EeE, so there is an equivalence of categories

$$(\mathsf{prj}\, E)/[\mathsf{add}\, eE] \xrightarrow{\sim} \mathsf{prj}(E/EeE).$$

Hence $\mathsf{prj}(E/EeE)$ is Krull–Schmidt.

If E is a finite-dimensional algebra over a field, then the definition coincides with the original definition of basic support τ-tilting modules by Adachi, Iyama and Reiten [Adachi et al. 2014, Definition 0.1(c)].

Finally we introduce the notion of torsion classes:

Definition 1.7. Let C be an essentially small additive category and T a full subcategory of $\mathsf{Mod}\, \mathsf{C}$.

 (i) We say that T is a *torsion class* if it is closed under factor modules and extensions.

 (ii) For a subcategory M of $\mathsf{Mod}\, \mathsf{C}$, we denote by $\mathsf{Fac}\, \mathsf{M}$ the subcategory of $\mathsf{Mod}\, \mathsf{C}$ consisting of factor objects of objects of M.

 (iii) We say that a torsion class T is *finitely generated* if there exists a full subcategory M of $\mathsf{mod}\, \mathsf{C}$ such that $\mathsf{T} = \mathsf{Fac}\, \mathsf{M}$. Clearly the objects in $\mathsf{Fac}\, \mathsf{M}$ are finitely generated C-modules, which are not necessarily finitely presented.

 (iv) An object t of a torsion class T is *Ext-projective* if $\mathrm{Ext}^1_{\mathsf{Mod}\, \mathsf{C}}(t, \mathsf{T}) = 0$. We denote by $\mathsf{P}(\mathsf{T})$ the full subcategory of T consisting of all Ext-projective objects of T.

2. Silting subcategories and co-*t*-structures

In this section, T is an essentially small, idempotent complete triangulated category.

Let (A, B) be a co-*t*-structure on T. It follows from the definition that

$$\mathsf{A} = \{t \in \mathsf{T} \mid \mathrm{Hom}(t, b) = 0 \text{ for all } b \in \mathsf{B}\},$$
$$\mathsf{B} = \{t \in \mathsf{T} \mid \mathrm{Hom}(a, t) = 0 \text{ for all } a \in \mathsf{A}\}.$$

In particular, both A and B are idempotent complete and extension closed. Hence so is the co-heart $\mathsf{S} = \mathsf{A} \cap \Sigma^{-1}\mathsf{B}$. Set

$$\mathsf{S} * \Sigma\mathsf{S} = \{t \in \mathsf{T} \mid \text{there is a triangle } s_1 \to s_0 \to t \to \Sigma s_1 \text{ with } s_0, s_1 \in \mathsf{S}\} \subseteq \mathsf{T}.$$

The following lemma will often be used without further remark:

Lemma 2.1. *There is an equality* $S * \Sigma S = \Sigma A \cap \Sigma^{-1} B$. *As a consequence,* $S * \Sigma S$ *is idempotent complete and extension closed.*

Proof. The inclusion $S * \Sigma S \subseteq \Sigma A \cap \Sigma^{-1} B$ is clear, because both S and ΣS are contained in $\Sigma A \cap \Sigma^{-1} B$, which is extension closed. Next we show the opposite inclusion. Let $t \in \Sigma A \cap \Sigma^{-1} B$. Then by Definition 1.1(iii) there is a triangle $a \to t \to b \to \Sigma a$ with $a \in A$ and $b \in B$. Since both t and Σa are in ΣA, so is b due to the fact that A is extension closed. Thus $b \in \Sigma A \cap B = \Sigma S$. Similarly, one shows that $a \in S$. Thus we obtain a triangle $\Sigma^{-1} b \to a \to t \to b$ with $\Sigma^{-1} b$ and a in S, meaning that $t \in S * \Sigma S$. $\qquad\square$

It is easy to see that $\operatorname{Hom}(s, \Sigma^{\geq 1} s') = 0$ for any $s, s' \in S$. That is, S is a presilting subcategory of T. The co-t-structure (A, B) is said to be *bounded* if

$$\bigcup_{n \in \mathbb{Z}} \Sigma^n B = T = \bigcup_{n \in \mathbb{Z}} \Sigma^n A.$$

Theorem 2.2 [Mendoza Hernández et al. 2013, Corollary 5.9]. *There is a bijection* $(A, B) \mapsto A \cap \Sigma^{-1} B$ *from the first of the following sets to the second*:

(i) *Bounded co-t-structures on* T.

(ii) *Silting subcategories of* T.

This result has the following consequence:

Theorem 2.3. *Let* (A, B) *be a bounded co-t-structure on* T *with co-heart* S. *Then there is a bijection* $(A', B') \mapsto A' \cap \Sigma^{-1} B'$ *from the first of the following sets to the second*:

(i) *Bounded co-t-structures* (A', B') *on* T *with* $A \subseteq A' \subseteq \Sigma A$.

(ii) *Silting subcategories of* T *which are in* $S * \Sigma S$.

Proof. Let (A', B') be a bounded co-t-structure on T with $A \subseteq A' \subseteq \Sigma A$. Then $B \supseteq B' \supseteq \Sigma B$. It follows that $A' \cap \Sigma^{-1} B' \subseteq \Sigma A \cap \Sigma^{-1} B = S * \Sigma S$. The last equality is by Lemma 2.1.

Let S' be a silting subcategory of T which is in $S * \Sigma S$. Let A' be the smallest extension closed subcategory of T containing $\Sigma^{\leq 0} S'$ and B' the smallest extension closed subcategory of T containing $\Sigma^{\geq 1} S'$. Then (A', B') is the bounded co-t-structure corresponding to S' as in Theorem 2.2; see [Mendoza Hernández et al. 2013, Corollary 5.9]. Since $S' \subseteq S * \Sigma S$, it follows that A' is contained in the smallest extension closed subcategory of T containing $\Sigma^{\leq 1} S$, which is exactly ΣA. Similarly, one shows that B' is contained in B, implying that A' contains A. Thus, $A \subseteq A' \subseteq \Sigma A$. $\qquad\square$

The co-*t*-structures in (i) are called *intermediate* with respect to (A, B). The silting subcategories in (ii) are called *2-term* with respect to S. Clearly, if (A′, B′) is intermediate with respect to (A, B), then (A, B) is intermediate with respect to (Σ^{-1}A′, Σ^{-1}B′). The next result is a corollary of Theorems 2.2 and 2.3:

Corollary 2.4. *Let* S *and* S′ *be two silting subcategories of* T. *If* S′ *is 2-term with respect to* S, *then* S *is 2-term with respect to* Σ^{-1}S′.

3. Two-term silting subcategories and support τ-tilting pairs

In this section, T is an essentially small, idempotent complete triangulated category, and S ⊆ T is a silting subcategory.

Remark 3.1.   (i) There is a functor

$$F : \mathsf{T} \to \operatorname{Mod} \mathsf{S}, \quad t \mapsto \mathsf{T}(-, t)|_{\mathsf{S}},$$

sometimes known as the restricted Yoneda functor.

(ii) By Yoneda's lemma, for $M \in \operatorname{Mod} \mathsf{S}$ and $s \in \mathsf{S}$, there is a natural isomorphism

$$\operatorname{Hom}_{\operatorname{Mod} \mathsf{S}}(\mathsf{S}(-, s), M) \xrightarrow{\sim} M(s);$$

see [Auslander 1974, p. 185].

(iii) By [Iyama and Yoshino 2008, Proposition 6.2(3)], the functor F from (i) induces an equivalence

$$(\mathsf{S} * \Sigma \mathsf{S})/[\Sigma \mathsf{S}] \xrightarrow{\sim} \operatorname{mod} \mathsf{S}. \tag{1}$$

This follows from that proposition by setting $\mathscr{X} = \mathsf{S}$, $\mathscr{Y} = \Sigma \mathsf{S}$, and observing that the proof works in the generality of the present paper.

Lemma 3.2. *Let* U *be a full subcategory of* S * ΣS. *For* $u \in \mathsf{U}$ *let*

$$s_1^u \xrightarrow{\sigma} s_0^u \longrightarrow u \longrightarrow \Sigma s_1^u \tag{2}$$

be a distinguished triangle in T *with* $s_0^u, s_1^u \in \mathsf{S}$. *Applying the functor* F *gives a projective presentation*

$$P_1^U \xrightarrow{\pi^u} P_0^U \longrightarrow U \longrightarrow 0 \tag{3}$$

in mod S, *and*

U *is a presilting subcategory* $\iff$ *the class* $\{\pi^u \mid u \in \mathsf{U}\}$ *has property* (S).

Proof. Clearly, F applied to the distinguished triangle (2) gives the projective presentation (3).

To get the bi-implication in the last line of the lemma, first note that for $u, u' \in \mathsf{U}$ we have

$$\mathsf{T}(u, \Sigma^{\geq 2} u') = 0 \tag{4}$$

since $u, u' \in \mathsf{S} * \Sigma\mathsf{S}$.

By Remark 3.1(ii), the map $\mathrm{Hom}_{\mathrm{mod}\,\mathsf{S}}(\pi, F(u'))$ is the same as

$$\mathsf{T}(s_0^u, u') \to \mathsf{T}(s_1^u, u'). \tag{5}$$

So the class $\{\pi^u \mid u \in \mathsf{U}\}$ has property (S) if and only if the morphism (5) is surjective for all $u, u' \in \mathsf{U}$. However, the distinguished triangle (2) induces an exact sequence

$$\mathsf{T}(s_0^u, u') \longrightarrow \mathsf{T}(s_1^u, u') \longrightarrow \mathsf{T}(\Sigma^{-1} u, u') \longrightarrow \mathsf{T}(\Sigma^{-1} s_0^u, u'),$$

where the last module is 0 since $u' \in \mathsf{S} * \Sigma\mathsf{S}$. So (5) is surjective if and only if $\mathsf{T}(\Sigma^{-1} u, u') \cong \mathsf{T}(u, \Sigma u') = 0$. This happens for all $u, u' \in \mathsf{U}$ if and only if U is presilting, because of (4). □

Theorem 3.3. *The functor $F : \mathsf{T} \to \mathrm{Mod}\,\mathsf{S}$ induces a surjection*

$$\Phi : \mathsf{U} \mapsto (F(\mathsf{U}), \mathsf{S} \cap \Sigma^{-1}\mathsf{U})$$

from the first of the following sets to the second:

  (i) *Presilting subcategories of T which are contained in $\mathsf{S} * \Sigma\mathsf{S}$.*

 (ii) *τ-rigid pairs of $\mathrm{mod}\,\mathsf{S}$.*

It restricts to a surjection Ψ from the first of the following sets to the second:

(iii) *Silting subcategories of T which are contained in $\mathsf{S} * \Sigma\mathsf{S}$.*

(iv) *Support τ-tilting pairs of $\mathrm{mod}\,\mathsf{S}$.*

Proof. We need to prove

 (a) The map Φ has values in τ-rigid pairs of $\mathrm{mod}\,\mathsf{S}$.

 (b) The map Φ is surjective.

 (c) The map Ψ has values in support τ-tilting pairs of $\mathrm{mod}\,\mathsf{S}$.

 (d) The map Ψ is surjective.

(a) Let U be a presilting subcategory of T which is contained in $\mathsf{S} * \Sigma\mathsf{S}$. For each $u \in \mathsf{U}$, there is a distinguished triangle $s_1 \to s_0 \to u \to \Sigma s_1$ with $s_0, s_1 \in \mathsf{S}$. Lemma 3.2 says that F sends the set of these triangles to a set of projective presentations (3) which has property (S), because U is presilting. It remains to show that for $u \in \mathsf{U}$ and $u' \in \mathsf{S} \cap \Sigma^{-1}\mathsf{U}$ we have $F(u)(u') = 0$. This is again true because $F(u)(u') = \mathsf{T}(u', u)$ and U is presilting.

(b) Let (M, E) be a τ-rigid pair of $\mathrm{mod}\,S$. For each $m \in M$ take a projective presentation

$$P_1 \xrightarrow{\pi^m} P_0 \longrightarrow m \longrightarrow 0 \tag{6}$$

such that the class $\{\pi^m \mid m \in M\}$ has property (S). By Remark 3.1(ii) there is a unique morphism $f_m : s_1 \to s_0$ in S such that $F(f_m) = \pi^m$. Moreover, $F(\mathrm{cone}(f_m)) \cong m$. Since (6) has property (S), it follows from Lemma 3.2 that the category

$$U_1 := \{\mathrm{cone}(f_m) \mid m \in M\}$$

is a presilting subcategory, and the inclusion $U_1 \subseteq S * \Sigma S$ is clear. Let U be the additive hull of U_1 and ΣE in $S * \Sigma S$. Now we show that U is a presilting subcategory of T. Let $e \in E$. Clearly we have $T(\mathrm{cone}(f_m) \oplus \Sigma e, \Sigma^2 e) = 0$. Applying $T(e, -)$ to a triangle $s_1 \xrightarrow{f_m} s_0 \to \mathrm{cone}(f_m) \to \Sigma s_1$, we have an exact sequence

$$T(e, s_1) \xrightarrow{f_m} T(e, s_0) \longrightarrow T(e, \mathrm{cone}(f_m)) \longrightarrow 0,$$

which is isomorphic to $P_1(e) \xrightarrow{\pi^m} P_0(e) \to m(e) \to 0$ by Remark 3.1(ii). The condition $M(E) = 0$ implies that $T(e, \mathrm{cone}(f_m)) = 0$. Thus the assertion follows. It is clear that $\Phi(U) = (M, E)$.

(c) Let U be a silting subcategory of T which is contained in $S * \Sigma S$.

Let $s \in S$ be an object of $\mathrm{Ker}\,F(U)$, i.e., $T(s, u) = 0$ for each $u \in U$. This implies that $U \oplus \mathrm{add}(\Sigma s)$ is also a silting subcategory of T in $S * \Sigma S$. It follows from [Aihara and Iyama 2012, Theorem 2.18] that Σs belongs to U, whence s belongs to $\Sigma^{-1}U$ and hence to $S \cap \Sigma^{-1}U$. This shows the inclusion $\mathrm{Ker}\,F(U) \subseteq S \cap \Sigma^{-1}U$. The reverse inclusion was shown in (a), so $\mathrm{Ker}\,F(U) = S \cap \Sigma^{-1}U$.

By Corollary 2.4, we have $S \subseteq (\Sigma^{-1}U) * U$. In particular, for $s \in S$, there is a distinguished triangle

$$s \longrightarrow u^0 \longrightarrow u^1 \longrightarrow \Sigma s. \tag{7}$$

Applying F, we obtain an exact sequence

$$F(s) \xrightarrow{f} F(u^0) \longrightarrow F(u^1) \longrightarrow 0. \tag{8}$$

For each $u \in U$, we have the commutative diagram

$$
\begin{array}{ccccc}
T(u^0, u) & \longrightarrow & T(s, u) & \longrightarrow & T(u^1, \Sigma u) = 0 \\
\downarrow & & \downarrow & & \\
\mathrm{Hom}_{\mathrm{mod}\,S}(F(u^0), F(u)) & \xrightarrow{\ f^*\ } & \mathrm{Hom}_{\mathrm{mod}\,S}(F(s), F(u)) & &
\end{array}
$$

The right vertical map is induced from the Yoneda embedding, so it is bijective. It follows that f^* is surjective, that is, f is a left $F(\mathsf{U})$-approximation. Altogether, we have shown that $\Phi(\mathsf{U})$ is a support τ-tilting pair of $\mathrm{mod}\,\mathsf{S}$.

(d) Let (M, E) be a support τ-tilting pair of $\mathrm{mod}\,\mathsf{S}$, and let U be the preimage of (M, E) under the map Φ constructed in (b).

By definition, for each $s \in \mathsf{S}$ there is an exact sequence $F(s) \xrightarrow{f} F(u_s^0) \rightarrow F(u_s^1) \rightarrow 0$ such that $u_s^0, u_s^1 \in \mathsf{U}$ and f is a left $F(\mathsf{U})$-approximation. By Yoneda's lemma, there is a unique morphism $\alpha : s \rightarrow u_s^0$ such that $F(\alpha) = f$. Form the distinguished triangle

$$s \xrightarrow{\;\alpha\;} u_s^0 \longrightarrow t_s \longrightarrow \Sigma s. \tag{9}$$

Let $\widetilde{\mathsf{U}}$ be the additive closure of U and $\{t_s \mid s \in \mathsf{U}\}$. We claim that $\widetilde{\mathsf{U}}$ is a silting subcategory of T contained in $\mathsf{S} * \Sigma\mathsf{S}$ such that $\Phi(\widetilde{\mathsf{U}}) = (\mathsf{M}, \mathsf{E})$.

First, $t_s \in u_s^0 * \Sigma s \subseteq \mathsf{S} * \Sigma\mathsf{S}$. Therefore, $\widetilde{\mathsf{U}} \subseteq \mathsf{S} * \Sigma\mathsf{S}$.

Second, by applying F to the triangle (9), we see that $F(t_s)$ and $F(u_s^1)$ are isomorphic in $\mathrm{mod}\,\mathsf{S}$. For $u \in \mathsf{U}$, consider the following commutative diagram.

$$
\begin{array}{ccccccc}
\mathsf{T}(u_s^0, u) & \xrightarrow{\;\;\alpha^*\;\;} & \mathsf{T}(s, u) & \longrightarrow & \mathsf{T}(t_s, \Sigma u) & \longrightarrow & \mathsf{T}(u_s^0, \Sigma u) = 0 \\
{\scriptstyle F(-)}\downarrow & & \cong\downarrow & & & & \\
\mathrm{Hom}_{\mathrm{mod}\,\mathsf{S}}(F(u_s^0), F(u)) & \xrightarrow[\;\;f^*\;\;]{} & \mathrm{Hom}_{\mathrm{mod}\,\mathsf{S}}(F(s), F(u)) & & & &
\end{array}
$$

By Remark 3.1(iii), the map $F(-)$ is surjective. Because f is a left $F(\mathsf{U})$-approximation, f^* is also surjective. So α^* is surjective too, implying that $\mathsf{T}(t_s, \Sigma u) = 0$. On the other hand, applying $\mathsf{T}(u, -)$ to the triangle (9), we obtain an exact sequence

$$\mathsf{T}(u, \Sigma u_s^0) \longrightarrow \mathsf{T}(u, \Sigma t_s) \longrightarrow \mathsf{T}(u, \Sigma^2 s).$$

The two outer terms are trivial, hence so is the middle term. Moreover, if $s' \in \mathsf{S}$, then applying $\mathsf{T}(t_{s'}, -)$ to the triangle (9) gives an exact sequence

$$\mathsf{T}(t_{s'}, \Sigma u_s^0) \longrightarrow \mathsf{T}(t_{s'}, \Sigma t_s) \longrightarrow \mathsf{T}(t_{s'}, \Sigma^2 s).$$

The two outer terms are trivial, hence so is the middle term. It follows that $\widetilde{\mathsf{U}}$ is presilting. It is then silting because it generates S.

Thirdly, $F(\widetilde{\mathsf{U}}) = F(\mathsf{U})$ because $F(t_s) \cong F(u_s^1)$.

Finally, $\mathsf{S} \cap \Sigma^{-1}\widetilde{\mathsf{U}} = \mathsf{E}$. This is because $\mathsf{S} \cap \Sigma^{-1}\widetilde{\mathsf{U}} \supseteq \mathsf{S} \cap \Sigma^{-1}\mathsf{U} = \mathsf{E}$ and $\mathsf{S} \cap \Sigma^{-1}\widetilde{\mathsf{U}} \subseteq \mathrm{Ker}\,F(\mathsf{U}) = \mathsf{E}$. $\qquad\square$

Theorem 3.4. *Assume that each object of* $\mathsf{S} * \Sigma\mathsf{S}$ *can be written as the direct sum of indecomposable objects which are unique up to isomorphism. Then the maps* Φ *and* Ψ *defined in* Theorem 3.3 *are bijective.*

Proof. It suffices to show the injectivity of Φ.

By Remark 3.1(iii), when we apply the functor $F : S * \Sigma S \to \text{mod } S$, we are in effect forgetting the indecomposable direct summands which are in ΣS. So if $F(u) \cong F(u')$ for $u, u' \in S * \Sigma S$, then there is an isomorphism $u \oplus \Sigma s \cong u' \oplus \Sigma s'$ for some $s, s' \in S$. By the assumption in the theorem, if we assume that u and u' do not have direct summands in ΣS, then $u \cong u'$.

Now let U and U' be two presilting subcategories of T contained in $S * \Sigma S$ such that $\Phi(U) = \Phi(U')$. Let U_1 and U_1' be respectively the full subcategories of U and U' consisting of objects without direct summands in ΣS. Then $U = U_1 \oplus (U \cap \Sigma S)$ and $U' = U_1' \oplus (U' \cap \Sigma S)$. Since $\Phi(U) = \Phi(U')$, it follows that $F(U_1) = F(U_1')$ and $U \cap \Sigma S = U' \cap \Sigma S$. The first equality, by the above argument, implies that $U_1 = U_1'$. Therefore $U = U'$, which shows the injectivity of Φ. $\square$

4. The Hom-finite Krull–Schmidt silting object case

In this section, $\Bbbk$ is a commutative ring, T is a triangulated category which is essentially small, Krull–Schmidt, $\Bbbk$-linear and Hom-finite, and $s \in T$ is a basic silting object.

We write $E = T(s, s)$ for the endomorphism ring and $S = \text{add}(s)$ for the associated silting subcategory.

Remark 4.1. (i) We write $\text{Mod } E$ for the abelian category of right E-modules, $\text{mod } E$ for the full subcategory of finitely presented modules, and $\text{prj } E$ for the full subcategory of finitely generated projective modules.

(ii) Since s is an additive generator of S, there is an equivalence

$$G : \text{Mod } S \xrightarrow{\sim} \text{Mod } E, \quad M \mapsto M(s),$$

which restricts to an equivalence

$$\text{mod } S \xrightarrow{\sim} \text{mod } E, \quad M \mapsto M(s).$$

This permits us to move freely between the "E-picture" and the "S-picture" which was used in the previous section.

(iii) The restricted Yoneda functor F from the S-picture corresponds to the functor

$$T \to \text{Mod } E, \quad t \mapsto T(s, t)$$

in the E-picture.

(iv) By [Auslander 1974, Proposition 2.2(e)] the functor $t \mapsto T(s, t)$ from (iii) restricts to an equivalence

$$Y : S \xrightarrow{\sim} \text{prj } E.$$

Since $S = \mathrm{add}(s)$ is closed under direct sums and summands, it is Krull–Schmidt, and it follows that so is $\mathrm{prj}\, E$.

(v) By Remark 3.1(iii) the functor $t \mapsto \mathsf{T}(s, t)$ from (iii) induces an equivalence

$$(\mathsf{S} * \Sigma\mathsf{S})/[\Sigma\mathsf{S}] \xrightarrow{\sim} \mathrm{mod}\, E. \tag{10}$$

Since $\mathsf{S} * \Sigma\mathsf{S}$ is obviously closed under direct sums, and under direct summands by Lemma 2.1, it is Krull–Schmidt. Hence so is $(\mathsf{S} * \Sigma\mathsf{S})/[\Sigma\mathsf{S}]$ and it follows that so is $\mathrm{mod}\, E$.

(vi) The additive category $\mathrm{prj}\, E$ is Krull–Schmidt by part (iv) and has additive generator E_E. The same is hence true for $(\mathrm{prj}\, E)/[\mathrm{add}\, eE]$ for each idempotent $e \in E$. It is not hard to check that the endomorphism ring of E_E in $(\mathrm{prj}\, E)/[\mathrm{add}\, eE]$ is E/EeE, so there is an equivalence of categories

$$(\mathrm{prj}\, E)/[\mathrm{add}\, eE] \xrightarrow{\sim} \mathrm{prj}(E/EeE).$$

In particular, $\mathrm{prj}(E/EeE)$ is Krull–Schmidt.

The following result is essentially already in [Aihara 2013, Proposition 2.16], [Fei and Derksen 2011, start of Section 5], and [Wei 2013, Proposition 6.1], all of which give triangulated versions of Bongartz's classic proof:

Lemma 4.2 (Bongartz completion). *Let $u \in \mathsf{S} * \Sigma\mathsf{S}$ be a presilting object. Then there exists an object $u' \in \mathsf{S} * \Sigma\mathsf{S}$ such that $u \oplus u'$ is a silting object.*

Proof. This has essentially the same proof as classic Bongartz completion: Since T is Hom-finite over the commutative ring $\Bbbk$, there is a right $\mathrm{add}(u)$-approximation $u_0 \to \Sigma s$. This gives a distinguished triangle $s \to u' \to u_0 \to \Sigma s$, and it is straightforward to check that u' has the desired properties. $\square$

The following result is essentially already contained in [Fei and Derksen 2011, Theorem 5.4]:

Proposition 4.3. *Let $u \in \mathsf{S} * \Sigma\mathsf{S}$ be a basic presilting object. Then*

$$u \text{ is a silting object} \iff \#_{\mathsf{T}}(u) = \#_{\mathsf{T}}(s).$$

Proof. The implication $\Longrightarrow$ is immediate from [Aihara and Iyama 2012, Theorem 2.27], and $\Longleftarrow$ is a straightforward consequence of that theorem and Lemma 4.2. $\square$

As a consequence, we have:

Corollary 4.4. *Let U be a presilting subcategory of T contained in $\mathsf{S} * \Sigma\mathsf{S}$. Then there exists $u \in \mathsf{U}$ such that $\mathsf{U} = \mathrm{add}(u)$.*

Proof. Suppose on the contrary that $\mathsf{U} \neq \mathsf{add}(u)$ for each $u \in \mathsf{U}$. Then U contains infinitely many isomorphism classes of indecomposable objects. In particular, there is a basic presilting object $u \in \mathsf{U}$ such that $\#_\mathsf{T}(u) = \#_\mathsf{T}(s) + 1$. By Lemma 4.2, there is an object $u' \in \mathsf{T}$ such that $u \oplus u'$ is a basic silting object of T. Therefore, $\#_\mathsf{T}(s) + 1 = \#_\mathsf{T}(u) \leq \#_\mathsf{T}(u \oplus u') = \#_\mathsf{T}(s)$, a contradiction. Here the last equality follows from Proposition 4.3. □

Theorem 3.3 in the current setting combined with Corollary 4.4 immediately yields the following result. For an object u of $\mathsf{S} * \Sigma\mathsf{S}$, let Σu_1 be its maximal direct summand in $\Sigma\mathsf{S}$.

Theorem 4.5. *The assignment*

$$u \mapsto (\mathsf{add}(F(u)), \mathsf{add}(u_1))$$

defines a bijection from the first of the following sets to the second:

(i) *Basic presilting objects of* T *which are in* $\mathsf{S} * \Sigma\mathsf{S}$, *modulo isomorphism.*

(ii) τ*-rigid pairs of* $\mathsf{mod}\,\mathsf{S}$.

It restricts to a bijection from the first of the following sets to the second:

(iii) *Basic silting objects of* T *which are in* $\mathsf{S} * \Sigma\mathsf{S}$, *modulo isomorphism.*

(iv) *Support* τ*-tilting pairs of* $\mathsf{mod}\,\mathsf{S}$.

As a consequence, if (M, E) is a τ-rigid pair of $\mathsf{mod}\,\mathsf{S}$, then there is an S-module M such that $\mathsf{M} = \mathsf{add}(M)$.

Next we move to the E-picture. Recall from Remark 4.1(ii) and (iv) that there are equivalences $G : \mathsf{Mod}\,\mathsf{S} \xrightarrow{\sim} \mathsf{Mod}\,E$ and $Y : \mathsf{S} \xrightarrow{\sim} \mathsf{prj}\,E$.

Theorem 4.6. *An E-module U is a support τ-tilting module if and only if the pair*

$$\left(G^{-1}(\mathsf{add}(U)), Y^{-1}(\mathsf{add}(eE))\right)$$

is a support τ-tilting pair of $\mathsf{mod}\,\mathsf{S}$ *for some idempotent $e \in E$.*

Consequently, the functor $\mathsf{T}(s, -) : \mathsf{T} \to \mathsf{Mod}\,E$ *induces a bijection from the first of the following sets to the second:*

(i) *Basic silting objects of* T *which are in* $\mathsf{S} * \Sigma\mathsf{S}$, *modulo isomorphism.*

(ii) *Basic support τ-tilting modules of* $\mathsf{mod}\,E$, *modulo isomorphism.*

Proof. We only prove the first assertion. The proof is divided into three parts. Let $u_p \in \mathsf{S} * \Sigma\mathsf{S}$ be such that u_p has no direct summand in $\Sigma\mathsf{S}$ and $F(u_p) = G^{-1}(U)$.

(a) It is clear that U is a τ-rigid E-module if and only if $G^{-1}(\mathsf{add}(U))$ is a τ-rigid subcategory of $\mathsf{mod}\,\mathsf{S}$.

(b) Let e be an idempotent of E and let $u_1 \in \mathsf{S}$ be such that $Y(u_1) = eE$. We have

$$Ue \cong \mathrm{Hom}_E(eE, U)$$
$$= \mathrm{Hom}_{\mathrm{Mod}\,\mathsf{S}}(\mathsf{S}(-, u_1), F(u_p))$$
$$\cong F(u_p)(u_1) \qquad\qquad \text{Remark 3.1(ii)}.$$

Therefore $Ue = 0$ if and only if $M(u') = 0$ for each $M \in \mathrm{add}(F(u_p)) = G^{-1}(\mathrm{add}(U))$ and each $u' \in \mathrm{add}(u_1) = Y^{-1}(\mathrm{add}(eE))$.

(c) Suppose that $(G^{-1}(\mathrm{add}(U)), Y^{-1}(\mathrm{add}(eE)))$ is a τ-rigid pair. Let u be the corresponding basic presilting object of T as in Theorem 4.5. More precisely, let $u = u_p \oplus \Sigma u_1$, where u_p and u_1 are as above. Then

$$\left(G^{-1}(\mathrm{add}(U)), Y^{-1}(\mathrm{add}(eE))\right) \text{ is a support } \tau\text{-tilting pair}$$

$$\Longleftrightarrow u \text{ is a silting object} \qquad\qquad \text{Theorem 4.5}$$
$$\Longleftrightarrow \#_{\mathsf{T}}(u) = \#_{\mathsf{T}}(s) \qquad\qquad \text{Proposition 4.3}$$
$$\Longleftrightarrow \#_{\mathsf{S}*\Sigma\mathsf{S}}(u) = \#_{\mathsf{S}}(s)$$
$$\Longleftrightarrow \#_{\mathsf{S}*\Sigma\mathsf{S}}(u) = \#_{\mathrm{prj}\,E}(E) \qquad\qquad \text{Remark 4.1(iv)}$$
$$\Longleftrightarrow \#_{(\mathsf{S}*\Sigma\mathsf{S})/[\Sigma\mathsf{S}]}(u) + \#_{\mathsf{S}*\Sigma\mathsf{S}}(\Sigma u_1) = \#_{\mathrm{prj}\,E}(E)$$
$$\Longleftrightarrow \#_{\mathrm{mod}\,E}(U) + \#_{\mathrm{prj}\,E}(eE) = \#_{\mathrm{prj}\,E}(E) \qquad \text{Remark 4.1(iv), (v)}$$
$$\Longleftrightarrow \#_{\mathrm{mod}\,E}(U) = \#_{\mathrm{prj}\,E}(E) - \#_{\mathrm{prj}\,E}(eE)$$
$$\Longleftrightarrow \#_{\mathrm{mod}\,E}(U) = \#_{(\mathrm{prj}\,E)/[\mathrm{add}\,eE]}(E)$$
$$\Longleftrightarrow \#_{\mathrm{mod}\,E}(U) = \#_{\mathrm{prj}(E/EeE)}(E/EeE) \qquad\qquad \text{Remark 4.1(vi)}$$
$$\Longleftrightarrow U \text{ is a support } \tau\text{-tilting module}. \qquad\qquad \square$$

5. Support τ-tilting pairs and torsion classes

In this section $\Bbbk$ is a commutative noetherian local ring and C is an essentially small, Krull–Schmidt, $\Bbbk$-linear and Hom-finite category.

The main result in this section is the following:

Theorem 5.1. *There is a bijection* $\mathsf{M} \mapsto \mathrm{Fac}\,\mathsf{M}$ *from the first of the following sets to the second*:

(i) *Support τ-tilting pairs* (M, E) *of* $\mathrm{mod}\,\mathsf{C}$.

(ii) *Finitely generated torsion classes* T *of* $\mathrm{Mod}\,\mathsf{C}$ *such that each finitely generated projective C-module has a left $\mathsf{P}(\mathsf{T})$-approximation*.

We start with the following observation:

Lemma 5.2. *Let* M *be a subcategory of* mod C. *The following conditions are equivalent*:

(i) M *is* τ-*rigid.*

(ii) $\mathrm{Ext}^1_{\mathrm{Mod}\,\mathsf{C}}(\mathsf{M}, \mathrm{Fac}\,\mathsf{M}) = 0.$

(iii) *Each* $m \in \mathsf{M}$ *has a minimal projective presentation*

$$0 \longrightarrow \Omega^2 m \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \longrightarrow m \longrightarrow 0$$

such that for each $m' \in \mathsf{M}$ *and each morphism* $f : P_1 \to m'$, *there exist morphisms* $a : P_0 \to m'$ *and* $b : P_1 \to \Omega^2 m$ *such that* $f = ad_1 + fd_2b.$

$$0 \longrightarrow \Omega^2 m \underset{b}{\overset{d_2}{\rightleftarrows}} P_1 \xrightarrow{d_1} P_0 \longrightarrow m \longrightarrow 0$$

with $f : P_1 \to m'$, $a : P_0 \to m'$

Proof. (i) $\Longrightarrow$ (ii): For each $m \in \mathsf{M}$, there exists a projective presentation $P_1 \xrightarrow{\pi} P_0 \to m \to 0$ such that $\mathrm{Hom}_{\mathrm{Mod}\,\mathsf{C}}(\pi, m')$ is surjective for each $m' \in \mathsf{M}$. Let $n \in \mathrm{Fac}\,\mathsf{M}$ be given and pick an epimorphism $p : m' \to n$ with $m' \in \mathsf{M}$. To show $\mathrm{Ext}^1_{\mathrm{Mod}\,\mathsf{C}}(m, n) = 0$, it is enough to show that each $f \in \mathrm{Hom}_{\mathrm{Mod}\,\mathsf{C}}(P_1, n)$ factors through π. Since p is an epimorphism and P_1 is projective, there exists $g : P_1 \to m'$ such that $f = pg$. Then there exists $h : P_0 \to m'$ such that $g = h\pi$, by the property of π.

$$\begin{array}{ccccc} P_1 & \xrightarrow{\pi} & P_0 & \longrightarrow & m \longrightarrow 0 \\ g \downarrow & \overset{f}{\searrow} \overset{h'}{\nearrow} & & & \\ m' & \xrightarrow{p} & n & & \end{array}$$

Thus $f = ph\pi$, and we have the assertion.

(ii) $\Longrightarrow$ (iii): For each $m \in \mathsf{M}$, take a minimal projective presentation $0 \to \Omega^2 m \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \to m \to 0$. Let $m' \in \mathsf{M}$ and $f : P_1 \to m'$ be given, set $n := \mathrm{Im}(fd_2)$ and let $0 \to n \xrightarrow{\iota} m' \xrightarrow{\pi} n' \to 0$ be an exact sequence. Then $\pi f : P_1 \to n'$ factors through $P_1 \to \mathrm{Im}\,d_1$. Since $n' \in \mathrm{Fac}\,\mathsf{M}$ and $\mathrm{Ext}^1_{\mathrm{Mod}\,\mathsf{C}}(m, \mathrm{Fac}\,\mathsf{M}) = 0$, there exists $g : P_0 \to n'$ such that $gd_1 = \pi f.$

$$\begin{array}{ccccccc} 0 \longrightarrow \Omega^2 m & \xrightarrow{d_2} & P_1 & \longrightarrow & \mathrm{Im}\,d_1 & \longrightarrow 0 & \qquad 0 \longrightarrow \mathrm{Im}\,d_1 \longrightarrow P_0 \longrightarrow m \longrightarrow 0 \\ f' \downarrow & & f \downarrow & & \downarrow & & \qquad\qquad \downarrow \overset{g}{\nearrow} \\ 0 \longrightarrow n & \xrightarrow{\iota} & m' & \xrightarrow{\pi} & n' & \longrightarrow 0 & \qquad\qquad\qquad n' \end{array}$$

Since π is an epimorphism and P_0 is projective, there exists $a : P_0 \to m'$ such that $g = \pi a$. Since $\pi(f - ad_1) = 0$, there exists $h : P_1 \to n$ such that $f = ad_1 + \iota h$. Since f' is surjective (by definition of n) and P_1 is projective, there exists $b : P_1 \to \Omega^2 m$ such that $h = f'b$.

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & \Omega^2 m & \underset{b}{\overset{d_2}{\rightleftarrows}} & P_1 & \overset{d_1}{\longrightarrow} & P_0 & \longrightarrow & m & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle f'} & {\scriptstyle h} & \downarrow{\scriptstyle f} & {\scriptstyle a} & \downarrow{\scriptstyle g} & & & & \\
0 & \longrightarrow & n & \underset{\iota}{\longrightarrow} & m' & \underset{\pi}{\longrightarrow} & n' & \longrightarrow & 0 & &
\end{array}
$$

Then we have $f = ad_1 + \iota f'b = ad_1 + fd_2b$.

(iii) $\implies$ (i): For each $m \in \mathsf{M}$, take a minimal projective presentation $0 \to \Omega^2 m \overset{d_2}{\longrightarrow} P_1 \overset{d_1}{\longrightarrow} P_0 \to m \to 0$ satisfying the assumption in (iii). We need to show that each $f : P_1 \to m'$ with $m' \in \mathsf{M}$ factors through d_1. By our assumption, there exist $a : P_0 \to m'$ and $b : P_1 \to \Omega^2 m$ such that $f = ad_1 + fd_2b$. Applying our assumption to $fd_2b : P_1 \to m'$, there exist $a' : P_0 \to m'$ and $b' : P_1 \to \Omega^2 m$ such that $fd_2b = a'd_1 + fd_2bd_2b'$. Thus $f = (a+a')d_1 + fd_2bd_2b'$. Repeating a similar argument gives

$$\mathrm{Hom}_{\mathsf{Mod}\,\mathsf{C}}(P_1, m) = \mathrm{Hom}_{\mathsf{Mod}\,\mathsf{C}}(P_0, m)d_1 + \mathrm{Hom}_{\mathsf{Mod}\,\mathsf{C}}(P_1, m)(\mathrm{rad}\,\mathrm{End}_{\mathsf{Mod}\,\mathsf{C}}(P_1))^n$$

for each $n \geq 1$, since $d_2 \in \mathrm{rad}\,\mathrm{Hom}_{\mathsf{Mod}\,\mathsf{C}}(\Omega^2 m, P_1)$. Since C is Hom-finite over $\Bbbk$, we have $(\mathrm{rad}\,\mathrm{End}_{\mathsf{Mod}\,\mathsf{C}}(P_1))^\ell \subset \mathrm{End}_{\mathsf{Mod}\,\mathsf{C}}(P_1)(\mathrm{rad}\,\Bbbk)$ for sufficiently large ℓ. Thus we have

$$\mathrm{Hom}_{\mathsf{Mod}\,\mathsf{C}}(P_1, m) = \bigcap_{n \geq 0} \left(\mathrm{Hom}_{\mathsf{Mod}\,\mathsf{C}}(P_0, m)d_1 + \mathrm{Hom}_{\mathsf{Mod}\,\mathsf{C}}(P_1, m)(\mathrm{rad}\,\Bbbk)^n \right).$$

The right-hand side is equal to $\mathrm{Hom}_{\mathsf{Mod}\,\mathsf{C}}(P_0, m)d_1$ itself by Krull's intersection theorem [Matsumura 1989]. $\qquad\square$

Proposition 5.3. *Let* (M, E) *be a support τ-tilting pair of* $\mathrm{mod}\,\mathsf{C}$. *Then* $\mathrm{Fac}\,\mathsf{M}$ *is a finitely generated torsion class with* $\mathsf{P}(\mathrm{Fac}\,\mathsf{M}) = \mathsf{M}$.

Proof. (i) We show that $\mathrm{Fac}\,\mathsf{M}$ is a torsion class. Clearly $\mathrm{Fac}\,\mathsf{M}$ is closed under factor modules. We show that $\mathrm{Fac}\,\mathsf{M}$ is closed under extensions. Let $0 \to x \to y \overset{f}{\to} z \to 0$ be an exact sequence in $\mathsf{Mod}\,\mathsf{C}$ such that $x, z \in \mathrm{Fac}\,\mathsf{M}$. Take an epimorphism $p : m \to z$ with $m \in \mathsf{M}$. Since $\mathrm{Ext}^1_{\mathsf{Mod}\,\mathsf{C}}(m, x) = 0$ by Lemma 5.2(ii), we have that p factors through f. Thus we have an epimorphism $x \oplus m \to y$, and $y \in \mathrm{Fac}\,\mathsf{M}$ holds. Hence $\mathrm{Fac}\,\mathsf{M}$ is a torsion class.

(ii) Since $\text{Ext}^1_{\text{Mod C}}(\mathsf{M}, \text{Fac}\,\mathsf{M}) = 0$ by Lemma 5.2(ii), each object in M is Ext-projective in $\text{Fac}\,\mathsf{M}$. It remains to show that if n is an Ext-projective object in $\text{Fac}\,\mathsf{M}$, then $n \in \mathsf{M}$. Let $P_1 \xrightarrow{f} P_0 \xrightarrow{e} n \to 0$ be a projective presentation. Since M is support τ-tilting, there exist exact sequences $P_i \xrightarrow{g_i} m_i \xrightarrow{h_i} m_i' \to 0$ with $m_i, m_i' \in \mathsf{M}$ and a left M-approximation g_i for $i = 0, 1$.

Let $\overline{\mathsf{C}} := \mathsf{C}/\operatorname{ann}\mathsf{M}$ for the annihilator ideal $\operatorname{ann}\mathsf{M}$ of M and $\overline{P_i} := P_i \otimes_{\mathsf{C}} \overline{\mathsf{C}}$. Then we have induced exact sequences $0 \to \overline{P_i} \xrightarrow{g_i} m_i \xrightarrow{h_i} m_i' \to 0$ for $i = 0, 1$ and $\overline{P_1} \xrightarrow{f} \overline{P_0} \xrightarrow{e} n \to 0$. We have a commutative diagram

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & \overline{P_1} & \xrightarrow{g_1} & m_1 & \xrightarrow{h_1} & m_1' & \longrightarrow & 0 \\
  & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle a} & & \downarrow{\scriptstyle b} & & \\
0 & \longrightarrow & \overline{P_0} & \xrightarrow{g_0} & m_0 & \xrightarrow{h_0} & m_0' & \longrightarrow & 0
\end{array}
$$

of exact sequences. Taking a mapping cone, we have an exact sequence

$$
0 \longrightarrow \overline{P_1} \xrightarrow{\left[\begin{smallmatrix} g_1 \\ f \end{smallmatrix}\right]} m_1 \oplus \overline{P_0} \xrightarrow{\left[\begin{smallmatrix} h_1 & 0 \\ a & -g_0 \end{smallmatrix}\right]} m_1' \oplus m_0 \xrightarrow{[\,b\,-h_0\,]} m_0' \longrightarrow 0.
$$

Since $\text{Ext}^1_{\text{Mod C}}(m_0', n) = 0$ by Lemma 5.2(ii), we have the following commutative diagram.

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & \overline{P_1} & \xrightarrow{\left[\begin{smallmatrix} g_1 \\ f \end{smallmatrix}\right]} & m_1 \oplus \overline{P_0} & \xrightarrow{\left[\begin{smallmatrix} h_1 & 0 \\ a & -g_0 \end{smallmatrix}\right]} & m_1' \oplus m_0 & \xrightarrow{[\,b\ -h_0\,]} & m_0' \longrightarrow 0 \\
  & & \| & & \downarrow{\scriptstyle [0\ 1]} & & \vdots & & \\
0 & \longrightarrow & \text{Ker}\,f & \longrightarrow & \overline{P_1} \xrightarrow{\ f\ } \overline{P_0} & \xrightarrow{\ e\ } & n & \longrightarrow & 0
\end{array}
$$

Taking a mapping cone, we have an exact sequence

$$
0 \longrightarrow \overline{P_1} \oplus \text{Ker}\,f \longrightarrow m_1 \oplus \overline{P_0} \oplus \overline{P_1} \longrightarrow m_1' \oplus m_0 \oplus \overline{P_0} \longrightarrow m_0' \oplus n \longrightarrow 0.
$$

Cancelling a direct summand of the form $\overline{P_1} \xrightarrow{\left[\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right]} \overline{P_0} \oplus \overline{P_1} \xrightarrow{[1\ 0]} \overline{P_0}$, we have an exact sequence

$$
0 \longrightarrow \text{Ker}\,f \longrightarrow m_1 \xrightarrow{c} m_1' \oplus m_0 \xrightarrow{d} m_0' \oplus n \longrightarrow 0.
$$

Since $\text{Im}\,c \in \text{Fac}\,\mathsf{M}$ and $m_0' \oplus n$ is Ext-projective in $\text{Fac}\,\mathsf{M}$, the epimorphism d splits. Thus $n \in \mathsf{M}$ as desired. $\qquad\square$

Now we are ready to prove Theorem 5.1.

Let M be a support τ-tilting subcategory of mod C. By definition, each representable C-module has a left M-approximation. Since $P(\operatorname{Fac} M) = M$ by Proposition 5.3, the map $M \mapsto \operatorname{Fac} M$ is well-defined from the set (i) to the set (ii), and it is injective.

We show that the map is surjective. For T in the set described in (ii), let $E := \bigcap_{m \in T} \operatorname{Ker} m$ and $M := P(T)$. We will show that (M, E) is a support τ-tilting pair of mod C. Since $\operatorname{Ext}^1_{\operatorname{Mod} C}(M, T) = 0$ and $\operatorname{Fac} M \subset T$, it follows from Lemma 5.2 that M is τ-rigid. For $s \in C$, take a left M-approximation $C(-, s) \xrightarrow{f} m$.

It remains to show $\operatorname{Coker} f \in M$. Since $\operatorname{Coker} f \in T$, we only have to show $\operatorname{Ext}^1_{\operatorname{Mod} C}(\operatorname{Coker} f, m') = 0$ for each $m' \in M$. Let $f = \iota \pi$ for $\pi : C(-, s) \to \operatorname{Im} f$ and $\iota : \operatorname{Im} f \to m$. Applying $\operatorname{Hom}_{\operatorname{Mod} C}(-, m')$ to the exact sequence $0 \to \operatorname{Im} f \xrightarrow{\iota} m \to \operatorname{Coker} f \to 0$, we have an exact sequence

$$\operatorname{Hom}_{\operatorname{Mod} C}(m, m') \xrightarrow{\iota^*} \operatorname{Hom}_{\operatorname{Mod} C}(\operatorname{Im} f, m')$$

$$\to \operatorname{Ext}^1_{\operatorname{Mod} C}(\operatorname{Coker} f, m') \to \operatorname{Ext}^1_{\operatorname{Mod} C}(m, m') = 0.$$

Let $g : \operatorname{Im} f \to m'$ be a morphism in Mod C. Since f is a left M-approximation, there exists $h : m \to m'$ such that $g\pi = hf$. Then $g = h\iota$. Thus $\iota^* : \operatorname{Hom}_{\operatorname{Mod} C}(m, m') \to \operatorname{Hom}_{\operatorname{Mod} C}(\operatorname{Im} f, m')$ is surjective, and we have $\operatorname{Ext}^1_{\operatorname{Mod} C}(\operatorname{Coker} f, m') = 0$. Consequently we have $\operatorname{Coker} f \in P(T) = M$. Thus the assertion follows. $\square$

References

[Adachi et al. 2014] T. Adachi, O. Iyama, and I. Reiten, "τ-tilting theory", *Compositio Math.* **150**:3 (2014), 415–452. MR 3187626 Zbl 06293659

[Aihara 2013] T. Aihara, "Tilting-connected symmetric algebras", *Algebr. Represent. Theory* **16**:3 (2013), 873–894. MR 3049676 Zbl 06175500

[Aihara and Iyama 2012] T. Aihara and O. Iyama, "Silting mutation in triangulated categories", *J. London Math. Soc.* (2) **85**:3 (2012), 633–668. MR 2927802 Zbl 1271.18011

[Auslander 1974] M. Auslander, "Representation theory of Artin algebras, I", *Comm. Algebra* **1** (1974), 177–268. MR 50 #2240 Zbl 0285.16028

[Bass 1968] H. Bass, *Algebraic K-theory*, W. A. Benjamin, New York–Amsterdam, 1968. MR 40 #2736 Zbl 0174.30302

[Beligiannis and Reiten 2007] A. Beligiannis and I. Reiten, *Homological and homotopical aspects of torsion theories*, Mem. Amer. Math. Soc. **883**, American Mathematical Society, Providence, 2007. MR 2009e:18026 Zbl 1124.18005

[Bondarko 2010] M. V. Bondarko, "Weight structures vs. *t*-structures; weight filtrations, spectral sequences, and complexes (for motives and in general)", *J. K-Theory* **6**:3 (2010), 387–504. MR 2746283 Zbl 05862078

[Fei and Derksen 2011] J. Fei and H. Derksen, "General presentation of algebras", preprint, 2011. arXiv 0911.4913v2

[Happel et al. 1996] D. Happel, I. Reiten, and S. O. Smalø, *Tilting in abelian categories and quasitilted algebras*, Mem. Amer. Math. Soc. **575**, American Mathematical Society, Providence, RI, 1996. MR 97j:16009 Zbl 0849.16011

[Iyama and Yoshino 2008] O. Iyama and Y. Yoshino, "Mutation in triangulated categories and rigid Cohen–Macaulay modules", *Invent. Math.* **172**:1 (2008), 117–168. MR 2008k:16028 Zbl 1140.18007

[Keller 2013] B. Keller, "The periodicity conjecture for pairs of Dynkin diagrams", *Ann. of Math.* (2) **177**:1 (2013), 111–170. MR 2999039 Zbl 06146418

[Matsumura 1989] H. Matsumura, *Commutative ring theory*, 2nd ed., Cambridge Stud. in Adv. Math. **8**, Cambridge University Press, Cambridge, 1989. MR 90i:13001 Zbl 0666.13002

[Mendoza Hernández et al. 2013] O. Mendoza Hernández, E. C. Sáenz Valadez, V. Santiago Vargas, and M. J. Souto Salorio, "Auslander–Buchweitz context and co-*t*-structures", *Appl. Categ. Structures* **21**:5 (2013), 417–440. MR 3097052 Zbl 1291.18017

[Pauksztello 2008] D. Pauksztello, "Compact corigid objects in triangulated categories and co-*t*-structures", *Cent. Eur. J. Math.* **6**:1 (2008), 25–42. MR 2009d:18020 Zbl 1152.18009

[Wei 2013] J. Wei, "Semi-tilting complexes", *Israel J. Math.* **194**:2 (2013), 871–893. MR 3047094 Zbl 1286.16011

[Woolf 2010] J. Woolf, "Stability conditions, torsion theories and tilting", *J. London Math. Soc.* (2) **82**:3 (2010), 663–682. MR 2012d:14026 Zbl 1214.18010

iyama@math.nagoya-u.ac.jp   *Graduate School of Mathematics,*
                                 Nagoya University Chikusa-ku, Nagoya, 464-8602, Japan

peter.jorgensen@ncl.ac.uk   *School of Mathematics and Statistics, Newcastle University,*
                                 Newcastle upon Tyne NE1 7RU, United Kingdom

dongyang2002@googlemail.com   *Department of Mathematics, Nanjing University,*
                                 Nanjing, 210093, China

msp

A p-adic Eisenstein measure for vector-weight automorphic forms

Ellen Eischen

We construct a p-adic Eisenstein measure with values in the space of vector-weight p-adic automorphic forms on certain unitary groups. This measure allows us to p-adically interpolate special values of certain vector-weight C^∞ automorphic forms, including Eisenstein series, as their weights vary. This completes a key step toward the construction of certain p-adic L-functions.

We also explain how to extend our methods to the case of Siegel modular forms and how to recover Nicholas Katz's p-adic families of Eisenstein series for Hilbert modular forms.

1. Introduction

The significance of p-adic families of Eisenstein series as a tool in number theory, especially for the construction of p-adic L-functions, is well established. For example, p-adic families of Eisenstein series play a key role in constructions of p-adic L-functions completed in [Serre 1973; Katz 1978; Deligne and Ribet 1980]. In a completely different direction, p-adic families of Eisenstein series also play a role in homotopy theory [Hopkins 1995; 2002; Ando et al. 2010].

Each of the constructions mentioned above concerns only automorphic forms of scalar weight. Automorphic forms on groups of rank 1 (for example, modular forms and Hilbert modular forms, which are the forms with which Katz, Deligne, Ribet, and Serre worked) can only have scalar weights. Automorphic forms on groups of higher rank, however, need not have scalar weights.

By a vector-weight automorphic form, we mean an automorphic form whose weight is an irreducible representation with highest weight $\lambda_n \geq \cdots \geq \lambda_1$ is not required to have $\lambda_i = \lambda_{i+1}$ for all i, i.e., an automorphic form whose weight is not required to be a one-dimensional representation. In order to complete a construction of p-adic L-functions for automorphic forms on unitary groups in full generality as in [Eischen et al. $\geq$ 2014], one needs a p-adic Eisenstein measure that takes values in the space of p-adic vector-weight automorphic forms. (By an *Eisenstein measure*, we mean a p-adic measure valued in a space of p-adic automorphic forms and whose values at locally constant functions are Eisenstein series.)

The main result of this paper is the construction in Section 5 of a p-adic measure that takes values in the space of automorphic forms on unitary groups of signature (n, n). In particular, Theorem 14 gives a p-adic Eisenstein measure with values in the space of vector-weight automorphic forms. As explained in Theorem 15, this measure, together with the results of Section 4, allows us to p-adically interpolate the values of certain vector-weight C^∞ (not necessarily holomorphic) automorphic forms, including Eisenstein series, as the (highest) weights of these automorphic forms vary. Note that this is the first ever construction of a p-adic Eisenstein measure taking values in the space of *vector*-weight automorphic forms on unitary groups.

We follow the approach of [Katz 1978, Chapters 4 and 5] more closely than we did in [Eischen 2013]. (There, we constructed a p-adic Eisenstein measure for scalar-weight automorphic forms on unitary groups of signature (n, n).) As a consequence, in Section 6, we easily recover Katz's Eisenstein measure from [1978, Chapters 4 and 5] as a special case of our results.

We also explain in Section 6 how to generalize the results of Section 5 to the case of Siegel modular forms, i.e., automorphic forms on symplectic groups. In that setting, in the case where $n = 1$, we are in exactly the situation in which Katz [1978] constructs a p-adic Eisenstein measure for Hilbert modular forms. As demonstrated in Section 6.1, the setup in the earlier sections of the paper makes the connection between our Eisenstein measure and the Eisenstein measure in [Katz 1978, Definition (4.2.5) and Equation (5.5.7)] almost transparent.

1.1. *Applications and context.* The main anticipated application of this paper is to the construction of p-adic L-functions for unitary groups, most immediately and crucially to [Eischen et al. $\geq$ 2014]. In particular, the L-functions in that paper are obtained through the "doubling method" (an approach described in [Gelbart et al.

1987, Part A; Cogdell 2006, Section 2]), which expresses values of *L*-functions in terms of values of Eisenstein series and values of cusp forms. The *p*-adic Eisenstein measure in [Eischen 2013, Section 4] suffices in the case of scalar weights, but if one does not restrict to scalar weights, one needs the results of the present paper.

The behavior of certain *L*-functions (for example, for unitary groups) is strongly tied to the behavior of certain Eisenstein series. For instance, Shimura [2000, Introduction] uses the algebraicity (up to a well-determined period) of values of Eisenstein series at CM points to prove the algebraicity (up to a well-determined period) of certain values of corresponding *L*-functions (normalized by a period). Analogously, Katz [1978, Introduction] uses the *p*-adic interpolation of values of certain Eisenstein series (normalized by a period) at CM points to *p*-adically interpolate certain values of *L*-functions (normalized by a period). Similarly, the *p*-adic families of Eisenstein series in the present paper play a key role in determining the behavior of the *L*-functions in [Eischen et al. ≥ 2014].

1.2. *Overview and structure of the paper.* In Section 2, we introduce the conventions with which we will work, as well as standard background results necessary for this paper. The conventions and background are similar to those in [Eischen 2012; 2013, Section 2]. The background is quite technical; we have summarized just what is needed for this paper. For the reader seeking further details, we recommend [Shimura 1997; 2000] for the theory of C^∞ automorphic forms and Eisenstein series on unitary groups, [Lan 2012; 2013] for the algebraic geometric background and a discussion of algebraically defined *q*-expansions, and [Hida 2004; 2005] for the theory of *p*-adic automorphic forms.

In Section 3, which relies in part on the results of [Eischen 2013, Section 2], we define certain scalar-weight Eisenstein series and automorphic forms on unitary groups of signature (n, n). This set includes the Eisenstein series defined in [Eischen 2013, Section 2] but also includes other automorphic forms. We need this larger space of automorphic forms in order to construct a *p*-adic measure with values in the space of vector-weight automorphic forms in Section 5, whereas in [Eischen 2013] we only were concerned with *p*-adic families of scalar-weight automorphic forms. Like in [Eischen 2013], we work adelically. The formulation of the main result of the section (Theorem 2) is closer to that of [Katz 1978, Theorem (3.2.3)], though, so that the reader can see parallels with the analogous construction in [Katz 1978, Section 3], which is useful in Section 6.1 when we compare our Eisenstein measure to the measure obtained in [Katz 1978, Definition (4.2.5) and Equation (5.5.7)].

Section 4 discusses differential operators that are necessary for comparing the values of certain C^∞ automorphic forms and certain *p*-adic automorphic forms. These differential operators are closely related to the differential operators discussed in [Eischen 2012, Sections 8 and 9]. Note that because we work with vector-weight

automorphic forms, and not just scalar-weight automorphic forms, we need more differential operators than we did in [Eischen 2013], which handled only the case of scalar-weight automorphic forms.

Section 5 contains the main results of the paper, namely the construction of a p-adic Eisenstein measure and the p-adic interpolation of values of certain automorphic forms. This is the heart of the paper. The format of Section 5 closely parallels the construction of a p-adic Eisenstein measure in [Katz 1978, Sections 3.4 and 4.2]. We also explain in Remark 16 precisely how the Eisenstein measure of [Eischen 2013, Section 4] and the Eisenstein measure given in Theorem 14 are related. For $n \geq 2$, the measure in Theorem 14 is on a larger group than the measure in [Eischen 2013, Section 4]. In order to construct a measure with values in the space of *vector*-weight automorphic forms without fixing a partition of n, this larger group is necessary. (The approach in [Eischen 2013] relied on a choice of a partition of n, but it turns out that with this larger group we do not need to fix a partition of n and can consider a larger class of automorphic forms all at once.) We also note that the construction of the measures in [Eischen 2014, Section 4] uses this measure as a starting point.

In Section 6, we comment on how to extend the results of this paper to the case of Siegel modular forms, i.e., automorphic forms on symplectic groups. The fact that our presentation in Section 5 closely follows the approach in [Katz 1978, Sections 3.4 and 4.2] also allows us to recover the Eisenstein measure of [Katz 1978, Definition (4.2.5) and Equation (5.5.7)] with ease in Section 6.1.

2. Conventions and background

In Section 2.1, we introduce the conventions that we will use throughout the paper. In Section 2.2, we briefly summarize the necessary background on automorphic forms on unitary groups. (See the start of Section 2.2 for references.)

2.1. *Conventions.* Once and for all, fix a CM field K with maximal totally real subfield E. Fix a prime p that is unramified in K and such that each prime of E dividing p splits completely in K. Fix embeddings

$$\iota_\infty : \bar{\mathbb{Q}} \hookrightarrow \mathbb{C},$$

$$\iota_p : \bar{\mathbb{Q}} \hookrightarrow \mathbb{C}_p,$$

and fix an isomorphism

$$\iota : \bar{\mathbb{C}}_p \xrightarrow{\sim} \mathbb{C}$$

satisfying $\iota \circ \iota_p = \iota_\infty$. From here on, we identify $\bar{\mathbb{Q}}$ with $\iota_p(\bar{\mathbb{Q}})$ and $\iota_\infty(\bar{\mathbb{Q}})$. Let $\mathbb{O}_{\mathbb{C}_p}$ denote the ring of integers in $\mathbb{C}_p$.

Fix a CM type Σ for $K/\mathbb{Q}$. For each element $\sigma \in \mathrm{Hom}(E, \bar{\mathbb{Q}})$, we also write σ to denote the unique element of Σ prolonging $\sigma : E \hookrightarrow \bar{\mathbb{Q}}$ (when no confusion

can arise). For each element $x \in K$, denote by $\bar{x}$ the image of x under the unique nontrivial element $\epsilon \in \mathrm{Gal}(K/E)$, and let $\bar{\sigma} = \sigma \circ \epsilon$.

Given an element a of E, we identify it with an element of $E \otimes \mathbb{R}$ via the embedding

$$E \hookrightarrow E \otimes \mathbb{R}$$
$$a \mapsto (\sigma(a))_{\sigma \in \Sigma}. \tag{1}$$

We identify $a \in K$ with an element of $K \otimes \mathbb{C} \xrightarrow{\sim} (E \otimes \mathbb{C}) \times (E \otimes \mathbb{C})$ via the embedding

$$K \hookrightarrow K \otimes \mathbb{C}$$
$$a \mapsto \left((\sigma(a))_{\sigma \in \Sigma}, (\bar{\sigma}(a))_{\sigma \in \Sigma}\right). \tag{2}$$

Let $d = (d_v)_{v \in \Sigma} \in \mathbb{Z}^{\Sigma}$, and let $a = (a_v)_{v \in \Sigma}$ be an element of $\mathbb{C}^{\Sigma}$ or $\mathbb{C}_p^{\Sigma}$. We denote by a^d the element of $\mathbb{C}$ or $\mathbb{C}_p$ defined by

$$a^d := \prod_{v \in \Sigma} a_v^{d_v}.$$

If $e = (e_v)_{v \in \Sigma} \in \mathbb{Z}^{\Sigma}$, we denote by $d + e$ the tuple defined by

$$d + e = (d_v + e_v)_{v \in \Sigma} \in \mathbb{Z}^{\Sigma}.$$

If $k \in \mathbb{Z}$, we denote by $k + d$ or $d + k$ the element

$$k + d = d + k = (d_v + k)_{v \in \Sigma} \in \mathbb{Z}^{\Sigma}.$$

For any ring R, we denote the ring of $n \times n$ matrices with coefficients in R by $M_{n \times n}(R)$. We denote by 1_n the multiplicative identity in $M_{n \times n}(R)$. Also, for any subring R of $K \otimes_E E_v$, with v a place of E, let $\mathrm{Her}_n(R)$ denote the space of Hermitian $n \times n$ matrices with entries in R. Given $x \in \mathrm{Her}_n(E)$,

$$x > 0$$

if $\sigma(x)$ is positive definite for every $\sigma \in \Sigma$.

2.1.1. *Adelic norms.* Let $|\cdot|_E$ denote the adelic norm on $E^{\times} \backslash \mathbb{A}_E^{\times}$ such that, for all $a \in \mathbb{A}_E^{\times}$,

$$|a|_E = \prod_v |a|_v,$$

where the right-hand product is over all places of E and where the absolute values are normalized so that

$$|v|_v = q_v^{-1},$$
$$q_v = \text{the cardinality of } \mathbb{O}_{Ev}/v\mathbb{O}_{Ev}$$

for all nonarchimedean primes v of the totally real field E. Consequently, for all $a \in E$,

$$\prod_{v \nmid \infty} |a|_v^{-1} = \prod_{v \in \Sigma} \sigma_v(a) \mathrm{Sign}(\sigma_v(a)),$$

where the product is over all archimedean places v of the totally real field E. We denote by $|\cdot|_K$ the adelic norm on $K^\times \backslash \mathbb{A}_K^\times$ such that, for all $a \in \mathbb{A}_K^\times$,

$$|a|_K = |a\bar{a}|_E.$$

For $a \in K$ and v a place of E, we let

$$|a|_v = |a\bar{a}|_v^{1/2}.$$

Given an element $a \in K$, we associate a with an element of $K \otimes \mathbb{R}$ via the embedding

$$a \mapsto (\sigma(a))_{\sigma \in \Sigma}.$$

For any field extension L/M, we write $N_{L/M}$ to denote the norm from L to M. Given an $\mathbb{O}_M$-algebra R, the norm map $N_{L/M}$ on L provides a group homomorphism

$$(\mathbb{O}_L \otimes R)^\times \to R^\times$$

in which $a \otimes r \mapsto N_{L/M}(a)r$. When the fields are clear, we shall just write N.

2.1.2. *Exponential characters.* For each archimedean place $v \in \Sigma$, denote by $\boldsymbol{e}_v$ the character of E_v (i.e., $\mathbb{R}$) defined by

$$\boldsymbol{e}_v(x_v) = e^{2\pi i x_v}$$

for all x_v in E_v. Denote by $\boldsymbol{e}_\infty$ the character of $E \otimes \mathbb{R}$ defined by

$$\boldsymbol{e}_\infty((x_v)_{v \in \Sigma}) = \prod_{v \mid \infty} \boldsymbol{e}_v(x_v).$$

Following our convention from (1), we put

$$\boldsymbol{e}_\infty(a) = \boldsymbol{e}_\infty\big((\sigma(a))_{\sigma \in \Sigma}\big) = e^{2\pi i \, \mathrm{tr}_{E/\mathbb{Q}}(a)}$$

for all $a \in E$. For each finite place v of E dividing a prime q of $\mathbb{Z}$, denote by $\boldsymbol{e}_v$ the character of E_v defined, for each $x_v \in E_v$, by

$$\boldsymbol{e}_v(x_v) = e^{-2\pi i y},$$

where $y \in \mathbb{Q}$ is the fractional part of $\mathrm{tr}_{E_v/\mathbb{Q}_q}(x_v) \in \mathbb{Q}_p$; that is, if we write $\mathrm{tr}_{E_v/\mathbb{Q}_q}(x_v) = \sum_{i=k}^\infty a_i p^i$ for some integer $k \leq 0$ and $a_i \in \{0, \dots, p-1\}$, then $y = \sum_{i=k}^0 a_i p^i$. We denote by $\boldsymbol{e}_{\mathbb{A}_E}$ the character of $\mathbb{A}_E$ defined by

$$\boldsymbol{e}_{\mathbb{A}_E}(x) = \prod_v \boldsymbol{e}_v(x_v) \quad \text{for all } x = (x_v) \in \mathbb{A}_E.$$

Remark 1. We identify $a \in E$ with the element $(\sigma_v(a))_v \in \mathbb{A}_E$, where $\sigma_v : E \hookrightarrow E_v$ is the embedding corresponding to v. Following this convention, we put

$$\boldsymbol{e}_{\mathbb{A}_E}(a) = \prod_v \boldsymbol{e}_v(\sigma_v(a)) \tag{3}$$

for all $a \in E$.

2.1.3. *Spaces of functions.* Given topological spaces X and Y, we let

$$\mathscr{C}(X, Y)$$

denote the space of continuous functions from X to Y.

2.2. *Background concerning automorphic forms on unitary groups.*

2.2.1. *Unitary groups of signature* (n, n). We now recall basic information about unitary groups and automorphic forms on unitary groups. (A more detailed discussion of unitary groups and automorphic forms on unitary groups appears in [Shimura 1997; 2000; Hida 2004; Harris et al. 2006; Eischen 2012; Lan 2013]; the analogous background for the case of Hilbert modular forms is the main subject of [Katz 1978, Section 1].)

The material in this section is similar to [Eischen 2013, Section 2.1]. Although we discussed embeddings of nondefinite unitary groups of various signatures into unitary groups of signature (n, n) there, we are primarily concerned only with unitary groups of signature (n, n) and definite unitary groups in this paper; in the sequel [Eischen 2014] we discuss pullbacks to various products of unitary groups occurring as subgroups.

Let V be a vector space of dimension n over the CM field K, and let $\langle\,,\,\rangle_V$ denote a positive definite hermitian pairing on V. Let $-V$ denote the vector space V with the negative definite hermitian pairing $-\langle\,,\,\rangle_V$. Let

$$W = 2V = V \oplus -V$$

$$\langle(v_1, v_2), (w_1, w_2)\rangle_W = \langle v_1, w_1\rangle_V + \langle v_2, w_2\rangle_{-V}.$$

The hermitian pairing $\langle\,,\,\rangle_W$ defines an involution $g \mapsto \tilde{g}$ on $\mathrm{End}_K(W)$ by

$$\langle g(w), w'\rangle_W = \langle w, \tilde{g}(w')\rangle_W$$

(where w and w' denote elements of W). This involution extends to an involution on $\mathrm{End}_{K \otimes_E R}(W \otimes_E R)$ for any E-algebra R. We denote by U the algebraic group such that, for any E-algebra R, the R-points of U are given by

$$U(R) = U(R, W) = \{g \in \mathrm{GL}_{K \otimes_E R}(W \otimes_E R) \mid g\tilde{g} = 1\}.$$

Similarly, we define $U(R, V)$ to be the algebraic group associated to $\langle\,,\,\rangle_V$ and $U(R, -V)$ to be the algebraic group associated to $\langle\,,\,\rangle_{-V}$. Note that $U(\mathbb{R})$ is of

signature (n, n). Also, the canonical embedding

$$V \oplus V \hookrightarrow W$$

induces an embedding

$$U(R, V) \times U(R, -V) \hookrightarrow U(R, W)$$

for all E-algebras R. When the E-algebra R over which we are working is clear from context or does not matter, we shall write $U(W)$ for $U(R, W)$, $U(V)$ for $U(R, V)$, and $U(-V)$ for $U(R, -V)$. We also sometimes write just U to denote $U(W)$.

We also have groups

$$GU(R) = GU(R, W) = \{g \in \mathrm{GL}_{K \otimes_E R}(W \otimes_E R) \mid g\tilde{g} \in R^\times\}.$$

We use the notation ω to denote the similitude character

$$\omega : GU(R) \to R^\times$$

$$g \mapsto g\tilde{g}.$$

When the E-algebra R over which we are working is clear from context or does not matter, we shall write $GU(W)$ for $GU(R, W)$. We shall also use the notation

$$G(R) = GU(R, W)$$

or write simply G or GU when the ring R is clear from context or does not matter. When $R = \mathbb{A}_E$ or $R = \mathbb{R}$, we write

$$G_+ := GU_+$$

to denote the subgroup of $G = GU$ consisting of elements such that the similitude factor at each archimedean place of E is positive.

For the space $W = V \oplus -V$ defined above, $U(W)$ and $GU(W)$ have signature (n, n). So we will sometimes write $U(n, n)$ and $GU(n, n)$, respectively, to refer to these groups.

We write $W = V_d \oplus V^d$, where V_d and V^d denote the maximal isotropic subspaces

$$V^d = \{(v, v) | v \in V\},$$
$$V_d = \{(v, -v) | v \in V\}.$$

Let P be the Siegel parabolic subgroup of $U(W)$ stabilizing V^d in $V_d \oplus V^d$ under the action of $U(W)$ on the right. Denote by M the Levi subgroup of P and by N the unipotent radical of P. Similarly, denote by GP the Siegel parabolic subgroup of $GU(W)$ stabilizing V^d in $V_d \oplus V^d$ under the action of $GU(W)$ on the right, and denote by GM the Levi subgroup of GP and by N the unipotent radical of GP. We also, similarly, denote by GP_+ the Siegel parabolic subgroup of GU_+ stabilizing

V^d in $V_d \oplus V^d$ under the action of GU_+ on the right, and denote by GM_+ the Levi subgroup of GP_+ and by N the unipotent radical of GP_+.

A choice of a basis $e_1, \ldots, e_n$ for V over K gives an identification of V with V^d (via $e_i \mapsto (e_i, e_i)$) and with V_d (via $e_i \mapsto (e_i, -e_i)$). The choice of a basis for V also identifies $GL_K(V)$ with $GL_n(K)$. With respect to the ordered basis $(e_1, e_1) \ldots, (e_n, e_n), (e_1, -e_1) \ldots, (e_n, -e_n)$ for W, M consists of the block diagonal matrices of the form

$$m(h) := ({}^t \bar{h}^{-1}, h)$$

with $h \in GL_n(K \otimes R)$, and GM consists of the block diagonal matrices of the form

$$m(h, \lambda) := ({}^t \bar{h}^{-1}, \lambda h)$$

with $h \in GL_n(K)$ and $\lambda \in E^\times$. Thus, the choice of basis $e_1, \ldots, e_n$ for V over K fixes identifications

$$M \xrightarrow{\sim} GL_K(V),$$

$$GM \xrightarrow{\sim} GL_K(V) \times E^\times.$$

These isomorphisms extend to isomorphisms

$$M(R) \xrightarrow{\sim} GL_{K \otimes_E R}(V \otimes_E R), \tag{4}$$

$$GM(R) \xrightarrow{\sim} GL_{K \otimes_E R}(V \otimes_E R) \times R^\times \tag{5}$$

for each E-algebra R.

We fix a Shimura datum $(G, X(W))$ and a corresponding Shimura variety $\mathrm{Sh}(W) = \mathrm{Sh}(U(n, n))$ according to the conditions in [Harris et al. 2006, Section 1.2] and [Eischen 2012, Section 2.2]. The symmetric domain $X(W)$ is holomorphically isomorphic to the tube domain consisting of $[E : \mathbb{Q}]$ copies of

$$\mathcal{H}_n = \{z \in M_{n \times n}(\mathbb{C}) \mid i({}^t \bar{z} - z) > 0\}.$$

When we need to emphasize over which ring R we work, we sometimes write $\mathrm{Sh}(R)$. Let $\mathcal{H}_\infty$ be the stabilizer in $G(\mathbb{R})$ of the point $i \cdot 1_n$. So $\prod_{\sigma \in \Sigma} \mathcal{H}_\infty$ is the stabilizer in $\prod_{\sigma \in \Sigma} G(\mathbb{R})$ of the point

$$\boldsymbol{i} = (i \cdot 1_n)_{\sigma \in \Sigma} \in \prod_{\sigma \in \Sigma} \mathcal{H}_n. \tag{6}$$

We can identify $G_+(\mathbb{R})/\mathcal{H}_\infty$ with $\mathcal{H}_n$. Given a compact open subgroup $\mathcal{H}$ of $G(\mathbb{A}_f)$, denote by $_\mathcal{H}\mathrm{Sh}(W)$ the Shimura variety whose complex points are given by

$$G(\mathbb{Q}) \backslash X \times G(\mathbb{A}_f)/\mathcal{H}.$$

This Shimura variety is a moduli space for abelian varieties together with a polarization, an endomorphism, and a level structure (dependent upon the choice of $\mathcal{H}$). Note that $_\mathcal{H}\mathrm{Sh}(W)$ consists of copies of quotients of spaces isomorphic to $\mathcal{H}_n$.

When we work with some other group H, we write $\mathrm{Sh}(H)$ instead of $\mathrm{Sh}(W)$.

2.2.2. *Automorphic forms on unitary groups.* Automorphic forms on unitary groups are typically discussed from any of the following three perspectives (which are equivalent over $\mathbb{C}$):

(1) Functions on a unitary group that satisfy an automorphy condition.

(2) C^∞ (or holomorphic) functions on a hermitian symmetric space (analogue of the upper half plane) that satisfy an automorphy condition.

(3) Sections of a certain vector bundle over a moduli space (a Shimura variety) parametrizing abelian varieties together with a polarization, endomorphism, and level structure.

Which perspective is most natural depends upon context. In this paper, we shall need all three perspectives. (In [Eischen 2012, Section 2], we provided a detailed discussion of automorphic forms and the relationships between different approaches to defining them.)

The relationship between the first two approaches to automorphic forms is reviewed in [Eischen 2013, p. 9; Shimura 2000, A8]. The relationship between the second two approaches to automorphic forms is discussed in [Eischen 2012, Section 2] and is similar to the analogous relationship for modular forms given in [Katz 1973, A1.1].

An automorphic form f on $U(n, n)$ has a weight, which is a representation ρ of $\mathrm{GL}_n \times \mathrm{GL}_n$. In the special case where this representation is of the form

$$\rho(a, b) = \det(a)^{k+\nu} \det(b)^{-\nu},$$

we shall say f *is an automorphic form of weight* (k, ν).

As explained in [Lan 2012; 2013], for the unitary groups of signature (n, n) there is a higher-dimensional analogue of the Tate curve (which we call the "Mumford object" in [Eischen 2012, Section 4.2; 2013, Section 2.2.11]), and so in analogue with the case for modular forms evaluated at the Tate curve, one obtains an algebraic q-expansion by evaluating an automorphic form at the Mumford object. Like in the case of modular forms, the coefficients of an algebraically defined q-expansion of a holomorphic automorphic form f of over $\mathbb{C}$ agree with the (analytically defined) Fourier coefficients of f [Lan 2012]. Also, like in the case of modular forms, there is a q-expansion principle for automorphic forms on unitary groups [Lan 2013, Proposition 7.1.2.15]; note that the q-expansion principle for automorphic forms over a Shimura variety requires the evaluation of an automorphic form at one cusp of each connected component. To apply the q-expansion principle, it is enough [Hida 2004, Section 8.4] to check the cusps parametrized by points of $GM_+(\mathbb{A}_E)$. (The author is grateful to thank Kai-Wen Lan for explaining this to her.) We shall

say "a cusp $m \in GM_+(\mathbb{A}_E)$" to mean "the cusp corresponding to the point m." The q-expansion of an automorphic form at a cusp $m(h, \lambda)$ is a sum of the form

$$\sum_{\beta \in L_{m(h,\lambda)}} a(\beta) q^{\beta},$$

where $L_{m(h,\lambda)}$ is a lattice in $\mathrm{Her}_n(E)$ dependent upon the choice of the cusp $m(h, \lambda)$ and $a(\beta) \in \mathbb{C}$ for all β (or, more generally, if f is a V-valued automorphic form for some $\mathbb{C}$-vector space V, $a(\beta) \in V$ for all β). We sometimes also write

$$\sum_{\beta \in \mathrm{Her}_n(E)} a(\beta) q^{\beta},$$

when we do not need to make the cusp explicit; in this case, we know that the coefficients $a(\beta)$ are zero outside of some lattice in $\mathrm{Her}_n(E)$ (namely, the lattice corresponding to the unspecified cusp).

Throughout the paper, all cusps m and corresponding lattices $L_m \subseteq \mathrm{Her}_n(K)$ determined by m are chosen so that the elements of L_m have p-integral coefficients.[1]

3. Eisenstein series on unitary groups

In this section, we introduce certain Eisenstein series on unitary groups of signature (n, n). These Eisenstein series are related to the ones discussed in [Eischen 2013, Section 2; Shimura 1997, Section 18; Katz 1978, Section (3.2)].

For $k \in \mathbb{Z}$ and $\nu = (\nu(\sigma))_{\sigma \in \Sigma} \in \mathbb{Z}^{\Sigma}$, we denote by $N_{k,\nu}$ the function

$$N_{k,\nu} : K^{\times} \to K^{\times}$$
$$b \mapsto \prod_{\sigma \in \Sigma} \sigma(b)^{k+2\nu(\sigma)} (\sigma(b)\bar{\sigma}(b))^{-(\nu(\sigma))}.$$

For all $b \in \mathbb{O}_E^{\times}$,

$$N_{k,\nu}(b) = N_{E/\mathbb{Q}}^k(b).$$

Theorem 2. *Let R be an $\mathbb{O}_K$-algebra, let $\nu = (\nu(\sigma)) \in \mathbb{Z}^{\Sigma}$, and let $k \geq n$ be an integer. Let*

$$F : (\mathbb{O}_K \otimes \mathbb{Z}_p) \times M_{n \times n}(\mathbb{O}_E \otimes \mathbb{Z}_p) \to R$$

be a locally constant function supported on $(\mathbb{O}_K \otimes \mathbb{Z}_p)^{\times} \times M_{n \times n}(\mathbb{O}_E \otimes \mathbb{Z}_p)$ that satisfies

$$F(ex, N_{K/E}(e^{-1})y) = N_{k,\nu}(e) F(x, y) \tag{7}$$

---

[1]Even without this choice for m and L_m, which we did not make a priori in [Eischen 2013], we could force the Fourier coefficients at all the non-p-integral elements of $\mathrm{Her}_n(K)$ to be zero, simply by our choice of a Siegel section at p later in this paper. In fact, in [Eischen 2013, Section 2.2], our choice of Siegel sections at p forced the Fourier coefficients at all the non-p-integral elements of $\mathrm{Her}_n(K)$ to be zero.

for all $e \in \mathbb{O}_K^\times$, $x \in \mathbb{O}_K \otimes \mathbb{Z}_p$, and $y \in M_{n \times n}(\mathbb{O}_E \otimes \mathbb{Z}_p)$. There is an automorphic form $G_{k,v,F}$ (on $U(n,n)$) of weight (k,v) defined over R whose q-expansion at a cusp $m \in GM_+(\mathbb{A}_E)$ is of the form $\sum_{0 < \beta \in L_m} c(\beta) q^\beta$ (where L_m is the lattice in $\mathrm{Her}_n(K)$ determined by m), with $c(\beta)$ a finite $\mathbb{Z}$-linear combination of terms of the form

$$F(a, N_{K/E}(a)^{-1}\beta) N_{k,v}(a^{-1} \det \beta) N_{E/\mathbb{Q}}(\det \beta)^{-n}$$

(where the linear combination is a sum over a finite set of p-adic units $a \in K$ dependent upon β and the choice of cusp $m \in GM$). When $R = \mathbb{C}$, these are the Fourier coefficients at $s = \frac{1}{2}k$ of the C^∞ automorphic form $G_{k,v,F}(z,s)$ (which is holomorphic at $s = \frac{1}{2}k$) that will be defined in Lemma 9.

(Above, the elements of $(\mathbb{O}_E \otimes \mathbb{Z}_p)^\times$ in $M_{n \times n}(\mathbb{O}_E \otimes \mathbb{Z}_p)$ are viewed as homomorphisms, i.e., multiplication by an element of $(\mathbb{O}_E \otimes \mathbb{Z}_p)^\times$, so as diagonal matrices in $M_{n \times n}(\mathbb{O}_E \otimes \mathbb{Z}_p)$. Also note that, when $\det \beta = 0$, the coefficient of q^β is 0, so we can restrict the discussion to F with support in $(\mathbb{O}_K \otimes \mathbb{Z}_p)^\times \times \mathrm{GL}_n(\mathbb{O}_E \otimes \mathbb{Z}_p)$.)

Proof. By an argument similar to Katz's argument at the beginning of the proof of [1978, Theorem (3.2.3)], every locally constant R-valued function F supported on $(\mathbb{O}_K \otimes \mathbb{Z}_p)^\times \times M_{n \times n}(\mathbb{O}_E \otimes \mathbb{Z}_p)$ that satisfies (7) is an R-linear combination of $\mathbb{O}_K$-valued functions F supported on $(\mathbb{O}_K \otimes \mathbb{Z}_p)^\times \times M_{n \times n}(\mathbb{O}_E \otimes \mathbb{Z}_p)$ that satisfy (7). So it is enough to prove the theorem for $\mathbb{O}_K$-valued functions F.

Now, if we can construct an automorphic form satisfying the conditions of the theorem over $R = \mathbb{C}$, then by the q-expansion principle [Lan 2013, Proposition 7.1.2.15], the case over R will follow for any $\mathbb{O}_K$-subalgebra R (in particular, for $R = \mathbb{O}_K$) of $\mathbb{C}$. By [Lan 2012], it sufficient to show that there is a $\mathbb{C}$-valued C^∞ automorphic form $G_{k,v,F}$ of weight (k,v) holomorphic at $s = \frac{1}{2}k$ whose Fourier coefficients (at $s = \frac{1}{2}k$) are as in the statement of the theorem. We will devote Section 3.1 to the construction of such an automorphic form. $\square$

3.1. *Construction of a C^∞ automorphic form over $\mathbb{C}$ whose Fourier coefficients meet the conditions of Theorem 2.* In this section, we construct the C^∞ automorphic form $G_{k,v,F}$ necessary to complete the proof of Theorem 2.

Let $\mathfrak{m}$ be an ideal that divides p^∞. Let χ be a unitary Hecke character of type A_0,

$$\chi : \mathbb{A}_K^\times \to \mathbb{C}^\times,$$

of conductor $\mathfrak{m}$, i.e.,

$$\chi_v(a) = 1$$

for all finite primes v in K and all $a \in K_v^\times$ such that

$$a \in 1 + \mathfrak{m}_v \mathbb{O}_{Kv}.$$

Let $\nu(\sigma)$ and $k(\sigma)$, $\sigma \in \Sigma$, denote integers such that the infinity type of χ is

$$\prod_{\sigma \in \Sigma} \sigma^{-k(\sigma)-2\nu(\sigma)} (\sigma \cdot \bar{\sigma})^{\frac{1}{2}k(\sigma)+\nu(\sigma)}. \tag{8}$$

For any $s \in \mathbb{C}$, we view $\chi \cdot |\cdot|_K^{-s} \otimes |\cdot|_E^{-ns}$ as a character of the parabolic subgroup $GP_+(\mathbb{A}_E) = GM_+(\mathbb{A}_E)N(\mathbb{A}_E) \subseteq G_+(\mathbb{A}_E)$ via the composition of maps

$$GP(\mathbb{A}_E) \xrightarrow{\mathrm{mod}\, N(\mathbb{A}_E)} GM(\mathbb{A}_E) \xrightarrow{(5)} \mathrm{GL}_{\mathbb{A}_K}(V \otimes_E \mathbb{A}_E) \times \mathrm{GL}_1(\mathbb{A}_E) \longrightarrow \mathbb{C}^\times,$$

where the last one is the map

$$(h, \lambda) \longmapsto |\lambda|_E^{-ns} \cdot \chi(\det h)|\det h|_K^{-s}.$$

Consider the induced representation

$$\begin{aligned}
I(\chi, s) &= \mathrm{Ind}_{GP_+(\mathbb{A}_E)}^{G_+(\mathbb{A}_E)} \left(\chi \cdot |\cdot|_K^{-s} \otimes |\omega(\cdot)|_K^{-ns/2} \right) \\
&\cong \bigotimes_v \mathrm{Ind}_{GP_+(E_v)}^{G_+(E_v)} \left(\chi_v \cdot |\cdot|_v^{-2s} \otimes |\omega(\cdot)|_v^{-ns} \right),
\end{aligned} \tag{9}$$

where the product is over all places of E.

Given a section $f \in I(\chi, s)$, the Siegel Eisenstein series associated to f is the $\mathbb{C}$-valued function of G defined by

$$E_f(g) = \sum_{\gamma \in GP_+(E) \backslash G_+(E)} f(\gamma g).$$

This function converges for $\Re(s) > 0$ and can be continued meromorphically to the entire complex plane.

Remark 3. As in [Eischen 2013], if we were working with normalized induction, then the function would converge for $\Re(s) > \frac{1}{2}n$, but we have absorbed the exponent $\frac{1}{2}n$ into the exponent s. (Our choice not to include the modulus character at this point is equivalent to shifting the plane on which the function converges by $\frac{1}{2}n$.)

All the poles of E_f are simple and there are at most finitely many of them. Details about the poles are given in [Tan 1999].

As we noted in [Eischen 2013, Section 2.2.4], if the Siegel section f factors as $f = \bigotimes_v f_v$, then E_f has a Fourier expansion such that, for all $h \in \mathrm{GL}_n(K)$ and $m \in \mathrm{Her}_n(K)$,

$$E_f \left(\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \begin{pmatrix} {}^t\bar{h}^{-1} & 0 \\ 0 & h \end{pmatrix} \right) = \sum_{\beta \in \mathrm{Her}_n(K)} c(\beta, h; f) e_{\mathbb{A}_E}(\mathrm{tr}(\beta m))$$

with $c(\beta, h; f)$ a complex number dependent only on the choice of section f, the hermitian matrix $\beta \in \mathrm{Her}_n(K)$, h_v for finite places v, and $(h \cdot {}^t\bar{h})_v$ for archimedean places v of E.

By [Shimura 1997, Sections 18.9, 18.10], the Fourier coefficients of the Siegel sections $f = \bigotimes_v f_v$ that we will choose below are products of local Fourier coefficients determined by the local sections f_v. More precisely, for each $\beta \in \mathrm{Her}_n(K)$,

$$c(\beta, h; f) = C(n, K) \prod_v c_v(\beta, h; f),$$

where

$$c_v(\beta, h; f) = \int_{\mathrm{Her}_n(K \otimes E_v)} f_v\left(\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & m_v \\ 0 & 1 \end{pmatrix} \begin{pmatrix} {}^t\bar{h}_v^{-1} & 0 \\ 0 & h_v \end{pmatrix}\right) e_v(-\mathrm{tr}(\beta_v m_v)) \, dm_v, \tag{10}$$

$$C(n, K) = 2^{n(n-1)[E:\mathbb{Q}]/2} |D_E|^{-n/2} |D_K|^{-n(n-1)/4}, \tag{11}$$

D_E and D_K are the discriminants of K and E, respectively, $\beta_v = \sigma_v(\beta)$ for each place v of E, and d_v denotes the Haar measure on $\mathrm{Her}_n(K_v)$ such that

$$\int_{\mathrm{Her}_n(\mathbb{O}_K \otimes_E E_v)} d_v x = 1 \quad \text{for each finite place } v \text{ of } E \tag{12}$$

and

$$d_v x := \left| \bigwedge_{j=1}^n dx_{jj} \bigwedge_{j<k} (2^{-1} dx_{jk} \wedge d\bar{x}_{jk}) \right| \quad \text{for each archimedean place } v \text{ of } E.$$

(Here x denotes the matrix whose ij-th entry is x_{ij}.)

Below, we recall [Eischen 2013, Lemma 19], which explains how the Fourier coefficients $c(\beta, h; f)$ transform when we change the point h. For each $h \in \mathrm{GL}_n(\mathbb{A}_K)$ and $\lambda \in \mathbb{A}_E^\times$, let $m(h, \lambda)$ denote the matrix

$$\begin{pmatrix} {}^t\bar{h}^{-1} & 0 \\ 0 & \lambda h \end{pmatrix}.$$

Generalizing (10), we define

$$c_v(\beta, m(h, \lambda); f)$$
$$= \int_{\mathrm{Her}_n(K \otimes E_v)} f_v\left(\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & m_v \\ 0 & 1 \end{pmatrix} m(h, \lambda)\right) e_v(-\mathrm{tr}(\beta_v m_v)) \, dm_v.$$

We also define $c(\beta, m(h, \lambda); f) = C(n, K) \prod_v c_v(\beta, m(h, \lambda); f)$.

Lemma 4 [Eischen 2013, Lemma 19]. *For each $h \in \mathrm{GL}_n(\mathbb{A}_K)$, $\lambda \in \mathbb{A}_E^\times$, and $\beta \in \mathrm{Her}_n(K)$,*

$$c\left(\beta, \begin{pmatrix} {}^t\bar{h}^{-1} & 0 \\ 0 & \lambda h \end{pmatrix}; f\right)$$
$$= \chi(\det(\bar{\lambda}\bar{h})^{-1}) \left| \det\left((\bar{\lambda}\bar{h})^{-1} \cdot (\lambda h)^{-1}\right) \right|_E^{n-s} |\lambda|_E^{-ns} c(\lambda^{-1} h^{-1} \beta {}^t\bar{h}^{-1}, 1_n; f). \tag{13}$$

Proof. Let $\eta = \left(\begin{smallmatrix} 0 & -1_n \\ 1_n & 0 \end{smallmatrix}\right)$. Observe that, for any $n \times n$ matrix m,

$$\eta \cdot m(h, \lambda) \cdot \eta^{-1} = m(\lambda^{-1}\,{}^t\bar{h}^{-1}, \lambda)$$

$$m(h, \lambda)^{-1} \cdot \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \cdot m(h, \lambda) = \begin{pmatrix} 1 & \lambda^t\bar{h}mh \\ 0 & 1 \end{pmatrix}.$$

Therefore,

$$\eta \cdot \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \cdot m(h, \lambda) = (\eta \cdot m(h, \lambda) \cdot \eta^{-1})\eta\left(m(h, \lambda)^{-1}\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}m(h, \lambda)\right)$$

$$= m(\lambda^{-1\,t}\bar{h}^{-1}, \lambda)\eta\begin{pmatrix} 1 & \lambda^t\bar{h}mh \\ 0 & 1 \end{pmatrix}.$$

So, for any place v of E and section $f_v \in \mathrm{Ind}_{GP(E_v)}^{G_+(E_v)}(\chi, s)$,

$$f_v\left(\eta\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} m(h_v, \lambda)\right)$$

$$= \chi_v(\det(\overline{\lambda_v h_v})^{-1})\left|\det(\overline{\lambda_v h_v})^{-1}\right|_v^{-2s}|\lambda|_v^{-ns} f_v\left(\eta\begin{pmatrix} 1 & \lambda^t\bar{h}_v m h_v \\ 0 & 1 \end{pmatrix}\right). \quad (14)$$

The lemma now follows from (14) and the fact that the Haar measure d_v satisfies $d_v(\lambda h_v x\,{}^t\bar{h}_v) = |\det(\lambda_v\,{}^t\bar{h}_v \cdot h_v)|_v^n d_v(x)$ for each place v of E. $\qquad\square$

So,

$$c\left(\beta, \begin{pmatrix} \lambda^{-1\,t}\bar{h}^{-1} & 0 \\ 0 & h \end{pmatrix}; f\right) = \chi(\lambda^n)|\lambda^{2n}|_E^{n-s}|\lambda|_E^{2ns}\left(\beta, \begin{pmatrix} {}^t\bar{h}^{-1} & 0 \\ 0 & \lambda h \end{pmatrix}; f\right)$$

$$= |\lambda^{2n^2}|_E \chi(\lambda^n)c\left(\beta, \begin{pmatrix} {}^t\bar{h}^{-1} & 0 \\ 0 & \lambda h \end{pmatrix}; f\right). \quad (15)$$

Below, we choose more specific Siegel sections $f = \bigotimes_v f_v$ and compute the corresponding Fourier coefficients.

3.1.1. *The Siegel section at ∞.* We now define a section $f_\infty^{k,v} = f_\infty^{k,v}(\bullet; i \cdot 1_n, \chi, s)$ in $\bigotimes_{v|\infty} \mathrm{Ind}_{GP_+(E_v)}^{G_+(E_v)}(\chi_v \cdot |\cdot|_v^{-2s} \otimes |\omega(\cdot)|_E^{-ns})$.

For each $\alpha = \prod_{v|\infty} \alpha_v \in \prod_{v|\infty} G(E_v)$, we write α_v in the form $\left(\begin{smallmatrix} a_v & b_v \\ c_v & d_v \end{smallmatrix}\right)$ with a_v, b_v, c_v, and d_v $n \times n$ matrices. Each element $\alpha \in G(E_v)$ acts on $z = \prod_{v|\infty} z_v \in \prod_{v|\infty} \mathcal{H}_n$ by

$$\alpha_v(z_v) = (a_v z_v + b_v)(c_v z_v + d_v)^{-1},$$

$$\alpha(z) = \prod_{v|\infty} \alpha_v(z_v).$$

Let

$$\lambda_{\alpha_v}(z_v) = \lambda(\alpha_v, z_v) = \overline{c_v} \cdot {}^t z_v + \overline{d_v},$$

$$\lambda_\alpha(z) = \lambda(\alpha, z) = \prod_{v|\infty} \lambda_{\alpha_v}(z_v),$$

$$\mu_{\alpha_v}(z_v) = \mu(\alpha_v, z_v) = c_v \cdot z_v + d_v,$$

$$\mu_\alpha(z) = \mu(\alpha, z) = \prod_{v|\infty} \mu_{\alpha_v}(z_v).$$

(These are the canonical automorphy factors. Properties of them are discussed in [Shimura 2000, Section 3.3], for example.) We write

$$j_{\alpha_v}(z_v) = j(\alpha_v, z_v) = \det \mu_{\alpha_v}(z_v),$$

$$j_\alpha(z) = j(\alpha, z) = \prod_{v|\infty} j_{\alpha_v}(z_v).$$

Note that

$$\det(\lambda_{\alpha_v}(z_v)) = \det(\overline{\alpha_v})\omega(\alpha_v)^{-n} j_{\alpha_v}(z_v) \tag{16}$$

$$= \det(\alpha_v)^{-1}\omega(\alpha_v)^n j_{\alpha_v}(z_v), \tag{17}$$

so

$$|\det(\lambda_{\alpha_v}(z_v))| = |j_{\alpha_v}(z_v)|.$$

Consistent with the notation in [Shimura 1997, Equation (10.4.3)], we define

$$j_\alpha^{k,\nu}(z) := j_\alpha(z)^{k+\nu} \det(\lambda_\alpha(z))^{-\nu}.$$

By (16) and (17), we see that

$$j_\alpha^{k,\nu}(z) = (\det(\overline{\alpha})\omega(\alpha)^{-n})^{-\nu} j_\alpha(z)^k$$

$$= (\det(\alpha)^{-1}\omega(\alpha)^n)^{-\nu} j_\alpha(z)^k.$$

If $\beta = \prod_{v|\infty} \beta_v$ is also an element of $\prod_{v|\infty} G(E_v)$, then

$$\lambda(\beta_v\alpha_v, z_v) = \lambda(\beta_v, \alpha_v z_v)\lambda(\alpha_v, z_v), \tag{18}$$

$$\mu(\beta_v\alpha_v, z_v) = \mu(\beta_v, \alpha_v z_v)\mu(\alpha_v, z_v). \tag{19}$$

Consistent with the notation in [Shimura 2000, Section 3], we define functions η and δ on $\mathscr{H}_n$ by

$$\eta(z) = i({}^t\overline{z} - z),$$

$$\delta(z) = \det\left(\tfrac{1}{2}\eta(z)\right)$$

for each $z \in \mathscr{H}_n$. So

$$\eta(i \cdot 1_n) = 2 \cdot 1_n,$$

$$\delta(i \cdot 1_n) = 1.$$

We also write η and δ to denote the functions $\prod_{\sigma \in \Sigma} \eta$ and $\prod_{\sigma \in \Sigma} \delta$, respectively, on $\prod_{\sigma \in \Sigma} \mathcal{H}_n$. So $\delta(i) = 1$. Also, note that

$$\delta(\alpha z) = \omega(\alpha)^n |j_\alpha(z)|^{-2} \delta(z) = \omega(\alpha)^n |j_\alpha(z) \det(\lambda_\alpha(z))|^{-1} \delta(z).$$

Following [Shimura 2000, Sections 3 and 5], given $(k, v) = \prod_{v \mid \infty} (k_v, v_v) \in (\mathbb{Z} \times \mathbb{Z})^\Sigma$, we define functions $f \|_{k,v}$ and $f|_{k,v}$ on $\prod_{\sigma \in \Sigma} \mathcal{H}_n$ by

$$(f \|_{k,v} \alpha)(z) = j_\alpha^{k,v}(z)^{-1} f(\alpha z),$$

$$f|_{k,v} \alpha = f \|_{k,v} (\omega(\alpha)^{-\frac{1}{2}} \alpha)$$

for each $\mathbb{C}$-valued function f on $\mathcal{H}_n$, point $z \in \mathcal{H}_n$, and element $\alpha \in G$. Note that $\omega(\alpha)^{-1/2} \alpha \in U(\eta_n)$ and, if $\omega(\alpha_v) = 1$ for all $v \in \Sigma$, then

$$f|_{k,v} \alpha = f \|_{k,v} \alpha.$$

More generally, for each function f on $\prod_{\sigma \in \Sigma} \mathcal{H}_n$ with values in some representation (V, ρ) of $\prod_{\sigma \in \Sigma} \mathrm{GL}_n(\mathbb{C}) \times \mathrm{GL}_n(\mathbb{C})$, we define functions $f \|_\rho$ and $f|_\rho$ on $\mathcal{H}_n$ by

$$(f \|_\rho \alpha)(z) = \rho(\mu_\alpha(z), \lambda_\alpha(z))^{-1} f(\alpha z),$$

$$f|_\rho \alpha = f \|_\rho (\omega(\alpha)^{-\frac{1}{2}} \alpha).$$

We also use the notation $f \|$ and $f|$ when we are working with just one copy of $\mathcal{H}_n$, rather than $[E : \mathbb{Q}]$ copies of $\mathcal{H}_n$ at once.

We define

$$f_\infty^{k,v} = \bigotimes_{v \mid \infty} f_v^{k,v}(\bullet; i \cdot 1_n, \chi, s) \in \bigotimes_{v \mid \infty} \mathrm{Ind}_{GP_+(E_v)}^{G_+(E_v)} (\chi_v \cdot | \cdot |_v^{-2s} \otimes |\omega(\cdot)|_E^{-ns})$$

by

$$f_\infty^{k,v}(\alpha; i \cdot 1_n, \chi, s)$$

$$= (\delta^{s - \frac{1}{2}k}|_{k,v} \alpha)(i \cdot 1_n)$$

$$= j_{\omega(\alpha)^{-1/2}\alpha}^{k,v}(i \cdot 1_n)^{-1} |j_{\omega(\alpha)^{-1/2}\alpha}(i \cdot 1_n)|^{-2} \omega(\omega(\alpha)^{-1/2}\alpha)^n |^{s - \frac{1}{2}k(\sigma_v)}$$

$$= j_{\omega(\alpha)^{-1/2}\alpha}^{k,v}(i \cdot 1_n)^{-1} |j_{\omega(\alpha)^{-1/2}\alpha}(i \cdot 1_n)|^{-2}|^{s - \frac{1}{2}k}.$$

Given $\alpha \in G$, we also define a function $f_\infty^{k,v}(\alpha; \bullet, \chi, s)$ on $\mathcal{H}_n$ by

$$f_\infty^{k,v}(\alpha; z, \chi, s) = (\delta^{s - \frac{1}{2}k}|_{k,v} \alpha)(z)$$

$$= j_{\omega(\alpha)^{-1/2}\alpha}^{k,v}(z)^{-1} |j_{\omega(\alpha)^{-1/2}\alpha}(z)|^{-2}|^{s - \frac{1}{2}k} \delta(z)^{s - \frac{1}{2}k}.$$

By (18) and (19), we see that if $g \in G$ is such that $g(i) = z$ then, for each $\alpha \in G$,

$$f_\infty^{k,v}(\alpha g; i \cdot 1_n, \chi, s) = f_\infty^{k,v}(\alpha; z, \chi, s) f_\infty^{k,v}(g; i \cdot 1_n, \chi, s) \delta(z)^{\frac{1}{2}k - s}.$$

For $k \in \mathbb{Z}$ and $\nu = (\nu_v)_{v \in \Sigma} \in \mathbb{Z}^{\Sigma}$, $f_{\infty}^{k,\nu}(\alpha; \bullet, \chi, s)$ is a holomorphic function on $\mathcal{H}_n$ at $s = \frac{1}{2}k$.

3.1.2. *The Fourier coefficients at archimedean places of E.* When there is an integer k such that

$$s = \tfrac{1}{2}k = \tfrac{1}{2}k(\sigma) \quad \text{for all } \sigma \in \Sigma$$

(i.e., when $f_{\infty}^{k,\nu}(\alpha; z, \chi, s)$ is a holomorphic function of $z \in \mathcal{H}_n$), [Shimura 1983, Equation (7.12)] describes the archimedean Fourier coefficients precisely:

$$c_v\big(\beta, 1_n; f_v^{k,\nu}\big(\bullet; i1_n, \chi, \tfrac{1}{2}k\big)\big)$$

$$= 2^{(1-n)n} i^{-nk} (2\pi)^{nk} \left(\pi^{n(n-1)/2} \prod_{t=0}^{n-1} \Gamma(k-t) \right)^{-1} \sigma_v (\det \beta)^{k-n} e\big(i \operatorname{tr}(\sigma_v(\beta))\big) \quad (20)$$

for each archimedean place v of E. Observe that, when $k \geq n$,

$$\prod_{v \mid \infty} c_v\big(\beta, h; f_v^{k,\nu}\big(\bullet; i1_n\chi, \tfrac{1}{2}k\big)\big) = 0$$

unless $\det(\beta) \neq 0$ and $\det(h) \neq 0$, i.e., unless β is of rank n. Also, note that in our situation β will be in $\operatorname{Her}_n(K)$, so $\prod_{v \in \Sigma} e\big(i \operatorname{tr}(\sigma_v(\beta))\big) = e(ib)$ for some $b \in \mathbb{Q}$, so $\prod_{v \in \Sigma} e\big(i \operatorname{tr}(\sigma_v(\beta))\big) = e(ib)$ is a root of unity.

3.1.3. *Siegel sections at p.* We work with Siegel sections at p that are similar to the ones in [Eischen 2013, Section 2.2.8] (we multiply those by $|\omega(g)|_p^{-ns}$ to account for a similitude factor).

Lemma 5 [Eischen 2013, Lemma 10]. *Let Γ be a compact and open subset of $\prod_{v \in \Sigma} \operatorname{GL}_n(\mathcal{O}_{Ev})$, and let $\widetilde{F}$ be a locally constant Schwartz function*

$$\widetilde{F} : \prod_{v \in \Sigma} (\operatorname{Hom}_{K_v}(V_v, V_{d,v}) \oplus \operatorname{Hom}_{K_v}(V_v, V_v^d)) \to R$$

$$(X_1, X_2) \qquad\qquad\qquad \mapsto \widetilde{F}(X_1, X_2)$$

(with R a subring of $\mathbb{C}$) whose support in the first variable is Γ and such that

$$\widetilde{F}(X, {}^t X^{-1} Y) = \prod_{v \in \Sigma} \chi_v(\det(X)) \widetilde{F}(1, Y) \qquad (21)$$

for all X in Γ and Y in $\prod_{v \in \Sigma} M_{n \times n}(E_v)$.[2] There is a Siegel section $f^{P\widetilde{F}(-X,Y)}$ at p whose Fourier coefficient at $\beta \in M_{n \times n}(E_v)$ is

$$c(\beta, 1; f^{P\widetilde{F}(-X,Y)}) = \operatorname{volume}(\Gamma) \cdot \widetilde{F}(1, {}^t\beta).$$

---

[2]The version of the right-hand side of (21) appearing in [Eischen 2013, Lemma 10] reads "$\chi_1 \chi_2^{-1}(\det(X)) F(1, Y)$". The characters denoted χ_1 and χ_2 in [Eischen 2013] have the property that $\chi_1 \chi_2^{-1}(a) = \prod_{v \in \Sigma} \chi_v(a)$ for all $a \in \prod_{v \in \Sigma} \mathcal{O}_{Ev}$. The function denoted by $\widetilde{F}$ in the current paper is denoted by F in [Eischen 2013].

We use the notation *PF*, for "partial Fourier transform", to be consistent with [Katz 1978, Section 3.1; Eischen 2013, Section 2.2.8], but we do not need to discuss partial Fourier transforms here.

As a direct consequence of Lemma 5, we obtain the following corollary:

Corollary 6. *For any locally constant Schwartz function $\widetilde{F}$ satisfying the conditions of Lemma 5 for some Γ with positive volume, there is a Siegel section $f_{\widetilde{F}}$ in $\bigotimes_{v \in \Sigma} \mathrm{Ind}_{P(E_v)}^{G(E_v)}(\chi_v \cdot |\cdot|^{-2s})$ whose local (at p) Fourier coefficient at β is $\widetilde{F}(1, {}^t\beta)$.*

Furthermore, we can significantly weaken the conditions placed on $\widetilde{F}$:

Corollary 7. *Let k be a positive integer. Let $\widetilde{F}$ be a locally constant Schwartz function*

$$\widetilde{F} : \prod_{v \in \Sigma}(M_{n \times n}(\mathbb{O}_{E v}) \times M_{n \times n}(\mathbb{O}_{E v})) \to R$$

whose support lies in $\prod_{v \in \Sigma}(\mathrm{GL}_n(\mathbb{O}_{E v}) \times M_{n \times n}(\mathbb{O}_{E v}))$ and which satisfies

$$\widetilde{F}(e, {}^te^{-1}y) = N_{E/\mathbb{Q}}(\det e)^k \widetilde{F}(1, y)$$

for all $e \in \mathrm{GL}_n(\mathbb{O}_E)$ contained in the support Γ in the first variable of $\widetilde{F}$. Suppose, furthermore, that Γ has positive volume. Then there is a Siegel section $f_{\widetilde{F}} \in \bigotimes_{v \in \Sigma} \mathrm{Ind}_{P(E_v)}^{G(E_v)}(\chi_v \cdot |\cdot|^{-2s})$ whose local (at p) Fourier coefficient at β is $\widetilde{F}(1, {}^t\beta)$.

Proof. Let $\widetilde{F}$ be a locally constant Schwartz function

$$\widetilde{F} : \prod_{v \in \Sigma}(M_{n \times n}(\mathbb{O}_{E v}) \times M_{n \times n}(\mathbb{O}_{E v})) \to R$$

whose support lies in $\prod_{v \in \Sigma}(\mathrm{GL}_n(\mathbb{O}_{E v}) \times M_{n \times n}(\mathbb{O}_{E v}))$ and which satisfies

$$\widetilde{F}(e, {}^te^{-1}y) = N_{E/\mathbb{Q}}(\det e)^k \widetilde{F}(1, y), \tag{22}$$

for all $e \in \mathrm{GL}_n(\mathbb{O}_E)$ contained in the support in the first variable of $\widetilde{F}$. Then, since $\widetilde{F}$ is locally constant, has compact support, and satisfies (22), there is a unitary Hecke character χ whose infinity type is as in (8) and such that the conductor $\mathfrak{m} = p^d$ for d a sufficiently large positive integer, so that

$$\widetilde{F} = a_1 F_1 + \cdots + a_l F_l$$

for some positive integer l and $a_1, \ldots, a_l \in R$, and functions $F_1, \ldots, F_l$ meeting the conditions of Corollary 6 (all for this *same character* χ but possibly with *different supports* $\Gamma_1, \ldots, \Gamma_l$, respectively, in the first variable).

Now, we define

$$f_{\widetilde{F}} := a_1 f_{F_1} + \cdots + a_l f_{F_l},$$

where $f_{F_1}, \ldots, f_{F_l}$ are the Siegel sections obtained in Corollary 6. Then $f_{\widetilde{F}}$ is a linear combination of elements of the module $\bigotimes_{v \in \Sigma} \mathrm{Ind}_{P(E_v)}^{G(E_v)}(\chi_v \cdot |\cdot|^{-2s})$. So,

$f_{\widetilde{F}}$ is itself an element of $\bigotimes_{v \in \Sigma} \operatorname{Ind}_{P(E_v)}^{G(E_v)}(\chi_v \cdot |\cdot|^{-2s})$. Now, the Fourier coefficient of a sum of Siegel sections is the sum of the Fourier coefficients of these Siegel sections. So, the Fourier coefficient at β of $f_{\widetilde{F}}$ is

$$a_1 F_1(1, {}^t\beta) + \cdots + a_l F_l(1, {}^t\beta) = \widetilde{F}(1, {}^t\beta). \qquad \square$$

3.1.4. *Siegel sections away from p and ∞.* We use the same Siegel sections at places $v \nmid p\infty$ as in [Eischen 2013, Section 2.2.9]. We now recall the key properties of these Siegel sections, which are described in more detail in [Shimura 1997, Section 18].

Let $\mathfrak{b}$ be an ideal in $\mathbb{O}_E$ prime to p. For each finite place v prime to p, there is a Siegel section $f_v^{\mathfrak{b}} = f_v^{\mathfrak{b}}(\bullet; \chi_v, s) \in \operatorname{Ind}_{P(E_v)}^{G(E_v)}(\chi_v, s)$ with the following property: by [Shimura 1997, Proposition 19.2], whenever the Fourier coefficient $c(\beta, m(1); f_v^{\mathfrak{b}})$ is nonzero,

$$\prod_{v \nmid p\infty} c(\beta, m(1); f_v^{\mathfrak{b}})$$
$$= N_{E/\mathbb{Q}}(\mathfrak{b}\mathbb{O}_E)^{-n^2} \prod_{i=0}^{n-1} L^p(2s - i, \chi_E^{-1}\tau^i)^{-1} \prod_{v \nmid p\infty} P_{\beta, v, \mathfrak{b}}(\chi_E(\pi_v)^{-1}|\pi_v|_v^{2s}), \quad (23)$$

where:

(1) the product is over primes of E;

(2) the Hecke character χ_E is the restriction of χ to E;

(3) the function $P_{\beta, v, \mathfrak{b}}$ is a polynomial that is dependent only on β, v, and $\mathfrak{b}$ and has coefficients in $\mathbb{Z}$ and constant term 1;

(4) the polynomial $P_{\beta, v, \mathfrak{b}}$ is identically 1 for all but finitely many v;

(5) τ is the Hecke character of E corresponding to K/E;

(6) π_v is a uniformizer of $O_{E,v}$, viewed as an element of $K^\times$ prime to p;

(7) $L^p(r, \chi_E^{-1}\tau^i) = \prod_{v \nmid p\infty \operatorname{cond} \tau} \left(1 - \chi_v(\pi_v)^{-1}\tau^i(\pi_v)|\pi_v|_v^r\right)^{-1}$.

3.1.5. *Global Fourier coefficients.* Recall that, by Lemma 4, the Fourier coefficients $c(\beta, h; f)$ are completely determined by the coefficients $c(\beta, 1_n; f)$. In Proposition 8, we combine the results of Sections 3.1.2, 3.1.3, and 3.1.4 in order to give the global Fourier coefficients of the Eisenstein series E_f.

Let χ be a unitary Hecke character as above and, furthermore, suppose the infinity type of χ is

$$\prod_{\sigma \in \Sigma} \sigma^{-k-2v(\sigma)}(\sigma\bar{\sigma})^{\frac{1}{2}k+v(\sigma)} \qquad (24)$$

(i.e., $k(\sigma) = k \in \mathbb{Z}$ for all $\sigma \in \Sigma$). Let $C(n, K)$ be the constant dependent only upon n and K defined in (11).

Proposition 8. *Let $k \geq n$, let $v = (v(\sigma)) \in \mathbb{Z}^\Sigma$, and let*

$$f_{k,v,\chi,\widetilde{F}} := f_{k,v,\chi,\mathfrak{b},\widetilde{F}} := \bigotimes_{v \in \Sigma} f_{\widetilde{F},v} \otimes f_\infty^{k,v}(\bullet; i 1_n, \chi, s) \otimes f^\mathfrak{b} \in \mathrm{Ind}_{P(\mathbb{A}_E)}^{G(\mathbb{A}_E)}(\chi \cdot |\cdot|_K^{-s}) \tag{25}$$

with χ as in (24), $\bigotimes_{v \in \Sigma} f_{\widetilde{F},v}$ the section at p from Corollary 6, $f_\infty^{k,v}$ the section at ∞ defined in Section 3.1.2, and $f^\mathfrak{b}$ the section away from p and ∞ defined in Section 3.1.4.

Then, at $s = \frac{1}{2}k$, all the nonzero Fourier coefficients $c(\beta, 1_n; f_{k,v,\chi,\widetilde{F}})$ are given by

$$D(n, K, \mathfrak{b}, p, k) \prod_{v \nmid p\infty} P_{\beta,v,\mathfrak{b}}(\chi_E(\pi_v)^{-1}|\pi_v|_v^k) \widetilde{F}(1, {}^t\beta) \prod_{v \in \Sigma} \sigma_v(\det \beta)^{k-n} e(i \operatorname{tr}_{E/\mathbb{Q}}(\beta)), \tag{26}$$

where

$$D(n, K, \mathfrak{b}, p, k)$$
$$= C(n, K) N(\mathfrak{b}\mathbb{O}_E)^{-n^2} \left(2^{(1-n)n} i^{-nk} (2\pi)^{nk} \left(\pi^{n(n-1)/2} \prod_{t=0}^{n-1} \Gamma(k-t) \right)^{-1} \right)^{[E:\mathbb{Q}]}$$
$$\times \prod_{i=0}^{n-1} L^p(k-i, \chi_E^{-1}\tau^i)^{-1}.$$

Proof. This follows directly from (11), Corollary 6, (23), and (20). □

Given $\widetilde{F}$ as above, define

$$\widetilde{F}_\chi : (\mathbb{O}_K \otimes \mathbb{Z}_p) \times M_{n \times n}(\mathbb{O}_E \otimes \mathbb{Z}_p) \to R$$

to be the locally constant function whose support lies in

$$(\mathbb{O}_K \otimes \mathbb{Z}_p)^\times \times M_{n \times n}(\mathbb{O}_E \otimes \mathbb{Z}_p)$$

and which is defined on $(\mathbb{O}_K \otimes \mathbb{Z}_p)^\times \times M_{n \times n}(\mathbb{O}_E \otimes \mathbb{Z}_p)$ by

$$\widetilde{F}_\chi(x, y) = \prod_{v \in \Sigma} \chi_v(x) \widetilde{F}(1, N_{K/E}(x)^t y), \tag{27}$$

where the product is over the primes in Σ dividing p. Then, for all $e \in \mathbb{O}_K^\times$,

$$\widetilde{F}_\chi(ex, N_{K/E}(e^{-1})y) = N_{k,v}(e)\widetilde{F}_\chi(x, y)$$

for all $x \in \mathbb{O}_K \otimes \mathbb{Z}_p$ and $y \in M_{n \times n}(\mathbb{O}_E \otimes \mathbb{Z}_p)$. On the other hand, any locally constant function

$$F : (\mathbb{O}_K \otimes \mathbb{Z}_p) \times M_{n \times n}(\mathbb{O}_E \otimes \mathbb{Z}_p) \to R$$

supported on $(\mathbb{O}_K \otimes \mathbb{Z}_p)^\times \times M_{n \times n}(\mathbb{O}_E \otimes \mathbb{Z}_p)$ which satisfies

$$F(ex, N_{K/E}(e)^{-1}y) = N_{E/\mathbb{Q}}(e)^k F(x, y)$$

for all $e \in \mathbb{O}_K^\times$, $x \in \mathbb{O}_K \otimes \mathbb{Z}_p$, and $y \in M_{n \times n}(\mathbb{O}_E \otimes \mathbb{Z}_p)$ can be written as a linear combination of such functions $\widetilde{F}_\chi$ for Hecke characters χ of infinity type (k, ν) and conductor dividing p^∞ and functions $\widetilde{F}$ as above.

Now, let

$$G_{k,\nu,\chi,\widetilde{F}} = D(n, K, \mathfrak{b}, p, k)^{-1} E_{f_{k,\nu,\chi,\widetilde{F}}}.$$

Applying Proposition 8, we see that the Fourier coefficients of the holomorphic function $G_{k,\nu,\widetilde{F}}(z, \frac{1}{2}k)$ on $\mathcal{H}_n$ are all finite $\mathbb{Z}$-linear combinations (over a finite set of p-adic units $a \in K$) of terms of the form

$$\widetilde{F}_\chi(a, N_{K/E}(a)^{-1}\beta) N_{k,\nu}(a^{-1} \det \beta) N_{E/\mathbb{Q}}(\det \beta)^{-n} \tag{28}$$

(Although π_ν from Proposition 8 is a place of E for all ν, the element a from (28) might be in K but not $\mathbb{O}_E$, depending on our choice of cusp. The effect of the change of a cusp $m \in GM_+(\mathbb{A}_E)$ on q-expansions is given in Lemma 4.)

Thus, we obtain the following result:

Lemma 9. *Let $k \in \mathbb{Z}_{\geq n}$ and $\nu \in \mathbb{Z}^\Sigma$. Let F be a locally constant function*

$$F : (\mathbb{O}_K \otimes \mathbb{Z}_p) \times M_{n \times n}(\mathbb{O}_E \otimes \mathbb{Z}_p) \to R$$

supported on $(\mathbb{O}_K \otimes \mathbb{Z}_p)^\times \times M_{n \times n}(\mathbb{O}_E \otimes \mathbb{Z}_p)$ which satisfies

$$F(ex, N_{K/E}(e)^{-1}y) = N_{k,\nu}(e) F(x, y)$$

for all $e \in \mathbb{O}_K^\times$, $x \in \mathbb{O}_K \otimes \mathbb{Z}_p$, and $y \in M_{n \times n}(\mathbb{O}_E \otimes \mathbb{Z}_p)$. Then there is a C^∞ automorphic form $G_{k,\nu,F}(z, s)$ (on $U(n, n)$) of weight (k, ν) that is holomorphic at $s = \frac{1}{2}k$ and whose Fourier expansion at $s = \frac{1}{2}k$ at a cusp $m \in GM_+(\mathbb{A}_E)$ is of the form $\sum_{0 < \beta \in L_m} c(\beta) q^\beta$ (where L_m is the lattice in $\mathrm{Her}_n(K)$ determined by m) with $c(\beta)$ a finite $\mathbb{Z}$-linear combination of terms of the form given in (28).

(We obtain $G_{k,\nu,F}$ as a linear combination of the automorphic forms $G_{k,\nu,\chi,\widetilde{F}}$.)

4. Differential operators

4.1. C^∞ differential operators. In this section, we summarize results on C^∞ differential operators that were studied extensively by Shimura [1984a; 1984b; 1997, Section 23; 2000, Section 12]. Let $T = M_{n \times n}(\mathbb{C})$; we identify T with the tangent space of $\mathcal{H}_n$. For each nonnegative integer d, let $\mathfrak{S}_d(T)$ denote the vector space of $\mathbb{C}$-valued homogeneous polynomial functions on T of degree d. (For instance, the e-th power of the determinant function, $\det^e$, is in $\mathfrak{S}_{ne}(T)$.) We denote by τ^d the representation of $\mathrm{GL}_n(\mathbb{C}) \times \mathrm{GL}_n(\mathbb{C})$ on $\mathfrak{S}_d(T)$ defined by

$$\tau^d(a, b)g(z) = g({}^t azb)$$

for all $a, b \in \mathrm{GL}_n(\mathbb{C})$, $z \in T$, and $g \in \mathfrak{S}_d(T)$.

The classification of the irreducible subspaces of polynomial representations of $GL_n(\mathbb{C})$ and of irreducible subspaces of τ^r for each r is provided in [Shimura 1984b, Section 2; 1997, Sections 12.6 and 12.7]. We summarize the key features needed for our results; further details can be found in those two references. Given a matrix $a \in M_{n \times n}(\mathbb{C})$, let $\det_j(a)$ denote the determinant of the upper left $j \times j$ submatrix of a. Each polynomial representation of $GL_n(\mathbb{C})$ can be composed into a direct sum of irreducible representations of $GL_n(\mathbb{C})$. Each irreducible representation ρ of $GL_n(\mathbb{C})$ contains a unique eigenvector p of highest weight $r_1 \geq \cdots r_n \geq 0$ (for a unique ordered n-tuple $r_1 \geq \cdots \geq r_n \geq 0$ of integers dependent on ρ), which is a common eigenvector of the upper triangular matrices of $GL_n(\mathbb{C})$ and satisfies

$$\rho(a)p = \prod_{j=1}^{n} \det_j(a)^{e_j} p,$$

$$e_j = r_j - r_{j+1}, \quad 1 \leq j \leq n-1, \tag{29}$$

$$e_n = r_n \tag{30}$$

for all a in the subgroup of upper triangular matrices in $GL_n(\mathbb{C})$. Also, for each ordered n-tuple $r_1 \geq \cdots \geq r_n \geq 0$, there is a unique corresponding irreducible polynomial representation of $GL_n(\mathbb{C})$. If ρ and σ are irreducible representations of $GL_n(\mathbb{C})$ then, by [Shimura 2000, Theorem 12.7], $\rho \otimes \sigma$ occurs in τ^r if and only if ρ and σ are representations of the same highest weights $r_1 \geq \cdots \geq r_n$ as each other and $r_1 + \cdots + r_n = r$. In this case, $\rho \otimes \sigma$ occurs with multiplicity one in τ^r, and the corresponding irreducible subspace of τ^r contains the polynomial $p(x) = \prod_{j=1}^{n} \det_j(x)^{e_j}$ (where e_j is defined as in (29) and (30)); this polynomial $p(x)$ is an eigenvector of highest weight with respect to both ρ and σ.

Let (Z, τ_Z) be an irreducible subspace of $(\mathfrak{S}_d, \tau)$ of highest weight $r_1 \geq \cdots \geq r_n$, and let $\zeta \in Z$. By [Shimura 1984b; 1997, Section 23; 2000, Section 13], there are C^∞ differential operators $D_k(\zeta)$ that act on C^∞ functions on $\mathcal{H}_n$ and have the property that, for all $\alpha \in U(\eta_n)$, $\zeta \in Z \subseteq \mathfrak{S}_d(T)$, and complex numbers s,

$$D_k(\zeta)(\delta^s \|_{k,\nu}\alpha) = i^d \psi_Z(-k-s)(\delta^s \|_{k,\nu}\alpha) \cdot \zeta({}^t\eta^{-1\,t}\overline{\lambda_\alpha}{}^t\mu_\alpha^{-1}), \tag{31}$$

where (as proved in [Shimura 1984b, Theorem 4.1])

$$\psi_Z(s) = \prod_{h=1}^{n} \prod_{j=1}^{r_h} (s - j + h).$$

If ρ is the representation of $GL_n(\mathbb{C}) \times GL_n(\mathbb{C})$, there is a differential operator D_ρ^Z (defined in [Eischen 2012, p. 222; Shimura 2000, Equation (12.20)]) such that for all C^∞ functions f on $\mathcal{H}_n$, $D_\rho^Z f$ is a $\mathrm{Hom}(Z, \mathbb{C})$-valued C^∞ function on $\mathcal{H}_n$ with

the property that

$$(D_\rho^Z f)\|_{\rho \otimes \tau_Z}\alpha = D_\rho^Z(f\|_\rho\alpha) \tag{32}$$

for all $\alpha \in G$. Furthermore, if ρ is defined by $\rho(a, b) = \det(b)^k$ then, as the proof of [Shimura 1997, Lemma 23.4] explains,

$$D_k(\zeta)f = (D_\rho^Z f)(\zeta).$$

When Z is a Σ-tuple $(Z_v)_{v\in\Sigma}$, we also use ψ_Z to denote $\prod_{v\in\Sigma}\psi_{Z_v}$.

So, for example, if $d \in \mathbb{Z}_{\geq 0}$ and $\zeta = \det^d$, then (31) becomes

$$D_k(\det^d)(\delta^s\|_{k,v}\alpha) = i^{nd}\psi_Z(-k-s)\delta^s\|_{k,v}\alpha \cdot \det^d({}^t\eta^{-1}\,{}^t\overline{\lambda}_\alpha \cdot {}^t\mu_\alpha^{-1})$$

$$= \left(\tfrac{1}{2}i\right)^{nd}\prod_{h=1}^{n}\prod_{j=1}^{d}(-k-s-j+h)\delta^{s-d}\|_{k+2d,v-d}\alpha.$$

Consequently, if $d = (d(\sigma))_{\sigma\in\Sigma} \in \mathbb{Z}_{\geq 0}^\Sigma$, then

$$\left(\prod_{\sigma\in\Sigma}D_k(\det^{d(\sigma)})\right)\left(G_{k,v,F}\left(z,\tfrac{1}{2}k\right)\right)$$

$$= \prod_{\sigma\in\Sigma}\left(\tfrac{1}{2}i\right)^{nd(\sigma)}\prod_{h=1}^{n}\prod_{j=1}^{d(\sigma)}(-k-j+h)G_{k+2d,v-d,F}\left(z,\tfrac{1}{2}k\right)$$

as in [Eischen 2013, Equation (43)].

As noted in [Shimura 1984b, Section 6], $G_{k,v,F}(z, s)$ is a special case of the automorphic form $G_{k,v,\zeta,F}(z, s)$ that satisfies

$$D_k(\zeta)\left(G_{k,v,F}\left(z,\tfrac{1}{2}k\right)\right) = \prod_{v\in\Sigma}i^{d_v}\psi_{Z_v}(-k)G_{k,v,\zeta,F}\left(z,\tfrac{1}{2}k\right),$$

where

$$D_k(\zeta) = \prod_{v\in\Sigma}D_k(\zeta_v).$$

The case where ζ is a highest-weight vector will be of particular interest to us.

4.2. *Rational representations.*

In order to generalize our discussion from the C^∞ setting to the p-adic setting, we introduce rational representations, following [Hida 2004, Section 8.1.2] (which, in turn, summarizes relevant results from [Hida 2000; Jantzen 1987]).

Let A be a ring or a sheaf of rings over a scheme. Let B denote the Borel subgroup of GL_n consisting of upper triangular matrices in GL_n. Let N denote the unipotent radical of B. Let $T \cong B/N$ denote the torus. Following the notation of

[Hida 2004, Section 8.1.2], for each character κ of T we define

$$R_A[\kappa] = \mathrm{Ind}_B^{\mathrm{GL}_n}(\kappa)$$
$$= \left\{ f : \mathrm{GL}_n/N \to \mathbf{A}^1 \mid f(ht) = \kappa(t)f(h) \text{ for all } t \in T, \ h \in \mathrm{GL}_n/N \right\}.$$

The group GL_n acts on $R_A[\kappa]$ via

$$(g \cdot f)(x) = f(g^{-1}x).$$

As noted in [Hida 2004, p. 332], there is a unique (up to an A-unit multiple) N-invariant linear form ℓ_{can} in the dual space $R_A[\kappa]^\vee$ that generates $(R_A[\kappa]^\vee)^N$ and can be normalized so that, for all $f \in R_A[\kappa]$,

$$\ell_{\mathrm{can}}(f) = f(1_n),$$

where 1_n denotes the origin in GL_n/N.

Note that, for each C^∞ automorphic form f on $\prod_{v \in \Sigma} \mathcal{H}_n$ such that $f\|_{k,v}\alpha = f$ (for all α in some congruence subgroup) and each highest-weight vector ζ in an irreducible representation of highest weight κ, we may view $D_k(\zeta)f$ as an $R_{\mathbb{C}}[\det^{k+v} \cdot \kappa] \otimes R_{\mathbb{C}}[\det^{-v} \cdot \kappa]$-valued function on $\mathcal{H}_n$. We define a corresponding character $\kappa_{k,v}(t_1, \ldots, t_n, t_{n+1}, \ldots, t_{2n}) = \prod_{i=1}^n t_i^{k+v} t_{i+n}^{-v}$ on $T(\mathbb{C}) \times T(\mathbb{C})$.

4.3. *The algebraic geometric setting.*

As explained in detail in [Eischen 2012, Section 8.4], which generalizes [Katz 1978, Section 2.3], the C^∞ differential operators discussed by Shimura have a geometric interpretation in terms of the Gauss–Manin connection. C^∞ automorphic forms can [Eischen 2012, Section 2] be interpreted as sections of a vector bundle on (the complex analytification of) the moduli spaces $\mathcal{M}_{n,n} = \mathrm{Sh}(W)$. Applying a differential operator (as discussed in [Eischen 2012, Sections 6–9]) to an automorphic form of weight ρ on $\mathcal{M}_{n,n}$ sends it to an automorphic form of weight $\rho \otimes \tau$ on $\mathcal{M}_{n,n}$.

We now recall the setting of [Eischen 2013, Section 3], as we will momentarily be in a similar (but not identical) situation. For any $\mathbb{O}_K$-algebra R, the R-valued points of $_{\mathcal{H}}\mathrm{Sh}(R)$ parametrize tuples $\underline{A}$ consisting of an abelian variety together with a polarization, endomorphism, and level structure. (We shall not need further details of these points here; see [Lan 2013, Chapter 1; Hida 2004, Chapter 7; Eischen 2012, Section 2] for more details.) Given a point $\underline{A}$ in $_{\mathcal{H}}\mathrm{Sh}(R)$, we write $\underline{\omega}_{A/R} = \underline{\omega}^+_{A/R} \oplus \underline{\omega}^-_{A/R}$ for the sheaf of one-forms on $\underline{A}$. (As in [Eischen 2012, Section 2], $\underline{\omega}^+_{A/R}$ and $\underline{\omega}^-_{A/R}$ are the rank-n submodules determined by the action of $\mathbb{O}_K$.) We identify $G(\mathbb{Q})\backslash X \times G(\mathbb{A}_f)/\mathcal{H}$ (which we identify with copies of $\mathcal{H}_n$) with the points of $_{\mathcal{H}}\mathrm{Sh}(\mathbb{C})$; we shall write $\underline{A}(z)$ to mean the point of $\underline{A}$ identified with $z \in \prod_{v \in \Sigma} \mathcal{H}_n$ under this identification. Under this identification, if we fix an ordered basis of differentials $u_1^\pm, \ldots, u_n^\pm$ for $\underline{\omega}^\pm_{A_{\mathrm{univ}}/\mathcal{H}_n}$, then an automorphic form

f on $\mathcal{H}_n$ corresponds to an automorphic form $\tilde{f}$ on $_{\mathcal{H}}\mathrm{Sh}(\mathbb{C})$ via

$$f(z) = \tilde{f}(\underline{A}(z), u_1^{\pm}(z), \ldots, u_n^{\pm}(z)),$$

Any other ordered basis of differentials for $\underline{\omega}_{\underline{A}/\mathbb{C}}^{\pm}$ is simply obtained by the linear action of $\mathrm{GL}_n(\mathbb{O}_K \otimes \mathbb{C}) \cong \mathrm{GL}_n(\mathbb{C}) \times \mathrm{GL}_n(\mathbb{C})$ on $\underline{\omega}(z) = \underline{\omega}(z)^+ \oplus \underline{\omega}(z)^-$, and

$$\tilde{f}\big(\underline{A}(z), g \cdot (u_1^{\pm}(z), \ldots, u_n^{\pm}(z))\big) = g \cdot \big(f(\underline{A}(z), u_1^{\pm}(z), \ldots, u_n^{\pm}(z))\big)$$

4.3.1. *A p-adic analogue.* In [Eischen 2012, Section 9], we discussed a p-adic analogue θ_ρ^Z of the differential operators D_ρ^Z. The differential operators θ_ρ^Z act on sections of certain vector bundles on the Igusa tower $T_{\infty,\infty}$ (a formal scheme over the ordinary locus of $_{\mathcal{H}}\mathrm{Sh}(R)$ for R a mixed characteristic discrete valuation ring with residue characteristic p); for details on the Igusa tower, see [Hida 2004, Section 8]. More precisely, θ_ρ^Z acts on sections of $R_{T_{\infty,\infty}}[\kappa]$ for various weights κ. By [Hida 2004, map (8.4)],

$$\ell_{\mathrm{can}} : H^0(T_{\infty,\infty}, R_{T_{\infty,\infty}}[\kappa]) \to V^N[\kappa] \qquad (33)$$

is an injective map into the space $V^N[\kappa] = V_{\infty,\infty}^N[\kappa]$ of p-adic modular forms of weight κ. Given a highest-weight vector ζ in Z, we define $\theta(\zeta) := \theta_k := \ell_{\mathrm{can}} \circ \theta_\rho^Z$, where $\rho(a, b) := \det(b)^k$.

In [Eischen 2012, Section 9], we gave a formula for the action of p-adic differential operators θ_ρ^Z on q-expansions. In particular, if the q-expansion of a scalar weight form $f \in H^0(T_{\infty,\infty}, R_{T_{\infty,\infty}}[\kappa])$ at a cusp $m \in GM$ is

$$f(q) = \sum_\beta a(\beta) q^\beta,$$

and ζ is a highest-weight vector, then it follows from the formulas in [Eischen 2012, Section 9] that

$$(\theta(\zeta)f)(q) = \sum_\beta a(\beta) \cdot \zeta(\beta) q^\beta. \qquad (34)$$

5. A *p*-adic Eisenstein measure with values in the space of vector-weight automorphic forms

5.1. *p-adic Eisenstein series.* As we explain in Theorem 10, when R is a (profinite) p-adic ring, we can extend Theorem 2 to the case of continuous (not necessarily locally constant) functions F. For the remainder of the paper, let N be as in Section 4.2.

Theorem 10. *Let R be a (profinite) p-adic $\mathbb{O}_K$-algebra. Fix an integer $k \geq n$, and let $\nu = (\nu(\sigma))_{\sigma \in \Sigma} \in \mathbb{Z}^\Sigma$. Let*

$$F : (\mathbb{O}_K \otimes \mathbb{Z}_p) \times M_{n \times n}(\mathbb{O}_E \otimes \mathbb{Z}_p) \to R$$

be a continuous function supported on $(\mathbb{O}_K \otimes \mathbb{Z}_p)^\times \times \mathrm{GL}_n(\mathbb{O}_E \otimes \mathbb{Z}_p)$ which satisfies

$$F(ex, N_{K/E}(e)^{-1}y) = N_{k,\nu}(e)F(x, y)$$

for all $e \in \mathbb{O}_K^\times$, $x \in \mathbb{O}_K \otimes \mathbb{Z}_p$ and $y \in \mathrm{GL}_n(\mathbb{O}_E \otimes \mathbb{Z}_p)$. Then there exists a p-adic automorphic form $G_{k,\nu,F}$ whose q-expansion at a cusp $m \in GM$ is of the form $\sum_{0 < \beta \in L_m} c(\beta)q^\beta$ (where L_m is the lattice in $\mathrm{Her}_n(K)$ determined by m), with $c(\beta)$ a finite $\mathbb{Z}$-linear combination of terms of the form

$$F(a, N_{K/E}(a)^{-1}\beta)N_{k,\nu}(a^{-1}\det\beta)N_{E/\mathbb{Q}}(\det\beta)^{-n}$$

(where the linear combination is the sum over a finite set of p-adic units $a \in K$ dependent upon β and the choice of cusp $m \in GM$).

Proof. The proof is similar to the proof of [Katz 1978, Theorem (3.4.1)]. We remind the reader of the idea of that result. For each integer $j \geq 1$, define

$$F_j : (\mathbb{O}_K \otimes \mathbb{Z}_p) \times M_{n \times n}(\mathbb{O}_E \otimes \mathbb{Z}_p) \to R/p^j R$$
$$F_j(x, y) = F(x, y) \bmod p^j R.$$

Then F_j is a locally constant function satisfying the conditions of Theorem 2. So, by the q-expansion principle for p-adic forms [Hida 2005, Corollary 10.4; Hida 2004, Section 8.4], there is a p-adic automorphic form $G_{k,\nu,F}$ whose q-expansion satisfies the conditions in the statement of the theorem. $\square$

Corollary 11. *Let R be a (profinite) p-adic $\mathbb{O}_K$-algebra, let $\nu = (\nu(\sigma))_{\sigma \in \Sigma} \in \mathbb{Z}^\Sigma$, and let $k \geq n$ be an integer. Let*

$$F : (\mathbb{O}_K \otimes \mathbb{Z}_p) \times M_{n \times n}(\mathbb{O}_E \otimes \mathbb{Z}_p) \to R$$

be a continuous function supported on $(\mathbb{O}_K \otimes \mathbb{Z}_p)^\times \times \mathrm{GL}_n(\mathbb{O}_E \otimes \mathbb{Z}_p)$ which satisfies

$$F(ex, N_{K/E}(e)^{-1}yz) = N_{k,\nu}(e)F(x, y)$$

for all $e \in \mathbb{O}_K^\times$, $x \in \mathbb{O}_K \otimes \mathbb{Z}_p$, and $y \in M_{n \times n}(\mathbb{O}_E \otimes \mathbb{Z}_p)$. Then

$$G_{k,\nu,F} = G_{n,0,N_{k-n,\nu}(x^{-1}N_{K/E}(x)^n \det y)F(x,y)}, \tag{35}$$

where

$$N_{k-n,\nu}(x^{-1}N_{K/E}(x)^n \det y)F(x, y),$$

denotes the function defined by

$$(x, y) \mapsto N_{k-n,\nu}(x^{-1}N_{K/E}(x)^n \det y)F(x, y).$$

on $(\mathbb{O}_K \otimes \mathbb{Z}_p)^\times \times M_{n \times n}(\mathbb{O}_E \otimes \mathbb{Z}_p)$ and extended by 0 to $(\mathbb{O}_K \otimes \mathbb{Z}_p) \times M_{n \times n}(\mathbb{O}_E \otimes \mathbb{Z}_p)$.

Proof. This follows from the q-expansion principle [Hida 2005, Corollary 10.4]. $\square$

Remark 12. We comment now on the relationship between the weight of $G_{n,0,F}$ and the p-adically continuous function F appearing in the subscript. By Corollary 11 and Theorem 2, we have that, if F is a locally constant function satisfying the conditions of Corollary 11, then the p-adic automorphic form $G_{n,0,N_{k-n,\nu}(x^{-1}N_{K/E}(x)^n \det y)F(x,y)}$ is the weight-(k, ν) p-adic automorphic form $G_{k,\nu,F}$. More generally, by (34), the p-adic automorphic form $G_{n,0,N_{k-n,\nu}(x^{-1}N_{K/E}(x)^n \det y)F(x,y)\zeta_\kappa(N_{K/E}(x)y^{-1})}$ is the weight-$(\kappa \cdot \kappa_{k,\nu})$ p-adic automorphic form $\theta(\zeta_\kappa)G_{k,\nu,F}$, where ζ_κ is a highest-weight vector for the representation of weight κ. In particular, the p-adic automorphic form $G_{n,0,N_{k-n,\nu}(x^{-1}N_{K/E}(x)^n \det y)F(x,y)\det(N_{K/E}(x)y^{-1})^d}$ is the p-adic automorphic form $\theta(\det^d)G_{n,0,N_{k-n,\nu}(x^{-1}N_{K/E}(x)^n \det y)F(x,y)\zeta_\kappa(N_{K/E}(x)y^{-1})}$ of weight $(k + 2d, \nu - d)$.

5.1.1. *CM points and pullbacks.* In this section, we compare the values of certain p-adic automorphic forms and C^∞ automorphic forms at CM points.[3] This material extends [Eischen 2013, Section 3.0.1] beyond the case of scalar weights. Let R be an $\mathbb{O}_K$-subalgebra of $\overline{\mathbb{Q}} \cap \iota_\infty^{-1}(\mathbb{O}_{\mathbb{C}_p})$ in which p splits completely. Note that the embeddings ι_∞ and ι_p restrict to R to give embeddings

$$\iota_\infty : R \hookrightarrow \mathbb{C},$$

$$\iota_p : R \hookrightarrow R_0 = \varprojlim_m R/p^m R.$$

Let $\underline{A}$ be a CM abelian variety with PEL structure over R, i.e., a CM point of the moduli space $_K\mathrm{Sh}(R)$ or, equivalently, a point of $\mathrm{Sh}(U(n) \times U(n)) \hookrightarrow \mathrm{Sh}(U(n,n))$. By extending scalars we may also view $\underline{A}$ as an abelian variety over $\mathbb{C}$ or R_0.

By an argument similar to [Eischen 2013, Section 3.0.1], there are complex and p-adic periods $\Omega = (\Omega^+, \Omega^-) \in (\mathbb{C}^\times)^n \times (\mathbb{C}^\times)^n$ and $c = (c^+, c^-) \in (\mathbb{O}_{\mathbb{C}_p}^\times)^n \times (\mathbb{O}_{\mathbb{C}_p}^\times)^n$, respectively, attached to each CM abelian variety $\underline{A}$ over R such that (if F is R-valued, so $G_{k,\nu,F}$ arises over R)

$$(\kappa \cdot \kappa_{k,\nu})^{-1}(\Omega) \prod_{\sigma \in \Sigma} \kappa_\sigma(2\pi i)\psi_Z(-k)G_{k,\nu,\zeta,F}\left(z; h, \chi, \mu, \tfrac{1}{2}k\right)$$
$$= (\kappa \cdot \kappa_{k,\nu})^{-1}(c)\theta(\zeta)G_{k,\nu,F}(\underline{A}), \quad (36)$$

where z is a point in $\prod_{\sigma \in \Sigma} \mathscr{H}_n$ corresponding to the CM abelian variety $\underline{A}$ viewed as an abelian variety over $\mathbb{C}$ (by extending scalars to $\mathbb{C}$). Here, Z is the irreducible subrepresentation of $\prod_{\nu \in \Sigma} \mathrm{GL}_n(\mathbb{C}) \times \mathrm{GL}_n(\mathbb{C})$ of highest weight $\kappa \in (\mathbb{Z}^n)^\Sigma$ and has ζ as a highest-weight vector; by $\kappa(a)$ with a a scalar, we mean κ evaluated at the n-tuple $(a, \ldots, a)$ in the torus. (The periods Ω and c can be defined uniformly

---

[3]The significance of CM points is that they correspond to points of $U(n) \times U(n) \subseteq U(n,n)$, which are the points used (for instance, by Shimura) to study algebraicity of values of Eisenstein series, which are used in turn to study algebraicity of values of certain L-functions (through the doubling method, or "pull back method", a construction of L-functions described in various sources, including [Gelbart et al. 1987, Part A; Cogdell 2006, Section 2]). Determining the *precise* values of these Eisenstein series at CM points is neither necessary nor generally computationally feasible at this time.

for all CM points at once [Katz 1978, Section 5.1]. For the present paper, though, this is not necessary.) Note that when $\kappa = \det^d$ (i.e., is the highest weight for a one-dimensional representation), we recover [Eischen 2013, Equation (45)].

5.2. Eisenstein measures. In analogue with [Katz 1978, Lemma (4.2.0)] (which handles the case of Hilbert modular forms), we have the following lemma (which applies to all integers $n \geq 1$):

Lemma 13. *Let R be a p-adic $\mathbb{O}_K$-algebra. Then the inverse constructions*

$$H(x, y) = \frac{1}{N_{n,0}(x N_{K/E}(x)^{-n} \det y)} F(x, y^{-1}), \tag{37}$$

$$F(x, y) = \frac{1}{N_{n,0}(x^{-1} N_{K/E}(x)^n \det y)} H(x, y^{-1}) \tag{38}$$

give an R-linear bijection between the set of continuous R-valued functions

$$F : (\mathbb{O}_K \otimes \mathbb{Z}_p)^\times \times \mathrm{GL}_n(\mathbb{O}_E \otimes \mathbb{Z}_p) \to R$$

satisfying

$$F(ex, N_{K/E}(e)^{-1} y) = N_{n,0}(e) F(x, y) \quad \text{for all } e \in \mathbb{O}_K^\times$$

and the set of continuous R-valued functions

$$H : (\mathbb{O}_K \otimes \mathbb{Z}_p)^\times \times \mathrm{GL}_n(\mathbb{O}_E \otimes \mathbb{Z}_p) \to R$$

satisfying

$$H(ex, N_{K/E}(e) y) = H(x, y) \quad \text{for all } e \in \mathbb{O}_K^\times.$$

Proof. The proof follows immediately from the properties of F and H. $\square$

Let

$$\mathscr{G}_n = ((\mathbb{O}_K \otimes \mathbb{Z}_p)^\times \times \mathrm{GL}_n(\mathbb{O}_E \otimes \mathbb{Z}_p))/\overline{\mathbb{O}_K^\times}, \tag{39}$$

where $\overline{\mathbb{O}_K^\times}$ denotes the p-adic closure of $\mathbb{O}_K^\times$ embedded diagonally, as $(e, N_{K/E}(e))$, in $(\mathbb{O}_K \otimes \mathbb{Z}_p)^\times \times \mathrm{GL}_n(\mathbb{O}_E \otimes \mathbb{Z}_p)$ (and, as before, $(\mathbb{O}_E \otimes \mathbb{Z}_p)^\times$ is embedded diagonally inside of $\mathrm{GL}_n(\mathbb{O}_E \otimes \mathbb{Z}_p)$). Then Lemma 13 gives a bijection between the R-valued continuous functions H on $\mathscr{G}_n$ and the R-valued continuous functions F on $(\mathbb{O}_K \otimes \mathbb{Z}_p)^\times \times \mathrm{GL}_n(\mathbb{O}_E \otimes \mathbb{Z}_p)$ satisfying $F(ex, N_{K/E}(e)^{-1} y) = N_{n,0}(e) F(x, y)$ for all $e \in \mathbb{O}_K^\times$.

For any (profinite) p-adic ring R, an R-valued p-adic measure on a (profinite) compact, totally disconnected topological space Y is a $\mathbb{Z}_p$-linear map

$$\mu : \mathscr{C}(Y, \mathbb{Z}_p) \to R$$

or, equivalently [Katz 1978, Section 4.0], an R'-linear map

$$\mu : \mathscr{C}(Y, R') \to R$$

for any p-adic ring R' such that R is an R'-algebra. Instead of $\mu(f)$, one typically writes

$$\int_Y f\, d\mu.$$

In Theorem 14, we specialize to the case where R is the ring $\mathcal{V}_{n,n}$ of p-adic automorphic forms on $U(n,n)$ and Y is the group $\mathcal{G}_n$ defined in (39).

Theorem 14 (a p-adic Eisenstein measure for vector-weight automorphic forms). *Let R be a profinite p-adic ring. There is a $\mathcal{V}_{n,n}$-valued p-adic measure $\mu = \mu_{\mathfrak{b},n}$ on $\mathcal{G}_n$ defined by*

$$\int_{\mathcal{G}_n} H\, d\mu_{\mathfrak{b},n} = G_{n,0,F}$$

for all continuous R-valued functions H on $\mathcal{G}_n$, with

$$F(x,y) = \frac{1}{N_{n,0}(x^{-1} N_{K/E}(x)^n \det y)} H(x, y^{-1})$$

extended by 0 to all of $(\mathcal{O}_K \otimes \mathbb{Z}_p) \times M_{n \times n}(\mathcal{O}_E \otimes \mathbb{Z}_p)$.

Proof. F is the function corresponding to H under the bijection in Lemma 13. The theorem then follows immediately from Theorem 10, Corollary 11, Lemma 13, and the q-expansion principle. $\qquad\square$

Note that the measure $\mu_{\mathfrak{b},n}$ depends only upon n and $\mathfrak{b}$. In Section 6, we relate the measure $\mu_{\mathfrak{b},n}$ to the Eisenstein measure in [Katz 1978, Definition (4.2.5) and Equation (5.5.7)] and comment on how $\mu_{\mathfrak{b},n}$ can be modified to the case of Siegel modular forms (i.e., automorphic forms on symplectic groups).

It follows from the definition of the measure $\mu_{\mathfrak{b},n}$ in Theorem 14 that, for each highest-weight vector ζ_κ of highest weight κ,

$$\int_{\mathcal{G}_n} H(x,y) \zeta_\kappa(N_{K/E}(x) y^{-1})\, d\mu_{\mathfrak{b},n} = \theta(\zeta_\kappa) G_{n,0,F(x,y)}.$$

Now, let $\underline{A}$ be an ordinary CM abelian variety with PEL structure over a subring R of $\overline{\mathbb{Q}} \cap \mathcal{O}_{\mathbb{C}_p}$, i.e., a CM point of the moduli space $_K\mathrm{Sh}(R)$, or equivalently, a point of $\mathrm{Sh}(U(n) \times U(n)) \hookrightarrow \mathrm{Sh}(U(n,n))$. As discussed above, by extending scalars, we may also view $\underline{A}$ as an abelian variety over $\mathbb{C}$ or over $R_0 = \varprojlim_m R/p^m R$. It follows from (36) and Corollary 11 that, for $F(x,y)$ locally constant, supported on $(\mathcal{O}_K \otimes \mathbb{Z}_p)^\times \times \mathrm{GL}_n(\mathcal{O}_E \otimes \mathbb{Z}_p)$ and satisfying

$$F(ex, N_{K/E}(e)^{-1} y) = N_{k,\nu}(e) F(x,y)$$

for all $e \in \mathbb{O}_K^\times$, $x \in \mathbb{O}_K \otimes \mathbb{Z}_p$, and $y \in \mathrm{GL}_n(\mathbb{O}_E \otimes \mathbb{Z}_p)$,

$$(\kappa \cdot \kappa_{k,\nu})^{-1}(c) \int_{\mathcal{G}_n} \frac{1}{N_{k,\nu}(x N_{K/E}(x)^{-n} \det y)} F(x, y^{-1}) \zeta_\kappa(N_{K/E}(x)y^{-1}) \, d\mu_{\mathfrak{b},n}(\underline{A})$$

$$= (\kappa \cdot \kappa_{k,\nu})^{-1}(\Omega) \prod_{\sigma \in \Sigma} \kappa_\sigma(2\pi i) \psi_Z(-k) G_{k,\nu,\zeta_\kappa,F}\left(z, \tfrac{1}{2}k\right), \quad (40)$$

and, for any $d = (d_v)_{v \in \Sigma} \in \mathbb{Z}_{\geq 0}^\Sigma$,

$$(\kappa_{k+2d,\nu-d})^{-1}(c)$$

$$\times \int_{\mathcal{G}_n} \frac{1}{N_{k,\nu}(x N_{K/E}(x)^{-n} \det y)} F(x, y^{-1}) \det(N_{K/E}(x)y^{-1})^d \, d\mu_{\mathfrak{b},n}(\underline{A})$$

$$= (\kappa_{k+2d,\nu-d})^{-1}(\Omega) \prod_{\sigma \in \Sigma} (2\pi i)^{nd} \psi_Z(-k) G_{k+2d,\nu-d,F(x,y)}\left(z, \tfrac{1}{2}k\right),$$

where z is a point in $\prod_{\sigma \in \Sigma} \mathcal{H}_n$ corresponding to the CM abelian variety $\underline{A}$ viewed as an abelian variety over $\mathbb{C}$ (by extending scalars to $\mathbb{C}$) and Ω and c are the periods from (36). Here, Z is the irreducible subrepresentation of $\prod_{\sigma \in \Sigma} \mathrm{GL}_n(\mathbb{C}) \times \mathrm{GL}_n(\mathbb{C})$ of highest weight κ and has ζ_κ as a highest-weight vector; by $\kappa(a)$ with a a scalar, we mean κ evaluated at the n-tuple $(a, \ldots, a)$ in the torus.

In other words, the p-adic measure $\mu_{\mathfrak{b},n}$ allows us to p-adically interpolate the values of the C^∞ (not necessarily holomorphic) function $G_{k,\nu,\zeta_\kappa,F}\left(z, \tfrac{1}{2}k\right)$ at CM points z.

Theorem 15. *For each ordinary abelian variety $\underline{A}$ defined over a (profinite) p-adic $\mathbb{O}_K$-algebra R_0, there is an R_0-valued p-adic measure $\mu(\underline{A}) := \mu_{\mathfrak{b},n}(\underline{A})$ defined by*

$$\int_{\mathcal{G}_n} H \, d\mu_{\mathfrak{b},n}(\underline{A}) = G_{n,0,F}(\underline{A})$$

for all continuous R-valued functions H on $\mathcal{G}_n$, with

$$F(x, y) = \frac{1}{N_{n,0}(x^{-1} N_{K/E}(x)^n \det y)} H(x, y^{-1})$$

extended by 0 to all of $(\mathbb{O}_K \otimes \mathbb{Z}_p) \times M_{n \times n}(\mathbb{O}_E \otimes \mathbb{Z}_p)$. If $R_0 = \varprojlim_m R/p^m R$ with $R \subseteq \overline{\mathbb{Q}}$, $\underline{A}$ is an ordinary CM point defined over R, and F is a locally constant function supported on $(\mathbb{O}_K \otimes \mathbb{Z}_p)^\times \times \mathrm{GL}_n(\mathbb{O}_E \otimes \mathbb{Z}_p)$ satisfying

$$F(ex, N_{K/E}(e)^{-1}y) = N_{k,\nu}(e) F(x, y)$$

for all $e \in \mathbb{O}_K^\times$, $x \in \mathbb{O}_K \otimes \mathbb{Z}_p$, and $y \in \mathrm{GL}_n(\mathbb{O}_E \otimes \mathbb{Z}_p)$, then

$$(\kappa \cdot \kappa_{k,\nu})^{-1}(c) \int_{\mathcal{G}_n} \frac{1}{N_{k,\nu}(x N_{K/E}(x)^{-n} \det y)} F(x, y^{-1}) \zeta_\kappa(N_{K/E}(x)y^{-1}) \, d\mu_{\mathfrak{b},n}(\underline{A})$$

$$= (\kappa \cdot \kappa_{k,\nu})^{-1}(\Omega) \prod_{\sigma \in \Sigma} \kappa_\sigma(2\pi i) \psi_Z(-k) G_{k,\nu,\zeta_\kappa,F}\left(z, \tfrac{1}{2}k\right),$$

with $z \in \prod_{v \in \Sigma} \mathcal{H}_n$ *corresponding to the ordinary CM abelian variety* $\underline{A}$ *viewed as an abelian variety over* $\mathbb{C}$.

The pullback of an automorphic form on $U(n, n)$ to $U(n) \times U(n)$ is automatically an automorphic form on the product of definite unitary groups $U(n) \times U(n)$. So Theorem 14 also gives a p-adic measure with values in the space of automorphic forms on the product of definite unitary groups $U(n) \times U(n)$. In [Eischen 2014, Section 4], we explain how to modify our construction to obtain p-adic measures with values in the space of automorphic forms on certain nondefinite groups.

Remark 16 (relationship to the Eisenstein measures in [Eischen 2013, Section 4]). For the curious reader, we briefly explain the relationship between the measure $\mu_{\mathfrak{b},n}$ defined in Theorem 14 and the measure ϕ defined in [Eischen 2013, Theorem 20]. For each $v \in \Sigma$, let $r_v = r(v) \leq n$ be a positive integer and let $r = (r_v)_v \in \mathbb{Z}^{\Sigma}$. As in [Eischen 2013, Equation (33)], let

$$T(r) = \prod_{v \in \Sigma} \underbrace{\mathbb{O}_{E_v}^{\times} \times \cdots \times \mathbb{O}_{E_v}^{\times}}_{r_v \text{ copies}}. \tag{41}$$

Let $\rho = \prod_{v \in \Sigma}(\rho_{1,v}, \ldots, \rho_{r(v),v})$ be a p-adic character on $T(r)$ (i.e., $\rho((\alpha_v)_{v \in \Sigma}) := \prod_{v \in \Sigma} \prod_{i=1}^{r(v)} \rho_{i,v}(\alpha_v)$ for all $\alpha = (\alpha_v)_{v \in \Sigma} \in T(r)$), let $n = n_{1,v} + \cdots + n_{r_v,v}$ be a partition of n for each $v \in \Sigma$, and let F_ρ be the function on $M_{n \times n}(E)$ defined by

$$F_\rho(x) := \prod_{v \in \Sigma} \prod_{i=1}^{r(v)} \rho_{i,v}(\det_{n_i}(x)),$$

with $\det_j$ defined as on page 2455. Let χ be a p-adic function supported on $(\mathbb{O}_K \otimes \mathbb{Z}_p)^{\times}/\overline{\mathbb{O}_K^{\times}}$ and extended by 0 to all of $\mathbb{O}_K \otimes \mathbb{Z}_p$. Let $H_{\rho,\chi}$ be the function corresponding via the bijection in Lemma 13 to the function $F_{\rho,\chi}$ supported on $\mathcal{G}_n$ (and extended by 0) defined by

$$F_{\rho,\chi}(x, y) = \chi(x) \mathbb{N}_{n,0}(x) F_\rho(N_{K/E}(x)\,{}^t y).$$

Then

$$\int_{\mathcal{G}_n} H_{\rho,\chi} \, d\mu_{\mathfrak{b},n} = \int_{(\mathbb{O}_K \otimes \mathbb{Z}_p)^{\times}/\overline{\mathbb{O}_K^{\times}} \times T(r)} (\chi, \rho) \, d\phi.$$

Note that the measure ϕ is dependent upon the choice of r and the choice of the partition of n, while the measure $\mu_{\mathfrak{b},n}$ is independent of both of these choices.

6. Remarks about the case of symplectic groups, Siegel modular forms, and Katz's Eisenstein measure for Hilbert modular forms

The case of Siegel modular forms is quite similar. We essentially just need to replace the CM field K with the totally real field E throughout. Once we have replaced

K by E, $N_{k,\nu}$ becomes $N_{E/\mathbb{Q}}^k$ and $N_{K/E}$ becomes the identity map. Consequently, (37) and (38) become

$$H(x, y) = \frac{1}{N_{E/\mathbb{Q}}(x^{1-n} \det y)^n} F(x, y^{-1}),$$

$$F(x, y) = \frac{1}{N_{E/\mathbb{Q}}(x^{-1+n} \det y)^n} H(x, y^{-1}).$$

To highlight the similarity with [Katz 1978, Section 4.2] we note that, when $n = 1$, these equations become

$$H(x, y) = \frac{1}{N_{E/\mathbb{Q}}(y)} F(x, y^{-1}),$$

$$F(x, y) = \frac{1}{N_{E/\mathbb{Q}}(y)} H(x, y^{-1}).$$

This relationship between H and F is similar to the relationship between the similar functions denoted H and F by Katz [1978, Section 4.2]. (The minor difference is due to the fact that, throughout the paper, his $F(x, y)$ is our $F(y, x)$.)

The differential operators are developed from the C^∞ perspective simultaneously for both unitary and symplectic groups in [Shimura 2000, Section 12]. As noted in [Eischen 2012, p. 4; 2012, Section 3.1.1; Panchishkin 2005; Courtieu and Panchishkin 2004], the algebraic geometric and p-adic formulation of the operators for Siegel modular forms (i.e., for symplectic groups) is similar. In the case of Siegel modular forms, the algebraic geometric formulation of the differential operators is discussed in [Harris 1981, Section 4]. Also, the case of symplectic groups is handled directly alongside the case of unitary groups in Hida's discussion [2004, Chapter 8] of p-adic automorphic forms. So the construction in this paper carries over with only minor changes (essentially, replacing K by E throughout) to the case of symplectic groups over a totally real field E and automorphic forms (Siegel modular forms) on those groups.

6.1. *The case n = 1.* Continuing with the symplectic case with $n = 1$, Theorem 2 becomes:

Theorem 17. *Let R be an $\mathbb{O}_E$-algebra and let $k \geq 1$ be an integer. For each locally constant function*

$$F : (\mathbb{O}_E \otimes \mathbb{Z}_p) \times (\mathbb{O}_E \otimes \mathbb{Z}_p) \to R$$

supported on $(\mathbb{O}_E \otimes \mathbb{Z}_p)^\times \times (\mathbb{O}_E \otimes \mathbb{Z}_p)^\times$ which satisfies

$$F(ex, e^{-1}y) = N_{E/\mathbb{Q}}(e)^k F(x, y) \tag{42}$$

for all $e \in \mathbb{O}_E^\times$, $x \in \mathbb{O}_E \otimes \mathbb{Z}_p$, and $y \in \mathbb{O}_E \otimes \mathbb{Z}_p$, there is a Hilbert modular form $G_{k,F}$ of weight k defined over R whose q-expansion at a cusp $m \in GM$ is of the form

$\sum_{\beta>0} c(\beta) q^\beta$ (*where* L_m *is the lattice in* E *determined by* m) *with* $c(\beta)$ *a finite* $\mathbb{Z}$-*linear combination of terms of the form*

$$F(a, (a)^{-1}\beta) N(a^{-1}\beta)^k N_{E/\mathbb{Q}}(\beta)^{-1}$$

(*where the linear combination is a sum over a finite set of* p-*integral* $a \in E$ *dependent upon* β *and the choice of cusp* $m \in GM$).

Still continuing with the symplectic case with $n = 1$, Theorem 14 becomes:

Theorem 18. *There is a measure* μ *on*

$$\mathcal{G} = ((\mathbb{O}_E \otimes \mathbb{Z}_p)^\times \times (\mathbb{O}_E \otimes \mathbb{Z}_p)^\times)/\overline{\mathbb{O}_E^\times}$$

(*with values in the space of* p-*adic Hilbert modular forms*), *defined by*

$$\int_{\mathcal{G}} H \, d\mu = G_{1,F}$$

for all continuous R-*valued functions* H *on* $\mathcal{G}$, *with*

$$F(x, y) = \frac{1}{N_{E/\mathbb{Q}}(y)} H(x, y^{-1})$$

extended by 0 *to all of* $(\mathbb{O}_E \otimes \mathbb{Z}_p) \times (\mathbb{O}_E \otimes \mathbb{Z}_p)$.

Note that we have essentially recovered the Eisenstein series and measure from [Katz 1978, Definition (4.2.5)]. (Again, the difference between Katz's order of the variables x and y and ours is due to the fact that, throughout the paper, his $F(x, y)$ is our $F(y, x)$.) The reader might notice the similarities with [Katz 1978, (5.5.1)–(5.5.7)]. In particular, let χ be a Grössencharacter of the CM field K whose conductor divides p^∞ and whose infinity type is

$$-k \sum_{\sigma \in \Sigma} \sigma - \sum_{\sigma \in \Sigma} d(\sigma)(\sigma - \bar{\sigma})$$

with $d(\sigma) \geq 0$ for all $\sigma \in \Sigma$ and $k \geq n$. We view χ as an $\mathbb{O}_{\mathbb{C}_p}$-valued character on $\mathbb{A}^{\infty,\times} \times \prod_{v \in \Sigma} \overline{\mathbb{Q}}$ (by restricting it to this group) and consider its restriction to the subring consisting of elements $((1_v)_{v \nmid p\infty}, a, a)$, with $a \in \mathbb{O}_K \otimes \mathbb{Z}_{(p)}$, which is a subring of

$$(\mathbb{O}_K \otimes \mathbb{Z}_p)^\times \xrightarrow{\sim} (\mathbb{O}_E \otimes \mathbb{Z}_p)^\times \times (\mathbb{O}_E \otimes \mathbb{Z}_p)^\times.$$

Then we have

$$\chi(\alpha) = \chi_{\text{finite}}(\alpha) \cdot \frac{\prod_{\sigma \in \Sigma} \sigma(\bar{\alpha})^{d(\sigma)}}{\prod_{\sigma \in \Sigma} \sigma(\alpha)^{k+d(\sigma)}},$$

$$\chi(x, y) = \chi_{\text{finite}}(x, y) \cdot \frac{\prod_{\sigma \in \Sigma} \sigma(x)^{d(\sigma)}}{\prod_{\sigma \in \Sigma} \sigma(y)^{k+d(\sigma)}},$$

with χ_{finite} a locally constant function. If

$$F(x, y) = \frac{1}{N(y)} \chi\left(x, \frac{1}{y}\right)$$

$$= \chi_{\text{finite}}\left(x, \frac{1}{y}\right) \cdot N(y)^{k-1} \prod_{\sigma \in \Sigma} \sigma(xy)^{d(\sigma)}, \tag{43}$$

then

$$\int_{\mathcal{G}} \chi(x, y) \, d\mu_{\mathfrak{b}, 1} = G_{1, F} \tag{44}$$

$$= G_{1, \chi_{\text{finite}}(x, 1/y) N(y)^{k-1} \prod_{\sigma \in \Sigma} \sigma(xy)^{d(\sigma)}} \tag{45}$$

$$= G_{k, \chi_{\text{finite}}(x, 1/y) \prod_{\sigma \in \Sigma} \sigma(xy)^{d(\sigma)}} \tag{46}$$

$$= \left(\prod_{\sigma \in \Sigma} \theta(\sigma)^{d(\sigma)}\right)(G_{k, \chi_{\text{finite}}(x, 1/y)}), \tag{47}$$

where $\theta(\sigma)$ denotes the (σ component of the) differential operator $\theta(\det)$ acting on automorphic forms in the one-dimensional, symplectic case. Note the similarity of (43) through (47) with [Katz 1978, Equations (5.5.6)–(5.5.7)].

Acknowledgements

References

[Ando et al. 2010] M. Ando, M. Hopkins, and C. Rezk, "Multiplicative orientations of KO-theory and of the spectrum of topological modular forms", preprint, 2010, http://www.math.uiuc.edu/~mando/papers/koandtmf.pdf.

[Cogdell 2006] J. Cogdell, "Lectures on integral representation of L-functions", unpublished notes, 2006, http://www.math.osu.edu/~cogdell/columbia-www.pdf.

[Courtieu and Panchishkin 2004] M. Courtieu and A. Panchishkin, *Non-Archimedean L-functions and arithmetical Siegel modular forms*, 2nd. ed., Lecture Notes in Mathematics **1471**, Springer, Berlin, 2004. MR 2005e:11056 Zbl 1070.11023

[Deligne and Ribet 1980] P. Deligne and K. A. Ribet, "Values of abelian L-functions at negative integers over totally real fields", *Invent. Math.* **59**:3 (1980), 227–286. MR 81m:12019 Zbl 0434.12009

[Eischen 2012] E. E. Eischen, "p-adic differential operators on automorphic forms on unitary groups", *Ann. Inst. Fourier (Grenoble)* **62**:1 (2012), 177–243. MR 2986270 Zbl 1257.11054

[Eischen 2013] E. E. Eischen, "A p-adic Eisenstein measure for unitary groups", *J. reine angew. Math.* (online publication April 2013).

[Eischen 2014] E. E. Eischen, "Differential operators, pullbacks, and families of automorphic forms", preprint, 2014. arXiv 1405.0721

[Eischen et al. ≥ 2014] E. E. Eischen, M. Harris, J.-S. Li, and C. M. Skinner, "*p*-adic *L*-functions for unitary groups", In preparation.

[Gelbart et al. 1987] S. Gelbart, I. Piatetski-Shapiro, and S. Rallis, *Explicit constructions of automorphic L-functions*, Lecture Notes in Mathematics **1254**, Springer, Berlin, 1987. MR 89k:11038 Zbl 0612.10022

[Harris 1981] M. Harris, "Special values of zeta functions attached to Siegel modular forms", *Ann. Sci. École Norm. Sup.* (4) **14**:1 (1981), 77–120. MR 82m:10046 Zbl 0465.10022

[Harris et al. 2006] M. Harris, J.-S. Li, and C. M. Skinner, "*p*-adic *L*-functions for unitary Shimura varieties, I: Construction of the Eisenstein measure", *Doc. Math.* Extra Vol. (2006), 393–464. MR 2008d:11042 Zbl 1143.11019

[Hida 2000] H. Hida, *Geometric modular forms and elliptic curves*, World Scientific, River Edge, NJ, 2000. MR 2001j:11022 Zbl 0960.11032

[Hida 2004] H. Hida, *p-adic automorphic forms on Shimura varieties*, Springer, New York, 2004. MR 2005e:11054 Zbl 1055.11032

[Hida 2005] H. Hida, "*p*-adic automorphic forms on reductive groups", pp. 147–254 in *Automorphic forms, I*, Astérisque **298**, Société Mathématique de France, Paris, 2005. MR 2006e:11060 Zbl 1122.11026

[Hopkins 1995] M. J. Hopkins, "Topological modular forms, the Witten genus, and the theorem of the cube", pp. 554–565 in *Proceedings of the International Congress of Mathematicians* (Zürich, 1994), vol. 1, edited by S. D. Chatterji, Birkhäuser, Basel, 1995. MR 97i:11043 Zbl 0848.55002

[Hopkins 2002] M. J. Hopkins, "Algebraic topology and modular forms", pp. 291–317 in *Proceedings of the International Congress of Mathematicians, Vol. I* (Beijing, 2002), edited by T. Li, Higher Ed. Press, Beijing, 2002. MR 2004g:11032 Zbl 1031.55007

[Jantzen 1987] J. C. Jantzen, *Representations of algebraic groups*, Pure and Applied Mathematics **131**, Academic Press, Boston, 1987. MR 89c:20001 Zbl 0654.20039

[Katz 1973] N. M. Katz, "*p*-adic properties of modular schemes and modular forms", pp. 69–190 in *Modular functions of one variable* (Antwerp, 1972), vol. III, edited by W. Kuyk and J.-P. Serre, Lecture Notes in Mathematics **350**, Springer, Berlin, 1973. MR 56 #5434 Zbl 0271.10033

[Katz 1978] N. M. Katz, "*p*-adic *L*-functions for CM fields", *Invent. Math.* **49**:3 (1978), 199–297. MR 80h:10039 Zbl 0417.12003

[Lan 2012] K.-W. Lan, "Comparison between analytic and algebraic constructions of toroidal compactifications of PEL-type Shimura varieties", *J. Reine Angew. Math.* **664** (2012), 163–228. MR 2980135 Zbl 1242.14022

[Lan 2013] K.-W. Lan, *Arithmetic compactifications of PEL-type Shimura varieties*, London Mathematical Society Monographs **36**, Princeton University Press, Princeton, NJ, 2013. MR 3186092 Zbl 1284.14004

[Panchishkin 2005] A. A. Panchishkin, "The Maass–Shimura differential operators and congruences between arithmetical Siegel modular forms", *Mosc. Math. J.* **5**:4 (2005), 883–918, 973–974. MR 2007k:11072 Zbl 1129.11021

[Serre 1973] J.-P. Serre, "Formes modulaires et fonctions zêta *p*-adiques", pp. 69–190 in *Modular functions of one variable* (Antwerp, 1972), vol. III, edited by W. Kuyk and J.-P. Serre, Lecture Notes in Mathematics **350**, Springer, Berlin, 1973. MR 53 #7949a Zbl 0277.12014

[Shimura 1983] G. Shimura, "On Eisenstein series", *Duke Math. J.* **50**:2 (1983), 417–476. MR 84k: 10019 Zbl 0519.10019

[Shimura 1984a] G. Shimura, "Differential operators and the singular values of Eisenstein series", *Duke Math. J.* **51**:2 (1984), 261–329. MR 85h:11031 Zbl 0546.10025

[Shimura 1984b] G. Shimura, "On differential operators attached to certain representations of classical groups", *Invent. Math.* **77**:3 (1984), 463–488. MR 86c:11034 Zbl 0558.10023

[Shimura 1997] G. Shimura, *Euler products and Eisenstein series*, CBMS Regional Conference Series in Mathematics **93**, Amer. Math. Soc., Providence, RI, 1997. MR 98h:11057 Zbl 0906.11020

[Shimura 2000] G. Shimura, *Arithmeticity in the theory of automorphic forms*, Mathematical Surveys and Monographs **82**, Amer. Math. Soc., Providence, RI, 2000. MR 2001k:11086 Zbl 0967.11001

[Tan 1999] V. Tan, "Poles of Siegel Eisenstein series on U(n, n)", *Canad. J. Math.* **51**:1 (1999), 164–175. MR 2000e:11073 Zbl 0963.11028

eeischen@email.unc.edu   *Department of Mathematics,*
                                The University of North Carolina at Chapel Hill, CB #3250,
                                Chapel Hill, NC 27599-3250, United States

Explicit points on the Legendre curve III

Douglas Ulmer

We continue our study of the Legendre elliptic curve $y^2 = x(x + 1)(x + t)$ over function fields $K_d = \mathbb{F}_p(\mu_d, t^{1/d})$. When $d = p^f + 1$, we have previously exhibited explicit points generating a subgroup $V_d \subset E(K_d)$ of rank $d - 2$ and of finite, p-power index. We also proved the finiteness of $\text{III}(E/K_d)$ and a class number formula: $[E(K_d) : V_d]^2 = |\text{III}(E/K_d)|$. In this paper, we compute $E(K_d)/V_d$ and $\text{III}(E/K_d)$ explicitly as modules over $\mathbb{Z}_p[\text{Gal}(K_d/\mathbb{F}_p(t))]$.

An errata was posted on 31 May 2017 in an online supplement.

1. Introduction

Let p be an odd prime number, $\mathbb{F}_p$ the field of p elements, and $K = \mathbb{F}_p(t)$ the rational function field over $\mathbb{F}_p$. Let E be the elliptic curve over K defined by $y^2 = x(x + 1)(x + t)$. In [Ulmer 2014b], we studied the arithmetic of E over the extension fields $K_d = \mathbb{F}_p(\mu_d, t^{1/d})$ for integers d not divisible by p. In particular, when $d = p^f + 1$, we exhibited explicit points generating a subgroup $V_d \subset E(K_d)$ of rank $d - 2$ and finite p-power index. Moreover, we showed that the Tate–Shafarevich group $\text{III}(E/K_d)$ is finite and its order satisfies $|\text{III}(E/K_d)| = [E(K_d) : V_d]^2$. Some of these results were generalized to other values of d in [Conceição et al. 2014].

Our goal in this paper is to study the quotient group $E(K_d)/V_d$ and the Tate–Shafarevich group $\text{III}(E/K_d)$ as modules over the group ring $\mathbb{Z}_p[\text{Gal}(K_d/K)]$. In fact, we will completely determine both modules in terms of combinatorial data coming from the action of the cyclic group $\langle p \rangle \subset (\mathbb{Z}/d\mathbb{Z})^\times$ on the set $\mathbb{Z}/d\mathbb{Z}$. Stating the most precise results requires some preliminaries that are given in the next section, so in this introduction, we state only the main qualitative results.

Theorem 1.1. *Let p be an odd prime number, and let $d = p^f + 1$. Let $K = \mathbb{F}_p(t)$, $K_d = \mathbb{F}_p(\mu_d, u)$ where $u^d = t$, and $G = \text{Gal}(K_d/K)$. Let E be the elliptic curve over K defined by $y^2 = x(x + 1)(x + t)$. Let V_d be the subgroup of $E(K_d)$ generated by the point $P = (u, u(u + 1)^{d/2})$ and its conjugates by G. Let $\text{III}(E/K_d)$ be the Tate–Shafarevich group of E over K_d. Then $E(K_d)/V_d$ and $\text{III}(E/K_d)$ are finite abelian p-groups with the following properties:*

---

(1) $E(K_d)/V_d$ and $\text{III}(E/K_d)$ are trivial if and only if $f \le 2$.

(2) The exponent of the group $E(K_d)/V_d$ is $p^{\lfloor (f-1)/2 \rfloor}$. The exponent of the group $\text{III}(E/K_d)$ is $p^{\lfloor f/3 \rfloor}$. Here $\lfloor x \rfloor$ is the greatest integer $\le x$.

(3) $(E(K_d)/V_d)^2$ and $\text{III}(E/K_d)$ are isomorphic as $\mathbb{Z}_p[G]$-modules if and only if $f \le 4$. If $f > 4$, they are not isomorphic as abelian groups.

(4) The Jordan–Hölder factors of $\text{III}(E/K_d)$ as $\mathbb{Z}_p[G]$-modules are the same as those of $E(K_d)/V_d$ with multiplicities doubled.

(5) There is a polynomial $F_f(T) \in \mathbb{Z}[1/2][T]$ depending on f but independent of p such that

$$|\text{III}(E/K_d)| = p^{F_f(p)}$$

for all $p > 2$.

Part (4) of the theorem may be viewed as an analogue of the Gras conjecture; see [Gras 1977; Mazur and Wiles 1984].

To my knowledge, the phenomenon of "interpolation in p" in part (5) has not been observed before. In fact, even more is true, namely that all of the invariants of $\text{III}(E/K_d)$ and $E(K_d)/V_d$ as abelian p-groups (i.e., the order of their p^a-torsion subgroups for all a) are described by polynomials independent of p.

Results on the exact structure of $E(K_d)/V_d$ and $\text{III}(E/K_d)$ as $\mathbb{Z}_p[G]$-modules will be stated in Section 3 after some preliminaries in Section 2.

In fact, we will prove results on the discriminant of the "new part" of $E(K_d)$ with its height pairing and on the $\mathbb{Z}_p[G]$-module structure of the "new part" of $\text{III}(E/K_d)$ for any d such that p is balanced modulo d in the sense of [Conceição et al. 2014, Definition 2.1]. (This is the situation in which there are points on $E(K_d)$ not coming from $E(K_e)$ for e a proper divisor of d.) In cases where we have explicit points (namely for $d = p^f + 1$ as in [Ulmer 2014b] or $d = 2(p^f - 1)$ as in [Conceição et al. 2014]), we obtain good control on $E(K_d)/V_d$ as well. Some of our results apply to other curves and their Jacobians and for $p = 2$. See Theorems 3.1.1, 3.2.1, and 3.3.1 for the main refined results.

The two key ideas that afford such strong control on Mordell–Weil and Tate–Shafarevich groups are (i) that the Néron model of E over $\mathbb{P}^1_{/\mathbb{F}_p(\mu_d)}$ is dominated by a product of curves, and (ii) ideas of Shioda and Dummigan that allow us to use crystalline cohomology to compute Tate cycles and Brauer groups for products of curves. Similar ideas were used by Dummigan [1995; 1999] to compute the discriminant of the Mordell–Weil lattice and the structure of the Tate–Shafarevich group for a constant supersingular elliptic curve over the function field of a Hermitian curve. In our case, the group of symmetries (essentially G above) is much smaller, the representation theory is much simpler, and as a result, we are able to boil the combinatorics down to very explicit statements.

Here is an outline of the rest of the paper. In Section 2, we consider the orbits of $\langle p \rangle \subset (\mathbb{Z}/d\mathbb{Z})^\times$ acting on $\mathbb{Z}/d\mathbb{Z}$. These orbits index certain $\mathbb{Z}_p[G]$-modules that we use to decompose and describe $E(K_d)$ and $\text{III}(E/K_d)$. In Section 3, we state the more precise results on $E(K_d)$ and $\text{III}(E/K_d)$ alluded to above. In Section 4, we work out the geometry relating the Néron model of E to a product of curves (which in fact are Fermat quotient curves) and the relations between the Mordell–Weil and Tate–Shafarevich groups of E and the Néron–Severi and Brauer groups of the product of curves. In Section 5, we work out the Néron–Severi group and the p-part of the Brauer group of a general product of curves in terms of crystalline cohomology. That this is possible (in the context of supersingular surfaces) was noted by Shioda [1991] and developed more fully by Dummigan [1995]. We use a somewhat different method than Dummigan did, yielding more general results, although his results would suffice for our application to the Legendre curve. In Section 6, we collect results on the cohomology of the curves appearing in the product mentioned above. These results give the raw material for Section 7, where we carry out the p-adic exercises needed to compute $E(K_d)$ and $\text{III}(E/K_d)$. In Section 8, we put all the pieces together and prove the main results. Finally, Section 9 contains various generalizations and complements.

2. Orbits, invariants, and representations

Throughout this section, p is an arbitrary prime number and d is a positive integer not divisible by p. We write $(\mathbb{Z}/d\mathbb{Z})^\times$ for the multiplicative group modulo d and $\langle p \rangle$ for the cyclic subgroup generated by p.

2.1. _Orbits._ Consider the action of $(\mathbb{Z}/d\mathbb{Z})^\times$ on the set $\mathbb{Z}/d\mathbb{Z}$ by multiplication. By restriction, the subgroup $\langle p \rangle$ acts on $\mathbb{Z}/d\mathbb{Z}$. We write $\widetilde{O} = \widetilde{O}_{d,p}$ for the set of orbits. Thus, if $o \in \widetilde{O}$ and $i \in o \subset \mathbb{Z}/d\mathbb{Z}$, then $o = \{i, pi, p^2i, \dots\}$.

Clearly the orbit through $0 \in \mathbb{Z}/d\mathbb{Z}$ is a singleton $\{0\}$. If d is even (and therefore p is odd), then the orbit through $d/2$ is also a singleton because $p(d/2) = (d/2)$ in $\mathbb{Z}/d\mathbb{Z}$. For reasons that will become apparent later, we will usually exclude these two orbits, and we define

$$O = O_{d,p} = \begin{cases} \widetilde{O} \setminus \{\{0\}\} & \text{if } d \text{ is odd,} \\ \widetilde{O} \setminus \{\{0\}, \{d/2\}\} & \text{if } d \text{ is even.} \end{cases}$$

Note that if $o \in \widetilde{O}$, then $\gcd(i, d)$ is the same for all $i \in o$, and we write $\gcd(o, d)$ for this common value. It will sometimes be convenient to consider only orbits with $\gcd(o, d) = 1$ (which one might call "new" orbits), so we define

$$O' = O'_{d,p} = \{o \in O \mid \gcd(o, d) = 1\}.$$

Note that $O'_{d,p}$ is just the set of cosets of $\langle p \rangle$ in $(\mathbb{Z}/d\mathbb{Z})^\times$. Note also that the set of orbits $o \in O$ with $\gcd(o, d) = e$ for a fixed $e < d/2$ is in bijection with $O'_{d/e,p}$.

2.2. Balanced orbits. From here through the end of Section 2.7, we assume that $d > 2$ so that $O_{d,p}$ is not empty.

As in [Conceição et al. 2014], we divide $(\mathbb{Z}/d\mathbb{Z})^\times$ into two subsets A and B where A and B consist of those classes with least positive residue in the intervals $(0, d/2)$ and $(d/2, d)$, respectively.

We say that an orbit o is *balanced* if we have $|o \cap A| = |o \cap B|$, and we say d is *balanced modulo p* if every orbit $o \in O'_{d,p}$ is balanced. For example, by [Conceição et al. 2014, §5.4, §5.5], d is balanced modulo p if d divides $p^f + 1$ or if d divides $2(p^f - 1)$ and the ratio $2(p^f - 1)/d$ is odd.

2.3. Invariants of orbits. Associated to each orbit o, we form a word on the two-letter alphabet $\{u, l\}$ (u for upper and l for lower) as follows. Choose a base point i so that the orbit $o = \{i, pi, p^2i, \ldots, p^{|o|-1}i\}$. The associated word $w = w_1 \cdots w_{|o|}$ is defined by

$$w_j = \begin{cases} l & \text{if } -p^{j-1}i \in A, \\ u & \text{if } -p^{j-1}i \in B. \end{cases}$$

(The reason for the minus signs is explained in Remark 6.4.1.) Thus, for example, if $p = 3$ and $d = 28$, the word associated to the orbit $\{6, 18, 26, 22, 10, 2\}$ with base point 6 is *ullluu*.

Note that w depends on the choice of $i \in o$. Changing the choice of i changes w by a cyclic permutation of the letters.

Given a word $w = w_1 \cdots w_{|o|}$, we define a sequence of integers a_j by $a_0 = 0$ and

$$a_j = a_{j-1} + \begin{cases} 1 & \text{if } w_j = u, \\ -1 & \text{if } w_j = l. \end{cases}$$

(So the word w is viewed as a sequence of instructions to go up or down.)

If o is balanced, then the word w associated to o has as many u's as l's and $a_{|o|} = 0$.

Definition 2.3.1. We say the base point i is *good* if $a_j \geq 0$ for $0 \leq j \leq |o|$. It is easy to see that every o has a good base point. The *standard base point* for an orbit o is the good base point with smallest least positive residue.

So for example, if $p = 3$, $d = 364$, and o is the orbit $\{7, 21, 63, 189, 203, 245\}$, then there is a unique good base point, namely 7, with associated word *uuulll*. On the other hand, if o is the orbit $\{37, 111, 333, 271, 85, 255\}$, then the good base points are 37 (with word *uullul*) and 85 (with word *uluull*), and the standard base point is 37. From now on, given an orbit, we choose the standard base point and form the word associated to that base point. This yields a well-defined function from

orbits to words. (It will be essential below to choose a good base point, but which good base point is chosen is of no import. We introduce the notion of standard base point simply for convenience.)

Now suppose that w is the word associated to a balanced orbit o. Then the first letter of w must be u and the last must be l, so we can write w in exponential form

$$w = u^{e_1} l^{e_2} \cdots l^{e_{2k}}$$

where each $e_j > 0$.

2.4. *The complementary case.* Suppose that $d > 2$ and d divides $p^f + 1$ for some f so that $-1 \in \langle p \rangle$. If $i \in A$, then $p^f i \in B$ and conversely. It follows that if $o \in O_{d,p}$ and w is the associated word, then the second half of w is the "complement" of the first half, i.e., each u is replaced with an l and each l is replaced with a u. More formally, if $w = w_1 w_2 \cdots w_{|o|}$, then $\{w_j, w_{|o|/2+j}\} = \{u, l\}$ for all $1 \leq j \leq |o|/2$.

A similar discussion applies when d divides $2(p^f - 1)$ with an odd quotient and o is an orbit with $\gcd(o, d)$ odd. Indeed, in this case, $p^f \equiv 1 + d/2 \pmod{d}$ and p^f is an element of order 2 in $(\mathbb{Z}/d\mathbb{Z})^\times$ that exchanges A and B. Thus, if o is an orbit with $\gcd(o, d)$ odd, then the associated word has second half equal to the complement of the first half.

These examples motivate the following definition:

Definition 2.4.1. We say an orbit o is *complementary* if it is balanced and the associated word $w = w_1 \cdots w_{|o|}$ satisfies $\{w_j, w_{|o|/2+j}\} = \{u, l\}$ for $1 \leq j \leq |o|/2$.

If o is complementary and we write the associated word in exponential form $w = u^{e_1} l^{e_2} \cdots l^{e_{2k}}$, then $e_{k+j} = e_j$. Since the last letter must be l, the last letter of the first half must be u and so k must be odd.

2.5. *Comparison with Dummigan's string diagrams.* Dummigan [1995] introduces certain words on the alphabet $\{X, O\}$ that he calls string diagrams. He works entirely in the context where $d = p^f + 1$ (so all orbits are complementary), and his diagrams are invariants of orbits closely related to our words $w(o)$. Indeed, given an orbit o with base point i and word $w(o)$, the associated string diagram is $s = s_1 \cdots s_f$ where

$$s_j = \begin{cases} O & \text{if } w_j = w_{j+1}, \\ X & \text{if } w_j \neq w_{j+1}. \end{cases}$$

He also defines circle diagrams by taking into account the rotations induced by a change of base point. It is easy to see that the map from words to string diagrams is 2-to-1 and that we could phrase our arguments in terms of Dummigan's string and circle diagrams. However, for most of our purposes, words as we have defined them are more convenient.

2.6. *More invariants.* We continue to assume that $d > 2$. Let o be a balanced orbit with associated word w written in exponential form as $w = u^{e_1} \cdots l^{e_{2k}}$. The exponents $e_1, \ldots, e_{2k}$ give one invariant of the orbit o.

A second invariant of the orbit o is its *height*, defined as

$$\mathrm{ht}(o) = \max\{e_1, e_1 - e_2 + e_3, \ldots, e_1 - e_2 + e_3 - \cdots + e_{2k-1}\}.$$

We may also describe the height as the maximum value of the function $i \mapsto a_i$ defined above. Note that in the complementary case, we have $\mathrm{ht}(o) = e_1 - e_2 + \cdots + e_k$.

We will define a third invariant in terms of invariant factors of certain bidiagonal matrices. To that end, consider the integer, $k \times k$, bidiagonal matrix

$$B = B(e_1, \ldots, e_{2k-1}) := \begin{pmatrix} p^{e_1} & -p^{e_2} & 0 & \cdots & \cdots \\ 0 & p^{e_3} & -p^{e_4} & \cdots & \cdots \\ 0 & 0 & p^{e_5} & \cdots & \cdots \\ \vdots & \vdots & \vdots & \ddots & \\ \vdots & \vdots & \vdots & & p^{e_{2k-1}} \end{pmatrix}$$

and define $d_1 \leq d_2 \leq \cdots \leq d_k$ as the exponents of the invariant factors of B so that B can be transformed into

$$A = \begin{pmatrix} p^{d_1} & 0 & 0 & \cdots & \cdots \\ 0 & p^{d_2} & 0 & \cdots & \cdots \\ 0 & 0 & p^{d_3} & \cdots & \cdots \\ \vdots & \vdots & \vdots & \ddots & \\ \vdots & \vdots & \vdots & & p^{d_k} \end{pmatrix}$$

by a series of integer row and column operations. We will discuss how to compute these invariants in the next subsection.

2.7. *Computing invariant factors.* We continue with the assumptions of the preceding subsection (so o is a balanced orbit), and we give two algorithms for computing the invariants $d_1, \ldots, d_k$ attached to o. This subsection is not needed for the statements of the main results in Section 3, so it may be skipped on a first reading.

Roughly speaking, the first algorithm picks out d_1 and continues inductively while the second picks out d_k and continues inductively. The second is more complicated than the first, but it gives valuable information in the complementary case; see Lemma 2.7.3 and Remark 2.7.4 below. Both algorithms are based on the well-known fact that the i-th invariant factor of a matrix B is

$$\gcd(i \times i \text{ minors of } B) / \gcd((i-1) \times (i-1) \text{ minors of } B).$$

To describe the results, we introduce the following notation: for $1 \leq i \leq j \leq 2k-1$, let $e_{ij} = e_i - e_{i+1} + e_{i+2} - \cdots \pm e_j$. Also, we say that two matrices are *equivalent* (denoted by $\sim$) if one can be transformed to the other by a series of integer row and column operations.

Lemma 2.7.1. *Assume that $k > 1$, let $e_1, \ldots, e_{2k-1}$ be positive integers, and let $d_1, \ldots, d_k$ be the integers attached as above to $B(e_1, \ldots, e_{2k-1})$. We have $d_1 = \min\{e_1, \ldots, e_{2k-1}\}$. Choose i such that $d_1 = e_i$, and define*

$$B' = \begin{cases} B(e_3, \ldots, e_{2k-1}) & \text{if } i = 1, \\ B(e_1, \ldots, e_{i-2}, e_{i-1,i+1}, e_{i+2}, \ldots, e_{2k-1}) & \text{if } 1 < i < 2k-1, \\ B(e_1, \ldots, e_{2k-3}) & \text{if } i = 2k-1. \end{cases}$$

Then $B(e_1, \ldots, e_{2k-1})$ is equivalent to $(p^{d_1}) \oplus B'$.

Note that we make no assumptions on the e_i other than positivity. The result can thus be applied inductively to B' and thus gives an algorithm for computing all of the d_j. For example, if $(e_1, \ldots, e_{2k}) = (4, 1, 3, 5, 4, 3, 5, 4, 2, 1, 2, 6)$, then the algorithm proceeds as follows:

$$B(4, 1, 3, 5, 4, 3, 5, 4, 2, 1, 2) \underset{(i=2)}{\sim} (p^1) \oplus B(6, 5, 4, 3, 5, 4, 2, 1, 2),$$

$$B(6, 5, 4, 3, 5, 4, 2, 1, 2) \underset{(i=7)}{\sim} (p^1) \oplus B(6, 5, 4, 3, 5, 4, 3),$$

$$B(6, 5, 4, 3, 5, 4, 3) \underset{(i=4)}{\sim} (p^3) \oplus B(6, 5, 6, 4, 3),$$

$$B(6, 5, 6, 4, 3) \underset{(i=5)}{\sim} (p^3) \oplus B(6, 5, 6),$$

$$B(6, 5, 6) \underset{(i=2)}{\sim} (p^5) \oplus B(7),$$

so the invariants d_j are 1, 1, 3, 3, 5, and 7.

Proof of Lemma 2.7.1. That $d_1 = \min\{e_1, \ldots, e_{2k-1}\}$ is evident from the description of d_1 as $\gcd\{p^{e_1}, \ldots, p^{e_{2k-1}}\}$.

Write B for $B(e_1, \ldots, e_{2k-1})$. If $i = 1$, then p^{e_1} divides $-p^{e_2}$, and a single column operation transforms B into $(p^{e_1}) \oplus B(e_3, \ldots, e_{2k-1})$. This is the desired result.

Similarly, if $i = 2k-1$, then $p^{e_{2k-1}}$ divides $-p^{e_{2k-2}}$, and a single row operation transforms B into $B(e_1, \ldots, e_{2k-3}) \oplus (p^{e_{2k-1}})$. This is the desired result.

Now consider the case where $1 < i < 2k-1$, and assume that i is odd. Then a row operation followed by a column operation transforms the submatrix

$$\begin{pmatrix} -p^{e_{i-1}} & 0 \\ p^{e_i} & -p^{e_{i+1}} \end{pmatrix}$$

of B into

$$\begin{pmatrix} 0 & -p^{e_{i-1,i+1}} \\ p^{e_i} & 0 \end{pmatrix}$$

and leaves the rest of B unchanged. Permuting rows and columns yields

$$(p^{e_i}) \oplus B(e_1, \ldots, e_{i-2}, e_{i-1,i+1}, e_{i+2}, \ldots, e_{2k-1}).$$

The case where $1 < i < 2k - 1$ and i is even is similar. We first transform the submatrix

$$\begin{pmatrix} p^{e_{i-1}} & -p^{e_i} \\ 0 & p^{e_{i+1}} \end{pmatrix}$$

of B into

$$\begin{pmatrix} 0 & -p^{e_i} \\ p^{e_{i-1,i+1}} & 0 \end{pmatrix}$$

and then permute rows and columns and multiply row 1 (containing $-p^{e_i}$) by -1 to arrive at

$$(p^{e_i}) \oplus B(e_1, \ldots, e_{i-2}, e_{i-1,i+1}, e_{i+2}, \ldots, e_{2k-1}). \qquad \square$$

Lemma 2.7.2. *Assume that $k > 1$, let $e_1, \ldots, e_{2k-1}$ be positive integers, and let $d_1, \ldots, d_k$ be the integers attached as above to $B(e_1, \ldots, e_{2k-1})$. We have*

$$d_k = \max\{e_{ij} \mid 1 \le i \le j \le 2k - 1, \; i \text{ and } j \text{ odd}\}.$$

Choose $i \le j$ odd such that $d_k = e_{ij}$. Define a subset $T \subset \{1, 2, 3\}$ and matrices B_α for $\alpha \in S$ as follows:

- *$1 \in T$ if and only if $i > 1$. If $i > 1$, let $B_1 = B(e_1, \ldots, e_{i-2})$.*
- *$2 \in T$ if and only if $i < j$. If $i < j$, let $B_2 = B(e_{i+1}, \ldots, e_{j-1})^t$ ($t = $ transpose).*
- *$3 \in T$ if and only if $j < 2k - 1$. If $j < 2k - 1$, let $B_3 = B(e_{j+2}, \ldots, e_{2k-1})$.*

Let $B' = \bigoplus_{\alpha \in T} B_\alpha$. Then $B(e_1, \ldots, e_{2k-1})$ is equivalent to $(p^{d_k}) \oplus B'$.

Since we always choose a good base point for an orbit, if $B(e_1, \ldots, e_{2k-1})$ is the matrix attached to a balanced orbit o, then the invariant d_k is equal to the height of o. We have not emphasized this in the statement of the lemma because the top invariant factor of a general bidiagonal matrix (e.g., the matrices B_α with $\alpha \in T$) need not be of the form e_{1j}.

This lemma applies equally well to lower-triangular bidiagonal matrices, so it gives another inductive algorithm for computing all of the d_j. For example, if

$$(e_1, \ldots, e_{2k-1}) = (4, 1, 3, 5, 4, 3, 5, 4, 2, 1, 2),$$

then (ignoring transposes) the algorithm proceeds as follows:

$$B(4, 1, 3, 5, 4, 3, 5, 4, 2, 1, 2) \underset{(i,j)=(1,7)}{\sim} (p^7) \oplus B(1, 3, 5, 4, 3) \oplus B(2, 1, 2),$$

$$B(1, 3, 5, 4, 3) \underset{(i,j)=(3,3)}{\sim} (p^5) \oplus B(1) \oplus B(3),$$

$$B(2, 1, 2) \underset{(i,j)=(1,3)}{\sim} (p^3) \oplus B(1),$$

so the invariants d_j are 1, 1, 3, 3, 5, and 7.

Proof of Lemma 2.7.2. We write B for $B(e_1, \ldots, e_{2k-1})$. The value of d_k can be seen from the description of the invariant factors of B in terms of minors. Indeed, note that

$$\det B = p^{e_1 + e_3 + \cdots + e_{2k-1}}.$$

On the other hand, the nonzero $(k-1) \times (k-1)$ minors of B are of two types. Those obtained by deleting row and column i are of the form $\pm \det B / p^{e_{2i-1}}$, and those obtained by deleting row i and column j with $j < i$ are of the form

$$\pm p^{e_1 + e_3 + \cdots + e_{2j-3}} p^{e_{2j} + e_{2j+2} + \cdots + e_{2i-2}} p^{e_{2i+1} + \cdots + e_{2k-1}}.$$

It follows that d_k is the maximum of e_{ij}, where $i \leq j$ and i and j are odd. This is the first claim in the statement of the lemma.

To obtain the asserted equivalence, choose $i \leq j$ odd such that $d_k = e_{ij}$. If $i > 1$, then the definition of e_{ij} implies the inequalities

$$e_{i-2,j} \leq e_{ij} \implies e_{i-2,i-1} \leq 0,$$

$$e_{i-4,j} \leq e_{ij} \implies e_{i-4,i-1} \leq 0,$$

$$\vdots$$

$$e_{1,j} \leq e_{ij} \implies e_{1,i-1} \leq 0.$$

It follows that we may eliminate the entry $-p^{e_{i-1}}$ from B by a series of column operations. More precisely, B is equivalent to $B(e_1, \ldots, e_{i-2}) \oplus B(e_i, \ldots, e_{2k-1})$.

Similarly, if $j < 2k - 1$, we have a series of inequalities $e_{ij} \geq e_{ij+2}$, ..., $e_{ij} \geq e_{i,2k-1}$ and these imply that by a series of row operations we may eliminate $-p^{e_{j+1}}$, i.e., B is equivalent to $B(e_1, \ldots, e_j) \oplus B(e_{j+2}, \ldots, e_{2k-1})$.

If $i > 1$ and $j < 2k - 1$, then we may perform both of the procedures above, so

$$B \sim B(e_1, \ldots, e_{i-2}) \oplus B(e_i, \ldots, e_j) \oplus B(e_{j+2}, \ldots, e_{2k-1}).$$

If $i = j$, then $B(e_i) = (p^{d_k})$ and we are done.

It remains to prove that if $i < j$, then $B(e_i, \ldots, e_j)$ is equivalent to $(p^{d_k}) \oplus B(e_{i+1}, \ldots, e_{j-1})^t$. To see this, we note that the definition of e_{ij} implies that $e_{i\ell} \geq 0$

and $e_{\ell j} \leq 0$ for all even ℓ with $i < \ell < j$. Using these inequalities, we transform $B(e_i, \ldots, e_j)$ by column operations into

$$\begin{pmatrix} 0 & -p^{e_{i+1}} & 0 & \cdots & \cdots \\ 0 & p^{e_{i+2}} & -p^{e_{i+3}} & \cdots & \cdots \\ \vdots & \vdots & \vdots & \ddots & \\ p^{d_k} & 0 & 0 & \cdots & p^{e_j} \end{pmatrix},$$

then by transposing rows into

$$\begin{pmatrix} p^{d_k} & 0 & 0 & \cdots & p^{e_j} \\ 0 & -p^{e_{i+1}} & 0 & \cdots & \cdots \\ 0 & p^{e_{i+2}} & -p^{e_{i+3}} & \cdots & \cdots \\ \vdots & \vdots & \vdots & \ddots & \\ 0 & 0 & \cdots & p^{e_{j-2}} & -p^{e_{j-1}} \end{pmatrix},$$

and finally by row operations and sign changes into $(p^{d_k}) \oplus B(e_{i+1}, \ldots, e_{j-1})^t$. $\square$

Lemma 2.7.3. *If o is complementary (so that k is odd and $e_{k+i} = e_i$ for $1 \leq i \leq k$), then we have $d_k = e_{1k}$, the other d_j come in pairs (i.e., $d_1 = d_2$, $d_3 = d_4, \ldots$), and*

$$d_{k-1} = d_{k-2} = \max\{e_{ij} \mid 2 \leq i \leq j \leq k-1, \ i \text{ and } j \text{ even}\}.$$

Proof. It is easy to see that $i = 1$ and $j = k$ achieves the maximum e_{ij}, so we have $d_k = e_{1k} = \mathrm{ht}(o)$. One application of Lemma 2.7.2 shows that $B(e_1, \ldots, e_{2k-1})$ is equivalent to

$$p^{d_k} \oplus B(e_2, \ldots, e_{k-1})^t \oplus B(e_2, \ldots, e_{k-1}).$$

Thus, the invariant factors $d_1, \ldots, d_{k-1}$ come in pairs. Applying the recipe of Lemma 2.7.2 for the top invariant factor to $B(e_2, \ldots, e_{k-1})$ gives the assertion on d_{k-1} and d_{k-2}. $\square$

Remark 2.7.4. Suppose that $e_1, \ldots, e_{2k}$ are the exponents of a word coming from a good base point (so $e_{1,j} \geq 0$ for all j), and suppose that $e_{1,2j+1}$ is maximum among $e_{1,\ell}$. Then the following four matrices and their transposes all have the same invariant factors: $B(e_1, \ldots, e_{2k-1})$, $B(e_2, \ldots, e_{2k})$, $B(e_{2j+2}, \ldots, e_{2k}, e_1, \ldots, e_{2j})$, and $B(e_{2j+3}, \ldots, e_{2k}, e_1, \ldots, e_{2j+1})$. Indeed (ignoring transposes), the first step of the second algorithm above shows that each of these matrices is equivalent to

$$(p^{e_{1,2j+1}}) \oplus B(e_2, \ldots, e_{2j}) \oplus B(e_{2j+3}, \ldots, e_{2k-1}).$$

2.8. *Representations of G.* Fix an algebraic closure $\bar{\mathbb{F}}_p$ of $\mathbb{F}_p$, and view μ_d as a subgroup of $\bar{\mathbb{F}}_p^\times$. Let $W(\bar{\mathbb{F}}_p)$ be the Witt vectors with coefficients in $\bar{\mathbb{F}}_p$, and let $\chi : \mu_d \to W(\bar{\mathbb{F}}_p)$ be the Teichmüller character so that $\chi(\zeta) \equiv \zeta \pmod{p}$ for

all $\zeta \in \mu_d$. Identifying $W(\bar{\mathbb{F}}_p)$ with a subring of $\bar{\mathbb{Q}}_p$, the $\bar{\mathbb{Q}}_p$-valued character group $\hat{\mu}_d$ of μ_d can be identified with $\mathbb{Z}/d\mathbb{Z}$ by associating χ^i with i.

The group $\langle p \rangle \subset (\mathbb{Z}/d\mathbb{Z})^\times$ acts on μ_d via exponentiation. This yields an action on $\hat{\mu}_d \cong \mathbb{Z}/d\mathbb{Z}$ under which p acts by multiplication by p. It is thus natural to consider the set $\tilde{O}$ of orbits of $\langle p \rangle$ on $\mathbb{Z}/d\mathbb{Z}$. If $i \in \mathbb{Z}/d\mathbb{Z}$ and o is the orbit of $\langle p \rangle$ through i, then the values of χ^i lie in the Witt vectors $W(\mathbb{F}_{p^{|o|}})$ and the values of $\sum_{i \in o} \chi^i$ lie in $\mathbb{Z}_p = W(\mathbb{F}_p)$.

Now fix a finite extension $\mathbb{F}_q$ of $\mathbb{F}_p(\mu_d)$ in $\bar{\mathbb{F}}_p$, and let $G_1 = \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$. The action of G_1 on μ_d factors through the homomorphism $G_1 \to \langle p \rangle$ that sends Fr_p, the p-power Frobenius, to p.

Let G be the semidirect product $\mu_d \rtimes G_1$. There is a canonical identification

$$G \cong \mathrm{Gal}(\mathbb{F}_q K_d/K) = \mathrm{Gal}(\mathbb{F}_q(u)/\mathbb{F}_p(t)).$$

To avoid confusion between number rings and group rings, we write H for μ_d. Let $\mathbb{Z}_p[H]$ and $\mathbb{Z}_p[G]$ be the group rings of H and G with coefficients in $\mathbb{Z}_p$. We also write $\Gamma = \mathbb{Z}_p[H]$, which we view as a $\mathbb{Z}_p[H]$-module in the obvious way. Letting G_1 act on Γ through its action on H makes Γ into a $\mathbb{Z}_p[G]$-module.

Proposition 2.8.1. (1) *There is a canonical isomorphism of $\mathbb{Z}_p[H]$-modules*

$$\Gamma = \bigoplus_{o \in \tilde{O}} \Gamma_o,$$

where Γ_o is a free $\mathbb{Z}_p$-module of rank $|o|$ on which H acts with character $\sum_{i \in o} \chi^i$.

(2) *For every orbit o, $\Gamma_o \subset \Gamma$ is stable under $\mathbb{Z}_p[G]$ and $\Gamma_o \otimes \mathbb{Q}_p$ is an absolutely irreducible $\mathbb{Q}_p[G]$-module.*

(3) *$\Gamma_o \otimes_{\mathbb{Z}_p} \mathbb{F}_p$ is an absolutely irreducible $\mathbb{F}_p[G]$ module.*

(4) *If $o \neq o'$, then $\Gamma_o \otimes_{\mathbb{Z}_p} \bar{\mathbb{Q}}_p \not\cong \Gamma_{o'} \otimes_{\mathbb{Z}_p} \bar{\mathbb{Q}}_p$ and $\Gamma_o \otimes_{\mathbb{Z}_p} \bar{\mathbb{F}}_p \not\cong \Gamma_{o'} \otimes_{\mathbb{Z}_p} \bar{\mathbb{F}}_p$ as G-modules.*

(5) *Suppose that $\mathbb{F}_q$ is a finite extension of $\mathbb{F}_{p^{|o|}}$. Fix $i \in \mathbb{Z}/d\mathbb{Z}$, and let o be the orbit of $\langle p \rangle$ through i. Make the Witt vectors $W(\mathbb{F}_q)$ into a $\mathbb{Z}_p[G]$-module by letting $\zeta \in \mu_d = H$ act by multiplication by ζ^i and letting $\mathrm{Fr}_p \in G_1 \subset G$ act by the Witt-vector Frobenius. Then we have an isomorphism of $\mathbb{Z}_p[G]$-modules*

$$W(\mathbb{F}_q) \cong \Gamma_o \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_{p^{|o|}})].$$

Proof. For (1), since $\sum_{i \in o} \chi^i$ takes values in $\mathbb{Z}_p$, setting

$$\pi_o = (1/d) \sum_{h \in H} \left(\sum_{i \in o} \chi^{-i}(h) \right) h,$$

we have $\pi_o \in \mathbb{Z}_p[H]$. Orthogonality of characters implies that the elements π_o form a system of orthogonal idempotents: we have $1 = \sum_{o \in \tilde{O}} \pi_o$ and $\pi_o \pi_{o'} = 0$ if $o \neq o'$. We define $\Gamma_o = \pi_o \Gamma$. This gives a direct-sum decomposition $\Gamma = \bigoplus_{o \in \tilde{O}} \Gamma_o$. It follows from the definition that Γ_o is a free $\mathbb{Z}_p$-module. We may compute its rank by noting that $\Gamma \otimes_{\mathbb{Z}_p} \overline{\mathbb{Q}}_p$ decomposes under H into lines where H acts by the characters χ^i with $i \in \mathbb{Z}/d\mathbb{Z}$, and the subspace $\Gamma_o \otimes_{\mathbb{Z}_p} \overline{\mathbb{Q}}_p$ is the direct sum of the lines where H acts by χ^i with $i \in o$, so Γ_o has $\mathbb{Z}_p$-rank $|o|$.

For (2), since $g\pi_o = \pi_o g$ for all $g \in \langle p \rangle$, it follows that Γ_o is stable under G. As an H-module, $\Gamma_o \otimes_{\mathbb{Z}_p} \overline{\mathbb{Q}}_p$ decomposes into lines where H acts via χ^i with $i \in o$, and $\langle p \rangle$ permutes these lines transitively, so Γ_o is absolutely irreducible as G-module.

Part (3) follows from a similar argument, using that d is relatively prime to p, so the χ^i are distinct modulo p.

Part (4) follows immediately from a consideration of characters.

For (5), first consider the case where $\mathbb{F}_q = \mathbb{F}_{p^{|o|}}$. Now $W(\mathbb{F}_{p^{|o|}})$ is a cyclic $\mathbb{Z}_p[G]$-module generated by 1 and with annihilator the left ideal generated by $[p^{|o|}] - 1$ and $\prod_{i \in o}([h] - \chi^i(h))$, where h is a generator of H. Using this, it is easy to check that $1 \mapsto \pi_o$ defines an isomorphism of $\mathbb{Z}_p[G]$-modules $W(\mathbb{F}_{p^{|o|}}) \to \Gamma_o$. The general case follows from this and the normal basis theorem for $\mathbb{F}_q$ over $\mathbb{F}_{p^{|o|}}$ (which yields an integral normal basis statement for the corresponding extension of Witt rings). $\square$

Remark 2.8.2. If M is a $\mathbb{Z}_p[G]$-module, we write M^o for $\pi_o M$. By definition, H acts on M^o by characters χ^i with $i \in o$. Note, however, that it is *not* clear *a priori* what the action of G_1 is on M^o. Indeed, the action of G_1 does not enter into the definition of π_o, and so we will have to determine the full action of G on M by other means. The reason for not using G_1 in the definition of π_o is that p may divide the order of G_1, and we prefer to avoid the resulting complications in the representation theory of G.

Remark 2.8.3. We showed in [Ulmer 2014b, Corollary 4.3] that the group V_d appearing in Theorem 1.1 is a cyclic module over $\mathbb{Z}[G]$ with relations $2\sum_i P_i = 2\sum_i(-1)^i P_i = 0$. It follows easily that $V_d \otimes \mathbb{Z}_p$ is isomorphic to

$$\bigoplus_{o \in O_{d,p}} \Gamma_o.$$

Since $E(K_d)$ is a G-invariant superlattice of V_d, the absolute irreducibility of Γ_o noted above implies that we also have an isomorphism of $\mathbb{Z}_p[G]$-modules

$$E(K_d) \otimes \mathbb{Z}_p \cong \bigoplus_{o \in O_{d,p}} \Gamma_o.$$

3. Refined results

In this section, we state results on Mordell–Weil and Tate–Shafarevich groups decomposed for the action of Galois. These imply the results stated in Theorem 1.1, and they also give information in many other contexts. The proofs will be given in Section 8.

Throughout, we fix a positive integer d prime to p and a finite extension $\mathbb{F}_q$ of $\mathbb{F}_p(\mu_d)$, and we set $G = \mathrm{Gal}(\mathbb{F}_q(u)/\mathbb{F}_p(t))$. For the results on discriminants and indices, the choice of $\mathbb{F}_q$ is not material, so we work over $K_d = \mathbb{F}_p(\mu_d, u)$. On the other hand, our results on the Tate–Shafarevich group depend significantly on the choice of $\mathbb{F}_q$.

3.1. *Discriminants.* We have seen in [Conceição et al. 2014] that the "new" part of $E(K_d)$ (i.e., the part not coming from $E(K_e)$ with e a proper divisor of d) is trivial if p is not balanced modulo d and has rank $\phi(d)$ if p is balanced modulo d. In this subsection, we refine this result by breaking up $E(K_d)$ for the action of G and by computing the p-part of the discriminant of the height pairing.

Recall that $E(K_d)$ carries a canonical real-valued height pairing that is nondegenerate modulo torsion. (See, e.g., [Ulmer 2014a, §4.3].) There is a rational-valued pairing $\langle \cdot, \cdot \rangle$ such that the canonical height pairing is $\langle \cdot, \cdot \rangle \log(|\mathbb{F}_p(\mu_d)|)$. For convenience, we work with the rational-valued pairing. The group $E(K_d) \otimes \mathbb{Z}_p$ inherits a $\mathbb{Q}_p$-valued pairing, and the direct-sum decomposition

$$E(K_d) \otimes \mathbb{Z}_p \cong \bigoplus_{o \in O} (E(K_d) \otimes \mathbb{Z}_p)^o$$

is an orthogonal decomposition for this pairing. We write $\mathrm{Disc}(E(K_d) \otimes \mathbb{Z}_p)^o$ for the discriminant restricted to one of the factors. This is well-defined up to the square of a unit in $\mathbb{Z}_p$, but we will compute it only up to units.

Recall the sequence $a_0, \ldots, a_{|o|}$ associated to o in Section 2.3 and the representation Γ_o defined in Section 2.8.

Theorem 3.1.1. (1) *We have an isomorphism of $\mathbb{Z}_p[G]$-modules*

$$(E(K_d) \otimes \mathbb{Z}_p)^o \cong \begin{cases} \Gamma_o & \textit{if } \gcd(o, d) < d/2 \textit{ and } p \textit{ is balanced modulo } d/\gcd(o, d), \\ 0 & \textit{otherwise.} \end{cases}$$

(2) *If $\gcd(o, d) < d/2$ and p is balanced modulo $d/\gcd(o, d)$, then up to a unit in $\mathbb{Z}_p$ we have*

$$\mathrm{Disc}(E(K_d) \otimes \mathbb{Z}_p)^o = p^a$$

where $a = 2\sum_{j=1}^{|o|} a_j$.

3.2. *Indices.* Now we suppose that

(a) $d = p^f + 1$ and $o \in O_{d,p}$ is any orbit, or

(b) $d = 2(p^f - 1)$ and $o \in O_{d,p}$ is such that $\gcd(o, d)$ is odd.

In these cases, the orbit o is complementary, and the word w associated to each o may be written in exponential form

$$w = u^{e_1} l^{e_2} \cdots u^{e_k} l^{e_1} u^{e_2} \cdots l^{e_k},$$

where each $e_j > 0$ and k is odd. In this case, $\mathrm{ht}(o) = e_1 - e_2 + \cdots + e_k$.

Let $V_d \subset E(K_d)$ be the subgroup generated by the explicit points as in [Ulmer 2014b, Remark 8.3] ($d = p^f + 1$) or [Conceição et al. 2014, Theorem 6.1] ($d = 2(p^f - 1)$).

Theorem 3.2.1. *Under the hypotheses* (a) *or* (b) *above, we have an isomorphism of $\mathbb{Z}_p[G]$-modules*

$$(E(K_d)/V_d)^o \cong \Gamma_o/p^e,$$

where $e = (f - \mathrm{ht}(o))/2$. When $\gcd(o, d) = 1$, $e = \sum_{j=1}^{(k-1)/2} e_{2j}$.

Under the assumptions of the theorem, it follows that $(E(K_d)/V_d)^o = 0$ if and only if the word corresponding to o has height f, and that occurs only for words equivalent up to rotation to $u^f l^f$.

3.3. *Tate–Shafarevich groups.* Recall the integers $d_1, \ldots, d_k$ attached to an orbit o in Section 2.6.

Theorem 3.3.1. *For any $d > 2$ prime to p and any $o \in O_{d,p}$, if $\gcd(o, d) < d/2$ and p is balanced modulo $d/\gcd(o, d)$, then:*

(1) *There is an isomorphism of $\mathbb{Z}_p[G]$-modules*

$$\mathrm{III}(E/\mathbb{F}_q(u))^o \cong \frac{\prod_{j=1}^{k} W_{d_j}(\mathbb{F}_q)}{W_{d_k}(\mathbb{F}_{p^{|o|}})}.$$

(2) *In particular, if $\mathbb{F}_q = \mathbb{F}_p(\mu_d)$ so that $\mathbb{F}_q(u) = K_d$ and $\gcd(o, d) = 1$, then*

$$\mathrm{III}(E/K_d)^o \cong \prod_{j=1}^{k-1} W_{d_j}(\mathbb{F}_{p^{|o|}}) \cong \prod_{j=1}^{k-1} \Gamma_o/p^{d_j}.$$

Under the assumptions of the theorem, it follows that $\mathrm{III}(E/\mathbb{F}_q(u))^o$ is trivial only when $\mathbb{F}_q = \mathbb{F}_p(\mu_d)$ and $k = 1$, and $k = 1$ occurs if and only if the word associated to o is $u^f l^f$.

4. Domination by a product of curves

In this section, we relate the arithmetic of $E/\mathbb{F}_q(u)$ to that of a suitable product of curves over $\mathbb{F}_q$.

4.1. *Basic data.* Fix an integer d relatively prime to p, let $\mathbb{F}_q$ be a finite extension of $\mathbb{F}_p(\mu_d)$, and let $G_1 = \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$.

Let $\mathscr{C}$ be the smooth, projective curve over $\mathbb{F}_p$ with affine model $z^d = x^2 - 1$. We write $P_\pm$ for the rational points $x = \pm 1$ and $z = 0$ on $\mathscr{C}$. Extending scalars, the group $\mu_2 \times \mu_d$ acts on $\mathscr{C} \times_{\mathbb{F}_p} \mathbb{F}_q$ by multiplying the x and z coordinates by roots of unity. There is also an action of G_1 on $\mathscr{C} \times_{\mathbb{F}_p} \mathbb{F}_q$ via the factor $\mathbb{F}_q$. Altogether we get an action of $(\mu_2 \times \mu_d) \rtimes G_1$ on $\mathscr{C} \times_{\mathbb{F}_p} \mathbb{F}_q$. To simplify notation, for the rest of this section, we let $\mathscr{C}$ denote the curve over $\mathbb{F}_q$.

Let $\mathscr{D}$ be the curve associated to $w^d = y^2 - 1$ so that $\mathscr{D}$ is isomorphic to $\mathscr{C}$. It has rational points $Q_\pm$ and an action of $(\mu_2 \times \mu_d) \rtimes G_1$ defined analogously to those of $\mathscr{C}$.

Let $\mathscr{S} = \mathscr{C} \times_{\mathbb{F}_q} \mathscr{D}$ be the product surface. We let the group $\Delta := \mu_2 \times \mu_d$ act on $\mathscr{S}$ "antidiagonally", i.e., with

$$(\zeta_2, \zeta_d)(x, y, z, w) = (\zeta_2 x, \zeta_2^{-1} y, \zeta_d z, \zeta_d^{-1} w).$$

Write $\mathrm{NS}(\mathscr{S})$ for the Néron–Severi group of $\mathscr{S}$ and $\mathrm{NS}'(\mathscr{S})$ for the orthogonal complement in $\mathrm{NS}(\mathscr{S})$ of the subgroup generated by the classes of the divisors $\mathscr{C} \times \{Q_+\}$ and $\{P_+\} \times \mathscr{D}$. (We could also describe $\mathrm{NS}'(\mathscr{S})$ as $\mathrm{DivCorr}((\mathscr{C}, P_+), (\mathscr{D}, Q_+))$, the group of divisorial correspondences between the two pointed curves; see [Ulmer 2011, §0.5.1, §2.8.4].) The intersection form on $\mathrm{NS}(\mathscr{S})$ restricts to a nondegenerate form on $\mathrm{NS}'(\mathscr{S})$. The action of Δ on $\mathscr{S}$ induces an action on $\mathrm{NS}'(\mathscr{S})$.

Let $G = \mu_d \rtimes G_1$. We let G act on $\mathscr{S}$ via its action on $\mathscr{C}$; this yields an action of G on $\mathrm{NS}'(\mathscr{S})$. We let G act on $E(\mathbb{F}_q(u))$ via the identification $G \cong \mathrm{Gal}(\mathbb{F}_q(u)/\mathbb{F}_p(t))$.

The main result of this section relates the arithmetic of the Legendre curve $E/\mathbb{F}_q(u)$ to that of $\mathscr{S}$.

Theorem 4.2. *With notation as above*:

(1) *There is a canonical isomorphism*

$$E(\mathbb{F}_q(u)) \otimes \mathbb{Z}[1/2d] \xrightarrow{\sim} (\mathrm{NS}'(\mathscr{S}) \otimes \mathbb{Z}[1/2d])^\Delta,$$

where the superscript Δ denotes the subgroup of invariants. This isomorphism is compatible with the G-actions, and under it, the height pairing on $E(K)$ corresponds to the intersection pairing on $\mathrm{NS}'(\mathscr{S})$.

(2) *There is a canonical isomorphism*

$$\text{Ш}(E/\mathbb{F}_q(u))[p^\infty] \xrightarrow{\sim} \mathrm{Br}(\mathscr{S})[p^\infty]^\Delta.$$

Here Br(𝒮) *is the* (*cohomological*) *Brauer group of 𝒮 and* [p^∞] *means the p-torsion subgroup. This isomorphism is compatible with the G-actions.*

The rest of this section is devoted to a proof of the theorem and the discussion of a mild generalization. Note that the theorem for odd values of d follows from the case of even d (by taking invariants by a suitable subgroup of G), so *for the rest of this section, we assume that d is even.*

4.3. *The basic geometric result.* The main step in the proof of Theorem 4.2 is to relate the Néron model of $E/\mathbb{F}_q(u)$ to a suitable quotient of 𝒮. To that end, recall the Weierstrass fibration $\mathcal{W} \to \mathbb{P}^1_u$ (whose fibers are the plane cubic reductions of E at places of $\mathbb{F}_q(u)$) and the Néron model $\mathcal{E} \to \mathbb{P}^1_u$, which is obtained from $\mathcal{W}$ by blowing up singular points in the fibers over $u = 0$, $u \in \mu_d$, and $u = \infty$. All this is discussed in detail in [Ulmer 2014b, §7].

Note that since we are assuming that d is even, $\mathcal{E}$ has two points at infinity that we denote $P'_\pm$, where the sign corresponds to the limiting value of $x/z^{d/2}$. Similarly, $\mathcal{D}$ has two points at infinity, denoted $Q'_\pm$.

Let $\widetilde{\mathcal{S}} = \widetilde{\mathcal{C} \times \mathcal{D}}$ be the blow-up of 𝒮 at the eight points $(P_\pm, Q'_\pm)$ and $(P'_\pm, Q_\pm)$. These points have stabilizers of order $d/2$ under the action of Δ, and they fall into two orbits, namely $\{(P_\pm, Q'_\pm)\}$ and $\{(P'_\pm, Q_\pm)\}$, under the Δ action. The action of the stabilizer on the projectivized tangent space at each of these points is trivial, so the action of Δ lifts canonically to $\widetilde{\mathcal{S}}$ and the exceptional fibers are fixed pointwise by the stabilizer of the corresponding point. The action of Δ on $\widetilde{\mathcal{S}}$ has other isolated fixed points, but we do not need to make them explicit.

We let $\widetilde{\mathcal{S}}/\Delta$ denote the quotient of $\widetilde{\mathcal{S}}$ by the action of Δ. This is a normal, projective surface with isolated cyclic quotient singularities. (They are in fact rational double points, but we will not need this fact.)

Now we define a rational map $\mathcal{S} \dashrightarrow \mathcal{W}$ by requiring that

$$(x, y, z, w) \mapsto ([X, Y, Z], u) = ([z^d, xyz^d, 1], zw),$$

where $([X, Y, Z], u)$ are the coordinates on a dense open subset of $\mathcal{W}$ as in [Ulmer 2014b, §7]. This induces a rational map $\phi : \widetilde{\mathcal{S}} \dashrightarrow \mathcal{W}$ that is obviously equivariant for the Δ action, where Δ acts trivially on $\mathcal{W}$. Thus, ϕ descends to a map on the quotient that we denote $\psi : \widetilde{\mathcal{S}}/\Delta \dashrightarrow \mathcal{W}$.

The following diagram shows the surfaces under consideration and various morphisms between them:

$$
\begin{array}{ccc}
\mathcal{C} \times \mathcal{D} = \mathcal{S} & \xleftarrow{\ \rho\ } & \widetilde{\mathcal{S}} \\
\pi \downarrow & & \searrow \phi \\
\widetilde{\mathcal{S}}/\Delta & \dashrightarrow[\psi] & \mathcal{W} \xleftarrow{\ \sigma\ } \mathcal{E}
\end{array}
$$

The quotient map π is finite, and we will see just below that the horizontal maps are birational morphisms.

Proposition 4.3.1. (1) *The rational map ϕ is in fact a morphism. Therefore, ψ is also a morphism and a birational isomorphism.*

(2) *ϕ contracts the strict transforms of $P_\pm \times \mathcal{D}$ and $\mathcal{C} \times Q'_\pm$ and is finite elsewhere.*

(3) *For generic $P \in \mathcal{C}$, ϕ sends $P \times \mathcal{D}$ to a bisection of $\mathcal{W} \to \mathbb{P}^1$, where the two points in each fiber are inverse to one another. Similarly, for generic $Q \in \mathcal{D}$, ϕ sends $\mathcal{C} \times Q$ to a bisection of $\mathcal{W} \to \mathbb{P}^1$, where the two points in each fiber are inverse to one another.*

(4) *The exceptional divisors over $P_\pm \times Q'_\pm$ map via ϕ to the torsion section $[0, 0, 1]$ of $\mathcal{W}$, and the exceptional divisors over $P'_\pm \times Q_\pm$ map via ϕ to the zero section $[0, 1, 0]$ of $\mathcal{W}$.*

In part (3), "P generic" means P with trivial stabilizer or, more explicitly, $P \neq P_\pm$, $P'_\pm$ and $x(P) \neq 0$. "Q generic" is similarly defined.

Proof. It is easy to see that ϕ has generic degree $2d$ and it factors through quotient $\widetilde{\mathcal{S}} \to \widetilde{\mathcal{S}}/\Delta$, which is finite of degree $2d$. This proves that ψ is birational.

That ϕ is everywhere defined and has the stated geometric properties is a straightforward but tedious exercise in coordinates that we omit. Since ϕ is a morphism, it follows that ψ is also a morphism. $\qquad\square$

4.4. *Proof of Theorem 4.2(1).* We prove part (1) of the theorem by using the geometry of the displayed diagram with the key input being Proposition 4.3.1. For typographical convenience, if A is a finitely generated abelian group, we write $A[1/2d]$ for $A \otimes \mathbb{Z}[1/2d]$.

By the Shioda–Tate isomorphism (e.g., [Ulmer 2014a, Chapter 4]), we have a direct-sum decomposition

$$\mathrm{NS}(\mathcal{E})[1/2d] \cong E(\mathbb{F}_q(u))[1/2d] \oplus T[1/2d],$$

where T is the subgroup of $\mathrm{NS}(\mathcal{E})$ generated by the zero section and the irreducible components of the fibers. Since $\mathcal{W}$ is obtained from $\mathcal{E}$ by contracting all components of fibers not meeting the zero section, we have

$$\mathrm{NS}(\mathcal{W})[1/2d] \cong E(\mathbb{F}_q(u))[1/2d] \oplus \langle O, F \rangle[1/2d],$$

where O and F are the classes of the zero section and a fiber of $\mathcal{W} \to \mathbb{P}^1$, respectively. These decompositions are orthogonal for the intersection pairings. The fibration $\mathcal{W} \to \mathbb{P}^1_u$ is the base change of a fibration $\mathcal{W} \to \mathbb{P}^1_t$, so G acts on $\mathcal{W}$ and $\mathrm{NS}(\mathcal{W})$. This action is trivial on $\langle O, F \rangle$, and the last displayed isomorphism is compatible with the G actions.

Since $\widetilde{\mathcal{F}}$ is obtained from $\mathcal{F}$ by blowing up eight points, we have an orthogonal decomposition

$$\mathrm{NS}(\widetilde{\mathcal{F}}) \cong \mathbb{Z}^8 \oplus \mathrm{NS}(\mathcal{F}) \cong \mathbb{Z}^{10} \oplus \mathrm{NS}'(\mathcal{F}).$$

The Néron–Severi group of the quotient $\widetilde{\mathcal{F}}/\Delta$ is obtained by taking invariants, at least after inverting $2d = |\Delta|$. Noting that Δ permutes the exceptional divisors of $\widetilde{\mathcal{F}} \to \mathcal{F}$ in two orbits and that it fixes the classes of $P \times \mathcal{D}$ and $\mathcal{C} \times Q$, we have

$$\mathrm{NS}(\widetilde{\mathcal{F}}/\Delta)[1/2d] \cong (\mathrm{NS}(\widetilde{\mathcal{F}})[1/2d])^\Delta \cong \mathbb{Z}[1/2d]^4 \oplus (\mathrm{NS}'(\mathcal{F})[1/2d])^\Delta.$$

The action of G on $\mathcal{C}$ induces an action on $\widetilde{\mathcal{F}}$ that descends to $\widetilde{\mathcal{F}}/\Delta$.

Now we consider the morphism $\psi : \widetilde{\mathcal{F}}/\Delta \to \mathcal{W}$, and use the information provided by Proposition 4.3.1. It is clear from the coordinate expression for $\mathcal{F} \dashrightarrow \mathcal{W}$ that ψ is equivariant for the G actions. Part (2) tells us that the kernel of $\mathrm{NS}(\widetilde{\mathcal{F}}/\Delta) \to \mathrm{NS}(\mathcal{W})$ has rank 2. Parts (3) and (4) allow us to determine it explicitly.

To that end, let f_1 and f_2 be the classes in $\mathrm{NS}(\widetilde{\mathcal{F}})$ of the curves $P \times \mathcal{D}$ and $\mathcal{C} \times Q$, respectively. Also, let e_1 and e_2 denote the classes in $\mathrm{NS}(\widetilde{\mathcal{F}})$ of the exceptional divisors over $P_+ \times Q'_+$ and $P'_+ \times Q_+$, respectively. Set $F_i = \pi_* f_i$ and $E_i = \pi_* e_i$ for $i = 1, 2$. Then E_1, E_2, F_1, and F_2 form a basis for the "trivial part" $\mathbb{Z}[1/2d]^4$ of $\mathrm{NS}(\widetilde{\mathcal{F}}/\Delta)[1/2d]$.

By part (3), $\psi_* F_1 = \psi_* F_2 = \phi_* f_1 = \phi_* f_2 =$ the class of a bisection of $\mathcal{W} \to \mathbb{P}^1$ with inverse points in each fiber. This class is easily seen to be $2O + dF$. Similarly, part (4) tells us that $\psi_* E_1 = \phi_* e_1 = O + (d/2)F$ (here we use that we have inverted 2), and $\psi_* E_2 = \phi_* e_2 = O$. The kernel of

$$\mathrm{NS}(\widetilde{\mathcal{F}}/\Delta)[1/2d] \to \mathrm{NS}(\mathcal{W})[1/2d]$$

is thus spanned by $F_1 - F_2$ and $F_1 - 2E_1$. Moreover, we have that ψ_* induces an isomorphism

$$(\mathrm{NS}'(\mathcal{F})[1/2d])^\Delta \cong \frac{\mathrm{NS}(\widetilde{\mathcal{F}}/\Delta)[1/2d]}{\langle F_1, F_2, E_1, E_2 \rangle} \cong \frac{\mathrm{NS}(\mathcal{W})[1/2d]}{\langle O, F \rangle}.$$

It follows that

$$(\mathrm{NS}'(\mathcal{F})[1/2d])^\Delta \cong E(\mathbb{F}_q(u))[1/2d]$$

and that this isomorphism is compatible with the height and intersection pairings and the G actions.

This completes the proof of part (1) of the theorem.

4.5. *Proof of Theorem 4.2(2).* Two fundamental results of Grothendieck [1968b] (see also [Ulmer 2014a, §5.3]) say that the Tate–Shafarevich group of $E/\mathbb{F}_q(u)$ and the Brauer group of $\mathcal{E}$ are canonically isomorphic and that the Brauer group of a surface is a birational invariant. Applying this to the diagram just before

Proposition 4.3.1 shows that $\text{III}(E/\mathbb{F}_q(u)) \cong \text{Br}(\widetilde{\mathcal{G}}/\Delta)$. Since the order of Δ is prime to p, we have

$$\text{Br}(\widetilde{\mathcal{G}}/\Delta)[p^\infty] \cong \text{Br}(\widetilde{\mathcal{G}})[p^\infty]^\Delta \cong \text{Br}(\mathcal{G})[p^\infty]^\Delta.$$

This yields the isomorphism stated in part (2) of the theorem, and this isomorphism is compatible with the G actions because the maps in the diagram above are G-equivariant.

4.6. *A higher-genus generalization.* The results in this section generalize readily to a higher-genus example. Specifically, fix an integer $r > 1$ prime to p, and let X be the smooth, proper curve over $\mathbb{F}_p(t)$ defined by

$$y^r = x^{r-1}(x+1)(x+t).$$

The genus of X is $r - 1$. We consider X and its Jacobian $J = J_X$ over extensions $\mathbb{F}_q(u)$ where $u^d = t$, d is prime to p, and $\mathbb{F}_q$ is a finite extension of $\mathbb{F}_p(\mu_d, \mu_r)$. When $d = p^f + 1$ and r divides d, there are explicit divisors on X yielding a subgroup of $J(\mathbb{F}_q(u))$ of rank $(r-1)(d-2)$ and finite index. This situation is studied in detail in [Berger et al. $\geq$ 2015].

Let $\mathcal{X} \to \mathbb{P}^1_u$ be the minimal regular model of X over the projective line whose function field is $\mathbb{F}_q(u)$. Let $\mathcal{C} = \mathcal{D}$ be the smooth, proper curve over $\mathbb{F}_q$ with equation

$$z^d = x^r - 1.$$

Then $\mathcal{C}$ and $\mathcal{D}$ carry actions of $\mu_r \times \mu_d$, and we let $\Delta = \mu_r \times \mu_d$ act on $\mathcal{S} = \mathcal{C} \times_{\mathbb{F}_q} \mathcal{D}$ "antidiagonally". Arguments parallel to those in the proof of Proposition 4.3.1 show that $\mathcal{X}$ is birationally isomorphic to $\mathcal{S}/\Delta$. Using this, the arguments proving Theorem 4.2 generalize readily to give isomorphisms

$$J(\mathbb{F}_q(u))[1/rd] \cong \text{NS}'(\mathcal{S})[1/rd]^\Delta$$

and

$$\text{III}(J/\mathbb{F}_q(u))[p^\infty] \cong \text{Br}(\mathcal{S})[p^\infty]^\Delta.$$

5. Arithmetic of a product of curves

In this section, k is a finite field of characteristic p, and $\mathcal{C}$ and $\mathcal{D}$ are smooth, projective curves over k. Our goal is to give a crystalline description of $\text{NS}'(\mathcal{C} \times \mathcal{D})$ and $\text{Br}(\mathcal{C} \times \mathcal{D})$. The former is due to Tate, and the latter was done under somewhat restrictive hypotheses by Dummigan [1999, p. 114] (by a method he says was inspired by a letter of the author). We use a variant of the method to give the result in general.

5.1. *Flat and crystalline cohomology.* For the rest of this section, we write W for the Witt-vectors $W(k)$ and σ for the Witt-vector Frobenius (lifting the p-power Frobenius of k).

Given a smooth projective variety $\mathcal{X}$ over k, we consider the crystalline cohomology groups of $\mathcal{X}$ and use the simplified notation

$$H^i(\mathcal{X}) := H^i_{\text{crys}}(\mathcal{X}/W)$$

for typographical convenience. These groups are W-modules with a σ-semilinear action of the absolute Frobenius, denoted F. When $\mathcal{X}$ is a curve, we also define a σ^{-1}-semilinear action of Verschiebung, denoted V, on $H^1(\mathcal{X})$ by requiring that $FV = VF = p$. We write A for the noncommutative ring $W\{F, V\}$ generated over W by F and V with relations $Fa = \sigma(a)F$, $aV = V\sigma(a)$, and $FV = VF = p$.

We will also consider cohomology of sheaves in the flat topology, say the *fppf* (faithfully flat, finitely presented) topology to fix ideas. Recall that $H^1(\mathcal{X}, \mathbb{G}_m) \cong \text{Pic}(\mathcal{X})$ and that we define the Brauer group of $\mathcal{X}$ by

$$\text{Br}(\mathcal{X}) := H^2(\mathcal{X}, \mathbb{G}_m).$$

If $\mathcal{X}$ is smooth and $\dim \mathcal{X} \leq 2$, it is known [Grothendieck 1968a] that this definition agrees with that via Azumaya algebras.

A well-known theorem of Weil asserts that $\mathcal{C}$ and $\mathcal{D}$ have k-rational divisors of degree 1. If P and Q are such, then the classes in $\text{NS}(\mathcal{C} \times_k \mathcal{D})$ of $P \times \mathcal{D}$ and $\mathcal{C} \times Q$ are independent of the choices of P and Q. We define $\text{NS}'(\mathcal{C} \times_k \mathcal{D})$ as the orthogonal complement in $\text{NS}(\mathcal{C} \times_k \mathcal{D})$ of these classes.

The goal of this section is to establish the following crystalline calculations of the Néron–Severi and Brauer groups of a product of curves.

Theorem 5.2. (1) *There is a functorial isomorphism*

$$\text{NS}'(\mathcal{C} \times_k \mathcal{D}) \otimes \mathbb{Z}_p \xrightarrow{\sim} (H^1(\mathcal{C}) \otimes_W H^1(\mathcal{D}))^{F=p}.$$

(2) *There is a functorial exact sequence*

$$0 \to ((H^1(\mathcal{C}) \otimes_W H^1(\mathcal{D}))^{F=p})/p^n \to (H^1(\mathcal{C})/p^n \otimes_W H^1(\mathcal{D})/p^n)^{F=V=p}$$
$$\to \text{Br}(\mathcal{C} \times_k \mathcal{D})_{p^n} \to 0.$$

Here the exponents mean the subgroups where F and V act as indicated, and "functorial" means that the displayed maps are equivariant for the action of $\text{Aut}(\mathcal{C}) \times \text{Aut}(\mathcal{D})$.

Proof. We write $\mathcal{X}$ for $\mathcal{C} \times_k \mathcal{D}$. Part (1) is essentially the crystalline Tate conjecture. More precisely, by a theorem of Tate [Waterhouse and Milne 1971], we have an isomorphism

$$\text{NS}(\mathcal{X}) \otimes \mathbb{Z}_p \cong H^2(\mathcal{X})^{F=p}.$$

Decomposing $\text{NS}(\mathcal{X})$ as $\mathbb{Z}^2 \oplus \text{NS}'(\mathcal{X})$ and $H^2(\mathcal{X})$ via the Künneth formula leads to the statement in part (1).

For part (2), we may assume that $\mathcal{C}$ and $\mathcal{D}$ have rational points. Indeed, the theorem of Weil alluded to above shows that there is an extension k'/k of degree prime to p such that $\mathcal{C}$ and $\mathcal{D}$ have k'-rational points. Using the Hochschild–Serre spectral sequences in crystalline and flat cohomologies and the fact that taking invariants under $\mathrm{Gal}(k'/k)$ is an exact functor on groups of p-power order shows that the theorem over k' implies the theorem over k. We thus assume that $\mathcal{C}$ and $\mathcal{D}$ have k-rational points.

Now consider the Kummer sequence

$$0 \to \mu_{p^n} \to \mathbb{G}_m \to \mathbb{G}_m \to 0$$

for the flat topology on $\mathcal{X}$. Taking flat cohomology yields

$$0 \to \mathrm{Pic}(\mathcal{X})/p^n \to H^2(\mathcal{X}, \mu_{p^n}) \to \mathrm{Br}(\mathcal{X})_{p^n} \to 0.$$

Let $T = \mathrm{Pic}(\mathcal{C})/p^n \oplus \mathrm{Pic}(\mathcal{D})/p^n$. The natural map $T \to \mathrm{Pic}(\mathcal{X})/p^n$ is an injection with cokernel $\mathrm{NS}'(\mathcal{X})/p^n$. Thus, we have a commutative diagram with exact rows and columns:

$$
\begin{array}{ccccccccc}
& & 0 & & 0 & & & & \\
& & \downarrow & & \downarrow & & & & \\
& & T & =\!=\!=\!=\!= & T & & & & \\
& & \downarrow & & \downarrow & & & & \\
0 & \longrightarrow & \mathrm{Pic}(\mathcal{X})/p^n & \longrightarrow & H^2(\mathcal{X}, \mu_{p^n}) & \longrightarrow & \mathrm{Br}(\mathcal{X})_{p^n} & \longrightarrow & 0 \\
& & \downarrow & & \downarrow & & \| & & \\
0 & \longrightarrow & \mathrm{NS}'(\mathcal{X})/p^n & \longrightarrow & H^2(\mathcal{X}, \mu_{p^n})/T & \longrightarrow & \mathrm{Br}(\mathcal{X})_{p^n} & \longrightarrow & 0 \\
& & \downarrow & & \downarrow & & & & \\
& & 0 & & 0 & & & &
\end{array}
$$

Using part (1), we have

$$\mathrm{NS}'(\mathcal{X})/p^n \cong ((H^1(\mathcal{C}) \otimes_{W(k)} H^1(\mathcal{D}))^{F=p})/p^n,$$

so to complete the proof, we must show that

$$H^2(\mathcal{X}, \mu_{p^n})/T \cong (H^1(\mathcal{C})/p^n \otimes H^1(\mathcal{D})/p^n)^{F=V=p}.$$

Let $\pi : \mathcal{C} \times \mathcal{D} \to \mathcal{D}$ be the projection on the second factor. We will compute $H^2(\mathcal{X}, \mu_{p^n})$ via the Leray spectral sequence for π. By a theorem of Artin proven

in [Grothendieck 1968b],

$$R^i\pi_*\mathbb{G}_m = \begin{cases} \mathbb{G}_m & \text{if } i = 0, \\ \underline{\text{Pic}}_{\mathscr{X}/\mathscr{D}} = \underline{\text{Pic}}_{\mathscr{C}/k} \times_k \mathscr{D} & \text{if } i = 1, \\ 0 & \text{if } i > 1. \end{cases}$$

It follows that

$$R^i\pi_*\mu_{p^n} = \begin{cases} \mu_{p^n} & \text{if } i = 0, \\ \underline{\text{Pic}}_{\mathscr{X}/\mathscr{D}}[p^n] = J_{\mathscr{C}}[p^n] & \text{if } i = 1, \\ \underline{\text{Pic}}_{\mathscr{X}/\mathscr{D}}/p^n = \mathbb{Z}/p^n\mathbb{Z} & \text{if } i = 2, \\ 0 & \text{if } i > 2. \end{cases}$$

(Here we abuse notation slightly — the k-group schemes on the right represent sheaves on k and so by restriction sheaves on $\mathscr{D}$.) Because $\mathscr{C}$ has a rational point, π has a section, so the Leray spectral sequence degenerates at E_2 and we have that $H^2(\mathscr{X}, \mu_{p^n})$ is an extension of

$$H^0(\mathscr{D}, \mathbb{Z}/p^n\mathbb{Z}), \quad H^1(\mathscr{D}, J_{\mathscr{C}}[p^n]), \quad \text{and} \quad H^2(\mathscr{D}, \mu_{p^n}).$$

The Kummer sequence on $\mathscr{D}$ shows that

$$H^2(\mathscr{D}, \mu_{p^n}) \cong \text{Pic}(\mathscr{D})/p^n,$$

which is an extension of $\mathbb{Z}/p^n\mathbb{Z}$ by $J_{\mathscr{D}}(k)/p^n$. Obviously, $H^0(\mathscr{D}, \mathbb{Z}/p^n\mathbb{Z}) \cong \mathbb{Z}/p^n\mathbb{Z}$.

To finish the proof, we must compute $H^1(\mathscr{D}, J_{\mathscr{C}}[p^n])$ in crystalline terms. First we make our notation a bit more precise. Let N be the sheaf on the flat site of $\text{Spec } k$ represented by the finite flat group scheme $J_{\mathscr{C}}[p^n] = \text{Pic}_{\mathscr{C}/k}[p^n]$. Let σ be the structure map $\mathscr{D} \to \text{Spec } k$ (which has a section because $\mathscr{D}$ has a rational point). Then $H^1(\mathscr{D}, J_{\mathscr{C}}[p^n])$ means $H^1(\mathscr{D}, \sigma^*N)$. Clearly, $\sigma_*\sigma^*N = N$. By [Milne 1980, Proposition III.4.16] applied to σ, if N' is the Cartier dual of N, we have

$$R^1\sigma_*\sigma^*N \cong \underline{\text{Hom}}_k(N', \underline{\text{Pic}}_{\mathscr{D}/k}) \cong \underline{\text{Hom}}_k(N, \underline{\text{Pic}}_{\mathscr{D}/k}).$$

Here $\underline{\text{Hom}}_k$ means the sheaf of homomorphisms of sheaves on the flat site of k, and we have used that $\text{Pic}_{\mathscr{C}/k}[p^n]$ is self-dual.

Now we consider the Leray spectral sequence for σ, which degenerates because σ has a section. The sequence of low-degree terms is

$$0 \to H^1(k, N) \to H^1(\mathscr{D}, \sigma^*N) \to H^0(k, \underline{\text{Hom}}_k(N, \underline{\text{Pic}}_{\mathscr{D}/k})) \to 0.$$

Using

$$0 \to N \to J_{\mathscr{C}} \xrightarrow{p^n} J_{\mathscr{C}} \to 0,$$

the equality of flat and étale cohomology for smooth group schemes, and Lang's theorem (namely that $H^1(k, J_{\mathscr{C}}) = 0$), we find that $H^1(k, N) = J_{\mathscr{C}}(k)/p^n$.

Noting that the argument above applies with the roles of $\mathscr{C}$ and $\mathscr{D}$ reversed, we see that $\mathrm{Pic}(\mathscr{C})/p^n$ and $\mathrm{Pic}(\mathscr{D})/p^n$ are direct factors of $H^2(\mathscr{X}, \mu_{p^n})$ and find that

$$H^2(\mathscr{X}, \mu_{p^n})/T \cong H^0(k, \underline{\mathrm{Hom}}_k(N, \underline{\mathrm{Pic}}_{\mathscr{D}/k})) \cong \mathrm{Hom}_k(J_{\mathscr{C}}[p^n], J_{\mathscr{D}}[p^n]).$$

We now turn to a crystalline description of the right-hand group. Letting $\mathbb{D}(\mathscr{C})$ and $\mathbb{D}(\mathscr{D})$ be the (contravariant) Dieudonné modules of the p-divisible groups of $J_{\mathscr{C}}$ and $J_{\mathscr{D}}$, respectively, the main theorem of Dieudonné theory (equivalence of categories) gives

$$\mathrm{Hom}(J_{\mathscr{C}}[p^n], J_{\mathscr{D}}[p^n]) = \mathrm{Hom}_A(\mathbb{D}(\mathscr{D})/p^n, \mathbb{D}(\mathscr{C})/p^n).$$

Here Hom_A means homomorphisms commuting with the action of $A = W\{F, V\}$, i.e., with the actions of F and V.

To finish, we use the result of Mazur and Messing [1974] that $\mathbb{D}(\mathscr{C}) \cong H^1(\mathscr{C})$ and $\mathbb{D}(\mathscr{D}) \cong H^1(\mathscr{D})$, and the duality $\mathbb{D}(\mathscr{D})^* \cong \mathbb{D}(\mathscr{D})(-1)$ (Tate twist), so that

$$\mathrm{Hom}_A(\mathbb{D}(\mathscr{D})/p^n, \mathbb{D}(\mathscr{C})/p^n) \cong (H^1(\mathscr{C})/p^n \otimes H^1(\mathscr{D})/p^n)^{F=V=p}. \qquad \square$$

Remark 5.2.1. By [Illusie 1979, Theorem 5.14], for a smooth projective surface $\mathscr{X}$ over an algebraically closed field k, we have

$$H^2(\mathscr{X}, \mathbb{Z}_p(1)) \cong H^2(\mathscr{X}/W(k))^{F=p}.$$

The proof of Theorem 5.2(2) can be adapted to show that (when $\mathscr{X}$ is a product of curves), this continues to hold at finite level: $H^2(\mathscr{X}, \mu_{p^n}) \cong H^2(\mathscr{X}/W_n(k))^{F=p}$. Conversely, a proof of this statement would yield a simple proof of part (2) of the theorem (over an algebraically closed field).

On the other hand, the proof above shows that $H^2(\mathscr{X}, \mu_{p^n})$ may be strictly bigger than $H^2(\mathscr{X}/W_n(k))^{F=p}$ over a finite ground field. The point is that when k is algebraically closed, $\mathrm{Pic}(\mathscr{C})/p^n$ is $\mathbb{Z}/p^n\mathbb{Z}$ (because $\mathrm{Pic}^0(\mathscr{C})$ is divisible), but it may be bigger when k is finite.

6. Cohomology of $\mathscr{C}$

In this section, we collect results on the crystalline cohomology of the curve $\mathscr{C}$ needed in the sequel. Some of them may already be available in the literature on Fermat curves, but for the convenience of the reader, we sketch arguments from first principles.

6.1. Lifting. From here until Section 6.5, $\mathscr{C}$ will denote the smooth projective model of the affine curve over $\mathbb{F}_p$ defined by $z^d = x^2 - 1$. (E.g., if d is even, $\mathscr{C}$ is the result of gluing $\mathrm{Spec}\,\mathbb{F}_p[x, z]/(z^d - x^2 + 1)$ and $\mathrm{Spec}\,\mathbb{F}_p[x', z']/(z'^d - x'^2 + 1)$ via $(x', z') = (x/z^{d/2}, 1/z)$. The case d odd is similar.) The projective curve has a

natural lifting to $W(\mathbb{F}_p) = \mathbb{Z}_p$ defined by the same equations. We write $\mathscr{C}/\mathbb{Z}_p$ for this lift. It is smooth and projective over $\mathbb{Z}_p$ with special fiber $\mathscr{C}$.

6.2. Actions. There is a canonical isomorphism $H^1_{\mathrm{crys}}(\mathscr{C}/\mathbb{Z}_p) \cong H^1_{\mathrm{dR}}(\mathscr{C}/\mathbb{Z}_p)$, where the left-hand side is the crystalline cohomology of $\mathscr{C}$ and the right-hand side is the algebraic de Rham cohomology of $\mathscr{C}/\mathbb{Z}_p$. We will use this isomorphism to make the crystalline cohomology explicit, endow it with a Hodge filtration, and describe the actions of Frobenius, Verschiebung, μ_d, and μ_2 on it.

Let q be a power of p congruent to 1 modulo d so that $\mathbb{F}_q$ contains $\mathbb{F}_p(\mu_d)$. Then $\mathscr{C}/W(\mathbb{F}_q) = \mathscr{C}/\mathbb{Z}_p \times_{\mathbb{Z}_p} W(\mathbb{F}_q)$ admits an action of the d-th roots of unity (acting on the coordinate z) and $\mu_2 = \pm 1$ (acting on the coordinate x).

Recall that the absolute Frobenius of $\mathscr{C}$ defines a $\mathbb{Z}_p$-linear homomorphism

$$F : H^1_{\mathrm{crys}}(\mathscr{C}/\mathbb{Z}_p) \to H^1_{\mathrm{crys}}(\mathscr{C}/\mathbb{Z}_p),$$

which induces a semilinear homomorphism

$$F : H^1_{\mathrm{crys}}(\mathscr{C}/W(\mathbb{F}_q)) \cong H^1_{\mathrm{crys}}(\mathscr{C}/\mathbb{Z}_p) \otimes_{\mathbb{Z}_p} W(\mathbb{F}_q) \to H^1_{\mathrm{crys}}(\mathscr{C}/W(\mathbb{F}_q))$$

(semilinear with respect to the Witt-vector Frobenius σ). We also have a σ^{-1}-semilinear endomorphism

$$V : H^1_{\mathrm{crys}}(\mathscr{C}/W) \to H^1_{\mathrm{crys}}(\mathscr{C}/W),$$

which is characterized by the formulas $FV = VF = p$.

Letting $\mathrm{Fr}_p \in \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ act on $\mathscr{C}/\mathbb{F}_q = \mathscr{C} \times_{\mathbb{F}_p} \mathbb{F}_q$ via the second factor, we get a semilinear endomorphism of $H^1(\mathscr{C}/W)$ that fixes $H^1(\mathscr{C}/\mathbb{Z}_p)$. Combining the actions of μ_d and Fr_p gives a $\mathbb{Z}_p$-linear action of $G = \mu_d \rtimes \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ on $H^1_{\mathrm{crys}}(\mathscr{C}/W)$.

6.3. A basis. By [Grothendieck 1961, 0_{III}, Corollaire 12.4.7], we may define elements of $H^1_{\mathrm{dR}}(\mathscr{C}/\mathbb{Z}_p)$ by giving hypercocycles for an affine cover. We do so as follows. For $i = 1, \ldots, \lfloor (d-1)/2 \rfloor$, let e_i be the class defined by the regular 1-form

$$\frac{z^{i-1}\,dz}{2x}.$$

Let U_1 be the affine curve defined by $z^d = x^2 - 1$ considered as a Zariski open subset of $\mathscr{C}/\mathbb{Z}_p$. Let U_2 be the complement of the closed set where $z = 0$ in $\mathscr{C}/\mathbb{Z}_p$.

Thus, U_1 and U_2 define an open cover of $\mathscr{C}/\mathbb{Z}_p$. For $i = 1, \ldots, \lfloor (d-1)/2 \rfloor$, the data

$$f_{12}^i = \frac{x}{z^i} \in \mathcal{O}_{\mathscr{C}/\mathbb{Z}_p}(U_1 \cap U_2),$$

$$\omega_1^i = \left(1 - \frac{2i}{d}\right)\frac{dx}{z^i} \in \Omega^1_{\mathscr{C}/\mathbb{Z}_p}(U_1),$$

$$\omega_2^i = \frac{ix\,dz}{z^{i+1}} - \frac{2i}{d}\frac{dx}{z^i} \in \Omega^1_{\mathscr{C}/\mathbb{Z}_p}(U_2)$$

satisfies $df_{12}^i = \omega_1^i - \omega_2^i$ and so defines a class in $H^1_{\mathrm{dR}}(\mathscr{C}/\mathbb{Z}_p)$ that we denote e_{d-i}.

Proposition 6.4. *The classes e_i $(0 < i < d, i \neq d/2)$ form a $\mathbb{Z}_p$-basis of $H^1_{\mathrm{dR}}(\mathscr{C}/\mathbb{Z}_p)$ and have the following properties*:

(1) *The cup product $H^1_{\mathrm{dR}}(\mathscr{C}/\mathbb{Z}_p) \times H^1_{\mathrm{dR}}(\mathscr{C}/\mathbb{Z}_p) \to \mathbb{Z}_p$ satisfies (and is determined by) the fact that for $0 < i < d$ and $0 < j < d$,*

$$e_i \cup e_j = \begin{cases} 1 & \text{if } i < d/2 \text{ and } j = d-i, \\ -1 & \text{if } i > d/2 \text{ and } j = d-i, \\ 0 & \text{otherwise.} \end{cases}$$

(2) *The classes e_i with $1 \leq i \leq \lfloor (d-1)/2 \rfloor$ form a $\mathbb{Z}_p$-basis of the submodule $H^0(\mathscr{C}/\mathbb{Z}_p, \Omega^1_{\mathscr{C}/\mathbb{Z}_p})$ of $H^1_{\mathrm{dR}}(\mathscr{C}/\mathbb{Z}_p)$, and the classes e_i with $\lfloor (d+1)/2 \rfloor \leq i \leq d-1$ project to a basis of the quotient module $H^1(\mathscr{C}/\mathbb{Z}_p, \mathcal{O}_{\mathscr{C}/\mathbb{Z}_p})$.*

(3) *The action of μ_d on $H^1_{\mathrm{crys}}(\mathscr{C}/W(\mathbb{F}_q)) \cong H^1_{\mathrm{dR}}(\mathscr{C}/\mathbb{Z}_p) \otimes_{\mathbb{Z}_p} W(\mathbb{F}_q)$ is given by*

$$[\zeta]e_i = \zeta^i e_i.$$

Also, $-1 \in \mu_2$ acts on $H^1_{\mathrm{crys}}(\mathscr{C}/W(\mathbb{F}_q))$ as multiplication by -1.

(4) *For $0 < i < d$, we have $F(e_i) = c_i e_{pi}$, where $c_i \in \mathbb{Z}_p$ satisfies*

$$\mathrm{ord}(c_i) = \begin{cases} 0 & \text{if } i > d/2, \\ 1 & \text{if } i < d/2. \end{cases}$$

(In e_{pi}, we read the subscript modulo d.)

(5) *If $o \in O_{d,p}$, $d/\gcd(d,o) > 2$, and p is balanced modulo $d/\gcd(d,o)$ (in the sense of Section 2.2), then $\prod_{i \in o} c_i = \pm p^{|o|/2}$. Equivalently, for all $i \in o$, $F^{|o|}e_i = \pm p^{|o|/2} e_i$.*

Proof. Once we know that the e_i form a basis, the formula in (1) determines the cup product. To check the formula, one computes in the standard way: the cup product $e_i \cup e_{d-j}$ is given by the sum over points in U_1 of the residue of the meromorphic differential $z^{i-j}\,dz/(2z)$, and this sum is 1 or 0 depending on whether $j = i$.

The formula in (1) implies that the classes e_i with $0 < i < d$ and $i \neq d/2$ are linearly independent in $H^1_{\mathrm{dR}}(\mathscr{C}/\mathbb{F}_p)$ and so they form an $\mathbb{F}_p$-basis since the genus of $\mathscr{C}$ is $(d - \gcd(d,2))/2$. It follows that the e_i form a $\mathbb{Z}_p$-basis of $H^1_{\mathrm{dR}}(\mathscr{C}/\mathbb{Z}_p)$.

It is clear from the definition that the e_i with $0 < i < d/2$ are in the submodule $H^0(\mathcal{C}/\mathbb{Z}_p, \Omega^1_{\mathcal{C}/\mathbb{Z}_p})$, and so they form a basis by a dimension count. Part (1) and Serre duality imply that the e_i with $d/2 < i < d$ project to a basis of $H^1(\mathcal{C}/\mathbb{Z}_p, \mathcal{O}_{\mathcal{C}/\mathbb{Z}_p})$. This proves part (2).

Part (3) follows immediately from the definition of the e_i.

It follows from part (3) that $F(e_i) = c_i e_{pi}$ for some $c_i \in \mathbb{Z}_p$. Indeed, Frobenius must send the subspace of $H^1(\mathcal{C}/W(k))$ where $[\zeta]$ acts by ζ^i to the subspace where it acts by ζ^{pi}. By (3), these subspaces are spanned by e_i and e_{pi}, respectively, so $F(e_i) = c_i e_{pi}$, and c_i must lie in $\mathbb{Z}_p$ since F acts on $H^1_{\mathrm{crys}}(\mathcal{C}/\mathbb{Z}_p)$. The assertion on the valuation of c_i follows from [Mazur 1972, Lemma, p. 665; 1973, top of p. 65]. This proves part (4).

For part (5), a standard calculation [Ireland and Rosen 1990, Chapter 11] gives the eigenvalues of $F^{|o|}$ in terms of Jacobi sums. Using the notation of [Conceição et al. 2014], $F^{|o|} e_i = \lambda(-1) J(\lambda, \chi^i) e_i$, where λ is a character of $k = \mathbb{F}_{p^{|o|}}$ of order 2 and χ is a character of order d. By [Conceição et al. 2014, Proposition 4.1], the Jacobi sum is $\pm p^{|o|/2}$. $\square$

Remark 6.4.1. Part (4) of the proposition is the reason for the minus signs in the definition of the word attached to an orbit in Section 2.3. Indeed, if $i < d/2$, so that e_i is in $H^0(\mathcal{C}/\mathbb{Z}_p, \Omega^1_{\mathcal{C}/\mathbb{Z}_p})$, then $F(e_i)$ is divisible by p (i.e., its "valuation" has gone up) whereas, if $i > d/2$, then $F(e_i)$ is not divisible by p (i.e., its "valuation" is still low).

6.5. *Generalization to $r > 2$.* Most of the above extends to the curve $\mathcal{C}_r$ defined by $z^d = x^r - 1$ for any r that is > 1 and relatively prime to p. We give the main statements; their proofs are entirely parallel to those in the case $r = 2$.

The curve $\mathcal{C}_r$ has an obvious lift to $\mathbb{Z}_p$ that we denote $\mathcal{C}_r/\mathbb{Z}_p$. This yields an identification $H^1_{\mathrm{crys}}(\mathcal{C}_r/\mathbb{Z}_p) \cong H^1_{\mathrm{dR}}(\mathcal{C}_r/\mathbb{Z}_p)$.

For $i \in \mathbb{Z}/d\mathbb{Z}$, we write $\langle i/d \rangle$ for the fractional part of i/d (for any representative of the class of i). We similarly define $\langle j/r \rangle$ for $j \in \mathbb{Z}/r\mathbb{Z}$. Let A be the subset of $\mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}/r\mathbb{Z}$ consisting of (i, j) where $i \neq 0$, $j \neq 0$, and $\langle i/d \rangle + \langle j/r \rangle > 1$. Let B be the subset where $i \neq 0$, $j \neq 0$, and $\langle i/d \rangle + \langle j/r \rangle < 1$. Let $S = A \cup B$.

There is a $\mathbb{Z}_p$-basis of $H^1_{\mathrm{dR}}(\mathcal{C}_r/\mathbb{Z}_p)$ consisting of classes $e_{i,j}$ with $(i, j) \in S$ with the following properties:

(1) $$e_{i,j} \cup e_{i',j'} = \pm \delta_{ii'} \delta_{jj'},$$

   where the sign is $+$ if $(i, j) \in A$ and $-$ if $(i, j) \in B$.

(2) The $e_{i,j}$ with $(i, j) \in A$ form a basis of $H^0(\mathcal{C}_r/\mathbb{Z}_p, \Omega^1_{\mathcal{C}_r/\mathbb{Z}_p})$, and the $e_{i,j}$ with $(i, j) \in B$ project to a basis of $H^1(\mathcal{C}_r/\mathbb{Z}_p, \mathcal{O}_{\mathcal{C}_r/\mathbb{Z}_p})$.

(3) If q is such that $\mathbb{F}_q$ contains $\mathbb{F}_p(\mu_d, \mu_r)$, then the action of $\mu_d \times \mu_r$ on $H^1(\mathscr{C}_r / W(\mathbb{F}_q))$ is given by

$$[\zeta_d, \zeta_r]e_{i,j} = \zeta_d^i \zeta_r^j e_{i,j}.$$

(4) $F(e_{i,j}) = c_{i,j} e_{pi,pj}$, where $c_{i,j} \in \mathbb{Z}_p$ satisfies

$$\operatorname{ord}_p(c_{i,j}) = \begin{cases} 0 & \text{if } (i,j) \in B, \\ 1 & \text{if } (i,j) \in A. \end{cases}$$

There is also a notion of balanced that we now explain. Let $H = (\mathbb{Z}/\operatorname{lcm}(d,r)\mathbb{Z})^\times$, and let H act on S by multiplication in both coordinates. Let $\langle p \rangle$ be the cyclic subgroup of H generated by p. If $(i,j) \in S$, we say *the ray through (i,j) is balanced* if, for all $t \in H$, the orbit $\langle p \rangle t(i,j)$ is evenly divided between A and B, i.e.,

$$|\langle p \rangle t(i,j) \cap A| = |\langle p \rangle t(i,j) \cap B|.$$

The final property of $\mathscr{C}_r$ we mention is:

(5) For $(i,j) \in S$, let $o = \langle p \rangle (i,j)$ and set

$$J_o = \prod_{(i',j') \in o} c_{i',j'}.$$

Then J_o is a root of unity times $p^{|o|/2}$ if and only if the ray through (i,j) is balanced.

To prove this, we note that the displayed product is an eigenvalue of $F^{|o|}$ on $H^1_{\text{crys}}(\mathscr{C}_r / \mathbb{Z}_p)$. This eigenvalue may be identified with a Jacobi sum, and arguments parallel to those in [Conceição et al. 2014, Proposition 4.1] using Stickelberger's theorem show that the Jacobi sum is a root of unity times $p^{|o|}$ if and only if the ray through (i,j) is balanced. In [Conceição et al. 2014], these roots of unity were always ± 1. If r divides d and d divides $p^f + 1$, then again these root of unity are ± 1. In the more general context, all we can say is that they are roots of unity of order at most $\gcd(\operatorname{lcm}(r,d), p-1)$.

To close this section, we note that the apparatus of orbits, words, and the associated invariants (as in Section 2) applies as well to the cohomology of $\mathscr{C}_r$ as soon as we replace "$i > d/2$" and "$i < d/2$" with "$(i,j) \in A$" and "$(i,j) \in B$", respectively.

7. *p*-adic exercises

Fix as usual an odd prime number p, a positive integer d relatively prime to p, and an extension $\mathbb{F}_q$ of $\mathbb{F}_p(\mu_d)$, and consider E over $\mathbb{F}_q(u)$ where $u^d = t$.

Using Theorems 4.2 and 5.2 reduces the problem of computing $E(\mathbb{F}_q(u))$ and $\operatorname{III}(E/\mathbb{F}_q(u))$ to exercises in semilinear algebra with raw data supplied by Proposition 6.4.

In this section, we carry out these p-adic exercises.

7.1. *Setup.* We write W for the Witt vectors $W(\mathbb{F}_q)$, W_n for $W_n(\mathbb{F}_q)$, $H^1(\mathscr{C})$ for $H^1_{\mathrm{crys}}(\mathscr{C}/W)$, and $H^1(\mathscr{D})$ for $H^1_{\mathrm{crys}}(\mathscr{D}/W)$, where $\mathscr{C} = \mathscr{D}$ is the curve over $\mathbb{F}_q$ studied in Section 6. The product $\mathscr{C} \times_{\mathbb{F}_q} \mathscr{D}$ carries an action of $\Delta = \mu_2 \times \mu_d$ acting "antidiagonally" as well as an action of $G = \mu_d \rtimes \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ acting on the factor $\mathscr{C}$.

Our goal is to compute

$$H := (H^1(\mathscr{C}) \otimes_W H^1(\mathscr{D}))^{\Delta, F=V=p}$$

and

$$H_n := (H^1(\mathscr{C}/W_n) \otimes_W H^1(\mathscr{D}/W_n))^{\Delta, F=V=p}.$$

For an orbit $o \in O_{d,p}$, we write H^o and H^o_n for the o parts of the corresponding groups, i.e., for the images of the projector π_o on H or H_n.

Since $H^1(\mathscr{C})$ and $H^1(\mathscr{D})$ free W-modules and the order of Δ is prime to p,

$$(H^1(\mathscr{C}/W_n) \otimes_W H^1(\mathscr{D}/W_n))^{\Delta} = ((H^1(\mathscr{C}) \otimes_W H^1(\mathscr{D}))/p^n)^{\Delta},$$
$$= ((H^1(\mathscr{C}) \otimes_W H^1(\mathscr{D}))^{\Delta})/p^n,$$

so the first step in both cases is to compute $M = (H^1(\mathscr{C}) \otimes_W H^1(\mathscr{D}))^{\Delta}$.

7.2. *A basis for M.* By Proposition 6.4(3), μ_2 acts as -1 on $H^1(\mathscr{C})$ and μ_d acts on e_i by χ^i. Thus, μ_2 acts trivially on $H^1(\mathscr{C}) \otimes_W H^1(\mathscr{D})$ and μ_d acts on $e_i \otimes e_j$ by χ^{i-j}. Therefore, we have

$$M \cong \bigoplus_{i \in \mathbb{Z}/d\mathbb{Z} \setminus \{0, d/2\}} W(e_i \otimes e_i).$$

We decompose $M = \bigoplus_{o \in O} M^o$, where

$$M^o = \bigoplus_{i \in o} W(e_i \otimes e_i).$$

For the rest of this section, we fix an orbit o and *we assume that* $\gcd(o, d) < d/2$ *and p is balanced modulo $d/\gcd(o, d)$*. By Theorem 3.1.1, this is the situation in which $E(\mathbb{F}_q(u) \otimes \mathbb{Z}_p)^o \neq 0$, and it turns out to be the situation in which we can say something nontrivial about $\text{III}(E/\mathbb{F}_q(u))^o$.

As a first step, we make a change of basis that is perhaps unnatural but has the virtue of simplifying the notation considerably. Namely, let $i \in o$ be the standard base point (see Definition 2.3.1), and let

$$d_{ip^j} = \begin{cases} c_{ip^j} & \text{if } w_j = l, \\ c_{ip^j}/p & \text{if } w_j = u, \end{cases}$$

where the p-adic integers c_{ip^j} are defined in Proposition 6.4(4). That proposition implies that the d_{ip^j} are units. Set $f_i = e_i \otimes e_i$, and for $j = 1, \ldots, |o| - 1$, set

$$f_{ip^j} = \left(\prod_{\ell=1}^{j} d_{pi^\ell}^2 \right) e_{ip^j} \otimes e_{ip^j}.$$

Then $\{f_j \mid j \in o\}$ forms a W-basis of M^o, and it follows from Proposition 6.4 parts (4) and (5) that for all $j \in o$ we have

$$F(f_j) = \begin{cases} p^2 f_{pj} & \text{if } j < d/2, \\ f_{pi} & \text{if } j > d/2. \end{cases}$$

(Here as usual, we read the subscripts modulo d.)

Similarly, we have

$$V(f_j) = \begin{cases} f_{p^{-1}j} & \text{if } p^{-1}j < d/2, \\ p^2 f_{p^{-1}j} & \text{if } p^{-1}j > d/2, \end{cases}$$

where "$p^{-1}j < d/2$" means that the least positive residue of $p^{-1}j$ is $< d/2$.

We have a remaining action of $G = \mu_d \rtimes \mathrm{Gal}(\mathbb{F}_q / \mathbb{F}_p)$ on M via its action on the first factor in $H^1(\mathscr{C}) \otimes_W H^1(\mathscr{D})$. Under this action, $\zeta \in \mu_d$ acts W-linearly as $[\zeta]f_j = \zeta^j f_j$ and $\mathrm{Fr}_p \in \mathrm{Gal}(\mathbb{F}_q / \mathbb{F}_p)$ acts semilinearly as $\mathrm{Fr}_p(\alpha f_j) = \sigma(\alpha) f_j$.

7.3. Modulo p case with $d = p^f + 1$ and $\mathbb{F}_q = \mathbb{F}_p(\mu_d)$.

As a very easy first case, we assume $d = p^f + 1$ and $\mathbb{F}_q = \mathbb{F}_p(\mu_d)$, and we compute H_1, which is just the subspace of M/p killed by F and by V. We saw just above that $F(f_i)$ is zero if and only if $i < d/2$, i.e., if and only if the first letter in the word associated to i is u. Similarly, $V(f_i) = 0$ if and only if the last letter of the word of i is l. This yields the first part of the following statement:

Proposition 7.3.1. *If $d = p^f + 1$ and $\mathbb{F}_q = \mathbb{F}_p(\mu_d)$, then*

$$H_1 := (H^1(\mathscr{C}/\mathbb{F}_q) \otimes_W H^1(\mathscr{D}/\mathbb{F}_q))^{\Delta, F=V=0}$$

is spanned over $\mathbb{F}_q$ by the classes f_i where the word of i has the form $u \cdots l$. If the first half of the word of o has the form $u^{e_1} l^{e_2} \cdots u^{e_k}$ with each $e_i > 0$, then the $\mathbb{F}_q$-dimension of H_1^o is k. We have

$$\dim_{\mathbb{F}_q} H_1 = \left(\frac{p-1}{2} \right) \left(\frac{p^{f-1}+1}{2} \right).$$

The dimension counts in the proposition will be proven at the end of Section 8.1 after we have proven Lemma 8.1.1.

7.4. *The basic equations.* We now make first reductions toward computing H^o and H^o_n in general. Focus on one orbit $o \in O$ with its standard base point i and associated word $w = w_1 \cdots w_{|o|}$.

Consider a typical element $c \in M^o$ (or in M^o_n):

$$c = \sum_{j=0}^{|o|-1} \alpha_j f_{ip^j},$$

where $\alpha_j \in W$ (or in W_n) and where we read the index j modulo $|o|$.

Then the class c satisfies $(F - p)(c) = 0$ if and only if

$$p\alpha_{j+1} = \begin{cases} \sigma(\alpha_j) & \text{if } w_j = l, \\ p^2\sigma(\alpha_j) & \text{if } w_j = u \end{cases}$$

for $j = 0, \ldots, |o| - 1$. Similarly, the class c satisfies $(V - p)(c) = 0$ if and only if

$$p\alpha_j = \begin{cases} p^2\sigma^{-1}(\alpha_{j+1}) & \text{if } w_j = l, \\ \sigma^{-1}(\alpha_{j+1}) & \text{if } w_j = u \end{cases}$$

for $j = 0, \ldots, |o| - 1$.

Note that when $w_j = l$, the equation coming from $V - p = 0$ follows from that coming from $F - p = 0$, and when $w_j = u$, then the equation coming from $F - p = 0$ follows from that coming from $V - p = 0$. Thus, c satisfies $(F - p)(c) = (V - p)(c) = 0$ if and only if

$$\begin{cases} \alpha_j = \sigma^{-1}p\alpha_{j+1} & \text{if } w_j = l, \\ \sigma p\alpha_j = \alpha_{j+1} & \text{if } w_j = u \end{cases} \tag{7.4.1}$$

for $j = 0, \ldots, |o| - 1$.

Note that α_{j+1} determines α_j when $w_j = l$, and α_j determines α_{j+1} when $w_j = u$. Thus, we may eliminate many of the variables α_j. More precisely, write the word w in exponential form: $w = u^{e_1}l^{e_2} \cdots l^{e_{2k}}$. Setting $\beta_0 = \alpha_0$ and

$$\beta_j = \alpha_{e_1+e_2+\cdots+e_{2j}}$$

for $1 \le j \le k$ (so that $\beta_k = \beta_0$), the class c is entirely determined by the β's. Indeed, for $\sum_{i=1}^{2j} e_i \le \ell \le \sum_{i=1}^{2j+1} e_i$, we have

$$\alpha_\ell = (\sigma p)^{\ell - \sum_{i=1}^{2j} e_i} \beta_j,$$

and for $\sum_{i=1}^{2j+1} e_i \le \ell \le \sum_{i=1}^{2j+2} e_i$, we have

$$\alpha_\ell = (\sigma^{-1}p)^{\sum_{i=1}^{2j+2} e_i - \ell} \beta_{j+1}.$$

The conditions on the α's translated to the β's become

$$(\sigma p)^{e_1}\beta_0 = (\sigma^{-1} p)^{e_2}\beta_1,$$
$$(\sigma p)^{e_3}\beta_1 = (\sigma^{-1} p)^{e_4}\beta_2,$$
$$\vdots$$
$$(\sigma p)^{e_{2k-1}}\beta_{k-1} = (\sigma^{-1} p)^{e_{2k}}\beta_k. \tag{7.4.2}$$

We refer to these as the *basic equations*.

The upshot is that the coordinates β define an embedding $H^o \hookrightarrow W^k$ (respectively, $H_n^o \hookrightarrow W_n^k$) with $c \mapsto (\beta_j)_{j=1,\ldots,k}$ whose image is characterized by the basic equations.

In the rest of this section, we will make this image more explicit in the "adic case" $H^o \hookrightarrow W^k$ and the "modulo p^n case" $H_n^o \hookrightarrow W_n^k$.

7.5. adic case. In this case, the β_j lie in W, which is torsion free, so the basic equations allow us to eliminate all β_j with $0 < j < k$ in favor of β_0. Indeed, the basic equations imply that

$$\beta_1 = \sigma^{e_1+e_2} p^{e_{1,2}}\beta_0,$$
$$\beta_2 = \sigma^{e_3+e_4} p^{e_3-e_4}\beta_1 = \sigma^{e_1+\cdots+e_4} p^{e_{1,4}}\beta_0,$$
$$\vdots$$
$$\beta_k = \sigma^{e_1+\cdots+e_{2k}} p^{e_{1,2k}}\beta_0 = \sigma^{|o|} p^{e_{1,2k}}\beta_0 = \sigma^{|o|}\beta_0, \tag{7.5.1}$$

where, as usual, e_{ij} denotes the alternating sum

$$e_{ij} = e_i - e_{i+1} + \cdots \pm e_j.$$

Note that $\beta_k = \beta_0$, so the last equation is satisfied if and only if $\beta_0 \in W(\mathbb{F}_{p^{|o|}})$. Note also that since i is a good base point, the e_{1j} are ≥ 0 for $1 \leq j \leq 2k$, so the exponents of p on the far right-hand sides of the equations above are nonnegative. Therefore, for any choice of $\beta_0 \in W(\mathbb{F}_{p^{|o|}})$, the equations give well-defined elements $\beta_j \in W(\mathbb{F}_{p^{|o|}}) \subset W$ solving the basic equations.

The upshot is that the map sending $c \mapsto \beta_0 = \alpha_0$ gives an isomorphism $H^o \cong W(\mathbb{F}_{p^{|o|}}) = \Gamma_o$. The inverse of this map is

$$\alpha_0 \mapsto \sum_{j=0}^{|o|-1} \sigma^j p^{a_j} \alpha_0 f_{ip^j},$$

where a_j is the function defined in Section 2.3. It is easy to see that this map is equivariant for the action of $G = \mu_d \rtimes \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$, where G acts on $W(\mathbb{F}_{p^{|o|}}) \cong \Gamma_o$ as in Proposition 2.8.1.

In summary:

Proposition 7.5.1. *Suppose that $o \in O_{d,p}$ is an orbit with $\gcd(d, o) < d/2$ and p is balanced modulo p. Then the map above induces an isomorphism of $\mathbb{Z}_p[G]$-modules*

$$H^o \cong \Gamma_o.$$

7.6. *Modulo p^n case.* To compute H_n^o, we should solve the basic equations (7.4.2) with the $\beta_j \in W_n$. We will do this for all sufficiently large n (to be made precise just below). We write $\beta_j^{(\nu)}$ for the Witt-vector components of β_j, and by convention, we set $\beta_j^{(\nu)} = 0$ if $\nu \leq 0$.

Recall that the *height* of an orbit with word $u^{e_1} l^{e_2} \cdots l^{e_{2k}}$ is

$$\mathrm{ht}(o) = \max\{e_1, e_{13}, \ldots, e_{1,2k-1}\}.$$

In other words, $\mathrm{ht}(o)$ is the maximum value of the sequence a_j associated to o in Section 2.6. For the rest of this section, *we assume that $n \geq \mathrm{ht}(o)$.*

Taking the ν-th Witt component in the basic equations (7.4.2) yields the following system of equations in $\mathbb{F}_q$:

$$
\begin{aligned}
\sigma^{2e_1} \beta_0^{(\nu - e_1)} &= \beta_1^{(\nu - e_2)}, \\
\sigma^{2e_3} \beta_1^{(\nu - e_3)} &= \beta_2^{(\nu - e_4)}, \\
&\vdots \\
\sigma^{2e_{2k-1}} \beta_{k-1}^{(\nu - e_{2k-1})} &= \beta_k^{(\nu - e_{2k})}.
\end{aligned}
\tag{7.6.1}
$$

Now suppose that $\nu \leq n - \mathrm{ht}(o)$ so that $\nu + e_1 \leq n$, $\nu + e_{13} \leq n$, etc. Considering the $\nu + e_1$ component of the first equation in (7.6.1), the $\nu + e_{13}$ component of the second equation, etc., leads to the chain of equalities

$$\beta_0^{(\nu)} = \sigma^{-2e_1} \beta_1^{(\nu - e_{12})} = \sigma^{-2(e_1 + e_3)} \beta_2^{(\nu - e_{14})}$$

$$= \cdots = \sigma^{-2(e_1 + e_3 + \cdots + e_{2k-1})} \beta_0^{(\nu - e_{1,2k})} = \sigma^{-|o|} \beta_0^{(\nu)}.$$

It follows that for $\nu \leq n - \mathrm{ht}(o)$, $\beta_0^{(\nu)}$ lies in $\mathbb{F}_{p^{|o|}}$.

Conversely, given Witt components $\beta_0^{(\nu)} \in \mathbb{F}_{p^{|o|}}$ for $\nu \leq n - \mathrm{ht}(o)$, there exists a solution $(\beta_0, \ldots, \beta_{k-1}) \in W_n^k$ of the basic equations with the given components. Indeed, we may complete β_0 to an element of W, use the equations (7.5.1) to define the other β_j, and then reduce modulo p^n.

Thus, the map $(\beta_0, \ldots, \beta_{k-1}) \mapsto \beta_0 \pmod{p^{n - \mathrm{ht}(o)}}$ defines a surjective homomorphism

$$H_n^o \to W_{n - \mathrm{ht}(o)}(\mathbb{F}_{p^{|o|}}) \tag{7.6.2}$$

whose kernel is easily seen to be $p^{n - \mathrm{ht}(o)} H_n^o$. Note that if $n_2 \geq n_1 \geq \mathrm{ht}(o)$, we have an isomorphism

$$p^{n_1 - \mathrm{ht}(o)} H_{n_1}^o \cong p^{n_2 - \mathrm{ht}(o)} H_{n_2}^o,$$

which sends (β_j) to $p^{n_2-n_1}(\beta_j)$. In this sense, the kernel of the surjection (7.6.2) is independent of n (as long as $n \geq \mathrm{ht}(o)$). Thus, to compute it, we may assume that $n = \mathrm{ht}(o)$ and compute $H^o_{\mathrm{ht}(o)}$.

Next we note that if $(\beta_j) \in H^o_{\mathrm{ht}(o)}$ and if ℓ is such that $\mathrm{ht}(o) = e_{1,2\ell+1} = e_{2\ell+2,2k}$, then

$$0 = p^{\mathrm{ht}(o)}\beta_k = p^{e_{2\ell+2,2k}}\beta_k$$
$$= p^{e_{2\ell+2,2k-2}}\beta_{k-1}$$
$$\vdots$$
$$= p^{e_{2\ell+2}}\beta_{\ell+1}.$$

Thus, after reordering, we may write the basic equations as a triangular system:

$$(\sigma p)^{e_{2\ell+3}}\beta_{\ell+1} = (\sigma^{-1}p)^{e_{2\ell+4}}\beta_{\ell+2},$$
$$\vdots$$
$$(\sigma p)^{e_{2k-1}}\beta_{k-1} = (\sigma^{-1}p)^{e_{2k}}\beta_k,$$
$$(\sigma p)^{e_1}\beta_k = (\sigma^{-1}p)^{e_2}\beta_1,$$
$$\vdots$$
$$(\sigma p)^{e_{2\ell-1}}\beta_{\ell-1} = (\sigma^{-1}p)^{e_{2\ell}}\beta_\ell,$$
$$(\sigma p)^{e_{2\ell+1}}\beta_\ell = 0.$$

Now introduce new variables γ_j indexed by $j \in \mathbb{Z}/k\mathbb{Z}$ and related to the β_j by

$$\gamma_{j-\ell} = \begin{cases} \sigma^{-e_1-e_2-\cdots-e_{2j}}\beta_j & \text{if } 1 \leq j \leq \ell, \\ \sigma^{e_{2j+1}+e_{2j+2}+\cdots+e_{2k}}\beta_j & \text{if } \ell+1 \leq j \leq k. \end{cases}$$

In these variables, the basic equations become

$$p^{e_{2\ell+3}}\gamma_1 = p^{e_{2\ell+4}}\gamma_2,$$
$$\vdots$$
$$p^{e_{2k-1}}\gamma_{k-\ell-1} = p^{e_{2k}}\gamma_{k-\ell},$$
$$p^{e_1}\gamma_{k-\ell} = p^{e_2}\gamma_{k+1-\ell},$$
$$\vdots$$
$$p^{e_{2\ell-1}}\gamma_{k-1} = p^{e_{2\ell}}\gamma_k,$$
$$p^{e_{2\ell+1}}\gamma_k = 0$$

or, in matrix form,

$$B(e_{2\ell+3}, \ldots, e_{2k}, e_1, \ldots, e_{2\ell+1}) \begin{pmatrix} \gamma_1 \\ \gamma_2 \\ \vdots \\ \gamma_k \end{pmatrix} = 0.$$

The upshot is that we have identified $H^o_{\mathrm{ht}(o)}$ with the kernel of $B(e_{2\ell+3}, \ldots, e_{2\ell+1})$ on $W^k_{\mathrm{ht}(o)}$. By Remark 2.7.4, this is the same as the kernel of $B(e_1, \ldots, e_{2k+1})$, and this kernel is described by the invariant factors d_j analyzed in Section 2.7.

To finish the discussion, we will unwind the action of $G = \mu_d \rtimes \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ under the isomorphisms above. The action of Fr_p on a class $c \in H^o_n$ goes over to the action of σ on the coordinates α_j and also on the coordinates β_j and γ_j. The action of $\zeta \in \mu_d$ on c goes over to multiplication by ζ^{ip^j} on α_j so to multiplication by $\zeta^{ip^{e_1+e_2+\cdots+e_{2j}}}$ on β_j and finally to multiplication by ζ^i on the γ_j.

The following statement summarizes the results of this subsection:

Proposition 7.6.1. *Suppose that $o \in O_{d,p}$ is an orbit with $\gcd(d, o) < d/2$ and p is balanced modulo p. Suppose that the word of o is $u^{e_1} \cdots l^{e_{2k}}$, and recall the invariants $d_1, \ldots, d_k$ attached to o in Section 2.6.*

(1) *For all $n \geq \mathrm{ht}(o)$, we have an exact sequence of $\mathbb{Z}_p[G]$-modules*

$$0 \to \bigoplus_{j=1}^k W_{d_j}(\mathbb{F}_q) \to H^o_n \to W_{n-\mathrm{ht}(o)}(\mathbb{F}_{p^{|o|}}) \to 0.$$

Here G acts on the Witt vectors as described in Proposition 2.8.1(5).

(2) *The cokernel of $H^o/p^n \to H^o_n$ is isomorphic to*

$$\frac{\bigoplus_{j=1}^k W_{d_j}(\mathbb{F}_q)}{W_{d_k}(\mathbb{F}_{p^{|o|}})}.$$

The first part was proven earlier in this subsection. The second follows from the fact that the composed map $H^o/p^n \to H^o_n \to W_{n-\mathrm{ht}(o)}(\mathbb{F}_{p^{|o|}})$ (see (7.6.2)) is obviously surjective with kernel $p^{n-\mathrm{ht}(o)} H^o/p^n H^o$ and $d_k = \mathrm{ht}(o)$.

Remark 7.6.2. The "dévissage" implicit in this subsection is captured by the middle column of the following diagram with exact rows and columns:

$$
\begin{array}{ccc}
0 & & 0 \\
\downarrow & & \downarrow \\
\end{array}
$$

$$
0 \longrightarrow \dfrac{p^{n-\mathrm{ht}(o)}\,H^o}{p^n\,H^o} \longrightarrow p^{n-\mathrm{ht}(o)}\,H_n^o \longrightarrow \mathrm{Br}^o[p^n] \longrightarrow 0
$$

$$
\downarrow \qquad\qquad\qquad \downarrow \qquad\qquad \big\|
$$

$$
0 \longrightarrow \dfrac{H^o}{p^n\,H^o} \longrightarrow H_n^o \longrightarrow \mathrm{Br}^o[p^n] \longrightarrow 0
$$

$$
\downarrow \qquad\qquad\qquad \downarrow \qquad\qquad \downarrow
$$

$$
\dfrac{H^o}{p^{n-\mathrm{ht}(o)}\,H^o} \xrightarrow{\ \cong\ } \dfrac{H_n^o}{p^{n-\mathrm{ht}(o)}\,H_n^0}
$$

$$
\downarrow \qquad\qquad\qquad \downarrow
$$

$$
0 \qquad\qquad\qquad 0
$$

Here $\mathrm{Br}^o[p^n]$ is the p^n-torsion in $\mathrm{Br}(\mathscr{C}\times_{\mathbb{F}_q}\mathscr{D})^{\Delta,o}$ and the middle row is the o part of the exact sequence in Theorem 5.2(2). The middle column is the o part of the exact sequence of [Artin 1974] on page 553 just after (3.2) and [Milne 1975, p. 521, line 6]; i.e., $U^2(p^\infty)=U^2(p^{\mathrm{ht}(o)})=p^{n-\mathrm{ht}(o)}\,H_n^o$ and $D^2(p^{n-\mathrm{ht}(o)})=H_n^o/p^{n-\mathrm{ht}(o)}\,H_n^o$. Note also that the top row above shows that $S\mapsto \mathrm{Br}(\mathscr{X}\times_k S)$ is not represented by an algebraic group, even as a functor on finite fields.

8. Proofs of the main results

In this section, we prove an easy lemma on counting words and then assemble the results from Sections 4, 5, and 7 to prove the theorems stated in Sections 1 and 3.

8.1. Counting patterns. Let f be a positive integer, let $d=p^f+1$, and let $S=\mathbb{Z}/d\mathbb{Z}\setminus\{0,d/2\}$. Let $\langle p\rangle\subset(\mathbb{Z}/d\mathbb{Z})^\times$ be the cyclic subgroup generated by p. Given $i\in S$, we define a string w of length f in the alphabet $\{u,l\}$, called the *pattern* associated to i, as $w=w_1\cdots w_f$, where

$$
w_j=\begin{cases} l & \text{if } -p^{j-1}i\in A,\\ u & \text{if } -p^{j-1}i\in B.\end{cases}
$$

If the orbit o of $\langle p\rangle$ through i has full size (i.e., size $2f$), then the pattern of i is the same thing as the first half of the word associated to i. If the orbit is smaller, then the pattern is a repetition of the $\lfloor f/|o|\rfloor$ copies of the word followed by the first half of the word. (Note that $f/|o|$ always has denominator 2 because the second half of the word is the complement of the first.) For example, if $p=f=3$ and $i=7$, then $o=\{7,21\}$, the associated word is ul, and the pattern is ulu. Patterns turn out to be more convenient than words for counting.

Let T be the set of tuples

$$T = \{(i_1, \ldots, i_f) \mid i_j \in \{0, \ldots, p-1\}, \text{ not all } i_j = (p-1)/2\}.$$

There is a bijection $T \to S$ that sends

$$(i_1, \ldots, i_f) \mapsto \left(1 + \sum_{j=1}^{f} i_j p^{j-1}\right).$$

If i corresponds to $(i_1, \ldots, i_f)$, then pi corresponds to $(p-1-i_f, i_1, \ldots, i_{f-1})$.

The first letter of the pattern of i is u if and only if the first element of the sequence $i_f, i_{f-1}, \ldots$ that is not equal to $(p-1)/2$ is in fact $< (p-1)/2$. More generally, if we have a word $w = u^{e_1} l^{e_2} \cdots u^{e_k}$ where k is odd, each $e_j > 0$, and $\sum e_j = f$, then $i \in S$ has pattern w if and only the following inequalities are satisfied:

$$i_f \le (p-1)/2, \quad i_{f-1} \le (p-1)/2,$$
$$\ldots, \quad i_{f-e_1+2} \le (p-1)/2, \quad i_{f-e_1+1} < (p-1)/2,$$
$$i_{f-e_1} \ge (p-1)/2, \quad i_{f-e_1-1} \ge (p-1)/2,$$
$$\ldots, \quad i_{f-e_1-e_2+2} \ge (p-1)/2, \quad i_{f-e_1-e_2+1} > (p-1)/2,$$
$$\vdots$$
$$i_{f-e_1-\cdots-e_{k-1}} \le (p-1)/2, \quad i_{f-e_1-\cdots-e_{k-1}-1} \le (p-1)/2,$$
$$\ldots, \quad i_{f-e_1-\cdots-e_k+2} \le (p-1)/2, \quad i_{f-e_1-\cdots-e_k+1} < (p-1)/2.$$

This leads to the following counts:

Lemma 8.1.1. (1) *Suppose $k > 0$ is odd and $e_1, \ldots, e_k$ are positive integers with $\sum e_j = f$. Then the number of elements $i \in S$ with pattern $w = u^{e_1} l^{e_2} \cdots u^{e_k}$ is*

$$\left(\frac{p-1}{2}\right)^k \left(\frac{p+1}{2}\right)^{f-k}.$$

(2) *The number of $i \in S$ whose pattern starts $lu \cdots$ is*

$$\left(\frac{p-1}{2}\right)\left(\frac{p^{f-1}+1}{2}\right),$$

and the number of $i \in S$ whose pattern starts $ll \cdots$ is

$$\left(\frac{p+1}{2}\right)\left(\frac{p^{f-1}-1}{2}\right).$$

Proof. Part (1) follows immediately from the inequalities just before the lemma. Part (2) is similar: the pattern of i starts $lu \cdots$ if and only if $i_f > (p-1)/2$ and

$$i_{f-1} < (p-1)/2,$$

$$\text{or} \quad i_{f-1} = (p-1)/2 \qquad\qquad \text{and} \quad i_{f-2} < (p-1)/2,$$

$$\text{or} \quad i_{f-1} = i_{f-2} = (p-1)/2 \quad \text{and} \quad i_{f-3} < (p-1)/2,$$

$$\vdots$$

The number of such i is

$$\left(\frac{p-1}{2}\right)\left(\frac{p-1}{2}p^{f-2} + \cdots + \frac{p-1}{2} + 1\right) = \left(\frac{p-1}{2}\right)\left(\frac{p^{f-1}+1}{2}\right).$$

Since the number of i whose pattern starts with l is clearly $(p^f - 1)/2$, the result for ll follows by subtracting. $\qquad\square$

End of the proof of Proposition 7.3.1. We saw above that the $\mathbb{F}_q$-dimension of H_1^o is the number $i \in o$ whose word has the form $u \cdots l$, i.e., begins with u and ends with l. If the word associated to the standard base point in o is $u^{e_1}l^{e_2}\cdots l^{e_{2k}}$ with $e_{i+k} = e_i$, then there are exactly k elements $i \in o$ whose word has the form $u \cdots l$; if i is the standard base point, they are

$$i, p^{e_1+e_2}i, \ldots, p^{e_1+\cdots+e_{2k-2}}i.$$

To compute the $\mathbb{F}_q$-dimension of H_1, we need only note that the number of $i \in S$ whose word has the form $u \cdots l$ is the same as the number of i whose pattern starts $lu \cdots$. Thus, part (2) of Lemma 8.1.1 finishes the proof. $\qquad\square$

8.2. *Proof of Theorems 3.1.1 and 3.2.1.* We now give the proofs of our results on the o-part of the Mordell–Weil group $E(K_d)$. We proved in [Conceição et al. 2014] that $(E(K_d) \otimes \mathbb{Z}_p)^o = 0$ unless o is an orbit with $\gcd(o, d) < d/2$ and p is balanced modulo $d/\gcd(d, o)$, so we make those hypotheses for the rest of the subsection.

The first step is to note that Theorem 4.2(1) and Theorem 5.2(1) imply that

$$(E(K_d) \otimes \mathbb{Z}_p)^o \cong (H^1(\mathscr{C}) \otimes_W H^1(\mathscr{D}))^{\Delta, o, F=p}.$$

This last group is denoted H^o in Section 7, where we proved an isomorphism $H^o \cong \Gamma_o$.

In order to prove the theorems, we need to consider H^o as a submodule of

$$M^o := (H^1(\mathscr{C}) \otimes_W H^1(\mathscr{D}))^{\Delta, o}.$$

This is a free W-module on which the cup product induces a perfect pairing. The restriction of that pairing to H^o corresponds to the height pairing on $E(K_d)$, so to compute the discriminant of the latter, it suffices to know the index of the

W-submodule of M^o generated by H^o. More precisely, the discriminant is p^{2a}, where

$$a = \mathrm{Len}_W(M^o/WH^o).$$

We saw above that $f_i, f_{pi}, \ldots, f_{p^{|o|-1}i}$ is a W-basis of M^o. Let $\eta_1, \eta_2, \ldots, \eta_{|o|}$ be a $\mathbb{Z}_p$-basis of W. Then the classes

$$c_\ell = \sum_{j=0}^{|o|-1} p^{a_j}\sigma^j(\eta_\ell) f_{ip^j}, \quad \ell = 1, \ldots, |o|,$$

form a $\mathbb{Z}_p$-basis of H^o. Here $j \mapsto a_j$ is the function associated to o in Section 2.3.

In matrix form, we have

$$\begin{pmatrix} c_1 \\ \vdots \\ c_{|o|} \end{pmatrix} = \begin{pmatrix} \sigma^0(\eta_1) & \sigma^1(\eta_1) & \cdots & \sigma^{|o|-1}(\eta_1) \\ \sigma^0(\eta_2) & \sigma^1(\eta_2) & \cdots & \sigma^{|o|-1}(\eta_2) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma^0(\eta_{|o|}) & \sigma^1(\eta_{|o|}) & \cdots & \sigma^{|o|-1}(\eta_{|o|}) \end{pmatrix} \begin{pmatrix} p^{a_1} & 0 & \cdots & 0 \\ 0 & p^{a_2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & p^{a_{|o|}} \end{pmatrix} \begin{pmatrix} f_i \\ f_{pi} \\ \vdots \\ f_{p^{|o|-1}i} \end{pmatrix}.$$

Since W is unramified over $\mathbb{Z}_p$, the determinant of the first matrix on the right is a unit. The determinant of the second matrix on the right is clearly $p^{a_1+\cdots+a_{|o|}}$, and this is the length of the quotient of M^o by the W-span of H^o. This proves that

$$\mathrm{Disc}(E(K_d) \otimes \mathbb{Z}_p)^o = p^{2(a_1+\cdots+a_{|o|})},$$

and this is the assertion of Theorem 3.1.1.

To prove Theorem 3.2.1, note that we have containments

$$V_d^o \subset E(K_d)^o \cong H^o \subset M^o$$

and we can compute the lengths of M^o/WH^o and M^o/WV_d^o via discriminants.

We just saw that

$$\mathrm{Len}_W \frac{M^o}{WH^o} = a_1 + \cdots + a_{|o|}.$$

Let us simplify the sum using that we are in the complementary case so that k is odd and $e_{k+j} = e_j$. We have

$$\sum_{j=1}^{|o|} a_j = \sum_{j=1}^{2k}(-1)^{j+1}\binom{e_j+1}{2} + e_j e_{1,j-1}$$

$$= \sum_{j=1}^{k}(-1)^{j+1}\binom{e_j+1}{2} + e_j e_{1,j-1} + \sum_{j=1}^{k}(-1)^{k+j+1}\binom{e_j+1}{2} + e_j e_{1,k+j-1}$$

$$= \sum_{j=1}^{k} e_j(e_{1,j-1} + e_{1,k+j-1}),$$

where the second equality uses that $e_{k+j} = e_j$ and the last equality uses that k is odd. Noting that $e_{1,j-1} + e_{1,k+j-1} = e_{1,k} = \mathrm{ht}(o)$, we find that

$$\sum_{j=1}^{|o|} a_j = \frac{|o|}{2}\,\mathrm{ht}(o).$$

On the other hand, it follows from [Ulmer 2014b, Theorem 8.2] (when $d = p^f + 1$) and [Conceição et al. 2014, Proposition 7.1] (when $d = 2(p^f - 1)$) that

$$\mathrm{Len}_W \frac{M^o}{WV_d^o} = \frac{|o|f}{2}.$$

Thus, we have

$$\log_p [E(K_d)^o : V_d^o] = \mathrm{Len}_W \frac{WH^o}{WV_d^o} = \frac{|o|}{2}(f - \mathrm{ht}(o)).$$

Since $V_d^o \cong \Gamma_o$ and Γ_o has a unique G-invariant superlattice of index $p^{|o|e}$, namely $p^{-e}\Gamma_o$, we must have

$$\frac{E(K_d)^o}{V_d^o} \cong p^{-(f-\mathrm{ht}(o))/2}\Gamma_o / \Gamma_o \cong \Gamma_o / p^{(f-\mathrm{ht}(o))/2}\Gamma_o.$$

Note also that when $\gcd(o, d) = 1$, we have $f = \sum_{j=1}^k e_j$ and $\mathrm{ht}(o) = e_1 - e_2 + \cdots + e_k$, so $(f - \mathrm{ht}(o))/2 = \sum_{j=1}^{(k-1)/2} e_{2j}$. These are exactly the assertions of Theorem 3.2.1, so this completes the proof.

8.3. *Proof of Theorem 3.3.1.* Let $\mathbb{F}_q$ be an extension of $\mathbb{F}_p(\mu_d)$, and consider E over $\mathbb{F}_q(u)$ with $u^d = t$.

The first step in the proof is to note that Theorem 4.2(2) and Theorem 5.2(2) give an isomorphism of $\mathbb{Z}_p[G]$-modules between $\mathrm{III}(E/\mathbb{F}_q(u))[p^n]^o$ and the cokernel of the map

$$((H^1(\mathscr{C}) \otimes_w H^1(\mathscr{D}))^{\Delta,o,F=p})/p^n \to (H^1(\mathscr{C})/p^n \otimes_W H^1(\mathscr{D})/p^n)^{\Delta,o,F=V=p}.$$

In the notation of Section 7, this is the cokernel of

$$H^o/p^n \to H_n^o,$$

and in Proposition 7.6.1(2), we showed that for all $n \geq \mathrm{ht}(o)$ this cokernel is

$$\frac{\bigoplus_{j=1}^k W_{d_j}(\mathbb{F}_q)}{W_{d_k}(\mathbb{F}_{p^{|o|}})},$$

where the d_j are the invariants associated to o in Section 2.6. This is precisely part (1) of the theorem. Part (2) follows immediately once we note that if $\gcd(o, d) = 1$, then $\mathbb{F}_{p^{|o|}} = \mathbb{F}_{p^{2f}} = \mathbb{F}_p(\mu_d)$.

8.4. *Exponents*. We prove parts (1) and (2) of Theorem 1.1. Clearly part (2) implies part (1).

By Theorem 3.2.1, the exponent of $(E(K_d)/V_d)^o$ is $p^{(f-\mathrm{ht}(o))/2}$. This is maximized when $\mathrm{ht}(o)$ is minimized. If f is odd, there is an $i \in \mathbb{Z}/d\mathbb{Z}$ with pattern $(ul)^f$ and the corresponding word has height 1. If f is even, the minimum value of $\mathrm{ht}(o)$ is 2, which is achieved by an orbit with pattern (and word) $(ul)^{f-1}uu(lu)^{f-1}ll$. By Lemma 8.1.1, any such word actually does arise as the word of some $i \in S$. Thus, the exponent of $E(K_d)/V_d$ is $p^{\lfloor(f-1)/2\rfloor}$.

By Theorem 3.3.1, the exponent of $\mathrm{III}(E/K_d)^o$ is $p^{d_{k-1}}$. By Lemma 2.7.3,

$$d_{k-1} = \max\{e_{ij} \mid 2 \leq i \leq j \leq k-1, \ i \text{ and } j \text{ even}\}.$$

Clearly the alternating sum $e_i - e_{i+1} + \cdots$ is maximized when it is a single term, and d_{k-1} is maximized by a word whose first half has the form $u^{e_1}l^{e_2}u^{e_3}$. In order for this to be the word associated to a good base point, we must have $e_1 \geq e_2$ and $e_2 \leq e_3$. Again, by Lemma 8.1.1, any such word actually does arise as the word of some $i \in S$. Thus, for a given f, the maximum value of $d_{k-1} = e_2$ is $\lfloor f/3 \rfloor$ and the exponent of $\mathrm{III}(E/K_d)$ is $p^{\lfloor f/3 \rfloor}$

8.5. *Comparison of E/V and* III. Now we prove parts (3) and (4) of Theorem 1.1.

For part (3), note that when $f = 1$ or 2, up to rotation all words have the form u^fl^f and by Theorems 3.2.1 and 3.3.1 the groups under discussion are trivial in these cases. If $f = 3$, up to rotation, every word is u^3l^3 or $(ul)^3$. In the latter case, both $((E(K_d)/V_d)^o)^2$ and $\mathrm{III}(E/K_d)^o$ are isomorphic to $(\Gamma_o/p)^2$. When $f = 4$, up to rotation, the possible words are u^4l^4 and u^2lul^2ul. In the former case, both $((E(K_d)/V_d)^o)^2$ and $\mathrm{III}(E/K_d)^o$ are trivial, and in the latter, they are both isomorphic to $(\Gamma_o/p)^2$.

For part (4), we note that by Proposition 2.8.1 Γ_o/p is an absolutely irreducible $\mathbb{Z}_p[G]$-module. Thus, all Jordan–Hölder factors of $(E(K_d)/V_d)^o$ and $\mathrm{III}(E/K_d)^o$ are Γ_o/p, and to prove part (4), it suffices to count the multiplicities. By Theorem 3.2.1, the multiplicity for $(E(K_d)/V_d)^o$ is $(f - \mathrm{ht}(o))/2$. By Theorem 3.3.1, that for $\mathrm{III}(E/K_d)^o$ is $d_1 + \cdots + d_{k-1}$. But from the definition,

$$\sum_{j=1}^{k} d_j = \sum_{j=1}^{k} e_{2j-1} = \sum_{j=1}^{k} e_j = f.$$

(Here we use that we are in the complementary case, so k is odd and $e_{j+k} = e_j$.) As noted just after Lemma 2.7.2, $d_k = \mathrm{ht}(o)$, so the total multiplicity of Γ_o/p in $\mathrm{III}(E/K_d)^o$ is $f - \mathrm{ht}(o)$. This completes the proof of part (4).

8.6. *Polynomial interpolation of orders*. Now we prove Theorem 1.1(5). Write $\mathrm{inv}(o)$ for $|o|(f - \mathrm{ht}(o))$ so that $|\mathrm{III}(E/K_d)^o| = p^{\mathrm{inv}(o)}$. Then $|\mathrm{III}(E/K_d)| = p^I$,

where

$$I = \sum_{o \in O_{d,p}} \text{inv}(o).$$

Recall that a word is "good" if it associated to a good base point of an orbit. Let $|\text{Aut}(w)|$ be the number of automorphisms of w, i.e., the number of rotations leaving w invariant. Then since $\text{inv}(o)$ only depends on the word associated to o,

$$I = \sum_{\text{good } w} \frac{|\{i \mid \text{the orbit through } i \text{ is } w\}|}{|\text{Aut}(w)|} \text{inv}(w).$$

Now $\text{inv}(w)/|\text{Aut}(w)|$ is the same for a word w as for the concatenation of several copies of w, so we may take the sum only over full-length words and consider i's whose *pattern* is w, where pattern is defined as in Section 8.1. Then

$$I = \sum_{\text{full length, good } w} \frac{\text{inv}(w)}{|\text{Aut}(w)|} |\{i \mid \text{the pattern of } i \text{ is } w\}|.$$

To finish, we note that by Lemma 8.1.1, $|\{i \mid \text{the pattern of } i \text{ is } w\}|$ is a polynomial in p. This shows that there is a polynomial F_f depending only on f with coefficients in $\mathbb{Z}[1/2]$ such that $I = F_f(p)$. It also shows that when I is not zero, (i.e., when there are words with nonzero invariant, i.e., when $f \geq 3$), the degree of F_f is f.

Here is an example. If $f = 3$, the good words are $u^3 l^3$, $ululul$, and ul. We have $\text{inv}(u^3 l^3) = 0$, $\text{inv}(ululul) = 12$, and $\text{inv}(ul) = 4$. Using Lemma 8.1.1, we find that

$$I = \frac{12}{3} \left(\frac{p-1}{2} \right)^3 = \frac{(p-1)^3}{2}.$$

It looks like an interesting and perhaps difficult problem to give a closed expression for F_f in general.

9. Complements

In the last section of the paper, we give four complementary results. Two of them recover much of the main theorem (specifically, the p-torsion in $\text{III}(E/K_d)$ and $(E(K_d)/V_d)$) using flat rather than crystalline cohomology. This gives a reassuring check on the combinatorial aspects of the main results. The third gives an extension of many of the results of the paper to characteristic $p = 2$. In the fourth, we briefly touch upon a generalization to higher-genus curves.

9.1. p-torsion in $\text{III}(E/K_d)$ via flat cohomology. It is possible to compute the p-Selmer group of E/K_d (and therefore the p-torsion in the Tate–Shafarevich group) using flat cohomology and the methods of [Ulmer 1991]. This yields a

second proof that $\text{III}(E/K_d)$ is trivial if and only if $f \leq 2$, and it provides a check on the crystalline calculation described in the main part of the paper.

We refer to [Ulmer 1991, §1] for the definition of the Selmer group denoted $\text{Sel}(K_d, p_E)$. It sits in an exact sequence

$$0 \rightarrow E(K_d)/pE(K_d) \rightarrow \text{Sel}(K_d, p_E) \rightarrow \text{III}(E/K_d)[p] \rightarrow 0.$$

Proposition 9.1.1. *With p, f, $d = p^f + 1$, and E as in the rest of the paper,*

(1) $\text{Sel}(K_d, p_E)$ *is an $\mathbb{F}_p$-vector space of dimension $(p-1)(p^{f-1}+1)f/2$, and*

(2) $\text{III}(E/K_d) = 0$ *if and only if $f \leq 2$.*

The proof of the proposition will occupy the rest of this section. Note that part (2) follows easily from part (1) since we know that $E(K_d)/pE(K_d)$ is an $\mathbb{F}_p$-vector space of dimension $p^f - 1$.

Let $A = A(E, dx/2y)$ be the Hasse invariant of E. By a simple calculation (see, e.g., [Husemöller 2004, §13, Proposition 3.5]), this is

$$A = \sum_{i=0}^{(p-1)/2} \binom{(p-1)/2}{i}^2 t^i.$$

Let α be a $(p-1)$-th root of A in $\overline{K}$, and let $F_{d,p}$ be the field $K_d(\alpha)$. Then $F_{d,p}$ is a Galois extension of K_d with group $\mathbb{F}_p^\times$. We let $I_{d,p} \rightarrow \mathbb{P}_u^1$ be the corresponding cover of smooth projective curves over $\mathbb{F}_q = \mathbb{F}_p(\mu_d)$. (Here I is for "Igusa".) Then the argument leading to [Ulmer 1991, Theorem 7.12b] yields an isomorphism

$$\text{Sel}(K_d, p_E) \cong H^0(I_{d,p}, \Omega^1_{I_{d,p}})^{\psi^{-1}, \mathscr{C}=0},$$

where $\mathscr{C} = 0$ indicates the kernel of the Cartier operator (i.e., the subspace of exact differentials) and ψ^{-1} denotes the subspace where $\text{Gal}(F_{d,p}/K_d) = \mathbb{F}_p^\times$ acts via the character ψ^{-1} where $\psi : \mathbb{F}_p^\times \rightarrow k^\times$ is the natural inclusion.

(Some of the results of [Ulmer 1991] used just above are stated for $p > 3$, but this is assumed only to guarantee that at places of potentially multiplicative reduction, E obtains multiplicative reduction over an extension of degree prime to p. This is true for the Legendre curve even when $p = 3$.)

Using the covering $I_{d,p} \rightarrow \mathbb{P}_u^1$ (which is ramified exactly where α has zeroes), we find that

$$H^0(I_{d,p}, \Omega^1_{I_{d,p}})^{\psi^{-1}} = \left\{ \frac{f(u)\,du}{\alpha^{p-2}} \,\middle|\, \deg(f) \leq N \right\},$$

where f is a polynomial of degree at most $N = (p-2)(p^f+1)/2 - 2$ when $d = p^f + 1$. (For $d = 1$, there is also ramification at infinity and we have $N = (p-5)/2$.) The crux of the proof is to compute the subspace killed by the Cartier operator.

To that end, we first make some calculations at level $d = 1$, i.e., on the curve $I_{1,p}$. Write

$$\frac{dt}{\alpha^{p-2}} = (f_0^p + tf_1^p + \cdots + t^{p-1}f_{p-1}^p)\,dt,$$

where the $f_i \in F_{1,p} = \mathbb{F}_p(t,\alpha)$. Since $(1/\alpha) = (A/\alpha^p)$, the f_i are all polynomials in t times $1/\alpha^{p-2}$. Note that $\mathscr{C}(t^i\,dt/\alpha^{p-2}) = f_{p-1-i}\,dt$ for $i = 0, \ldots, p-1$.

The key step in the proof of the proposition is the following calculation of dimensions of certain spaces spanned by the f_i. In it, we use angle brackets to denote the $\mathbb{F}_q$-span of the terms within.

Lemma 9.1.2. (1) $\dim_{\mathbb{F}_q}\langle f_{p-1}, f_{p-2}, \ldots, f_{(p+3)/2}\rangle = (p-3)/2$.

(2) *We have equalities and containments*

$$\langle f_{p-1}, \ldots, f_{(p+3)/2}\rangle = \langle f_{p-2}, \ldots, f_{(p+1)/2}\rangle = \cdots = \langle f_{(p-1)/2}, \ldots, f_2\rangle$$
$$\subsetneq \langle f_{(p-1)/2}, \ldots, f_1\rangle = \langle f_{(p-3)/2}, \ldots, f_0\rangle$$

and

$$\langle f_{(p-3)/2}, \ldots, f_0\rangle = \langle f_{(p-5)/2}, \ldots, f_0, tf_{p-1}\rangle = \cdots = \langle f_0, tf_{p-1}, \ldots, tf_{(p+3)/2}\rangle.$$

Proof. Recall that $K = K_1 = \mathbb{F}_p(t)$. First, we note that $E(K)/pE(K) = 0$ by [Ulmer 2014b, Propositions 5.2 and 6.1], and using the BSD formula as in [Ulmer 2014b, §10] shows that $\text{Ш}(E/K) = 0$. Thus, $\text{Sel}(K, p_E) = 0$.

On the other hand, as we noted above, $\text{Sel}(K, p_E)$ is isomorphic to the kernel of the Cartier operator on

$$\left\{\frac{f(t)\,dt}{\alpha^{p-2}} \;\middle|\; \deg(f) \le (p-5)/2\right\}.$$

Since this kernel is trivial, we find that $f_{p-1}, \ldots, f_{(p+3)/2}$ are linearly independent, and this is the first claim of the lemma.

Now set $g_0 = -A' = -dA/dt$ and $g_i = iA - tA'$, and compute that $A'dt = -\alpha^{p-2}\,d\alpha$ so that $d\alpha = g_0\,dt/\alpha^{p-2}$ and $d(t^i\alpha) = t^{i-1}g_i\,dt/\alpha^{p-2}$ for $i \ge 0$. These exact differentials provide relations among the f_i. More precisely, note that g_0 has degree $(p-3)/2$ and nonzero constant term, so $\mathscr{C}(g_0dt/\alpha^{p-2}) = 0$ implies that a linear combination of $f_{p-1}, \ldots, f_{(p+1)/2}$ is zero, and f_{p-1} and $f_{(p+1)/2}$ appear in this relation with nonzero coefficients. This implies that

$$\langle f_{p-1}, \ldots, f_{(p+3)/2}\rangle = \langle f_{p-2}, \ldots, f_{(p+1)/2}\rangle,$$

which is the first equality displayed in part (2) of the lemma.

To obtain the rest of the equalities in that display, we set $h_0 = g_0$ and

$$h_i = \binom{(p-1)/2}{i}^2 t^{i-1} g_i + h_{i-1}$$

$$= \sum_{\ell=1}^{i} \binom{(p-1)/2}{\ell}^2 t^{\ell-1} g_\ell + g_0$$

for $i = 1, \ldots, (p-3)/2$. One checks inductively that h_i has degree $(p-3)/2+i$ and its nonzero term of lowest degree is $-(i+1)\binom{(p-1)/2}{i+1}^2 t^i$. Thus, $\mathscr{C}(h_i\, dt/\alpha^{p-2}) = 0$ gives a relation among $f_{p-1-i}, \ldots, f_{(p+1)/2-i}$, where the coefficients of f_{p-1-i} and $f_{(p+1)/2-i}$ are nonzero. These relations give the desired equalities between spans.

The proper containment in the second line of the first display in part (2) of the lemma is equivalent to saying that f_1 and $\langle f_{(p-1)/2}, \ldots, f_2 \rangle$ are linearly independent. One way to see this is to note that the $\alpha^{p-2} f_i$ are polynomials in t and since the degree of A^{p-2} is congruent to 1 modulo p, $\alpha^{p-2} f_1$ has degree strictly greater than $\alpha^{p-2} f_i$ for $i = 2, \ldots, p-1$. Thus, f_1 and $\langle f_{p-1}, \ldots, f_2 \rangle$ are linearly independent.

To obtain the remaining equalities of part (2), we consider the exact differentials $t^{i-1} g_i\, dt/\alpha^{p-2}$ for $i = (p+1)/2, \ldots, p-1$. In this range, $t^{i-1} g_i$ has degree $(p-3)/2+i$ and lowest term of degree $i-1$. For $i = (p+1)/2$, we get a relation among $f_{(p-1)/2}, \ldots, f_0$ with $f_{(p-1)/2}$ and f_0 appearing, yielding the last equality in the first display of part (2). For $i = (p+3)/2, \ldots, p-1$, we get relations among $f_{p-i}, \ldots, tf_{(3p+1)/2-i}$ with f_{p-i} and $tf_{(3p+1)/2-i}$ appearing, and these relations give the equalities in the second display of part (2). □

We may now compute the rank of the Cartier operator on $H^0(I_{d,p}, \Omega^1_{I_{d,p}})^{\psi^{-1}}$; in other words,

$$R := \dim_{\mathbb{F}_q} \mathscr{C}\left(\left\{ \frac{f(u)\, du}{\alpha^{p-2}} \,\middle|\, \deg(f) \le (p-2)(p^f+1)/2 - 2 \right\}\right).$$

Noting that $u = t/u^{p^f}$ and $du = u^{-p^f}\, dt$, we find that

$$\mathscr{C}(u^{i+pj}\, du/\alpha^{p-2}) = u^{j-(i+1)p^{f-1}} f_i\, du$$

for $0 \le i \le p-1$ and

$$0 \le j \le \begin{cases} \frac{1}{2}(p-3)p^{f-1} + \frac{1}{2}(p^{f-1}-1) & \text{if } i \le p-3, \\ \frac{1}{2}(p-3)p^{f-1} + \frac{1}{2}(p^{f-1}-3) & \text{if } i = p-2, p-1. \end{cases}$$

This implies that the image of $\mathscr{C}$ will be spanned by spaces of the form $u^e \langle f_a, \ldots, f_b \rangle$. To compute the dimension, we observe that if $e_1, \ldots, e_\ell$ are integers pairwise noncongruent modulo d and if $V_1, \ldots V_\ell$ are $\mathbb{F}_q$-vector spaces spanned by subsets of $\{t^j f_i \mid 0 \le i \le p-1,\ j \in \mathbb{Z}\}$, then the subspaces $u^{e_i} V_i$ of $F_{d,p}$ are linearly independent over $\mathbb{F}_q$. This plus the information in Lemma 9.1.2 suffices to compute R.

An elaborate and somewhat unpleasant exercise in bookkeeping that we omit leads to

$$R = \frac{(p-3)}{2}\frac{(p-1)}{2}p^{f-1} + \frac{(p-3)}{2}\frac{(p^f+3)}{2} + \frac{p-1}{2}(p^{f-1}-1),$$

which in turn implies that

$$\dim_{\mathbb{F}_q}\ker(\mathscr{C}) = N+1-R = \frac{(p-1)}{2}\frac{(p^{f-1}+1)}{2}.$$

Since $[\mathbb{F}_q : \mathbb{F}_p] = 2f$, this completes the proof of Proposition 9.1.1.

The analysis above yields quite a bit more information about $\mathrm{Sel}(K, p_E)$:

Corollary 9.1.3. *The differentials*

$$\omega_{i,j} = u^{pj-ip^f}h_i(t)\,du/\alpha^{p-2} = u^{i+pj}t^{-i}h_i(t)\,du/\alpha^{p-2}$$

for $0 \le i \le (p-3)/2$ and $0 \le j \le (p^{f-1}-1)/2$ are regular and exact, and they give an $\mathbb{F}_q$-basis for

$$\mathrm{Sel}(K, p_E) \cong H^0(I_{p,d}, \Omega^1_{I_{p,d}})^{\psi^{-1}, \mathscr{C}=0}.$$

Proof. The proof of Proposition 9.1.1 shows that the displayed differentials are exact and lie in the ψ^{-1} eigenspace. They are obviously linearly independent, and since the number of them is the dimension of $\mathrm{Sel}(K, p_E)$ over $\mathbb{F}_q$, they form an $\mathbb{F}_q$-basis. $\qquad\square$

We can also deduce results on the structure of $\mathrm{Sel}(K, p_E)$ as a module over $\mathbb{F}_p[G]$:

Corollary 9.1.4. *If $o \in O$ is an orbit whose pattern is $u^{e_1}l^{e_2}\cdots u^{e_k}$, then the multiplicity of Γ_o/p in $\mathrm{Sel}(K, p_E)$ is k, and its multiplicity in $\text{Ш}(E/K_d)$ is $k-1$.*

Proof. The previous corollary shows that as an $\mathbb{F}_p[G]$-module, $\mathrm{Sel}(K_d, p_E)$ is the direct sum

$$\bigoplus_{\substack{0 \le i \le (p-3)/2 \\ 0 \le j \le (p^{f-1}-1)/2}} \mathbb{F}_q u^{i+pj}.$$

If $\ell \in o$, then by Proposition 2.8.1(5), $\mathbb{F}_q u^\ell \cong (\Gamma_o/p)^{2f/|o|}$.

Now an orbit o appears in the discussion above as many times as there are $\ell \in o$ that can be written $\ell = 1+i+pj$ with $0 \le i \le (p-3)/2$ and $0 \le j \le (p^{f-1}-1)/2$. Writing $\ell = \sum_{k=1}^{f} i_k p^{k-1}$ as in Section 8.1, we see that ℓ can be written $\ell = 1+i+pj$ with i and j "small" in the sense above if and only if the word associated to ℓ begins and ends with the letter u. Thus, if the word of o is $u^{e_1}\cdots u^{e_{k'}}l^{e_1}\cdots l^{e_{k'}}$, then the number of times o arises is k'.

To finish, we note that the pattern of the standard base point of o is the first half of $w(o)^{2f/|o|}$, and written in exponential form, this has $k = k'(2f/|o|)$ runs of u's. Thus, Γ_o/p appears k times in $\mathrm{Sel}(K_d, p_E)$. This proves our claim about $\mathrm{Sel}(K_d, p_E)$.

The claim about $\mathrm{III}(E/K_d)$ follows from the fact that as an $\mathbb{F}_p[G]$-module, $E(K_d)/p$ is the direct sum of all Γ_o/p with $o \in O$ each taken with multiplicity 1. (This follows immediately from Remark 2.8.3.) $\qquad\square$

We need one more result from [Ulmer 1991]. To state it, recall that the Selmer group for the isogeny $\mathrm{Fr} : E \to E^{(p)}$ over $F_{p,d}$ is naturally a subgroup of

$$F_{p,d}^{\times}/F_{p,d}^{\times p} \cong \Omega_{\log}^1(F_{p,d}),$$

where the latter is the space of meromorphic, logarithmic differentials on $I_{p,d}$. In [Ulmer 1991, §5], we defined a logarithmic differential dq/q attached to $E/F_{p,d}$ that depends only on the choice of a $(p-1)$-th root α of A (or, what amounts to the same thing, a nontrivial point of order p in $E^{(p)}(F_{p,d})$).

Lemma 9.1.5. *We have an equality*

$$\frac{dq}{q} = \frac{\alpha^2 \, du}{u(t-1)} = \frac{\alpha^2 \, du}{u(u^d - 1)}$$

of meromorphic differentials on $I_{p,d}$ and a calculation of Selmer groups:

$$\mathrm{Sel}(F_{p,d}, \mathrm{Fr}_E) = \mathbb{F}_p \frac{dq}{q}.$$

Proof. The same argument as in [Ulmer 1991, Theorem 7.6] shows that the Selmer group $\mathrm{Sel}(F_{p,d}, \mathrm{Fr}_E)$ is isomorphic to the group of logarithmic differentials with simple poles at places where E has multiplicative reduction and zeros of order p at places where E has supersingular reduction. An easy exercise using the covering $I_{p,d} \to \mathbb{P}_u^1$ shows that the only such differentials are the $\mathbb{F}_p$-multiples of $\alpha^2 du/u(t-1)$. Since dq/q lies in this Selmer group (as the image of the chosen point of order p on $E^{(p)}(F_{p,d})$), it is a nonzero multiple of $\alpha^2 du/u(t-1)$. Which multiple it is will not be material for what follows, so we omit the check that dq/q is $\alpha^2 du/u(t-1)$ on the nose. $\qquad\square$

9.2. *p-torsion in $E(K_d)/V_d$ via flat cohomology.* The results of [Ulmer 1991; Broumas 1997] also afford good control on the p-torsion in $E(K_d)/V_d$. We continue with the notation of the previous subsection. In particular, we assume that $d = p^f + 1$.

We state our result in terms of the decomposition of $E(K_d)/V_d$ as a module over $\mathbb{Z}_p[G]$ (in fact over $\mathbb{F}_p[G]$ since we are concerned only with the p-torsion).

Proposition 9.2.1. *We have*

$$\ker(p : E(K_d)/V_d \to E(K_d)/V_d)^o = \begin{cases} \Gamma_o/p & \text{if the word of } o \text{ is not } u^f l^f, \\ 0 & \text{if the word of } o \text{ is } u^f l^f. \end{cases}$$

Proof. First, we note that an easy application of the snake lemma shows that

$$\ker(p : E(K_d)/V_d \to E(K_d)/V_d) \cong \ker(V_d/p \to E(K_d)/p).$$

Moreover, we have an injection

$$E(K_d)/p \hookrightarrow \mathrm{Sel}(K_d, p_E), \qquad (9.2.1)$$

so it will suffice to compute the kernel of the composed map $V_d/p \to \mathrm{Sel}(K_d, p_E)$. We will do this by using Broumas' wonderful formula for (9.2.1) and the explicit calculation of $\mathrm{Sel}(K_d, p_E)$ in the preceding subsection.

Recall that V_d/p is isomorphic as an $\mathbb{F}_p[G]$-module to $\bigoplus_{o \in O} \Gamma_o/p$ and that this $\mathbb{F}_p[G]$-module is cyclic, generated by the point $P(u) = (u, u(u+1)^{d/2})$ defined in [Ulmer 2014b, §3].

As noted in the previous section, we have

$$\mathrm{Sel}(K_d, p_E) \cong H^0(I_{p,d}, \Omega^1_{i_{p,d}})^{\mathscr{C}=0, \, \psi^{-1}}.$$

Using [Ulmer 1991, Proposition 5.3], the space of exact differentials above can be identified with a subgroup of the additive group of K_d via the map $\omega \mapsto \alpha^p \omega/(dq/q)$, where dq/q is the differential computed in Lemma 9.1.5 and α is a root of $\alpha^{p-1} = A$. The main theorem of [Broumas 1997] gives an explicit formula for the composition

$$\mu : E(K_d) \to \mathrm{Sel}(K_d, p_E) \to K_d.$$

To state the result, write

$$(x(x+1)(x+t))^{(p-1)/2} = x^p M(x) + Ax^{p-1} + \text{lower-order terms}$$

and let $\wp_A(z) = z^p - Az$. Then (after a considerable amount of boiling down), Broumas' formula says

$$\mu(P(u)) = u(u+1)^{(p^f+1)/2} M(u) - \wp_A(u(u+1)^{(p^f-1)/2}).$$

(We note that there is a typo in [Broumas 1997] in the case $p = 3$; Namely, in (36) on page 140, "$2\mathscr{D}a_2/a_2 + \mathscr{D}a_6/a_6$" should be replaced with "$(2\mathscr{D}a_2/a_2 + \mathscr{D}a_6/a_6)x$".)

The last displayed quantity is an element of the polynomial ring $\mathbb{F}_q[u]$, and we are going to compute it modulo the ideal generated by $t = u^d$.

To see that this will suffice for our purposes, recall from Corollary 9.1.3 the exact differentials $\omega_{i,j}$ giving an $\mathbb{F}_q$-basis for the Selmer group. Using Lemma 9.1.5, we find that

$$f_{i,j} := \alpha^p \omega_{i,j}/(dq/q) = u^{1+i+pj} t^{-i} h_i(t)(t-1)$$

for $0 \le i \le (p-3)/2$ and $0 \le j \le (p^{f-1}-1)/2$. Thus, in order to write $\mu(P(u))$ in terms of the $f_{i,j}$, it suffices to know $\mu(P(u))$ modulo t.

Straightforward computation from the definition shows that

$$M(u) \equiv \frac{(u+1)^{(p-1)/2} - 1}{u} \quad \text{and} \quad A \equiv 1 \pmod{t \mathbb{F}_q[u]}.$$

Thus,

$$\mu(P(u)) \equiv (u+1)^{(p^f+p)/2} - (u+1)^{(p^f+1)/2} - u^p(u^p+1)^{(p^f-1)/2} + u(u+1)^{(p^f-1)/2}$$

$$= (u+1)^{(p^f-p)/2}\big((u+1)^p - (u+1)^{(p+1)/2}$$
$$- u^p(u^p+1)^{(p^f-p^{f-1})/2} + u(u+1)^{(p-1)/2}\big)$$

$$\equiv (u+1)^{(p^f-p)/2}(1-(u+1)^{(p-1)/2})$$

$$= -u\left(\sum_{j=0}^{(p-3)/2}\binom{(p-1)/2}{i+1}u^i\right)(1+u^p)^{(p-1)/2}\cdots(1+u^{p^{f-1}})^{(p-1)/2}.$$

(To pass from the second line to the third, note that the sum of the first and third terms inside the large parentheses is congruent to 1 modulo t.)

The last expression makes it clear that $\mu(P(u))$ (mod $t\mathbb{F}_q[u]$) is the sum of terms cu^ℓ where u^ℓ appears with nonzero coefficient if and only if $\ell = 1 + \sum i_k p^{k-1}$ with $i_1 \le (p-3)/2$ and $i_k \le (p-1)/2$ for $2 \le k \le f$. It follows that $\mu(P(u))$ is a linear combination (with nonvanishing coefficients) of the $f_{i,j}$ where $\ell = 1 + i + pj$ satisfies the same condition.

Now by Proposition 2.8.1(5), the $\mathbb{F}_p[G]$-modules $\mathbb{F}_q u^\ell$ with ℓ satisfying the conditions just above are pairwise nonisomorphic. Thus, the $\mathbb{F}_p[G]$-submodule of the Selmer group generated by $\mu(P(u))$ is the direct sum of the corresponding Γ_o/p. The orbits in question are precisely those with word $u^f l^f$, and this shows that the image of $V_d/p \to E(K_d)/p$ is isomorphic to

$$\bigoplus_{\substack{o \in O \\ w(o) = u^f l^f}} \Gamma_o/p.$$

The kernel is thus the sum of the Γ_o/p, where o runs through orbits with words not equal to $u^f l^f$.   □

The proposition allows us to recover large parts of Theorem 1.1: it shows that $(E(K_d)/V_d$ is nontrivial if and only if $f > 2$, and together with Corollary 9.1.4, it shows that $\text{Ш}(E/K_d)$ is not isomorphic to $(E(K_d)/V_d)^2$ as an abelian group if $f > 4$.

9.3. *An extension to $p = 2$.* In this subsection, we explain how the main results of the paper can be extended to the case where $p = 2$.

To that end, let p be an arbitrary prime number and let E' be the elliptic curve over $K' = \mathbb{F}_p(t')$ defined by

$$y^2 + xy + t'y = x^3 + t'x^2.$$

As explained in [Ulmer 2014b, §11; Conceição et al. 2014, §11], if $p > 2$ and we identify K' and K by sending t' to $t/16$, then E and E' are 2-isogenous. Moreover,

for $d = p^f + 1$, the fields $K'_d = \mathbb{F}_p(\mu_d, t'^{1/d})$ and $K_d = \mathbb{F}_p(\mu_d, t^{1/d})$ can be identified as extensions of K. Having done so, one finds that the subgroup $V'_d \subset E'(K'_d)$ defined in [Ulmer 2013, Remark 8.10(3)] is carried over to $V_d \subset E(K_d)$. It follows that Theorem 1.1 and its refinements in Section 3 hold for $E'(K'_d)/V'_d$ and $\text{Ш}(E'/K'_d)$.

Now the equation above also defines an elliptic curve when $p = 2$. Moreover, the Néron model of E'/K'_d is dominated by a product of curves (two copies of the curve $\mathscr{C}'$ over $\mathbb{F}_p(\mu_d)$ defined by $z^d = x(1-x)$); see [Conceição et al. 2014, Theorem 11.2(5)]. Thus, the methods of this paper may be used to compute $E'(K'_d)/V'_d$ and $\text{Ш}(E'/K'_d)$ as modules over $\mathbb{Z}_p[\text{Gal}(K'_d/K)]$. Most of the results have the same form, and the proofs are mostly parallel, so we will briefly discuss some of the differences and then state the results.

The analogue of the geometric analysis leading to Theorem 4.2 gives an isomorphism

$$(E'(K'_d)/\text{tor}) \otimes \mathbb{Z}[1/d] \xrightarrow{\sim} (\text{NS}'(\mathscr{C} \times \mathscr{C}) \otimes \mathbb{Z}[1/d])^{\mu_d},$$

where the μ_d in the exponent is acting antidiagonally. (In fact, the most natural way to state this would be with the arrow going the other way and with the target being the subgroup of $E'(K'_d)$ generated by the point in [Ulmer 2013, Theorem 8.1(2)] and its Galois conjugates. This subgroup is free of rank $d - 1$ and is a complement to the torsion subgroup.) The analogue of the isomorphism of Tate–Shafarevich and Brauer groups in Theorem 4.2(2) goes through for E' without change.

The analysis of the arithmetic of a product in Section 5 was done there also for $p = 2$, and the description of the cohomology of $\mathscr{C}$ in Section 6 works for $\mathscr{C}'$ as well with very minor changes. The p-adic exercises in Section 7 also work essentially unchanged.

Altogether, one finds that the obvious analogues of Theorem 1.1 parts (1) through (4) hold for E'/K'_d. Similar analogues hold for the refined Theorems 3.2.1 and 3.3.1.

There are a few differences to report as well. For example, part (5) of Theorem 1.1 does not extend to $p = 2$. Indeed, the polynomial appearing there does not even take integral values at $p = 2$. The correct statement can be deduced from the proof in Section 8.6 by noting that the number of elements in $\mathbb{Z}/d\mathbb{Z} \setminus \{0\}$ with a given pattern is 1 (rather than $(p - 1)^a (p + 1)^b / 2^f$ as in Lemma 8.1.1).

The results of Sections 9.1 and 9.2 also extend to E'. One finds that the order of $\text{Sel}(K'_d, p_{E'})$ is $2^{f-1} f + 1$. The refined results of Corollary 9.1.4 and Proposition 9.2.1 hold as stated. However, the details of the 2-descent have a different flavor because E' has a 2-torsion point over K' so the kernel of p is the direct sum of the kernels of Frobenius and Verschiebung and the differential dq/q is zero. We leave the details as an exercise for the interested reader.

9.4. *Higher genus.* Let p be a prime number and r and d integers relatively prime to p, and consider the curve X defined by

$$y^r = x^{r-1}(x+1)(x+t)$$

over $\mathbb{F}_p(t)$ and its extensions $\mathbb{F}_q(u)$ with $u^d = t$. The genus of X is $r-1$, and its Jacobian J has interesting arithmetic over $\mathbb{F}_q(u)$ for many values of d.

For simplicity, we will only discuss the case where r divides d, $d = p^f + 1$, and $\mathbb{F}_q = \mathbb{F}_p(\mu_d)$. We write K_d for $\mathbb{F}_q(u)$. In [Berger et al. ≥ 2015], explicit divisors are given on X whose classes in $J(K_d)$ generate subgroup V_d of rank $(r-1)(d-2)$ and finite, p-power index. Moreover, it is shown there that we have a class-number formula

$$|\text{Ш}(J/K_d)| = [J(K_d) : V_d]^2.$$

Most of the results of this paper extend to this situation and give an explicit calculation of $\text{Ш}(J/K_d)$ and $J(K_d)/V_d$ as modules over the group ring $\mathbb{Z}_p[G]$, where $G = \mu_d \rtimes \text{Gal}(\mathbb{F}_q/\mathbb{F}_p)$.

Indeed, we saw in Section 4.6 that the minimal regular model $\mathscr{X} \to \mathbb{P}^1_u$ of X/K_d is birational to the quotient of a product of curves by a finite group. The product is $\mathscr{S} = \mathscr{C} \times \mathscr{C}$, where $\mathscr{C}$ is the smooth proper curve over $\mathbb{F}_q$ defined by $z^d = x^r - 1$. We deduce from this a connection between the Mordell–Weil and Tate–Shafarevich groups of J and the Néron–Severi and Brauer groups of $\mathscr{S}$ as at the end of Section 4.6. These groups are described in crystalline terms in Section 5.

As we saw in Section 6.5, the crystalline cohomology of $\mathscr{C}$ breaks up into lines indexed by the set

$$S = \{(i, j) \in (\mathbb{Z}/d\mathbb{Z}) \times (\mathbb{Z}/r\mathbb{Z}) \mid i \neq 0, \ j \neq 0, \ \langle i/d \rangle + \langle j/r \rangle \neq 1\}.$$

The subspace $H^0(\mathscr{C}/\mathbb{Z}_p, \Omega^1_{\mathscr{C}/\mathbb{Z}_p})$ is generated by the lines indexed by (i, j) with $\langle i/d \rangle + \langle j/r \rangle < 1$. Calling this subset A and letting $B = S \setminus A$, we may use A and B to define words associated to orbits of $\langle p \rangle$ acting diagonally on S and to define a notion of balanced as discussed at the end of Section 6.5.

The p-adic exercises of Section 7 go through essentially unchanged, and interpreting "balanced" as above, we find that Theorem 1.1 parts (1) through (4) and the refined results in Theorems 3.1.1, 3.2.1, and 3.3.1 hold as stated. An interpolation result, as in part (5) of Theorem 1.1, also holds with a polynomial F that depends on r and f but not on p.

Exploring the arithmetic of J for other values of r and d looks like an interesting project. In particular, one may ask about other systematic sources of nontorsion points on J as in [Conceição et al. 2014] and about the relative abundance or scarcity of balanced rays for fixed p and varying r and d as in [Pomerance and Ulmer 2013].

Acknowledgment

It is a pleasure to thank the anonymous referee for a very careful reading of the paper and several valuable suggestions.

References

[Artin 1974] M. Artin, "Supersingular $K3$ surfaces", *Ann. Sci. École Norm. Sup.* (4) **7** (1974), 543–567. MR 51 #8116 Zbl 0322.14014

[Berger et al. ≥ 2015] L. Berger, C. Hall, R. Pannekoek, J. Park, R. Pries, S. Sharif, A. Silverberg, and D. Ulmer, "Explicit unbounded ranks for a family of Jacobians over global function fields", in preparation.

[Broumas 1997] A. Broumas, "Effective p-descent", *Compositio Math.* **107**:2 (1997), 125–141. MR 98h:11070 Zbl 1035.14006

[Conceição et al. 2014] R. P. Conceição, C. Hall, and D. Ulmer, "Explicit points on the Legendre curve II", *Math. Res. Lett.* **21**:2 (2014), 261–280. MR 3247055 Zbl 06350080

[Dummigan 1995] N. Dummigan, "The determinants of certain Mordell–Weil lattices", *Amer. J. Math.* **117**:6 (1995), 1409–1429. MR 97a:11083 Zbl 0914.11033

[Dummigan 1999] N. Dummigan, "Complete p-descent for Jacobians of Hermitian curves", *Compositio Math.* **119**:2 (1999), 111–132. MR 2001e:11066 Zbl 0985.11028

[Gras 1977] G. Gras, "Classes d'idéaux des corps abéliens et nombres de Bernoulli généralisés", *Ann. Inst. Fourier* (*Grenoble*) **27**:1 (1977), 1–66. MR 56 #8534 Zbl 0336.12004

[Grothendieck 1961] A. Grothendieck, "Éléments de géométrie algébrique, III: Étude cohomologique des faisceaux cohérents, I", *Inst. Hautes Études Sci. Publ. Math.* 11 (1961), 167. MR 29 #1209 Zbl 0118.36206

[Grothendieck 1968a] A. Grothendieck, "Le groupe de Brauer, II: Théorie cohomologique", pp. 67–87 in *Dix exposés sur la cohomologie des schémas*, North-Holland, Amsterdam, 1968. MR 39 #5586b Zbl 0198.25803

[Grothendieck 1968b] A. Grothendieck, "Le groupe de Brauer, III: Exemples et compléments", pp. 88–188 in *Dix exposés sur la cohomologie des schémas*, North-Holland, Amsterdam, 1968. MR 39 #5586c Zbl 0198.25901

[Husemöller 2004] D. Husemöller, *Elliptic curves*, 2nd ed., Graduate Texts in Mathematics **111**, Springer, New York, 2004. MR 2005a:11078 Zbl 1040.11043

[Illusie 1979] L. Illusie, "Complexe de de Rham–Witt et cohomologie cristalline", *Ann. Sci. École Norm. Sup.* (4) **12**:4 (1979), 501–661. MR 82d:14013 Zbl 0436.14007

[Ireland and Rosen 1990] K. Ireland and M. Rosen, *A classical introduction to modern number theory*, 2nd ed., Graduate Texts in Mathematics **84**, Springer, New York, 1990. MR 92e:11001 Zbl 0712.11001

[Mazur 1972] B. Mazur, "Frobenius and the Hodge filtration", *Bull. Amer. Math. Soc.* **78** (1972), 653–667. MR 48 #8507 Zbl 0258.14006

[Mazur 1973] B. Mazur, "Frobenius and the Hodge filtration (estimates)", *Ann. of Math.* (2) **98** (1973), 58–95. MR 48 #297 Zbl 0261.14005

[Mazur and Messing 1974] B. Mazur and W. Messing, *Universal extensions and one dimensional crystalline cohomology*, Lecture Notes in Mathematics **370**, Springer, Berlin, 1974. MR 51 #10350 Zbl 0301.14016

[Mazur and Wiles 1984] B. Mazur and A. Wiles, "Class fields of abelian extensions of **Q**", *Invent. Math.* **76**:2 (1984), 179–330. MR 85m:11069 Zbl 0545.12005

[Milne 1975] J. S. Milne, "On a conjecture of Artin and Tate", *Ann. of Math.* (2) **102**:3 (1975), 517–533. MR 54 #2659 Zbl 0343.14005

[Milne 1980] J. S. Milne, *Étale cohomology*, Princeton Mathematical Series **33**, Princeton University Press, 1980. MR 81j:14002 Zbl 0433.14012

[Pomerance and Ulmer 2013] C. Pomerance and D. Ulmer, "On balanced subgroups of the multiplicative group", pp. 253–270 in *Number theory and related fields* (Newcastle, Australia, 2012), edited by J. M. Borwein et al., Springer Proc. Math. Stat. **43**, Springer, New York, 2013. MR 3081046 Zbl 06190327

[Shioda 1991] T. Shioda, "Mordell–Weil lattices and sphere packings", *Amer. J. Math.* **113**:5 (1991), 931–948. MR 92m:11066 Zbl 0756.14010

[Ulmer 1991] D. L. Ulmer, "p-descent in characteristic p", *Duke Math. J.* **62**:2 (1991), 237–265. MR 92i:11068 Zbl 0742.14028

[Ulmer 2011] D. Ulmer, "Elliptic curves over function fields", pp. 211–280 in *Arithmetic of L-functions* (Park City, UT, 2009), edited by C. Popescu et al., IAS/Park City Math. Ser. **18**, Amer. Math. Soc., Providence, RI, 2011. MR 2882692 Zbl 05995056

[Ulmer 2013] D. Ulmer, "On Mordell–Weil groups of Jacobians over function fields", *J. Inst. Math. Jussieu* **12**:1 (2013), 1–29. MR 3001733 Zbl 06124083

[Ulmer 2014a] D. Ulmer, "Curves and Jacobians over function fields", pp. 281–337 in *Arithmetic geometry over global function fields*, edited by F. Bars et al., Springer, Basel, 2014.

[Ulmer 2014b] D. Ulmer, "Explicit points on the Legendre curve", *J. Number Theory* **136** (2014), 165–194. MR 3145329 Zbl 1297.11055

[Waterhouse and Milne 1971] W. C. Waterhouse and J. S. Milne, "Abelian varieties over finite fields", pp. 53–64 in *1969 Number Theory Institute* (Stony Brook, NY, 1969), Proc. Sympos. Pure Math. **20**, Amer. Math. Soc., Providence, RI, 1971. MR 47 #3397 Zbl 0216.33102

ulmer@math.gatech.edu   *School of Mathematics, Georgia Institute of Technology, 686 Cherry Street, Atlanta, GA 30332, United States*

Explicit Gross–Zagier and Waldspurger formulae

Li Cai, Jie Shu and Ye Tian

We give an explicit Gross–Zagier formula which relates the height of an explicitly constructed Heegner point to the derivative central value of a Rankin L-series. An explicit form of the Waldspurger formula is also given.

1. Main results

1A. *Introduction.* The Gross–Zagier formula and the Waldspurger formula are probably the two most important analytic tools known at present for studying the still largely unproven conjecture of Birch and Swinnerton-Dyer. Much work has already been done on both formulae. In particular, the recent book by Yuan, Zhang and Zhang [Yuan et al. 2013] establishes what is probably the most general case

of the Gross–Zagier formula. Nevertheless, when it comes to actual applications to the arithmetic of elliptic curves or abelian varieties, one very often needs a more explicit form of the Gross–Zagier formula than that given in [Yuan et al. 2013], and similarly a more explicit form of the Waldspurger formula than one finds in the existing literature. This is clearly illustrated, for example, by the papers [Bertolini and Darmon 1997; Tian 2014; Tian et al. 2013; Coates et al. 2014]. Our aim here is to establish what we believe are the most general explicit versions of both formulae, namely Theorems 1.5 and 1.6 for the Gross–Zagier formula, and Theorems 1.8 and 1.9 for the Waldspurger formula. Our methods have been directly inspired by [Yuan et al. 2013], and also the ideas of [Gross 1988] and [Gross and Prasad 1991].

In the remainder of this introduction, we would like to explain in detail our explicit formulae in the simplest and most important case of modular forms over $\mathbb{Q}$. Let ϕ be a newform of weight 2, level $\Gamma_0(N)$, with Fourier expansion $\phi = \sum_{n=1}^{\infty} a_n q^n$ normalized so that $a_1 = 1$. Let K be an imaginary quadratic field of discriminant D and χ a primitive ring class character over K of conductor c, i.e., a character of $\mathrm{Pic}(\mathbb{O}_c)$, where $\mathbb{O}_c$ is the order $\mathbb{Z} + c\mathbb{O}_K$ of K. Assume the Heegner conditions (first introduced by Birch in a special case):

(1) $(c, N) = 1$, no prime divisor p of N is inert in K, and p must split in K if $p^2 | N$.

(2) $\chi([\mathfrak{p}]) \neq a_p$ for any prime $p|(N, D)$, where $\mathfrak{p}$ is the unique prime ideal of $\mathbb{O}_K$ above p and $[\mathfrak{p}]$ is its class in $\mathrm{Pic}(\mathbb{O}_c)$.

Let $L(s, \phi, \chi)$ be the Rankin L-series of ϕ and the theta series ϕ_χ associated to χ (without the local Euler factor at infinity). It follows from the Heegner conditions that the sign in the functional equation of $L(s, \phi, \chi)$ is -1. Let $(\phi, \phi)_{\Gamma_0(N)}$ denote the Petersson norm of ϕ:

$$(\phi, \phi)_{\Gamma_0(N)} = \iint_{\Gamma_0(N)\backslash \mathcal{H}} |\phi(z)|^2 \, dx \, dy, \quad z = x + iy.$$

Let $X_0(N)$ be the modular curve over $\mathbb{Q}$ whose $\mathbb{C}$-points parametrize isogenies $E_1 \to E_2$ between elliptic curves over $\mathbb{C}$ whose kernels are cyclic of order N. By the Heegner conditions, there exists a proper ideal $\mathcal{N}$ of $\mathbb{O}_c$ such that $\mathbb{O}_c / \mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}$. For any proper ideal $\mathfrak{a}$ of $\mathbb{O}_c$, let $P_\mathfrak{a} \in X_0(N)$ be the point representing the isogeny $\mathbb{C}/\mathfrak{a} \to \mathbb{C}/\mathfrak{a}\mathcal{N}^{-1}$, which is defined over the ring class field H_c over K of conductor c and only depends on the class of $\mathfrak{a}$ in $\mathrm{Pic}(\mathbb{O}_c)$. Let $J_0(N)$ be the Jacobian of $X_0(N)$. Writing ∞ for the cusp at infinity on $X_0(N)$, we have the morphism from $X_0(N)$ to $J_0(N)$ over $\mathbb{Q}$ given by $P \mapsto [P - \infty]$. Let P_χ be the point

$$P_\chi = \sum_{[\mathfrak{a}] \in \mathrm{Pic}(\mathbb{O}_c)} [P_\mathfrak{a} - \infty] \otimes \chi([\mathfrak{a}]) \in J_0(N)(H_c) \otimes_{\mathbb{Z}} \mathbb{C}$$

and write P_χ^ϕ for the ϕ-isotypical component of P_χ.

The following theorem was proved in the case $c = 1$ in the celebrated work by Gross and Zagier [1986], and follows immediately from the general explicit Gross–Zagier formula in Theorem 1.5 (see Special case 2, and the Example following).

Theorem 1.1. *Let ϕ, χ be as above satisfying the Heegner conditions* (1) *and* (2). *Then*

$$L'(1, \phi, \chi) = 2^{-\mu(N,D)} \cdot \frac{8\pi^2 (\phi, \phi)_{\Gamma_0(N)}}{u^2 \sqrt{|Dc^2|}} \cdot \hat{h}_K(P_\chi^\phi),$$

where $\mu(N, D)$ is the number of prime factors of the greatest common divisor of N and D, $u = [\mathbb{O}_c^\times : \mathbb{Z}^\times]$ is half of the number of roots of unity in $\mathbb{O}_c$, and $\hat{h}_K$ is the Néron–Tate height on $J_0(N)$ over K. In particular, if ϕ is associated to an elliptic curve E over $\mathbb{Q}$ via Eichler–Shimura theory and $f : X_0(N) \to E$ is a modular parametrization mapping the cusp ∞ to the identity $O \in E$, then the Heegner divisor $P_\chi^0(f) := \sum_{[\mathfrak{a}] \in \mathrm{Pic}(\mathbb{O}_c)} f(P_\mathfrak{a}) \otimes \chi([\mathfrak{a}]) \in E(H_c)_\mathbb{C}$ satisfies

$$L'(1, E, \chi) = 2^{-\mu(N,D)} \cdot \frac{8\pi^2 (\phi, \phi)_{\Gamma_0(N)}}{u^2 \sqrt{|Dc^2|}} \cdot \frac{\hat{h}_K(P_\chi^0(f))}{\deg f},$$

where $\hat{h}_K$ is the Néron–Tate height on E over K and $\deg f$ is the degree of the morphism f.

Comparing the above Gross–Zagier formula with the conjecture of Birch and Swinnerton-Dyer for $L(E/K, s)$, we immediately are led to:

Conjecture. *Let E be an elliptic curve defined over $\mathbb{Q}$ of conductor N and let K be an imaginary quadratic field of discriminant D such that for any prime ℓ dividing N, either ℓ splits in K, or ℓ is ramified in K and E has nonsplit semistable reduction at ℓ. Let $f : X_0(N) \to E$ be a modular parametrization mapping ∞ to O. Let $\mathcal{N} \subset \mathbb{O}_K$ be any ideal with $\mathbb{O}_K/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}$, let $P \in X_0(N)(H_K)$ be the point representing the isogeny $(\mathbb{C}/\mathbb{O}_K \to \mathbb{C}/\mathcal{N}^{-1})$, and write $P_K(f) := \mathrm{Tr}_{H_K/K} f(P) \in E(K)$. Assume $P_K(f)$ is not torsion. Then*

$$\sqrt{\#\mathrm{III}(E/K)} = 2^{-\mu(N,D)} \cdot \frac{[E(K) : \mathbb{Z}P_K(f)]}{C \cdot [\mathbb{O}_K^\times : \mathbb{Z}^\times] \cdot \prod_{\ell | N/(N,D)} m_\ell},$$

where $m_\ell = [E(\mathbb{Q}_\ell) : E^0(\mathbb{Q}_\ell)]$ and C is the positive integer such that if ω_0 is a Néron differential on E then $f^* \omega_0 = \pm C \cdot 2\pi i \phi(z) \, dz$.

We next state our explicit Waldspurger formula over $\mathbb{Q}$. Let $\phi = \sum_{n=1}^\infty a_n q^n$ in $S_2(\Gamma_0(N))$ be a newform of weight 2 and level $\Gamma_0(N)$. Let K be an imaginary quadratic field and $\chi : \mathrm{Gal}(H_c/K) \to \mathbb{C}^\times$ a character of conductor c. Assume the conditions:

(i) $(c, N) = 1$ and, if $p|(N, D)$, then $p^2 \nmid N$.

(ii) Let S be the set of places $p|N\infty$ nonsplit in K such that, for a finite prime p, $\mathrm{ord}_p(N)$ is odd if p is inert in K, and $\chi([\mathfrak{p}]) = a_p$ if p is ramified in K. Then S has even cardinality.

It follows that the sign of the functional equation of the Rankin L-series $L(s, \phi, \chi)$ is $+1$. Let B be the quaternion algebra over $\mathbb{Q}$ ramified exactly at places in S. Note that condition (ii) implies that there exists an embedding of K into B, which we fix once and for all. Let $R \subset B$ be an order of discriminant N with $R \cap K = \mathbb{O}_c$. Such an order exists and is unique up to conjugation by $\widehat{K}^\times$. Here, for an abelian group M, we define $\widehat{M} = M \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}}$, where $\widehat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$ with p running over all primes. By the reduction theory of definite quadratic forms, the coset $X := B^\times \backslash \widehat{B}^\times / \widehat{R}^\times$ is finite, say of order n. Let $g_1, \ldots, g_n$ in $\widehat{B}^\times$ represent the distinct classes $[g_1], \ldots, [g_n]$. For each $i = 1, \ldots, n$, let $\Gamma_i = (B^\times \cap g_i \widehat{R}^\times g_i^{-1})/\{\pm 1\}$. Then Γ_i is a finite group, and we denote its order by w_i. Let $\mathbb{Z}[X]$ denote the free $\mathbb{Z}$-module of formal sums $\sum_{i=1}^n a_i[g_i]$ with $a_i \in \mathbb{Z}$, and define a height pairing on $\mathbb{Z}[X]$ by

$$\left\langle \sum a_i[g_i], \sum b_i[g_i] \right\rangle = \sum_{i=1}^n a_i b_i w_i,$$

which is positive definite on $\mathbb{R}[X] := \mathbb{Z}[X] \otimes_{\mathbb{Z}} \mathbb{R}$ and has a natural Hermitian extension to $\mathbb{C}[X] := \mathbb{Z}[X] \otimes_{\mathbb{Z}} \mathbb{C}$. Define the degree of a vector $\sum a_i[g_i] \in \mathbb{Z}[X]$ to be $\sum a_i$ and let $\mathbb{Z}[X]^0$ denote the degree-0 submodule of $\mathbb{Z}[X]$. Then $\mathbb{Z}[X]$ and $\mathbb{Z}[X]^0$ are endowed with actions of Hecke operators T_p, S_p, $p \nmid N$, which are linear and defined as follows: For any prime $p \nmid N$, $B_p^\times / R_p^\times \cong \mathrm{GL}_2(\mathbb{Q}_p)/\mathrm{GL}_2(\mathbb{Z}_p)$ can be identified with the set of $\mathbb{Z}_p$-lattices in a 2-dimensional vector space over $\mathbb{Q}_p$. Then, for any $g = (g_v) \in \widehat{B}^\times$,

$$S_p([g]) = [g^{(p)} s_p(g_p)] \quad \text{and} \quad T_p([g]) = \sum_{h_p} [g^{(p)} h_p],$$

where $g^{(p)}$ is the p-off part of g, namely $g^{(p)} = (g_v^{(p)})$ with $g_v^{(p)} = g_v$ for all $v \neq p$ and $g_p^{(p)} = 1$; if g_p corresponds to lattice Λ, then $s_p(g_p)$ is the coset corresponding to the homothetic lattice $p\Lambda$; and h_p runs over $p+1$ lattices $\Lambda' \subset \Lambda$ with $[\Lambda : \Lambda'] = p$. There is a unique line $V_\phi \subset \mathbb{C}[X]^0$ where T_p acts as a_p and S_p acts trivially for all $p \nmid N$. Recall that the fixed embedding of K into B induces a map

$$\mathrm{Pic}(\mathbb{O}_c) = K^\times \backslash \widehat{K}^\times / \widehat{\mathbb{O}}_c^\times \longrightarrow X = B^\times \backslash \widehat{B}^\times / \widehat{R}^\times, \quad t \longmapsto x_t,$$

using which we define an element in $\mathbb{C}[X]$,

$$P_\chi := \sum \chi^{-1}(t) x_t,$$

and let P_χ^ϕ be its projection to the line V_ϕ. The following explicit height formula for P_χ^ϕ, which was proved by Gross [1987] in some cases, is a special case of the

explicit Waldspurger formulas in Theorems 1.8 and 1.10 (with Proposition 3.8).

Theorem 1.2. *Let* (ϕ, χ) *be as above satisfying the conditions* (i) *and* (ii)*. Then we have*

$$L(1, \phi, \chi) = 2^{-\mu(N, D)} \cdot \frac{8\pi^2 (\phi, \phi)_{\Gamma_0(N)}}{u^2 \sqrt{|Dc^2|}} \cdot \langle P_\chi^\phi, P_\chi^\phi \rangle,$$

where $\mu(N, D)$ *and* u *are as in Theorem 1.1. Let* $f = \sum_i f(g_i) w_i^{-1}[g_i]$ *be any nonzero vector on the line* V_ϕ*, and let* $P_\chi^0(f) = \sum_{t \in \mathrm{Pic}(\mathbb{O}_c)} f(t) \chi(t)$*. Then the above formula can be rewritten as*

$$L(1, \phi, \chi) = 2^{-\mu(N, D)} \cdot \frac{8\pi^2 (\phi, \phi)_{\Gamma_0(N)}}{u^2 \sqrt{|Dc^2|}} \cdot \frac{|P_\chi^0(f)|^2}{\langle f, f \rangle}.$$

Notation for first two sections. We denote by F the base number field of degree $d = [F : \mathbb{Q}]$ over $\mathbb{Q}$ and $\mathbb{O} = \mathbb{O}_F$ its ring of integers with different δ. Let $\mathbb{A} = F_{\mathbb{A}}$ be the adèle ring of F and $\mathbb{A}_f$ its finite part. For any $\mathbb{Z}$-module M, we let $\widehat{M} = M \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}}$ and $\widehat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$. For example, $\widehat{F} = \mathbb{A}_f$. Let $|\cdot|_{\mathbb{A}} : \mathbb{A}^\times \to \mathbb{R}_+^\times$ denote the standard adelic absolute value, so that $d(ab) = |a|_{\mathbb{A}} db$ for any Haar measure db on $\mathbb{A}$. Let $|\cdot|_v$ denote the absolute value on $F_v^\times$ for each place v of F, with $|x|_{\mathbb{A}} = \prod_v |x_v|_v$ for any $x = (x_v) \in \mathbb{A}^\times$. For any nonzero fractional ideal b of F, let $\|b\|$ denote the norm of b. For any $x \in \mathbb{A}_f^\times$, we also write $\|x\|$ for $\|b_x\|$, where b_x is the ideal corresponding to x, so that $\|x\| = |x|_{\mathbb{A}}^{-1}$; and for any nonzero fractional ideal b we also write $|b|_{\mathbb{A}}$ for $|x_b|_{\mathbb{A}}$ for any $x_b \in \mathbb{A}_f^\times$ whose corresponding ideal is b, so that $|b|_{\mathbb{A}} = \|b\|^{-1}$. For a finite place v, sometimes we also denote by v its corresponding prime ideal and write $q_v = \#\mathbb{O}/v$. For a fractional ideal b of F, we write $|b|_v = |x_b|_v$ for $x_b \in F_v$ with $x_b \mathbb{O}_v = b\mathbb{O}_v$, denote by $\mathrm{ord}_v(b)$ the additive valuation of b at v such that $\mathrm{ord}_v(v) = 1$, and write $v\|b$ if $\mathrm{ord}_v(b) = 1$. We denote by ∞ the set of infinite places of F. Denote by $L(s, 1_F)$ the complete L-series for the trivial Hecke character 1_F on $\mathbb{A}^\times$, so that $L(s, 1_F) = \Gamma_{\mathbb{R}}(s)^{r_1} \Gamma_{\mathbb{C}}(s)^{r_2} \zeta_F(s)$, where r_1 and r_2 are the number of real and complex places of F, $\zeta_F(s)$ is the usual Dedekind zeta function of F, $\Gamma_{\mathbb{R}}(s) = \pi^{-s/2} \Gamma(s/2)$, and $\Gamma_{\mathbb{C}}(s) = 2(2\pi)^{-s} \Gamma(s)$. For each place v of F, let $L(s, 1_v)$ denote the local Euler factor of $L(s, 1_F)$ at v. Let D_F denote the absolute discriminant of F, and $\delta \subset \mathbb{O}$ the different of F, so that $\|\delta\| = |D_F|$.

In the first two sections, we let K be a quadratic extension over F, $D = D_{K/F} \subset \mathbb{O}$ be the relative discriminant of K over F, and D_K be the absolute discriminant of K. Let K^{ab} be the maximal abelian extension over K and $\sigma : K_{\mathbb{A}}^\times/K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ be the Artin reciprocity map in class field theory. For any nonzero ideal b of $\mathbb{O}$, let $\mathbb{O}_b = \mathbb{O} + b\mathbb{O}_K$ be the unique $\mathbb{O}$-order of K satisfying $[\mathbb{O}_K : \mathbb{O}_b] = \#\mathbb{O}/b$, and we call b its conductor. For any finite place v of F, $\mathbb{O}_{b,v} = \mathbb{O}_b \otimes_{\mathbb{O}} \mathbb{O}_v$ only depends on $\mathrm{ord}_v b$. Thus, for a fractional ideal b and a finite place v of F, $\mathbb{O}_{b,v}$ makes sense if

$\operatorname{ord}_v b \geq 0$. Let $\operatorname{Pic}_{K/F}(\mathbb{O}_b) = \widehat{K}^\times / K^\times \widehat{F}^\times \widehat{\mathbb{O}}_b^\times$. Then there is an exact sequence

$$\operatorname{Pic}(\mathbb{O}_F) \longrightarrow \operatorname{Pic}(\mathbb{O}_b) \longrightarrow \operatorname{Pic}_{K/F}(\mathbb{O}_b) \longrightarrow 0.$$

Let κ_b be the kernel of the first map, which has order 1 or 2 if F is totally real and K is a totally imaginary quadratic extension over F (see [Washington 1997, Theorem 10.3]).

For any algebraic group G over F, let $G_{\mathbb{A}} = G(\mathbb{A})$ be the group of adelic points on G. For a finite set S of places of F, let $G_S = \prod_{v \in S} G(F_v)$ (resp. $G_{\mathbb{A}}^{(S)} = G(\mathbb{A})^{(S)}$) be the S-part of $G_{\mathbb{A}}$ (resp. the S-off part of $G_{\mathbb{A}}$) viewed as a subgroup of $G_{\mathbb{A}}$ naturally so that the S-off components (resp. S-components) are constant 1. More generally, for a subgroup U of $G_{\mathbb{A}}$ of the form $U = U_T U^T$ for some set T of places disjoint with S, where $U_T \subset \prod_{v \in T} G(F_v)$ and $U^T = \prod_{v \notin T} U_v$ with U_v a subgroup of $G(F_v)$, we may define $U^{(S)}$, U_S, and view them as subgroups of U similarly. For any ideal b of $\mathbb{O}$, we also write $U^{(b)}$ for $U^{(S_b)}$ and U_b for U_{S_b}, where S_b is the set of places dividing b. Let $U_0(N)$ and $U_1(N)$ denote subgroups of $\operatorname{GL}_2(\widehat{\mathbb{O}})$ defined by

$$U_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \operatorname{GL}_2(\widehat{\mathbb{O}}) \;\middle|\; c \in N\widehat{\mathbb{O}} \right\},$$

$$U_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in U_0(N) \;\middle|\; d \equiv 1 \bmod N\widehat{\mathbb{O}} \right\}.$$

When F is a totally real field and σ is an automorphic cuspidal representation of level N such that σ_v is a discrete series for all $v | \infty$, for an automorphic form ϕ of level $U_1(N)$ we let $(\phi, \phi)_{U_0(N)}$ denote the Petersson norm defined using the invariant measure $dx \, dy / y^2$ on the upper half-plane.

1B. *The explicit Gross–Zagier formula.* Let F be a totally real number field of degree d, $\mathbb{A} = \mathbb{A}_F$ the adèle ring of F, and $\mathbb{A}_f$ its finite part. Let $\mathbb{B}$ be an incoherent quaternion algebra over $\mathbb{A}$, totally definite at infinity. For each open compact subgroup U of $\mathbb{B}_f^\times = (\mathbb{B} \otimes_{\mathbb{A}} \mathbb{A}_f)^\times$, let X_U be the Shimura curve over F associated to U and $\xi_U \in \operatorname{Pic}(X_U)_{\mathbb{Q}}$ the normalized Hodge class on X_U, that is, the unique line bundle which has degree one on each geometrically connected component and is parallel to

$$\omega_{X_U/F} + \sum_{x \in X_U(\bar{F})} (1 - e_x^{-1}) x.$$

Here $\omega_{X_U/F}$ is the canonical bundle of X_U and e_x is the ramification index of x in the complex uniformization of X_U, i.e., for a cusp x, $e_x = \infty$, so that $1 - e_x^{-1} = 1$; for a noncusp x, e_x is the ramification index of any preimage of x in the map $X_{U'} \to X_U$ for any sufficiently small open compact subgroup U' of U such that each geometrically connected component of $X_{U'}$ is a free quotient of $\mathcal{H}$ under the complex uniformization. For any two open compact subgroups $U_1 \subset U_2$ of $\mathbb{B}_f^\times$,

there is a natural surjective morphism $X_{U_1} \to X_{U_2}$. Let X be the projective limit of the system $(X_U)_U$, which is endowed with the Hecke action of $\mathbb{B}^\times$ where $\mathbb{B}_\infty^\times$ acts trivially. Note that each X_U is the quotient of X by the action of U.

Let A be a simple abelian variety over F parametrized by X in the sense that there is a nonconstant morphism $X_U \to A$ over F for some U. Then, by Eichler–Shimura theory, A is of strict GL(2)-type in the sense that $M := \mathrm{End}^0(A) = \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ is a field and $\mathrm{Lie}(A)$ is a free module of rank one over $M \otimes_{\mathbb{Q}} F$ by the induced action. Let

$$\pi_A = \mathrm{Hom}_\xi^0(X, A) := \varinjlim_U \mathrm{Hom}_{\xi_U}^0(X_U, A),$$

where $\mathrm{Hom}_{\xi_U}^0(X_U, A)$ denotes the morphisms in $\mathrm{Hom}(X_U, A) \otimes_{\mathbb{Z}} \mathbb{Q}$ using ξ_U as a base point: if ξ_U is represented by a divisor $\sum_i a_i x_i$ on $X_{U,\bar{F}}$, then for $f \in \mathrm{Hom}_F(X_U, A) \otimes_{\mathbb{Z}} \mathbb{Q}$,

$$f \in \pi_A \Longleftrightarrow \sum_i a_i f(x_i) = 0 \text{ in } A(\bar{F})_{\mathbb{Q}} := A(\bar{F}) \otimes_{\mathbb{Z}} \mathbb{Q}.$$

For each open compact subgroup U of $\mathbb{B}_f^\times$, let J_U denote the Jacobian of X_U. Then

$$\pi_A = \mathrm{Hom}^0(J, A) := \varinjlim_U \mathrm{Hom}^0(J_U, A),$$

where $\mathrm{Hom}^0(J_U, A) = \mathrm{Hom}_F(J_U, A) \otimes_{\mathbb{Z}} \mathbb{Q}$. The action of $\mathbb{B}^\times$ on X induces a natural $\mathbb{B}^\times$-module structure on π_A so that $\mathrm{End}_{\mathbb{B}^\times}(\pi_A) = M$ and there is a decomposition $\pi_A = \bigotimes_M \pi_{A,v}$, where $\pi_{A,v}$ are absolutely irreducible representations of $\mathbb{B}_v^\times$ over M. Using the Jacquet–Langlands correspondence, one can define the complete L-series of π_A,

$$L(s, \pi_A) = \prod_v L(s, \pi_{A,v}) \in M \otimes_{\mathbb{Q}} \mathbb{C},$$

as an entire function of $s \in \mathbb{C}$. Let $L(s, A, M)$ denote the L-series of the ℓ-adic Galois representation with coefficients in $M \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ associated to A (without local Euler factors at infinity); then $L_v(s, A, M) = L\left(s - \frac{1}{2}, \pi_v\right)$ for all finite places v of F. Let $A^\vee$ denote the dual abelian variety of A. There is a perfect $\mathbb{B}^\times$-invariant pairing

$$\pi_A \times \pi_{A^\vee} \longrightarrow M$$

given by

$$(f_1, f_2) = \mathrm{Vol}(X_U)^{-1}(f_{1,U} \circ f_{2,U}^\vee), \quad f_{1,U} \in \mathrm{Hom}(J_U, A), \ f_{2,U} \in \mathrm{Hom}(J_U, A^\vee),$$

where $f_{2,U}^\vee : A \to J_U$ is the dual of $f_{2,U}$ composed with the canonical isomorphism $J_U^\vee \simeq J_U$. Here $\mathrm{Vol}(X_U)$ is defined by a fixed invariant measure on the upper

half-plane. It follows that $\pi_{A^\vee}$ is dual to π_A as representations of $\mathbb{B}^\times$ over M. For any fixed open compact subgroup U of $\mathbb{B}_f^\times$, define the U-pairing on $\pi_A \times \pi_{A^\vee}$ by

$$(f_1, f_2)_U = \mathrm{Vol}(X_U)(f_1, f_2), \quad f_1 \in \pi_A, \ f_2 \in \pi_{A^\vee},$$

which is independent of the choice of measure defining $\mathrm{Vol}(X_U)$. If A is an elliptic curve and we identify $A^\vee$ with A canonically then, for any morphism $f : X_U \to A$, we have $(f, f)_U = \deg f$, the degree of the finite morphism f.

Let K be a totally imaginary quadratic extension over F with associated quadratic character η on $\mathbb{A}^\times$. Let L be a finite extension of M and $\chi : K^\times \backslash K_{\mathbb{A}}^\times \to L^\times$ an L-valued Hecke character of finite order. Let $L(s, A, \chi)$ be the L-series (without Euler factors at infinity) of the ℓ-adic Galois representations associated to A tensored with the induced representation of χ from $\mathrm{Gal}(\overline{K}/K)$ to $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Assume that

$$\omega_A \cdot \chi|_{\mathbb{A}^\times} = 1,$$

where ω_A is the central character of π_A on $\mathbb{A}_f^\times$ and that, for each finite place v of F,

$$\epsilon(\pi_{A,v}, \chi_v) = \chi_v \eta_v(-1)\epsilon(\mathbb{B}_v),$$

where $\epsilon(\mathbb{B}_v) = 1$ if $\mathbb{B}_v$ is split and is -1 otherwise, and $\epsilon(\pi_{A,v}, \chi_v) = \epsilon\left(\frac{1}{2}, \pi_{A,v}, \chi_v\right)$ is the local root number of $L(s, \pi_A, \chi)$. It follows that the global root number of the L-series $L(s, \pi_A, \chi)$ is -1 and there is an embedding of $K_{\mathbb{A}}$ into $\mathbb{B}$ over $\mathbb{A}$. We fix such an embedding once for all and then view $K_{\mathbb{A}}^\times$ as a subgroup of $\mathbb{B}^\times$.

Let N be the conductor of π^{JL}, D the relative discriminant of K over F, and $c \subset \mathbb{O}$ the ideal that is maximal such that χ is trivial on $\prod_{v \nmid c} \mathbb{O}_{K_v}^\times \prod_{v|c}(1 + c\mathbb{O}_{K,v})$. Define the set of places v of F dividing N,

$$\Sigma_1 := \{v | N \text{ nonsplit in } K \mid \mathrm{ord}_v(c) < \mathrm{ord}_v(N)\}.$$

Let $c_1 = \prod_{\mathfrak{p}|c, \mathfrak{p} \notin \Sigma_1} \mathfrak{p}^{\mathrm{ord}_\mathfrak{p} c}$ be the Σ_1-off part of c, N_1 the Σ_1-off part of N, and $N_2 = N/N_1$.

Let v be a place of F and ϖ_v a uniformizer of F_v. Then there exists an $\mathbb{O}_v$-order R_v of $\mathbb{B}_v$ with discriminant $N\mathbb{O}_v$ such that $R_v \cap K_v = \mathbb{O}_{c_1,v}$. Such an order R_v is called admissible for $(\pi_v.\chi_v)$ if it also satisfies the conditions (1) and (2) that follow. Note that up to $K_v^\times$-conjugate there is a unique such order when $v \nmid (c_1, N)$, and that $\mathbb{B}$ must be split at places $v|(c_1, N)$ by Lemma 3.1.

(1) If $v|(c_1, N)$, then R_v is the intersection of two maximal orders R_v', R_v'' of $\mathbb{B}_v$ such that $R_v' \cap K_v = \mathbb{O}_{c,v}$ and

$$R_v'' \cap K_v = \begin{cases} \mathbb{O}_{c/N,v} & \text{if } \mathrm{ord}_v(c/N) \geq 0, \\ \mathbb{O}_{K,v} & \text{otherwise.} \end{cases}$$

Note that, for $v|(c_1, N)$, there is a unique order up to $K_v^\times$-conjugate satisfying condition (1), unless $\mathrm{ord}_v(c_1) < \mathrm{ord}_v(N)$. In the case $0 < \mathrm{ord}_v(c_1) < \mathrm{ord}_v(N)$,

v must split in K by the definition of Σ_1 and there are exactly two $K_v^\times$-conjugacy classes of orders satisfying condition (1), which are conjugate to each other by a normalizer of $K_v^\times$ in $\mathbb{B}_v^\times$. Fix an F_v-algebra isomorphism $K_v \cong F_v^2$ and identify $\mathbb{B}_v$ with $\mathrm{End}_{F_v}(K_v)$. Then the two classes contain, respectively, orders $R_{i,v} = R_{i,v}' \cap R_{i,v}''$, $i = 1, 2$ as in (1) such that $R_{i,v}' = \mathrm{End}_{\mathbb{O}}(\mathbb{O}_c)$, $i = 1, 2$, $R_{1,v}'' = \mathrm{End}_{\mathbb{O}_v}((\varpi_v^{n-c}, 1)\mathbb{O}_{K_v})$ and $R_{2,v}'' = \mathrm{End}_{\mathbb{O}_v}((1, \varpi_v^{n-c})\mathbb{O}_{K_v})$.

(2) If $0 < \mathrm{ord}_v(c_1) < \mathrm{ord}_v(N)$, then R_v is $K_v^\times$-conjugate to some $R_{i,v}$ such that χ_i has conductor $\mathrm{ord}_v(c)$, where χ_i, $i = 1, 2$, is defined by $\chi_1(a) = \chi_v(a, 1)$ and $\chi_2(b) = \chi_v(1, b)$.

Definition 1.3. An $\widehat{\mathbb{O}}$-order $\mathcal{R}$ of $\mathbb{B}_f$ is called admissible for (π, χ) if, for every finite place v of F, $\mathcal{R}_v := \mathcal{R} \otimes_{\widehat{\mathbb{O}}} \mathbb{O}_v$ is admissible for (π_v, χ_v). Note that an admissible order $\mathcal{R}$ for (π, χ) is of discriminant $N\widehat{\mathbb{O}}$ such that $\mathcal{R} \cap \widehat{K} = \widehat{\mathbb{O}}_{c_1}$.

Let $\mathcal{R}$ be an $\widehat{\mathbb{O}}$-order of $\mathbb{B}_f$ with discriminant N such that $\mathcal{R} \cap K_{\mathbb{A}_f} = \widehat{\mathbb{O}}_{c_1}$ and that $\mathcal{R}_v := \mathcal{R} \otimes_{\widehat{\mathbb{O}}} \mathbb{O}_v$ is admissible for (π_v, χ_v) at all places v. Note that $\mathcal{R}_v$ is unique up to $K_v^\times$-conjugate for any $v \nmid (c_1, N)$.

Let $U = \mathcal{R}^\times$ and $U^{(N_2)} := \mathcal{R}^\times \cap \mathbb{B}_f^{\times(N_2)}$. For any finite place $v | N_1$, $\mathbb{B}_v$ must be split (by Lemma 3.1(5)). Let $Z \cong \mathbb{A}_f^\times$ denote the center of $\mathbb{B}_f^\times$. The group $U^{(N_2)}$ has a decomposition $U^{(N_2)} = U' \cdot (Z \cap U^{(N_2)})$, where $U' = \prod_{v \nmid N_2 \infty} U_v'$ is so that, for any finite place $v \nmid N_2$, $U_v' = U_v$ if $v \nmid N$ and $U_v' \cong U_1(N)_v$ otherwise. View ω as a character on Z. We may define a character on $U^{(N_2)}$ that is ω on $Z \cap U^{(N_2)}$ and trivial on U'. This character is also denoted by ω.

Definition 1.4. Let $V(\pi, \chi)$ denote the space of forms $f \in \pi_A \otimes_M L$ which are ω-eigenforms under $U^{(N_2)}$ and χ_v^{-1}-eigenforms under $K_v^\times$ for all places $v \in \Sigma_1$. The space $V(\pi, \chi)$ is actually a one-dimensional L-space (see Proposition 3.7).

Consider the Hecke action of $K_{\mathbb{A}}^\times \subset \mathbb{B}^\times$ on X. Let $X^{K^\times}$ be the F-subscheme of X of fixed points of X under $K^\times$. The theory of complex multiplication asserts that every point in $X^{K^\times}(\overline{F})$ is defined over K^{ab} and that the Galois action is given by the Hecke action under the reciprocity law. Fix a point $P \in X^{K^\times}$ and let $f \in V(\pi, \chi)$ be a nonzero vector. Define a Heegner cycle associated to (π, χ) by

$$P_\chi^0(f) := \sum_{t \in \mathrm{Pic}_{K/F}(\mathbb{O}_{c_1})} f(P)^{\sigma_t} \chi(t) \in A(K^{\mathrm{ab}})_{\mathbb{Q}} \otimes_M L,$$

where $\mathrm{Pic}_{K/F}(\mathbb{O}_{c_1}) = \widehat{K}^\times / K^\times \widehat{F}^\times \widehat{\mathbb{O}}_{c_1}^\times$ and $t \mapsto \sigma_t$ is the reciprocity law map in class field theory. The Néron–Tate height pairing over K gives a $\mathbb{Q}$-linear map $\langle \, , \rangle_K : A(\overline{K})_{\mathbb{Q}} \otimes_M A^\vee(\overline{K})_{\mathbb{Q}} \to \mathbb{R}$. Let $\langle \, , \rangle_{K,M} : A(\overline{K})_{\mathbb{Q}} \otimes_M A^\vee(\overline{K})_{\mathbb{Q}} \to M \otimes_{\mathbb{Q}} \mathbb{R}$ be the unique M-bilinear pairing such that $\langle \, , \rangle_K = \mathrm{tr}_{M \otimes \mathbb{R}/\mathbb{R}} \langle \, , \rangle_{K,M}$. The pairing $\langle \, , \rangle_{K,M}$ induces an L-linear Néron–Tate pairing over K,

$$\langle \, , \rangle_{K,L} : (A(\overline{K})_{\mathbb{Q}} \otimes_M L) \otimes_L (A^\vee(\overline{K})_{\mathbb{Q}} \otimes_M L) \longrightarrow L \otimes_{\mathbb{Q}} \mathbb{R}.$$

The $\mathbb{B}^\times$-invariant M-linear pairing $(\,,\,)_U : \pi_A \times \pi_{A^\vee} \to M$ induces a $\mathbb{B}^\times$-invariant L-linear pairing

$$(\,,\,)_U : (\pi_A \otimes_M L) \times (\pi_{A^\vee} \otimes_M L) \longrightarrow L.$$

The Hilbert newform ϕ in the Jacquet–Langlands correspondence σ of π_A on $\mathrm{GL}_2(\mathbb{A})$ is the form satisfying these conditions:

- ϕ is of level $U_1(N)$.

- For each $v | \infty$, the action of $\mathrm{SO}_2(\mathbb{R}) \subset \mathrm{GL}_2(F_v)$ on ϕ is given by $\sigma(k_\theta)\phi = e^{4\pi i \theta}\phi$, where $k_\theta = \left(\begin{smallmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{smallmatrix}\right) \in \mathrm{SO}_2(\mathbb{R})$.

- Let $d^\times a$ be the Tamagawa measure so that $\mathrm{Res}_{s=1} \int_{|a|\le 1, a\in F^\times\backslash\mathbb{A}^\times} |a|^{s-1}\, d^\times a = \mathrm{Res}_{s=1} L(s, 1_F)$; then

  $$L(s, \pi) = 2^d \cdot |\delta|_{\mathbb{A}}^{s-1/2} \cdot Z(s, \phi) \quad \text{with } Z(s, \phi) = \int_{F^\times\backslash\mathbb{A}^\times} \phi\left(\begin{smallmatrix} a & \\ & 1 \end{smallmatrix}\right)|a|_{\mathbb{A}}^{s-1/2}\, d^\times a,$$

  where δ is the different of F.

Note that $\phi(g)\overline{\phi}(g)$ is a function on

$$\mathrm{GL}_2(F)_+\backslash\mathrm{GL}_2(F_\infty)_+ \times \mathrm{GL}_2(\mathbb{A}_f)/Z(\mathbb{A}) \cdot (U_{1,\infty} \times U_0(N))$$
$$\cong \mathrm{GL}_2(F)_+\backslash\mathcal{H}^d \times \mathrm{GL}_2(\mathbb{A}_f)/U_0(N)\mathbb{A}_f^\times.$$

We define the Petersson norm $(\phi, \phi)_{U_0(N)}$ by the integration of $\phi\overline{\phi}$ with measure $dx\, dy/y^2$ on each upper half-plane. One main result of this paper is the following:

Theorem 1.5 (explicit Gross–Zagier formula). *Let F be a totally real field of degree d. Let A be an abelian variety over F parametrized by a Shimura curve X over F and ϕ the Hilbert holomorphic newform of parallel weight 2 on $\mathrm{GL}_2(\mathbb{A})$ associated to A. Let K be a totally imaginary quadratic extension over F with relative discriminant D and discriminant D_K. Let $\chi : K_{\mathbb{A}}^\times/K^\times \to L^\times$ be a finite Hecke character of conductor c over some finite extension L of $M := \mathrm{End}^0(A)$. Assume that:*

(1) $\omega_A \cdot \chi|_{\mathbb{A}^\times} = 1$, where ω_A is the central character of π_A;

(2) for any place v of F, $\epsilon(\pi_{A,v}, \chi_v) = \chi_v\eta_v(-1)\epsilon(\mathbb{B}_v)$.

For any nonzero forms $f_1 \in V(\pi_A, \chi)$ and $f_2 \in V(\pi_{A^\vee}, \chi^{-1})$, we have an equality in $L \otimes_{\mathbb{Q}} \mathbb{C}$,

$$L'^{(\Sigma)}(1, A, \chi) = 2^{-\#\Sigma_D} \cdot \frac{(8\pi^2)^d \cdot (\phi, \phi)_{U_0(N)}}{u_1^2\sqrt{|D_K|\|c_1^2\|}} \cdot \frac{\langle P_\chi^0(f_1), P_{\chi^{-1}}^0(f_2)\rangle_{K,L}}{(f_1, f_2)_{\mathscr{R}^\times}},$$

where

$$\Sigma := \{v | (N, Dc) \mid \text{if } v \| N \text{ then } \text{ord}_v(c/N) \geq 0\},$$

$$\Sigma_D := \{v | (N, D) \mid \text{ord}_v(c) < \text{ord}_v(N)\},$$

the ideal $c_1 | c$ is the Σ_1-off part of c as before, $u_1 = \#\kappa_{c_1} \cdot [\mathbb{O}_{c_1}^\times : \mathbb{O}^\times]$ and κ_{c_1} is the kernel of the morphism from $\mathrm{Pic}(\mathbb{O})$ to $\mathrm{Pic}(\mathbb{O}_{c_1})$, which has order 1 or 2, and $(\phi, \phi)_{U_0(N)}$ is the Petersson norm with respect to the measure $dx\, dy / y^2$ on the upper half-plane.

Remark. The assumption $\omega_A|_{\mathbb{A}^\times} \cdot \chi = 1$ implies $L(s, A, \chi) = L(s, A^\vee, \chi^{-1})$. Let $\phi^\vee$ be the Hilbert newform associated to $A^\vee$. Then $(\phi^\vee, \phi^\vee)_{U_0(N)} = (\phi, \phi)_{U_0(N)}$.

We may state the above theorem in simpler way under some assumptions. First assume that ω_A is unramified and, if $v \in \Sigma_1$, then $v \nmid c$.

Given this, $c_1 = c$. Fix an infinite place τ of F and let B be the nearby quaternion algebra whose ramification set is obtained from that of $\mathbb{B}$ by removing τ. Then there is an F-embedding of K into B which we fix once and for all and view $K^\times$ as an F-subtorus of $B^\times$. Let R be an admissible $\mathbb{O}$-order of B for (π, χ), by which we mean that $\widehat{R}$ is an admissible $\widehat{\mathbb{O}}$-order of $\mathbb{B}_f = \widehat{B}$ for (π, χ). Note that R is of discriminant N and that $R \cap K = \mathbb{O}_c$. Let $U = \widehat{R}^\times \subset \widehat{B}^\times$ and let X_U be the Shimura curve of level U, so that it has complex uniformization

$$X_{U,\tau}(\mathbb{C}) = B_+^\times \backslash \mathscr{H} \times \widehat{B}^\times / U \cup \{\text{cusps}\},$$

where $B_+^\times$ is the subgroup of elements $x \in B^\times$ with totally positive norms. Let $u = \#\kappa_c \cdot [\mathbb{O}_c^\times : \mathbb{O}^\times]$. By Proposition 3.8, we have that $V(\pi_A, \chi) \subset (\pi_A \otimes_M L)^{\widehat{R}^\times}$.

Special case 1. Further assume that $(N, Dc) = 1$. Then there is a nonconstant morphism $f : X_U \to A$ mapping a Hodge class on X_U to the torsion of A and, for any two such morphisms $f_1, f_2 : X_U \to A$, $n_1 f_1 = n_2 f_2$ for some nonzero integers n_1, n_2. Let h_0 be the unique fixed point of $K^\times$ and let $P = [h_0, 1] \in X_U$. Replace χ by χ^{-1}; there is a nonconstant morphism $X_U \to A^\vee$ with similar uniqueness. For any such $f_1 : X_U \to A$ and $f_2 : X_U \to A^\vee$, let $(f_1, f_2) = f_1 \circ f_2^\vee$. Then we have an equality in $L \otimes_\mathbb{Q} \mathbb{C}$,

$$L'(1, A, \chi) = \frac{(8\pi^2)^d (\phi, \phi)_{U_0(N)}}{u^2 \cdot \sqrt{|D_K| \| c^2 \|}} \cdot \frac{\langle P_\chi^0(f_1), P_{\chi^{-1}}^0(f_2) \rangle_{K,L}}{(f_1, f_2)_U}.$$

Special case 2. Further assume that ω_A is trivial — or, more generally, that $\omega_A(\varpi_v)$ is in $\mathrm{Aut}(A)^2 \subset M^{\times 2}$ for all places v dividing (N, D) but not c, where ϖ_v is a uniformizer of F_v. For each place v that divides (N, D) but not c, $K_v^\times$ normalizes $R_v^\times$ (see Lemma 3.4) and a uniformizer ϖ_{K_v} of K_v induces an automorphism $T_{\varpi_{K_v}} : X_U \to X_U$ over F. Note that $\chi_v(\varpi_{K_v}) \in \mathrm{Aut}(A) \subset M^\times$. There exists a nonconstant morphism $f : X_U \to A$ mapping a Hodge class to the torsion point

such that $T_{\varpi_{K_v}} f = \chi^{-1}(\varpi_{K_v}) f$ for each place v dividing (N, D) but not c. Such an f has the same uniqueness property as in special case 1. Then, for any such $f_1 : X_U \to A$ and $f_2 : X_U \to A^\vee$, we have an equality in $L \otimes_\mathbb{Q} \mathbb{C}$,

$$L'^{(\Sigma)}(1, A, \chi) = 2^{-\#\Sigma_D} \cdot \frac{(8\pi^2)^d(\phi, \phi)_{U_0(N)}}{u^2 \cdot \sqrt{|D_K| \|c^2\|}} \cdot \frac{\langle P^0_\chi(f_1), P^0_{\chi^{-1}}(f_2)\rangle_{K,L}}{(f_1, f_2)_U},$$

where Σ is now the set of places $v | (cD, N)$ of F such that, if $v \| N$, then $v \nmid D$.

Example. Let $\phi \in S_2(\Gamma_0(N))$ be a newform. Let K be an imaginary quadratic field of discriminant D and χ a primitive character of $\mathrm{Pic}(\mathbb{O}_c)$. Assume that (ϕ, χ) satisfies the Heegner conditions (1)–(2) in Theorem 1.1; then, by Lemma 3.1(1) and (3), $\epsilon(\phi, \chi) = -1$ and $B = M_2(\mathbb{Q})$. The Heegner conditions also imply that there exist $a, b \in \mathbb{Z}$ with $(N, a, b) = 1$ such that $a^2 - 4Nb = Dc^2$. Fix an embedding of K into B by

$$(Dc^2 + \sqrt{Dc^2})/2 \longmapsto \begin{pmatrix} (Dc^2 + a)/2 & -1 \\ Nb & (Dc^2 - a)/2 \end{pmatrix}.$$

Then $R := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}) \mid N | c \right\}$ is an order of B such that $\widehat{R} \cap K = \mathbb{O}_c$. Let A be an abelian variety associated to ϕ via Eichler–Shimura theory and $f : X_0(N) \to A$ any nonconstant morphism mapping cusp ∞ to $O \in A$. Then $f \in V(\pi_A, \chi)$. Let $z \in \mathcal{H}$ be the point fixed by $K^\times$; then $Nbz^2 - az + 1 = 0$, $\mathbb{O}_c = \mathbb{Z} + \mathbb{Z}z^{-1}$, and $\mathfrak{n}^{-1} = \mathbb{Z} + \mathbb{Z}N^{-1}z^{-1}$, so that $\mathbb{O}_c/\mathfrak{n} \cong \mathbb{Z}/N\mathbb{Z}$. The point on $X_0(N)$ corresponding to z via complex uniformization represents the isogeny $\mathbb{C}/(\mathbb{Z} + \mathbb{Z}z) \to \mathbb{C}/(N^{-1}\mathbb{Z} + \mathbb{Z}z)$, or $\mathbb{C}/\mathbb{O}_c \to \mathbb{C}/\mathfrak{n}^{-1}$. Thus Theorem 1.1 now follows from Theorem 1.5.

For various arithmetic applications, we may need explicit formulas for different test vectors, which we now give. Let v be a finite place of F, fix $\langle\, , \rangle_v$ a $\mathbb{B}_v^\times$-invariant pairing on $\pi_{A,v} \times \pi_{A^\vee,v}$ and a Haar measure dt_v on $F_v^\times \backslash K_v^\times$. For any $f'_{1,v} \in \pi_{A,v}$, $f'_{2,v} \in \pi_{A^\vee,v}$ with $\langle f'_{1,v}, f'_{2,v}\rangle_v \neq 0$, let

$$\beta^0(f'_{1,v}, f'_{2,v}) = \beta^0(f'_{1,v}, f'_{2,v}, dt_v) = \int_{F_v^\times \backslash K_v^\times} \frac{\langle \pi_{A,v}(t_v) f'_{1,v}, f'_{2,v}\rangle_v}{\langle f'_{1,v}, f'_{2,v}\rangle_v} \chi_v(t_v) \, dt_v.$$

For any two nonzero pure tensor forms $f' = \bigotimes_v f'_v$, $f'' = \bigotimes_v f''_v \in \pi$, we say that f' and f'' differ at a place v if f'_v and f''_v are not parallel, and that they coincide otherwise. This is independent of the decompositions. In particular, if two nonzero pure tensor forms coincide locally everywhere then they are the same up to a scalar.

Theorem 1.6 (variation of the Gross–Zagier formula). *Let (A, χ), $f_1 \in V(\pi_A, \chi)$ and $f_2 \in V(\pi_{A^\vee}, \chi^{-1})$ be as in Theorem 1.5. Let S be a finite set of finite places of F, $f'_1 \in \pi_A$, $f'_2 \in \pi_{A^\vee}$ be vectors such that f'_i and f_i coincide for any $v \notin S$,*

$i = 1, 2,$ *and* $\langle f'_{1,v}, f'_{2,v} \rangle_v \neq 0$ *and* $\beta^0(f'_{1,v}, f'_{2,v}) \neq 0$ *for any* $v \in S.$ *Define*

$$P^0_\chi(f'_1) = \frac{\#\operatorname{Pic}(\mathbb{O}_{c_1})}{\operatorname{Vol}(K^\times \widehat{F}^\times \backslash \widehat{K}^\times, dt)} \cdot \int_{K^\times \widehat{F}^\times \backslash \widehat{K}^\times} f'_1(P)^{\sigma_t} \chi(t)\, dt,$$

and define $P^0_{\chi^{-1}}(f'_2)$ *similarly. Then, with notations as in Theorem 1.5, we have*

$$L'^{(\Sigma)}(1, A, \chi)$$
$$= 2^{-\#\Sigma_D} \cdot \frac{(8\pi^2)^d \cdot (\phi, \phi)_{U_0(N)}}{u_1^2 \sqrt{|D_K| \|c_1^2\|}} \cdot \frac{\langle P^0_\chi(f'_1), P^0_{\chi^{-1}}(f'_2) \rangle_{K,L}}{(f'_1, f'_2)^\times_{\mathscr{R}}} \cdot \prod_{v \in S} \frac{\beta^0(f_{1,v}, f_{2,v})}{\beta^0(f'_{1,v}, f'_{2,v})},$$

which is independent of the choice of Haar measure dt_v *for* $v \in S.$

Example. Let A be the elliptic curve $X_0(36)$ with the cusp ∞ as the identity point and let $K = \mathbb{Q}(\sqrt{-3})$. Let $p \equiv 2 \bmod 9$ be a prime; then the field $L' = K(\sqrt[3]{p})$ is contained in H_{3p}. Let $\chi : \operatorname{Gal}(L'/K) \to K^\times$ be the character mapping σ to $(\sqrt[3]{p})^{\sigma-1}$. Fix the embedding $K \to M_2(\mathbb{Q})$ mapping $w := (-1 + \sqrt{-3})/2$ to $\left(\begin{smallmatrix} -1 & -p/6 \\ 6/p & 0 \end{smallmatrix} \right)$.

For $f' = \operatorname{id} : X_0(36) \to A$, let $P \in X_0(36)$ be the point corresponding to $-pw/6 \in \mathscr{H}$. The Heegner divisor $P^0_\chi(f')$ is

$$P^0_\chi(f') = \frac{1}{9} \sum_{t \in \operatorname{Pic}(\mathbb{O}_{6p})} f'(P)^{\sigma_t} \chi(t).$$

One can show that $P^0_\chi(f')$ is nontrivial (see [Satgé 1987; Dasgupta and Voight 2009; Cai et al. 2014]) and then it follows that the prime p is the sum of two rational cubes. By the variation formula, one can easily obtain the height formula of $P^0_\chi(f')$: let $\phi \in S_2(\Gamma_0(36))$ be the newform associated to A, and note that $\#\Sigma_D = 1$, $u_1 = 1$ and $c_1 = p$ in the variation

$$L'(1, A, \chi) = 9 \cdot \frac{8\pi^2 \cdot (\phi, \phi)_{\Gamma_0(36)}}{\sqrt{3}p^2} \cdot \langle P^0_\chi(f'), P^0_{\chi^{-1}}(f') \rangle_{K,K}.$$

In fact, $U = \mathscr{R}^\times$ in Theorem 1.5 is given by

$$\mathscr{R} = \left\{ \begin{pmatrix} a & b/6 \\ 6c & d \end{pmatrix} \in M_2(\widehat{\mathbb{Q}}) \;\middle|\; a, b, c, d \in \widehat{\mathbb{Z}},\; p^{-1}b + pc,\; a + pc - d \in 6\widehat{\mathbb{Z}} \right\}$$

and $f \in V(\pi_A, \chi)$ is a χ_v^{-1}-eigenform for $v = 2, 3$. Then

$$(f', f') = \frac{\operatorname{Vol}(X_U)}{\operatorname{Vol}(X_0(36))} = \frac{2}{9}.$$

The ratio $\beta^0(f_v, f_v)/\beta^0(f'_v, f'_v)$ equals 1 at $v = 2$, and 4 at $v = 3$.

1C. *The explicit Waldspurger formula.* Let F be a general base number field. Let B be a quaternion algebra over F and π a cuspidal automorphic representation of $B_{\mathbb{A}}^{\times}$ with central character ω. Let K be a quadratic field extension of F and η the quadratic Hecke character on $F^{\times} \backslash \mathbb{A}^{\times}$ associated to the quadratic extension. Let χ be a Hecke character on $K_{\mathbb{A}}^{\times}$. Write $L(s, \pi, \chi)$ for the Rankin L-series $L(s, \pi^{\mathrm{JL}} \times \pi_{\chi})$, where π^{JL} is the Jacquet–Langlands correspondence of π on $\mathrm{GL}_2(\mathbb{A})$ and π_{χ} is the automorphic representation of $\mathrm{GL}_2(\mathbb{A})$ corresponding to the theta series of χ, so that $L(s, \pi_{\chi}) = L(s, \chi)$. Assume that

$$\omega \cdot \chi|_{\mathbb{A}^{\times}} = 1.$$

Then, for any place v of F, the local root number $\epsilon\left(\frac{1}{2}, \pi_v, \chi_v\right)$ of the Rankin L-series is independent of the choice of additive character. We also assume that, for all places v of F,

$$\epsilon\left(\tfrac{1}{2}, \pi_v, \chi_v\right) = \chi_v \eta_v(-1) \epsilon(B_v),$$

where $\epsilon(B_v) = -1$ if B_v is division and $+1$ otherwise. It follows that the global root number $\epsilon\left(\frac{1}{2}, \pi, \chi\right)$ equals $+1$ and there exists an F-embedding of K into B. We fix such an embedding once and for all and view $K^{\times}$ as an F-subtorus of $B^{\times}$.

Let N be the conductor of π^{JL}, D the relative discriminant of K over F, $c \subset \mathbb{O}$ the ideal maximal such that χ is trivial on $\prod_{v \nmid c} \mathbb{O}_{K_v}^{\times} \prod_{v \mid c} (1 + c\mathbb{O}_{K,v})$. Define the following set of places v of F dividing N:

$$\Sigma_1 := \{v | N \text{ nonsplit in } K \mid \mathrm{ord}_v(c) < \mathrm{ord}_v(N)\},$$

Let $c_1 = \prod_{\mathfrak{p}|c, \mathfrak{p} \notin \Sigma_1} \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}} c}$ be the Σ_1-off part of c, N_1 the Σ_1-off part of N, and $N_2 = N/N_1$ the Σ_1-part of N.

Let R be an admissible $\mathbb{O}$-order of B for (π, χ) in the sense that R_v is admissible for (π_v, χ_v) for every finite place v of F. It follows that R is an $\mathbb{O}$-order with discriminant N such that $R \cap K = \mathbb{O}_{c_1}$.

Let $U = \prod_v U_v \subset B_{\mathbb{A}}^{\times}$ be a compact subgroup such that, for any finite place v, $U_v = R_v^{\times}$, and that, for any infinite place v of F, U_v is a maximal compact subgroup of $B_v^{\times}$ such that $U_v \cap K_v^{\times}$ is the maximal compact subgroup of $K_v^{\times}$. For any finite place $v|N_1$, B_v must be split. Let $Z \cong \mathbb{A}_f^{\times}$ denote the center of $\widehat{B}^{\times}$. The group $U^{(N_2 \infty)}$ has a decomposition $U^{(N_2 \infty)} = U' \cdot (Z \cap U^{(N_2 \infty)})$, where $U' = \prod_{v \nmid N_2 \infty} U_v'$ is such that, for any finite place $v \nmid N_2$, $U_v' = U_v$ if $v \nmid N$ and $U_v' \cong U_1(N)_v$ otherwise. View ω as a character on Z and we may define a character on $U^{(c_2 \infty)}$ that is ω on $Z \cap U^{(c_2 \infty)}$ and trivial on U'; we also denote this character by ω.

Definition 1.7. Let $V(\pi, \chi)$ denote the space of forms $f = \bigotimes_v f_v \in \pi$ such that f is an ω-eigenform under $U^{(N_2 \infty)}$; for all places $v \in \Sigma_1$, f is a χ_v^{-1}-eigenform under $K_v^{\times}$; and, for any infinite place v, f is a χ_v^{-1}-eigenform under $U_v \cap K_v^{\times}$ with weight minimal. The space $V(\pi, \chi)$ is actually one-dimensional (see Proposition 3.7).

Let r, s, t be integers such that $B \otimes_{\mathbb{Q}} \mathbb{R} = \mathbb{H}^r \times M_2(\mathbb{R})^s \times M_2(\mathbb{C})^t$, and let X_U denote the U-level real manifold

$$X_U = B_+^\times \backslash (\mathcal{H}_2^s \times \mathcal{H}_3^t) \times \widehat{B}^\times / U,$$

which has finitely many connected components, where $\mathcal{H}_2$, $\mathcal{H}_3$ are the usual hyperbolic spaces of dimension two and three, respectively. Define the volume of X_U, denoted by $\mathrm{Vol}(X_U)$, as follows:

- If $s + t > 0$, then X_U is the disjoint union of manifolds of dimension $2s + 3t$,

$$X_U = B_+^\times \backslash (\mathcal{H}_2^s \times \mathcal{H}_3^t) \times \widehat{B}^\times / U = \bigsqcup_i \Gamma_i \backslash (\mathcal{H}_2^s \times \mathcal{H}_3^t),$$

  for some discrete subgroup $\Gamma_i \subset B_+^\times \cap \prod_{v | \infty, B_v \text{ not division}} (B_v)^\times$, then define the volume of X_U with the measure $dx\,dy/(4\pi y^2)$ on $\mathcal{H}_2$ and the measure $dx\,dy\,dv/\pi^2 v^3$ on $\mathcal{H}_3$. Here the notation $\mathcal{H}_3$ is the same as in [Vignéras 1980].

- If $s + t = 0$, then F is totally real and B is totally definite. For any open compact subgroup U of $\widehat{B}^\times$, the double coset $B^\times \backslash \widehat{B}^\times / U$ is finite; let $g_1, \ldots, g_n \in \widehat{B}^\times$ be a complete set of representatives for the coset. Let $\mu_Z = \widehat{F}^\times \cap U$; then, for any $g \in \widehat{B}^\times$, $B^\times \cap gUg^{-1}/\mu_Z$ is a finite set. Define the volume of X_U to be the mass of U:

$$\mathrm{Vol}(X_U) = \mathrm{Mass}(U) = \sum_{i=1}^n \frac{1}{\#(B^\times \cap g_i U g_i^{-1})/\mu_Z}.$$

For any automorphic forms $f_1 \in \pi$ and $f_2 \in \widetilde{\pi}$, $\langle f_1, f_2 \rangle_{\mathrm{Pet}}$ is the Petersson pairing of f_1, f_2, defined by

$$\langle f_1, f_2 \rangle_{\mathrm{Pet}} = \int_{B^\times \mathbb{A}^\times \backslash B_{\mathbb{A}}^\times} f_1(g) f_2(g)\, dg,$$

where dg is the Tamagawa measure on $F^\times \backslash B^\times$, so that $B^\times \mathbb{A}^\times \backslash B_{\mathbb{A}}^\times$ has total volume 2. For any $f_1 \in V(\pi, \chi)$ and $f_2 \in V(\widetilde{\pi}, \chi^{-1})$, one may define the U-level pairing as

$$\langle f_1, f_2 \rangle_U = \tfrac{1}{2} \langle f_1, f_2 \rangle_{\mathrm{Pet}} \cdot \mathrm{Vol}(X_U).$$

For any $f \in V(\pi, \chi)$, define the c_1-level period of $f \in V(\pi, \chi)$ as follows: let $\overline{K_\infty^\times / F_\infty^\times}$ be the closure of $K_\infty^\times / F_\infty^\times$ in the compact group $K_{\mathbb{A}}^\times / \mathbb{A}^\times K^\times$ and endow $\overline{K_\infty^\times / F_\infty^\times}$ with the Haar measure dh of total volume one; then, let

$$P_\chi^0(f) = \sum_{t \in \mathrm{Pic}_{K/F}(\mathbb{O}_{c_1})} f^0(t) \chi(t), \quad f^0(t) = \int_{\overline{K_\infty^\times / F_\infty^\times}} f(th) \chi(h)\, dh.$$

The function $f^0(t)\chi(t)$ on $K_{\mathbb{A}}^\times$ is constant on $K_{\Sigma_1}^\times$, so can be viewed as a function on $\mathrm{Pic}_{K/F}(\mathbb{O}_{c_1}) = \widehat{K}^\times / K^\times \widehat{F}^\times \widehat{\mathbb{O}}_{c_1}^\times$. Note that, when F is totally real and all infinite places v of F are inert in K, $f^0 = f$.

Notations. Let b be an integral ideal of F; we define the relative regulator R_b to be the quotient of the regulator of $\mathbb{O}_b^\times$ by the regulator of $\mathbb{O}^\times$ and $w_b = \#\mathbb{O}_{b,\text{tor}}^\times / \#\mathbb{O}_{\text{tor}}^\times$. Denote by κ_b the kernel of the natural homomorphism from $\text{Pic}(\mathbb{O})$ to $\text{Pic}(\mathbb{O}_b)$. Define $v_b = 2^{-r_{K/F}} R_b^{-1} \cdot \#\kappa_b \cdot w_b$, where $r_{K/F} = \text{rank}\, \mathbb{O}_K^\times - \text{rank}\, \mathbb{O}^\times$. For example, if F is a totally real field of degree d and K is a totally imaginary quadratic field extension over F, then $v_b = 2^{1-d} \cdot \#\kappa_b \cdot [\mathbb{O}_b^\times : \mathbb{O}^\times]$, where $\kappa_b \subset \kappa_1$ and $\#\kappa_1 = 1$ or 2 [Washington 1997, Theorem 10.3].

For an infinite place v of F, let U_v denote the maximal compact subgroup of $\text{GL}_2(F_v)$, which is O_2 if v is real and U_2 if v is complex, and let $U_{1,v} \subset U_v$ denote its subgroup of diagonal matrices $\left(\begin{smallmatrix} a & \\ & 1 \end{smallmatrix}\right)$ for $a \in F_v^\times$ with $|a|_v = 1$. For a generic $(\mathfrak{g}_v, U_v)$-module σ_v and a nontrivial additive character ψ_v of F_v, let $\mathscr{W}(\sigma_v, \psi_v)$ be the ψ_v-Whittaker model of σ_v. There is an invariant bilinear pairing on $\mathscr{W}(\sigma_v, \psi_v) \times \mathscr{W}(\widetilde{\sigma}_v, \psi^{-1})$,

$$\langle W_1, W_2 \rangle_v := \int_{F_v^\times} W_1 \left[\begin{pmatrix} a & \\ & 1 \end{pmatrix} \right] W_2 \left[\begin{pmatrix} a & \\ & 1 \end{pmatrix} \right] d^\times a,$$

with the measure $d^\times a = L(1, 1_v)\, da/|a|_v$, where da equals $[F_v : \mathbb{R}]$ times the usual Lebesgue measure on F_v. Let $W_0 \in \mathscr{W}(\sigma_v, \psi_v)$ be the vector invariant under $U_{1,v}$ with minimal weight such that

$$L(s, \pi_v) = Z(s, W_0), \quad \text{where}\ \ Z(s, W_0) := \int_{F_v^\times} W_{\sigma_v} \left[\begin{pmatrix} a & \\ & 1 \end{pmatrix} \right] |a|_v^{s-1/2}\, d^\times a$$

with $d^\times a$ the Tamagawa measure. Similarly, define $\widetilde{W}_0$ for $\widetilde{\sigma}_v$. Then $\Omega_{\sigma_v} := \langle W_0, \widetilde{W}_0 \rangle_v$ is an invariant of σ_v which is independent of the choice of ψ_v (see an explicit formula for Ω_{σ_v} before Lemma 3.14). We associate to (σ_v, χ_v) a constant by

$$C(\sigma_v, \chi_v) := \begin{cases} 2^{-1}\pi \cdot \Omega_{\sigma_v}^{-1} & \text{if } K_v \text{ is nonsplit,} \\ \Omega_{\sigma_v \otimes \chi_{1,v}} \cdot \Omega_{\sigma_v}^{-1} & \text{if } K_v \text{ is split,} \end{cases} \tag{1-1}$$

where for split $K_v \cong F_v^2$, embedded into $M_2(F_v)$ diagonally, the character χ_1 is given by $\chi_{1,v}(a) := \chi_v \left[\left(\begin{smallmatrix} a & \\ & 1 \end{smallmatrix}\right) \right]$. If v is a real place of F and σ_v is a discrete series of weight k, then $C(\sigma_v, \chi_v) = 4^{k-1}\pi^{k+1}\Gamma(k)^{-1}$ when $K_v \cong \mathbb{C}$, and $C(\sigma_v, \chi_v) = 1$ when $K_v \cong \mathbb{R}^2$.

Let σ be the Jacquet–Langlands correspondence of π to $\text{GL}_2(\mathbb{A})$; the normalized new vector $\phi^0 = \bigotimes_v \phi_v \in \sigma$ is the one fixed by $U_1(N)$ and ϕ_v is fixed by $U_{1,v}$ with weight minimal for all $v|\infty$ such that

$$L(s, \sigma) = |\delta|_{\mathbb{A}}^{s-1/2} Z(s, \phi^0), \quad \text{where}\ \ Z(s, \phi^0) := \int_{F^\times \backslash \mathbb{A}^\times} \phi^0 \begin{pmatrix} a & \\ & 1 \end{pmatrix} |a|_{\mathbb{A}}^{s-1/2}\, d^\times a$$

with the Tamagawa measure on $\mathbb{A}^\times$, so that

$$\text{Res}_{s=1} \int_{|a| \leq 1, a \in F^\times \backslash \mathbb{A}^\times} |a|^{s-1}\, d^\times a = \text{Res}_{s=1} L(s, 1_F).$$

When F is a totally real field and σ a cuspidal automorphic representation such that σ_v is a discrete series for any infinite place v, the normalized new vector ϕ^0 is not parallel to the Hilbert newform ϕ: they are different at infinity. If σ is unitary and ϕ^0 is the normalized new vector of σ, then $\bar{\sigma} \cong \tilde{\sigma}$ and $\overline{\phi^0}$ is the normalized new vector of $\bar{\sigma}$. We will see that $(\phi, \phi)_{U_0(N)} = (2\pi)^d \langle \phi_0, \bar{\phi}_0 \rangle_{U_0(N)}$.

Theorem 1.8 (explicit Waldspurger formula). *Let F be a number field. Let B be a quaternion algebra over F and π an irreducible cuspidal automorphic representation of $B_{\mathbb{A}}^\times$ with central character ω. Let K be a quadratic field extension of F and χ a Hecke character of $K_{\mathbb{A}}^\times$. Assume that:*

(1) $\omega \cdot \chi|_{\mathbb{A}^\times} = 1$;

(2) $\epsilon\left(\frac{1}{2}, \pi_v, \chi_v\right) = \chi_v \eta_v(-1)\epsilon(B_v)$ *for all places v of F.*

Then, for any nonzero forms $f_1 \in V(\pi, \chi)$ and $f_2 \in V(\tilde{\pi}, \chi^{-1})$, we have

$$L^{(\Sigma)}\left(\tfrac{1}{2}, \pi, \chi\right) = 2^{-\#\Sigma_D + 2} \cdot C_\infty \cdot \frac{\langle \phi_1^0, \phi_2^0 \rangle_{U_0(N)}}{v_{c_1}^2 \sqrt{|D_K| \|c_1\|^2}} \cdot \frac{P_\chi^0(f_1) P_{\chi^{-1}}^0(f_2)}{\langle f_1, f_2 \rangle_{\hat{R}^\times}},$$

where $\phi_1^0 \in \pi^{\mathrm{JL}}$ and $\phi_2^0 \in \tilde{\pi}^{\mathrm{JL}}$ are normalized new vectors, Σ is the set of places $v|(cD, N)\infty$ of F such that if $v\|N$ then $\mathrm{ord}_v(c/N) \geq 0$, and if $v|\infty$ then $K_v \cong \mathbb{C}$. The constant $C_\infty = \prod_{v|\infty} C_v$, $c_1|c$ and Σ_D are the same as in Theorem 1.5, and $C_v = C(\pi_v^{\mathrm{JL}}, \chi_v)$ is given in (1-1).

For many applications, we need an explicit form of the Waldspurger formula for different test vectors. The following variation of the formula is useful. For each place v of F, fix a $B_v^\times$-invariant pairing $\langle \, , \, \rangle_v$ on $\pi_v \times \tilde{\pi}_v$. Here, if $v|\infty$, we mean it is the restriction of a $B_v^\times$-invariant pairing on the corresponding smooth representations. For any $f'_{1,v} \in \pi_v$, $f'_{2,v} \in \tilde{\pi}_v$ with $\langle f'_{1,v}, f'_{2,v} \rangle_v \neq 0$, define $\beta^0(f'_{1,v}, f'_{2,v})$ as in Theorem 1.6.

Theorem 1.9 (variation of the Waldspurger formula). *Let (π, χ) and $f_1 \in V(\pi, \chi)$, $f_2 \in V(\tilde{\pi}, \chi^{-1})$ be as in Theorem 1.8. Let S be a finite set of places of F, $f'_1 \in \pi$, $f'_2 \in \tilde{\pi}$ be pure vectors which coincide with f_1, f_2 respectively outside S such that $\langle f'_{1,v}, f'_{2,v} \rangle_v \neq 0$ and $\beta^0(f'_{1,v}, f'_{2,v}) \neq 0$ for all $v \in S$. Here β^0 is similarly defined as in Theorem 1.6. Define*

$$P_\chi^0(f'_1) = \frac{\#\mathrm{Pic}_{K/F}(\mathbb{O}_{c_1})}{\mathrm{Vol}(K^\times \mathbb{A}^\times \backslash K_{\mathbb{A}}^\times, dt)} \cdot \int_{K^\times \mathbb{A}^\times \backslash K_{\mathbb{A}}^\times} f'(t) \chi(t) \, dt,$$

and define $P_{\chi^{-1}}^0(f'_2)$ similarly. Then, in the notation of Theorem 1.8, we have

$$L^{(\Sigma)}\left(\tfrac{1}{2}, \pi, \chi\right) = 2^{-\#\Sigma_D + 2} \cdot C_\infty \cdot \frac{\langle \phi_1^0, \phi_2^0 \rangle_{U_0(N)}}{v_{c_1}^2 \sqrt{|D_K| \|c_1^2\|}} \cdot \frac{P_\chi^0(f'_1) P_{\chi^{-1}}^0(f'_2)}{\langle f'_1, f'_2 \rangle_{\hat{R}^\times}} \cdot \prod_{v \in S} \frac{\beta^0(f_{1,v}, f_{2,v})}{\beta^0(f'_{1,v}, f'_{2,v})},$$

Example. Let $\phi = \sum a_n q^n \in S_2(\Gamma_0(N))$ be a newform of weight 2 and p a good ordinary prime of ϕ, K an imaginary quadratic field of discriminant D and χ a character of $\mathrm{Gal}(H_c/K)$ of conductor c that is prime to p. Assume that the conditions (i)–(ii) in Theorem 1.2 are satisfied. Let B be the quaternion algebra, π the cuspidal automorphic representation on $B_{\mathbb{A}}^{\times}$, and identify $\widetilde{\pi}$ with $\bar{\pi}$. Let $f \in \pi^{\widehat{R}^{\times}} = V(\pi, \chi)$ be a nonzero test vector as in Theorem 1.8. Define the p-stabilization of f by

$$f^{\dagger} = f - \alpha^{-1}\pi \begin{pmatrix} 1 \\ & p \end{pmatrix} f,$$

where α is the unit root of $X^2 - a_p X + p$ and $\beta = p/\alpha$ is another root. By the variation of the Waldspurger formula and Theorem 1.2, one may easily obtain a formula for $P_{\chi}^0(f^{\dagger})$, which is used to give the interpolation property of anticyclotomic p-adic L-functions:

$$L(1, \phi, \chi) = 2^{-\mu(N,D)} \cdot \frac{8\pi^2(\phi, \phi)_{\Gamma_0(N)}}{[\mathbb{O}_c^{\times} : \mathbb{Z}^{\times}]^2 \sqrt{|Dc^2|}} \cdot \frac{|P_{\chi}^0(f^{\dagger})|^2}{(f^{\dagger}, f^{\dagger})_{\widehat{R}^{\times}}} \cdot e_p,$$

where

$$e_p = \frac{\beta^0(W, \overline{W})}{\beta^0(W^{\dagger}, \overline{W^{\dagger}})} = \frac{L(2, 1_p)}{L(1, \pi_p, \mathrm{ad})} \cdot (1 - \alpha^{-1}\chi_1(p))^{-1}(1 - \beta^{-1}\chi_1^{-1}(p))^{-1}.$$

Here W is a new vector of the Whittaker model $\mathscr{W}(\pi_p, \psi_p)$ with $\psi_p(x) = e^{-2\pi i \iota(x)}$, where $\iota : \mathbb{Q}_p/\mathbb{Z}_p \to \mathbb{Q}/\mathbb{Z}$ is the natural embedding and $W^{\dagger} := W - \alpha^{-1}\pi_p \begin{pmatrix} 1 \\ & p \end{pmatrix}W$ is its stabilization, where $K_p^{\times} \cong \mathbb{Q}_p^{\times 2}$ is embedded into $\mathrm{GL}_2(\mathbb{Q}_p)$ as a diagonal subgroup and $\chi_1(a) = \chi \begin{pmatrix} a \\ & 1 \end{pmatrix}$.

Now we consider the situation that:

(1) F is a totally real field and K is a totally imaginary quadratic extension over F,

(2) for any place $v | \infty$ of F, π_v^{JL} is a unitary discrete series of weight 2,

(3) $(c, N) = 1$.

Let ϕ be the Hilbert newform as in Theorem 1.5 (which is different from the one we chose in Theorem 1.8). We are going to give an explicit form of the Waldspurger formula following [Gross 1988], which is quoted in many references. Let $X = B^{\times} \backslash \widehat{B}^{\times}/\widehat{R}^{\times}$ and let $g_1, \ldots, g_n \in \widehat{B}^{\times}$ be a complete set of representatives of X. Write $[g] \in X$ for the class of an element $g \in \widehat{B}^{\times}$. For each g_i, let $\Gamma_i = (B^{\times} \cap g_i \widehat{R}^{\times} g_i^{-1})/\mathbb{O}^{\times}$, which is finite, and denote by w_i its order. Let $\mathbb{Z}[X]$ be the free $\mathbb{Z}$-module (of rank #X) of formal sums $\sum_i a_i[g_i]$. There is a height pairing on $\mathbb{Z}[X] \times \mathbb{Z}[X]$ defined by

$$\left\langle \sum a_i[g_i], \sum b_i[g_i] \right\rangle = \sum_i a_i b_i w_i.$$

By Eichler's norm theorem, the norm map

$$\mathrm{N} : X \longrightarrow C_+, \quad \text{where } X := B^{\times} \backslash \widehat{B}^{\times}/\widehat{R}^{\times}, \; C_+ := F_+^{\times} \backslash \widehat{F}^{\times}/\widehat{\mathbb{O}}^{\times},$$

is surjective. For each $c \in C_+$, let $X_c \subset X$ be the preimage of c and $\mathbb{Z}[X_c]$ be the submodule of $\mathbb{Z}[X]$ supported on X_c. Then $\mathbb{Z}[X] = \bigoplus_{c \in C_+} \mathbb{Z}[X_c]$. Let $\mathbb{Z}[X_c]^0$ be the submodule of classes $\sum a_i[g_i] \in \mathbb{Z}[X_c]$ with degree $\sum_i a_i = 0$, and let $\mathbb{Z}[X]^0 = \bigoplus_{c \in C_+} \mathbb{Z}[X_c]^0$ and $\mathbb{C}[X]^0 = \mathbb{Z}[X]^0 \otimes_{\mathbb{Z}} \mathbb{C}$. Note that $V(\pi, \chi) \subset \pi^{\widehat{R}^\times}$ by Proposition 3.8, and then there is an injection

$$V(\pi, \chi) \longrightarrow \mathbb{C}[X]^0, \quad f \mapsto \sum f([g_i])w_i^{-1}[g_i],$$

so we can view $V(\pi, \chi)$ as a line on $\mathbb{C}[X]^0$. It follows that $\langle f, f \rangle = \langle f, f \rangle_{\widehat{R}^\times}$. The fixed embedding $K \to B$ induces a map

$$\mathrm{Pic}(\mathbb{O}_c) \longrightarrow X, \quad t \longmapsto x_t,$$

using which we define an element in $\mathbb{C}[X]$,

$$P_\chi := \sum_{t \in \mathrm{Pic}(\mathbb{O}_c)} \chi^{-1}(t) x_t,$$

and let P_χ^π be its projection to the line $V(\pi, \chi)$. Then the explicit formula in Theorem 1.8 implies:

Theorem 1.10. *Let (π, χ) be as above with conditions (1)–(3). The height of P_χ^π is given by the formula*

$$L^{(\Sigma)}\left(\tfrac{1}{2}, \pi, \chi\right) = 2^{-\#\Sigma_D} \cdot \frac{(8\pi^2)^d \cdot (\phi, \phi)_{U_0(N)}}{u^2\sqrt{|D_K|}\|c\|^2} \cdot \langle P_\chi^\pi, P_\chi^\pi \rangle,$$

where

$$\Sigma := \{v|(N, D)\infty | \text{if } v\|N \text{ then } v \nmid D\}, \quad \Sigma_D := \{v|(N, D)\},$$

$u = \#\kappa_c \cdot [\mathbb{O}_c^\times : \mathbb{O}^\times]$, *and $\phi \in \pi^{\mathrm{JL}}$ is the Hilbert newform as in Theorem 1.5. For any nonzero vector $f \in V(\pi, \chi)$, let $P_\chi^0(f) = \sum_{t \in \mathrm{Pic}(\mathbb{O}_c)} f(t)\chi(t)$; then we have*

$$L^{(\Sigma)}\left(\tfrac{1}{2}, \pi, \chi\right) = 2^{-\#\Sigma_D} \cdot \frac{(8\pi^2)^d \cdot (\phi, \phi)_{U_0(N)}}{u^2\sqrt{|D_K|}\|c\|^2} \cdot \frac{|P_\chi^0(f)|^2}{\langle f, f \rangle}.$$

Remark. When c and N have a common factor, one can still formulate an explicit formula in the spirit of Gross by defining a system of height pairings $\langle\,,\,\rangle_U$ in the same way as Theorem 1.8.

As a byproduct, we obtain the following result about the relation between the Petersson norm of a newform and a special value of the adjoint L-function:

Proposition 1.11. *Let F be a totally real field and σ a cuspidal unitary automorphic representation of $\mathrm{GL}_2(\mathbb{A})$ of conductor N such that, for any $v|\infty$, σ_v is a discrete*

series of weight k_v. Let ϕ be the Hilbert newform in σ as in Theorem 1.5. Then

$$\frac{L^{(S)}(1, \sigma, \mathrm{ad})}{(\phi, \phi)_{U_0(N)}} = 2^{d-1+\sum_{v|\infty} k_v} \cdot \|N\delta^{-2}\|^{-1} \cdot h_F^{-1},$$

where S is the set of finite places v of F with $\mathrm{ord}_v(N) \geq 2$ and $\mathrm{ord}_v(N) > \mathrm{ord}_v(C)$, C is the conductor of the central character of σ, h_F is the ideal class number of F, and

$$(\phi, \phi)_{U_0(N)} = \iint_{X_{U_0(N)}} |\phi|^2 \left(\bigwedge_{v|\infty} y_v^{k_v-2} \, dx_v \, dy_v \right), \quad z_v = x_v + y_v i.$$

Or, equivalently,

$$\frac{L^{(S\infty)}(1, \sigma, \mathrm{ad})}{(\phi, \phi)_{U_0(N)}} = \tfrac{1}{2} \cdot \|N\delta^{-2}\|^{-1} \cdot h_F^{-1} \cdot \prod_{v|\infty} \frac{4^{k_v} \pi^{k_v+1}}{\Gamma(k_v)}.$$

Proof. This follows from Proposition 2.1, Lemma 2.2, and Proposition 3.11. Here [Tunnell 1978, Proposition 3.4] is also used.   □

Example. Assume that $F = \mathbb{Q}$ and σ is the cuspidal automorphic representation associated to a cuspidal newform $\phi \in S_k(\mathrm{SL}_2(\mathbb{Z}))$. Then we have that

$$L(1, \sigma, \mathrm{ad}) = 2^k \cdot (\phi, \phi)_{\mathrm{SL}_2(\mathbb{Z})}, \quad L^{(\infty)}(1, \sigma, \mathrm{ad}) = \frac{2^{2k-1}\pi^{k+1}}{\Gamma(k)} \cdot (\phi, \phi)_{\mathrm{SL}_2(\mathbb{Z})}.$$

2. Reduction to local theory

We now explain how to obtain the explicit formulas in Theorems 1.5 and 1.8 from the original Waldspurger formula and the general Gross–Zagier formula proved in [Yuan et al. 2013]. We first consider the Waldspurger formula. Let B be a quaternion algebra over a number field F and π a cuspidal automorphic representation on $B_{\mathbb{A}}^\times$ with central character ω. Let K be a quadratic field extension over F and χ be a Hecke character on $K_{\mathbb{A}}^\times$. Assume that: (1) $\omega \cdot \chi|_{\mathbb{A}^\times} = 1$; and (2) for any place v of F, $\epsilon\left(\tfrac{1}{2}, \pi_v, \chi_v\right) = \chi_v \eta_v(-1)\epsilon(B_v)$. Define the Petersson pairing on $\pi \otimes \tilde{\pi}$ by

$$\langle f_1, f_2 \rangle_{\mathrm{Pet}} = \int_{B^\times \mathbb{A}^\times \backslash B_{\mathbb{A}}^\times} f_1(g) f_2(g) \, dg$$

with the Tamagawa measure, so that the volume of $B^\times \mathbb{A}^\times \backslash B_{\mathbb{A}}^\times$ is 2. Let P_χ denote the period functional on π

$$P_\chi(f) = \int_{K^\times \mathbb{A}^\times \backslash K_{\mathbb{A}}^\times} f(t) \chi(t) \, dt \quad \text{for all } f \in \pi.$$

Then Waldspurger's period formula [Waldspurger 1985; Yuan et al. 2013, Theorem 1.4] says that, for any pure tensors $f_1 \in \pi$, $f_2 \in \tilde{\pi}$ with $\langle f_1, f_2 \rangle_{\mathrm{Pet}} \neq 0$,

$$\frac{P_\chi(f_1)P_{\chi^{-1}}(f_2)}{\langle f_1, f_2\rangle_{\text{Pet}}} = \frac{L\left(\frac{1}{2}, \pi, \chi\right)}{2L(1, \pi, \text{ad})L(2, 1_F)^{-1}} \cdot \prod_v \beta(f_{1,v}, f_{2,v}), \qquad (2\text{-}1)$$

where $L(1, \pi, \text{ad})$ is defined using the Jacquet–Langlands lifting of π. Here, for any place v of F, let $\langle \, , \, \rangle_v : \pi_v \times \tilde{\pi}_v \to \mathbb{C}$ be a nontrivial invariant pairing; then

$$\beta(f_{1,v}, f_{2,v}) = \frac{L(1, \eta_v)L(1, \pi_v, \text{ad})}{L\left(\frac{1}{2}, \pi_v, \chi_v\right)L(2, 1_{F_v})} \int_{K_v^\times/F_v^\times} \frac{\langle \pi(t_v)f_{1,v}, f_{2,v}\rangle_v}{\langle f_{1,v}, f_{2,v}\rangle_v} \chi(t_v) \, dt_v,$$

where local Haar measures dt_v are chosen so that $\bigotimes_v dt_v = dt$ is the Haar measure on $K_{\mathbb{A}}^\times/\mathbb{A}^\times$ in the definitions of P_χ and $P_{\chi^{-1}}$, and the volume of $K^\times \backslash K_{\mathbb{A}}^\times/\mathbb{A}^\times$ with respect to dt is $2L(1, \eta)$. Note that the Haar measure dt is different from the one used in [Yuan et al. 2013, Theorem 1.4]. To obtain the explicit formula, we first relate $P_\chi(f)$, $L(1, \pi, \text{ad})$, and $\langle f_1, f_2\rangle_{\text{Pet}}$ to the corresponding objects with levels in Theorem 1.8, and reduce to local computation.

For our purpose, it is more convenient to normalize local additive characters and local Haar measures as follows. Take the additive character $\psi = \bigotimes_v \psi_v$ on $\mathbb{A}$ given by

$$\psi_v(a) = \begin{cases} e^{2\pi i a} & \text{if } F_v = \mathbb{R}, \\ e^{4\pi i \text{Re}(a)} & \text{if } F_v = \mathbb{C}, \\ \psi_p(\text{tr}_{F/\mathbb{Q}_p}(a)) & \text{if } F_v \text{ is a finite extension of } \mathbb{Q}_p \text{ for some prime } p, \end{cases}$$

where $\psi_p(b) = e^{-2\pi i \iota(b)}$ and $\iota : \mathbb{Q}_p/\mathbb{Z}_p \to \mathbb{Q}/\mathbb{Z}$ is the natural embedding. It turns out that ψ is a character on $F \backslash \mathbb{A}$. For any place v of F, let da_v denote the Haar measure on F_v self-dual to ψ_v and let $d^\times a_v$ denote the Haar measure on $F_v^\times$ defined by $d^\times a_v = L(1, 1_v) \, da_v/|a_v|_v$. Let L be a separable quadratic extension of F_v or a quaternion algebra over F_v, and q the reduced norm on L; then (L, q) is a quadratic space over F_v. Fix the Haar measure dx on L to be the one self-dual with respect to ψ_v and q, in the sense that $\widehat{\widehat{\Phi}}(x) = \Phi(-x)$ for any $\Phi \in S(L)$, where $\widehat{\Phi}(y) := \int_L \Phi(x)\psi_v(\langle x, y\rangle) \, dx$ is the Fourier transform of Φ and $\langle x, y\rangle = q(x+y) - q(x) - q(y)$ is the bilinear form on L associated to q. Fix the Haar measure $d^\times x$ on $L^\times$ to be the one defined by

$$d^\times x = \begin{cases} L(1, 1_v)^2 \dfrac{dx}{|q(x)|_v} & \text{if } L = F_v^2, \\[2ex] L(1, 1_L) \dfrac{dx}{|q(x)|_v} & \text{if } L \text{ is a quadratic field extension over } F_v, \\[2ex] L(1, 1_v) \dfrac{dx}{|q(x)|_v^2} & \text{if } L \text{ is a quaternion algebra.} \end{cases}$$

Endow $L^\times/F_v^\times$ with the quotient Haar measure. Let K be a quadratic field extension of F and B a quaternion algebra over F. For local Haar measures on $K_v^\times/F_v^\times$ and

$B_v^\times / F_v^\times$, their product Haar measures on $K_{\mathbb{A}}^\times / \mathbb{A}^\times$ and $B_{\mathbb{A}}^\times / \mathbb{A}^\times$ satisfy

$$\mathrm{Vol}(K^\times \backslash K_{\mathbb{A}}^\times / \mathbb{A}^\times) = 2L(1, \eta) \quad \text{and} \quad \mathrm{Vol}(B^\times \backslash B_{\mathbb{A}}^\times / \mathbb{A}^\times) = 2.$$

Thus, these measures can be taken as the ones used in the above statement of Waldspurger's formula. From now on, we always use these measures and the additive character ψ on $\mathbb{A}$.

2A. Petersson pairing formula. Let σ be a cuspidal automorphic representation of $\mathrm{GL}_2(\mathbb{A})$ and $\widetilde{\sigma}$ its contragredient; let N be the unipotent subgroup $N = \{ \left(\begin{smallmatrix} 1 & x \\ & 1 \end{smallmatrix} \right) \mid x \in F \}$ of GL_2. View ψ as a character on $N(F) \backslash N(\mathbb{A})$ and the Haar measure da on $\mathbb{A}$ as the one on $N(\mathbb{A})$. For any $\phi \in \sigma$, let $W_\phi \in \mathcal{W}(\sigma, \psi)$ be the Whittaker function associated to ϕ,

$$W_\phi(g) := \int_{N(F) \backslash N(\mathbb{A})} \phi(ng) \overline{\psi(n)} \, dn.$$

Recall there is a $\mathrm{GL}_2(F_v)$-pairing on $\mathcal{W}_{\sigma_v, \psi_v} \times \mathcal{W}_{\widetilde{\sigma}_v, \psi_v^{-1}}$: for any local Whittaker functions $W_{1,v} \in \mathcal{W}(\sigma_v, \psi_v)$, $W_{2,v} \in \mathcal{W}(\widetilde{\sigma}_v, \psi_v^{-1})$,

$$\langle W_{1,v}, W_{2,v} \rangle_v = \int_{F_v^\times} W_{1,v} \begin{pmatrix} a & \\ & 1 \end{pmatrix} W_{2,v} \begin{pmatrix} a & \\ & 1 \end{pmatrix} d^\times a.$$

Define the Petersson pairing on $\sigma \times \widetilde{\sigma}$ by

$$\langle \phi_1, \phi_2 \rangle_{\mathrm{Pet}} := \int_{Z(\mathbb{A}) \, \mathrm{GL}_2(F) \backslash \mathrm{GL}_2(\mathbb{A})} \phi_1(g) \phi_2(g) \, dg, \quad \phi_1 \in \sigma, \ \phi_2 \in \widetilde{\sigma},$$

where $Z \cong F^\times$ is the center of GL_2.

Proposition 2.1. *For any pure tensors $\phi_1 \in \sigma$, $\phi_2 \in \widetilde{\sigma}$, with $W_{\phi_i} = \bigotimes_v W_{i,v}, i = 1, 2$,*

$$\langle \phi_1, \phi_2 \rangle_{\mathrm{Pet}} = 2L(1, \sigma, \mathrm{ad}) L(2, 1_F)^{-1} \prod_v \alpha(W_{1,v}, W_{2,v}), \tag{2-2}$$

where, for any place v of F,

$$\alpha(W_{1,v}, W_{2,v}) = \frac{1}{L(1, \sigma_v, \mathrm{ad}) L(1, 1_v) L(2, 1_v)^{-1}} \cdot \langle W_{1,v}, W_{2,v} \rangle.$$

Proof. We may assume that the cuspidal automorphic representation σ is also unitary and identify $\widetilde{\sigma}$ with $\bar{\sigma}$. Let $G = \mathrm{GL}_2$ over F, P the parabolic subgroup of upper triangular matrices in G, and let $U = \prod_v U_v$ be a maximal compact subgroup of $G(\mathbb{A})$. For any place v of F, with respect to the Iwasawa decomposition of $G(F_v)$,

$$g = a \begin{pmatrix} 1 & x \\ & 1 \end{pmatrix} \begin{pmatrix} 1 & \\ & b \end{pmatrix} k \in G(F_v), \quad a, b \in F_v^\times, \ x \in F_v, \ k \in U_v.$$

Choose the measure dk on U_v such that $dg = |b| \, dx \, d^\times a \, d^\times b \, dk$ is the fixed local Haar measure on $G(F_v)$. For v nonarchimedean, U_v has volume $L(2, 1_v)^{-1} |\delta_v|^{1/2}$

with respect to dk and has volume $L(2, 1_v)^{-1}|\delta_v|^2$ with respect to the fixed measure on $G(F_v)$; for v archimedean, U_v has volume $L(2, 1_v)^{-1}$ with respect to dk.

By [Jacquet and Chen 2001, Lemma 2.3], for any Bruhat–Schwartz function $\Phi_v \in \mathcal{S}(F_v^2)$ we have

$$\int_{F_v^\times \times U_v} \Phi([0, b]k)|b|^2 \, d^\times b \, dk = \widehat{\Phi}_v(0),$$

where $\widehat{\Phi}_v$ is the Fourier transformation of Φ_v and $\widehat{\Phi}_v(0)$ is independent of the choice of the additive character ψ_v. For any $\Phi \in \mathcal{S}(\mathbb{A}^2)$, let

$$F(s, g, \Phi) = |\det g|^s \int_{\mathbb{A}^\times} \Phi([0, b]g)|b|^{2s} \, d^\times b,$$

and define the Eisenstein series

$$E(s, g, \Phi) := \sum_{\gamma \in P(F)\backslash G(F)} F(s, \gamma g, \Phi), \quad \mathrm{Re}(s) \gg 0.$$

By the Poisson summation formula,

$$E(s, g, \Phi) = |\det g|^s \int_{F^\times \backslash \mathbb{A}^\times} \left(\sum_{\xi \in F^2 \backslash \{0\}} \Phi(a\xi g) \right) |a|^{2s} \, d^\times a$$

$$= |\det g|^s \int_{|a| \geq 1} \left(\sum_{\xi \in F^2 \backslash \{0\}} \Phi(a\xi g) \right) |a|^{2s} \, d^\times a$$

$$+ |\det g|^{s-1} \int_{|a| \geq 1} \left(\sum_{\xi \in F^2 \backslash \{0\}} \widehat{\Phi}(g^{-1}\xi^t a) \right) |a|^{2-2s} \, d^\times a$$

$$+ |\det g|^{s-1} \widehat{\Phi}(0) \int_{|a| \leq 1} |a|^{2s-2} \, d^\times a - |\det g|^s \Phi(0) \int_{|a| \leq 1} |a|^{2s} \, d^\times a.$$

It follows that $E(s, g, \Phi)$ has meromorphic continuation to the whole s-plane, has possible poles only at $s = 0$ and 1, and its residue at $s = 1$ is equal to

$$\mathrm{Res}_{s=1} E(s, g, \Phi) = \widehat{\Phi}(0) \lim_{s \to 1} (s - 1) \int_{|a| \leq 1} |a|^{2s-2} \, d^\times a = \tfrac{1}{2} \widehat{\Phi}(0) \, \mathrm{Res}_{s=1} L(s, 1_F),$$

which is independent of g. By unfolding the Eisenstein series and Fourier expansions of ϕ_i,

$$Z(s, \phi_1, \phi_2, \Phi) := \int_{[Z\backslash G]} \phi_1(g)\phi_2(g)E(s, g, \Phi) \, dg$$

$$= \int_{N(\mathbb{A})\backslash G(\mathbb{A})} |\det g|^s W_{\phi_1}(g) W_{\phi_2}(g) \Phi([0, 1]g) \, dg$$

has an Euler product if $\Phi \in S(\mathbb{A}^2)$ is a pure tensor. For each place v of F and $\Phi_v \in S(F_v^2)$, denote

$$Z(s, W_{1,v}, W_{2,v}, \Phi_v) = \int_{N(F_v)\backslash G(F_v)} |\det g|^s W_{1,v}(g) W_{2,v}(g) \Phi_v([0,1]g)\, dg,$$

which has meromorphic continuation to the whole s-plane; and moreover, for $v \nmid \infty$, the fractional ideal of $\mathbb{C}[q_v^s, q_v^{-s}]$ of all $Z(s, W_{1,v}, W_{2,v}, \Phi_v)$ with $W_{1,v} \in \mathcal{W}(\sigma_v, \psi_v)$, $W_{2,v} \in \mathcal{W}(\widetilde{\sigma}_v, \psi_v^{-1})$ and $\Phi_v \in \mathscr{S}(F_v^2)$ is generated by $L(s, \sigma_v \times \widetilde{\sigma}_v)$. It is also known ([Jacquet and Chen 2001, p. 51]) that, for each v,

$$Z(1, W_{1,v}, W_{2,v}, \Phi_v)$$
$$= \int_{F_v^\times} W_{1,v}\begin{pmatrix} a & \\ & 1 \end{pmatrix} W_{2,v}\begin{pmatrix} a & \\ & 1 \end{pmatrix} d^\times a \cdot \iint_{F_v^\times \times U_v} \Phi_v([0, b]k)|b|^2 \, d^\times b\, dk,$$

with the Haar measures chosen above. Let $\Phi = \bigotimes_v \Phi_v \in \mathscr{S}(\mathbb{A}^2)$ be a pure tensor such that $\widehat{\Phi}(0) \neq 0$ and take residue at $s = 1$ on the two sides of

$$Z(s, \phi_1, \phi_2, \Phi) = \prod_v Z(s, W_{1,v}, W_{2,v}, \Phi_v).$$

We have

$$\langle \phi_1, \phi_2 \rangle_{\text{Pet}} \operatorname{Res}_{s=1} E(s, g, \Phi) = \operatorname{Res}_{s=1} L(s, \sigma \times \widetilde{\sigma}) \widehat{\Phi}(0) \prod_v \frac{\langle W_{1,v}, W_{2,v} \rangle_v}{L(1, \sigma_v \times \widetilde{\sigma}_v)},$$

or

$$\frac{L(1, \sigma, \text{ad})}{\langle \phi_1, \phi_2 \rangle_{\text{Pet}}} = \frac{1}{2} \prod_v \frac{L(1, \sigma_v, \text{ad})L(1, 1_{F_v})}{\langle W_{1,v}, W_{2,v} \rangle_v}.$$

The formula in the proposition follows. □

2B. *U-level pairing.*

Lemma 2.2. *Let B be a quaternion algebra over a number field F and denote by r, s, t integers such that $B \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{H}^r \times M_2(\mathbb{R})^s \times M_2(\mathbb{C})^t$. For $U \subset \widehat{B}^\times$ an open compact subgroup, the volume of X_U, defined after Definition 1.7, is given by*

$$\text{Vol}(X_U) = 2(4\pi^2)^{-d} \#(\mathbb{A}_f^\times / F^\times U_Z) \cdot \frac{\text{Vol}(U_Z)}{\text{Vol}\, U},$$

where $U_Z = U \cap \widehat{F}^\times$ and the volumes $\text{Vol}(U_Z)$ and $\text{Vol}\, U$ are with respect to Tamagawa measure, so that

$$\text{Vol}(\text{GL}_2(\mathbb{O}_v)) = L(2, 1_v)^{-1} \text{Vol}(\mathbb{O}_v)^4,$$
$$\text{Vol}(B_v^\times) = L(2, 1_v)^{-1} \text{Vol}(\mathbb{O}_v)^4 (q_v - 1)^{-1} \quad \text{for } B_v \text{ division.}$$

In particular, if U contains $\widehat{\mathbb{O}}^\times$ then — where h_F is the class number of F —

$$\text{Vol}(X_U) = 2(4\pi^2)^{-d} |D_F|^{-1/2} \cdot h_F \cdot \text{Vol}(U)^{-1}.$$

Proof (see also [Yuan et al. 2013] *for the case $s = 1$ and $t = 0$).* Let q be the reduced norm on B, and $B^1 := \{b \in B^\times \mid q(b) = 1\}$. For each place v of F, we have the exact sequence

$$1 \longrightarrow B_v^1 \longrightarrow B_v^\times \longrightarrow q(B_v^\times) \longrightarrow 1,$$

and define the Haar measure dh_v on B_v^1 so that the Haar measure on $q(B_v^\times)$ — obtained by the restriction of the Haar measure on $F_v^\times$ — equals the quotient of the Haar measure on $B_v^\times$ by dh_v. The product of these local measures give the Tamagawa measure on $B_{\mathbb{A}}^1$, so that $\mathrm{Vol}(B^1 \backslash B_{\mathbb{A}}^1) = 1$. This follows from the fact that the Tamagawa numbers of B^1 and $B^\times$ are 1 and 2, respectively. Assume that $B \otimes_{\mathbb{Q}} \mathbb{R} = \mathbb{H}^r \times M_2(\mathbb{R})^s \times M_2(\mathbb{C})^t$. We assume that $s + t > 0$ first and let $\Sigma \subset \infty$ be the subset of infinite places of F where B splits. By the strong approximation theorem, $B_{\mathbb{A}}^1 = B^1 B_\infty^1 U^1$, where $U^1 = U \cap B_{\mathbb{A}_f}^1$ is an open compact subgroup of $B_{\mathbb{A}_f}^1$. It follows that

$$B^1 \backslash B_{\mathbb{A}}^1 = B^1 \backslash B^1 B_\infty^1 U^1 = (\Gamma \backslash B_\Sigma^1) B_\infty^{1,\Sigma} U^1,$$

where $\Gamma = B^1 \cap U^1$, and we identify $\Gamma \backslash B_\Sigma^1$ with the fundamental domain of this quotient.

For a real place v of F, $B_v^1 \cong \mathrm{SL}_2(\mathbb{R})$. By the Iwasawa decomposition, any element is uniquely of the form

$$\begin{pmatrix} 1 & x \\ & 1 \end{pmatrix} \begin{pmatrix} y^{1/2} & \\ & y^{-1/2} \end{pmatrix} \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}, \quad x \in \mathbb{R}, \ y \in \mathbb{R}_+, \ \theta \in [0, 2\pi).$$

The measure on B_v^1 is $dx\,dy\,d\theta / 2y^2$ with $dx\,dy$ the usual Lebesgue measure, and θ has volume 2π. For a complex place v of F, $B_v^1 \cong \mathrm{SL}_2(\mathbb{C})$. By the Iwasawa decomposition, any element in $\mathrm{SL}_2(\mathbb{C})$ is uniquely of form

$$\begin{pmatrix} 1 & z \\ & 1 \end{pmatrix} \begin{pmatrix} v^{1/2} & \\ & v^{-1/2} \end{pmatrix} u, \quad z \in \mathbb{C}, \ v \in \mathbb{R}_+, \ u \in \mathrm{SU}_2,$$

The measure on B_v^1 is $dx\,dy\,dv\,du / v^3$ with $z = x + yi$, dx, dy, dv the usual Lebesgue measure, and du has volume $8\pi^2$ (see [Vignéras 1980]). It follows that

$$\mathrm{Vol}(\Gamma \backslash B_\Sigma^1) = 2^{-t}(4\pi^2)^{s+2t} w_U^{-1} \cdot \mathrm{Vol}\left(\Gamma \backslash (\mathcal{H}_2^s \times \mathcal{H}_3^t), \frac{dx\,dy}{4\pi y^2} \wedge \frac{dx\,dy\,dv}{\pi^2 v^3}\right),$$

where $w_U = \#\{\pm 1\} \cap U$. But also, for any infinite place $v \notin \Sigma$, $\mathrm{Vol}(B_v^1) = 4\pi^2$. Thus,

$$w_U^{-1} \cdot 2^{-t}(4\pi^2)^d \cdot \mathrm{Vol}\left(\Gamma \backslash (\mathcal{H}_2^s \times \mathcal{H}_3^t), \frac{dx\,dy}{4\pi y^2} \wedge \frac{dx\,dy\,dv}{\pi^2 v^3}\right) \cdot \mathrm{Vol}(U^1) = 1,$$

where $d = [F : \mathbb{Q}]$. Let $B_+^\times \subset B^\times$ be the subgroup of elements whose norms are positive at all real places. Now consider the natural map

$$(B^1 \cap U^1) \backslash (\mathcal{H}_2^s \times \mathcal{H}_3^t) \longrightarrow (B_+^\times \cap U) \backslash (\mathcal{H}_2^s \times \mathcal{H}_3^t),$$

whose degree is just

$$[(B_+^\times \cap U) : (B^1 \cap u^1)\mu_U] = [\det(B_+^\times \cap U) : \mu_U^2] = [\mu_U' : \mu_U^2].$$

Here $\mu_U = F^\times \cap U$ and $\mu_U' = F_+^\times \cap \det U$, subgroups of $\mathbb{O}_F^\times$ with finite index. It follows that

$$\mathrm{Vol}(X_U) = \mathrm{Vol}((B_+^\times \cap U) \backslash (\mathcal{H}_2^s \times \mathcal{H}_3^t)) \cdot \#(F_+^\times \backslash \widehat{F}^\times / \det U)$$

$$= \frac{2^t w_U}{(4\pi^2)^d \cdot \mathrm{Vol}(U^1) \cdot [\mu_U' : \mu_U^2]} \cdot \#(F_+^\times \backslash \widehat{F}^\times / \det U).$$

Note that

$$\frac{\#(\widehat{F}^\times / F_+^\times \det U)}{\#(\widehat{F}^\times \backslash F^\times U_Z)} = [F^\times U_Z : F_+^\times \det U] = [F^\times : F_+^\times] \frac{\mathrm{Vol}(U_Z)}{\mathrm{Vol}(\det U)} [\mu_U' : \mu_U].$$

Since $[F^\times : F_+^\times] = 2^{r+s}$, $[\mu_U : \mu_U^2] = 2^{r+s+t-1} w_U$, and $\mathrm{Vol}\, U = \mathrm{Vol}(U^1)\, \mathrm{Vol}(\det U)$, we have

$$\mathrm{Vol}(X_U) = 2(4\pi^2)^{-d} \#(\widehat{F}^\times / F^\times U_Z) \cdot \frac{\mathrm{Vol}(U_Z)}{\mathrm{Vol}(U)}.$$

Now assume $s = t = 0$. The Tamagawa number of $B^\times$ is 2, $\mathrm{Vol}(B_v^\times / F_v^\times) = 4\pi^2$ for any $v | \infty$, and the decomposition

$$B^\times \mathbb{A}^\times \backslash B_\mathbb{A}^\times = F_\infty^\times \backslash B_\infty^\times \times B^\times \widehat{F}^\times \backslash \widehat{B}^\times.$$

It follows that $\mathrm{Vol}(B^\times \widehat{F}^\times \backslash \widehat{B}^\times) = 2(4\pi^2)^{-d}$. Let $\gamma_1, \ldots, \gamma_h$ be a complete set of representatives in $\widehat{B}^\times$ of the coset $B^\times \backslash \widehat{B}^\times / U$. Consider the natural map

$$B^\times \backslash B^\times \gamma_i U \longrightarrow B^\times \widehat{F}^\times \backslash B^\times \widehat{F}^\times \gamma_i U,$$

whose degree is $\#\widehat{F}^\times / F^\times U_Z$. Now

$$\mathrm{Vol}(B^\times \widehat{F}^\times \backslash B^\times \widehat{F}^\times \gamma_i U) = \mathrm{Vol}\left(\frac{\gamma_i (U/U_Z)\gamma_i^{-1}}{(B^\times \cap \gamma_i U \gamma_i^{-1})/\mu_Z} \right) = \frac{\mathrm{Vol}(U)/\mathrm{Vol}(U_Z)}{\#(B^\times \cap \gamma_i U \gamma_i^{-1})/\mu_Z}.$$

Thus,

$$2(4\pi^2)^{-d} = \mathrm{Vol}(B^\times \widehat{F}^\times \backslash \widehat{B}^\times)$$

$$= (\#\widehat{F}^\times / F^\times U_Z)^{-1} \cdot \frac{\mathrm{Vol}(U)}{\mathrm{Vol}(U_Z)} \cdot \sum_{i=1}^{h} \frac{1}{\#(B^\times \cap \gamma_i U \gamma_i^{-1})/\mu_Z}. \qquad \square$$

2C. c_1-level periods. Now take $f_1 \in V(\pi, \chi)$, $f_2 \in V(\widetilde{\pi}, \chi^{-1})$ to be nonzero test vectors as defined before. Let $\sigma = \pi^{\mathrm{JL}}$ and take $\phi_1 \in \sigma$ and $\phi_2 \in \widetilde{\sigma}$ to be normalized new vectors. The c_1-level periods $P_\chi^0(f_1)$, $P_{\chi^{-1}}^0(f_2)$ are related to the periods in Waldspurger's formula by the following lemma:

Lemma 2.3. *Let $b \subset \mathbb{O}$ be a nonzero ideal of F and denote by $\mathrm{Pic}_{K/F}(\mathbb{O}_b)$ the group $\widehat{K}^\times / K^\times \widehat{F}^\times \widehat{\mathbb{O}}_b^\times$. Then there is a relative class number formula,*

$$L^{(b)}(1, \eta) \cdot \| D_{K/F} b^2 \delta \|^{1/2} \cdot 2^{-r_{K/F}} = \frac{\# \mathrm{Pic}_{K/F}(\mathbb{O}_b) \cdot R_b}{\# \kappa_b \cdot w_b},$$

where $r_{K/F} = \mathrm{rank}\, \mathbb{O}_K^\times - \mathrm{rank}\, \mathbb{O}^\times$, $w_b = [\mathbb{O}_{b,\mathrm{tor}}^\times : \mathbb{O}_{\mathrm{tor}}^\times]$, R_b is the quotient of the regulator of $\mathbb{O}_b^\times$ by that of $\mathbb{O}^\times$, and κ_b is the kernel of the natural morphism from $\mathrm{Pic}(\mathbb{O})$ to $\mathrm{Pic}(\mathbb{O}_b)$. Define a constant $\nu_b := 2^{-r_{K/F}} R_b^{-1} \cdot \# \kappa_b w_b$. Then

$$P_\chi(f) = 2 L_{c_1}(1, \eta) \| D c_1^2 \delta \|^{-1/2} \nu_{c_1}^{-1} \cdot P_\chi^0(f).$$

Proof. There are exact sequences

$$1 \longrightarrow \kappa_b \longrightarrow \widehat{F}^\times / F^\times \widehat{\mathbb{O}}_F^\times \longrightarrow \widehat{K}^\times / K^\times \widehat{\mathbb{O}}_b^\times \longrightarrow \widehat{K}^\times / K^\times \widehat{F}^\times \widehat{\mathbb{O}}_b^\times \longrightarrow 1$$

and

$$1 \longrightarrow \mathbb{O}_K^\times / \mathbb{O}_b^\times \longrightarrow \widehat{\mathbb{O}}_K^\times / \widehat{\mathbb{O}}_b^\times \longrightarrow \widehat{K}^\times / K^\times \widehat{\mathbb{O}}_b^\times \longrightarrow \widehat{K}^\times / K^\times \widehat{\mathbb{O}}_K^\times \longrightarrow 1.$$

It follows that

$$\# \mathrm{Pic}_{K/F}(\mathbb{O}_b) = \# \widehat{K}^\times / K^\times \widehat{F}^\times \widehat{\mathbb{O}}_b^\times = \frac{h_K}{h_F} \cdot [\widehat{\mathbb{O}}_K^\times : \widehat{\mathbb{O}}_b^\times] \cdot [\mathbb{O}_K^\times : \mathbb{O}_b^\times]^{-1} \cdot \# \kappa_b,$$

where $h_K = \# \widehat{K}^\times / K^\times \widehat{\mathbb{O}}_K^\times$ is the ideal class number of K and similarly for h_F. By the class number formula for F and K,

$$\mathrm{Res}_{s=1} L(s, 1_F) = 2^{r_F + 1} \frac{R_F h_F}{w_F \sqrt{|D_F|}}, \quad \mathrm{Res}_{s=1} L(s, 1_K) = 2^{r_K + 1} \frac{R_K h_K}{w_K \sqrt{|D_K|}},$$

where $r_F = \mathrm{rank}\, \mathbb{O}_F^\times$, D_F is the discriminant of F, R_F is the regulator of $\mathbb{O}^\times$, h_F the ideal class number of F, $w_F = \# \mathbb{O}_{\mathrm{tor}}^\times$, and similar for r_K, D_K, R_K, h_K and w_K. Noting that $|D_K|/|D_F| = |D_{K/F} \delta|_{\mathbb{A}}^{-1}$ and $[\widehat{\mathbb{O}}_K^\times : \widehat{\mathbb{O}}_b^\times]^{-1} = L_b(1, \eta) |b|$, we have that

$$L(1, \eta) = \frac{h_K}{h_F} \cdot 2^{r_{K/F}} \frac{R_K w_K^{-1}}{R_F w_F^{-1}} \cdot \| D_{K/F} \delta \|^{-1/2}$$

$$= \# \mathrm{Pic}_{K/F}(\mathbb{O}_b) \cdot L_b(1, \eta) \cdot 2^{r_{K/F}} \cdot [\mathbb{O}_K^\times : \mathbb{O}_b^\times] \frac{R_K w_K^{-1}}{R_F w_F^{-1}} (\# \kappa_b)^{-1} \cdot \| D_{K/F} b^2 \delta \|^{-1/2}.$$

The relative class number formula then follows. $\square$

Let N be the conductor of $\sigma = \pi^{\mathrm{JL}}$, let $U \subset \widehat{B}^\times$ be an open compact subgroup, and recall

$$\langle f_1, f_2 \rangle_U = \tfrac{1}{2} \langle f_1, f_2 \rangle_{\mathrm{Pet}} \mathrm{Vol}(X_U), \quad \langle \phi_1, \phi_2 \rangle_{U_0(N)} = \tfrac{1}{2} \langle \phi_1, \phi_2 \rangle_{\mathrm{Pet}} \mathrm{Vol}(X_{U_0(N)}).$$

Applying Proposition 2.1, Lemma 2.2, and Lemma 2.3, Waldspurger's formula (2-1) implies the following:

Proposition 2.4. *Let $U = \prod_v U_v \subset \widehat{B}^\times$ be an open compact subgroup with $\widehat{\mathcal{O}}^\times \subset U$. Let $\gamma_v = \mathrm{Vol}(U_0(N)_v)^{-1} \mathrm{Vol}(U_v)$ for all finite places v and $\gamma_v = 1$ for $v | \infty$. Let $\phi_1 \in \pi^{\mathrm{JL}}$, $\phi_2 \in \widetilde{\pi}^{\mathrm{JL}}$ be any forms with $\langle \phi_1, \phi_2 \rangle_{U_0(N)} \neq 0$ and let $\alpha(W_{1,v}, W_{2,v})$ be the corresponding local constants defined in Proposition 2.1. Let $f_1 \in \pi$, $f_2 \in \widetilde{\pi}$ be any pure tensors with $(f_1, f_2)_{\mathrm{Pet}} \neq 0$ and $\beta(f_{1,v}, f_{2,v})$ the corresponding constants defined in (2-1). Then we have*

$$(2 L_{c_1}(1, \eta) |D c_1^2 \delta|_{\mathbb{A}}^{1/2} v_{c_1}^{-1})^2 \cdot \frac{P_\chi^0(f_1) P_{\chi^{-1}}^0(f_2)}{\langle f_1, f_2 \rangle_U}$$
$$= \frac{L\left(\tfrac{1}{2}, \pi, \chi\right)}{\langle \phi_1, \phi_2 \rangle_{U_0(N)}} \cdot \prod_v \alpha(W_{1,v}, W_{2,v}) \beta(f_{1,v}, f_{2,v}) \gamma_v, \quad (2\text{-}3)$$

where v_{c_1} is defined as in Lemma 2.3.

It is now clear that the explicit Waldspurger formula will follow from the computation of these local factors. In the next section, we will choose ϕ_1, ϕ_2 to be normalized new vectors in π^{JL} and $\widetilde{\pi}^{\mathrm{JL}}$, respectively, choose nonzero $f_1 \in V(\pi, \chi)$, $f_2 \in V(\widetilde{\pi}, \chi)$, and compute the related local factors in (2-3).

We obtain the explicit Gross–Zhang formula from the Yuan–Zhang–Zhang formula in a similar way. Let F be a totally real field and X a Shimura curve over F associated to an incoherent quaternion algebra $\mathbb{B}$. Let A be an abelian variety over F parametrized by X and let $\pi_A = \mathrm{Hom}_\xi^0(X, A)$ be the associated automorphic representation of $\mathbb{B}^\times$ over the field $M := \mathrm{End}^0(A)$ and ω its central character. Let K be a totally imaginary quadratic extension over F and $\chi : K_{\mathbb{A}}^\times \to L^\times$ a finite-order Hecke character over a finite extension L of M such that $\omega \cdot \chi|_{\mathbb{A}^\times} = 1$ and, for all places v of F, $\epsilon\left(\tfrac{1}{2}, \pi_A, \chi\right) = \chi_v \eta_v(-1) \epsilon(\mathbb{B}_v)$. Fix an embedding $K_{\mathbb{A}} \to \mathbb{B}$ with $K_{\mathbb{A}}^\times \to \mathbb{B}^\times$, let $P \in X^{K^\times}(K^{\mathrm{ab}})$, and define

$$P_\chi(f) = \int_{K_{\mathbb{A}}^\times / K^\times \mathbb{A}^\times} f(P)^{\sigma_t} \otimes_M \chi(t) \, dt \in A(K^{\mathrm{ab}})_{\mathbb{Q}} \otimes_M L,$$

where we use the Haar measure so that the total volume of $K_{\mathbb{A}}^\times / K^\times \mathbb{A}^\times$ is $2L(1, \eta)$, and η is the quadratic Hecke character on $\mathbb{A}^\times$ associated to the extension K/F. We further assume for all nonarchimedean places v that the compact subgroup $\mathcal{O}_{K_v}^\times / \mathcal{O}_v^\times$ has a volume in $\mathbb{Q}^\times$, and fix a local invariant pairing $(\, , \,)_v$ on $\pi_{A,v} \times \pi_{A^\vee, v}$ with

values in M. Define $\beta(f_{1,v}, f_{2,v}) \in L$ for $(f_{1,v}, f_{2,v})_v \neq 0$ by

$$\beta(f_{1,v}, f_{2,v}) = \frac{L(1, \eta_v)L(1, \pi_v, \mathrm{ad})}{L(\frac{1}{2}, \pi_v, \chi_v)L(2, 1_{F_v})} \int_{K_v^\times/F_v^\times} \frac{(\pi(t_v)f_{1,v}, f_{2,v})_v}{(f_{1,v}, f_{2,v})_v} \chi(t_v) \, dt_v \in L,$$

where we take an embedding of L into $\mathbb{C}$, and the above integral lies in L and does not depend on the embedding.

Then, for any pure tensors $f_1 \in \pi_A$, $f_2 \in \pi_{A^\vee}$ with $(f_1, f_2) \neq 0$, Yuan et al. [2013] obtained the following celebrated formula as an identity in $L \otimes_{\mathbb{Q}} \mathbb{C}$:

$$\frac{\langle P_\chi(f_1), P_{\chi^{-1}}(f_2) \rangle_{K,L}}{\mathrm{Vol}(X_U)^{-1}(f_1, f_2)_U} = \frac{L'(\frac{1}{2}, \pi_A, \chi)}{L(1, \pi_A, \mathrm{ad})L(2, 1_F)^{-1}} \prod_v \beta(f_{1,v}, f_{2,v}). \qquad (2\text{-}4)$$

Note that we use height over K whereas that used in [Yuan et al. 2013] is over F, the Haar measure to define $P_\chi(f)$ is different from theirs by $2L(1, \eta)$, and the measure to define $\mathrm{Vol}(X_U)$ is different from theirs by 2. Similar to Proposition 2.4, we have:

Proposition 2.5. *Let $U = \prod_v U_v \subset \widehat{B}^\times$ be a pure product open compact subgroup such that $\widehat{\mathcal{O}}^\times \subset U$. Let $\gamma_v = \mathrm{Vol}(U_0(N)_v) \mathrm{Vol}(U_v)^{-1}$ for all finite places v and $\gamma_v = 1$ for $v|\infty$. Let $\phi \in \pi_A^{\mathrm{JL}}$ be any nonzero form and let $\alpha(W_v, \overline{W}_v)$ be the corresponding local constants defined in Proposition 2.1. Let $f_1 \in \pi_A$, $f_2 \in \pi_{A^\vee}$ be any pure tensors with $(f_1, f_2) \neq 0$ and $\beta(f_{1,v}, f_{2,v})$ the corresponding constants defined in (2-4). Then we have*

$$(2L_{c_1}(1, \eta)|Dc_1^2\delta|_{\mathbb{A}}^{1/2}v_{c_1}^{-1})^2 \cdot \frac{\langle P_\chi^0(f_1), P_{\chi^{-1}}^0(f_2) \rangle_{K,L}}{(f_1, f_2)_U}$$

$$= \frac{L'(\frac{1}{2}, \pi_A, \chi)}{\langle \phi, \phi \rangle_{U_0(N)}} \prod_v \alpha_v(W_{1,v}, W_{2,v})\beta_v(f_{1,v}, f_{2,v})\gamma_v. \qquad (2\text{-}5)$$

We will study the local factors appearing in formulas in Propositions 2.4 and 2.5 in the next section.

2D. *Proofs of main results.* In this subsection, we prove Theorems 1.5, 1.6, 1.8, 1.9 and 1.10, assuming local results proved in Section 3.

Proof of Theorem 1.8. We first give a proof of the explicit Waldspurger formula. In (2-3), take nonzero $f_1 \in V(\pi, \chi)$, $f_2 \in V(\widetilde{\pi}, \chi^{-1})$, and ϕ_1^0 (resp. ϕ_2^0) the normalized new vector of π^{JL} (resp. $\widetilde{\pi}^{\mathrm{JL}}$). Let $W_{\phi_i^0} := W_i = \bigotimes_v W_{i,v}$ be the corresponding Whittaker functions of ϕ_i^0, $i = 1, 2$. Let $R \subset B$ be the order, as defined in Theorem 1.8, and $U = \widehat{R}^\times$. Denote

$$\alpha := \alpha(W_{1,v}, W_{2,v}) \cdot |\delta|_v^{1/2}, \quad \beta := \beta(f_{1,v}, f_{2,v}) \cdot |D\delta|_v^{-1/2}.$$

Then (2-3) becomes

$$4|Dc_1^2\delta^2|_{\mathbb{A}}^{1/2} v_{c_1}^{-2} \frac{P_\chi^0(f_1)P_{\chi^{-1}}^0(f_2)}{\langle f_1, f_2 \rangle_U}$$

$$= \frac{L^{(\Sigma)}\left(\frac{1}{2}, \pi, \chi\right)}{\langle \phi_1^0, \phi_2^0 \rangle_{U_0(N)}} L_\Sigma\left(\tfrac{1}{2}, \pi, \chi\right) L_{c_1}(1, \eta)^{-2} |c_1|_{\mathbb{A}}^{-1} \prod_v \alpha_v \beta_v \gamma_v .$$

Let Σ be the set in Theorem 1.8, $\Sigma_\infty = \Sigma \cap \infty$ and $\Sigma_f = \Sigma \setminus \Sigma_\infty$. Comparing with the formula (2-3), the proof of the explicit formula in Theorem 1.8 is reduced to showing that

$$L_{\Sigma_f}\left(\tfrac{1}{2}, \pi, \chi\right) L_{c_1}(1, \eta)^{-2} |c_1|_{\mathbb{A}}^{-1} \prod_{v \nmid \infty} \alpha_v \beta_v \gamma_v = 2^{\#\Sigma_D}$$

and

$$L_{\Sigma_\infty}\left(\tfrac{1}{2}, \pi, \chi\right) \prod_{v | \infty} \alpha_v \beta_v \gamma_v = C_\infty^{-1},$$

which are given by Lemma 3.13 and Lemma 3.14. $\qquad\square$

Proof of Theorem 1.10. Given the hypotheses of Theorem 1.10, identify $\widetilde{\pi}$ with $\bar{\pi}$; by Theorem 1.8,

$$L^{(\Sigma)}\left(\tfrac{1}{2}, \pi, \chi\right) = 2^{-\#\Sigma_D+2}(4\pi^3)^d \frac{\langle \phi^0, \overline{\phi^0} \rangle_{U_0(N)}}{v_{c_1}^2 \sqrt{|D_K| \|c_1^2\|}} \frac{|P_\chi^0(f)|^2}{\langle f_1, f_2 \rangle_U}.$$

The formula in Theorem 1.10 follows by noting these facts:

(i) $v_{c_1} = 2^{1-d} u_1$.

(ii) $\langle \phi^0, \overline{\phi^0} \rangle_{U_0(N)} = (2\pi)^{-d} (\phi, \phi)_{U_0(N)}$, where ϕ is the Hilbert newform of π_A^{JL}. This is obtained by applying the formula in Proposition 2.1 to ϕ and ϕ^0, and the comparison of local Whittaker pairings at infinity; see the discussion before Proposition 3.12.

(iii) Let $g_1, \ldots, g_n \in \widehat{B}^\times$ be a complete set of representatives of $X = B^\times \backslash \widehat{B}^\times / \widehat{R}^\times$ and let $w_i = \#(B^\times \cap g_i \widehat{R}^\times g_i^{-1} / \mathbb{O}^\times)$; then, as in the proof of Lemma 2.2, for $U = \widehat{R}^\times$,

$$\langle f, \bar{f} \rangle_U = 2^{-1} \operatorname{Vol}(X_U) \langle f, \bar{f} \rangle_{\mathrm{Pet}} = \sum_{i=1}^n |f(g_i)|^2 w_i^{-1}$$

$$= \left\langle \sum f(g_i) w_i^{-1}[g_i], \sum f(g_i) w_i^{-1}[g_i] \right\rangle$$

$$= \langle f, f \rangle,$$

where we identify f with its image under the map $V(\pi, \chi) \to \mathbb{C}[X]$ and $\langle , \rangle$ is the height pairing on $\mathbb{C}[X]$. $\qquad\square$

Proof of Theorem 1.5. To show the explicit Gross–Zagier formula in Theorem 1.5, similarly to above, we apply the formula (2-5) in Proposition 2.5 to nonzero forms $f_1 \in V(\pi_A, \chi)$, $f_2 \in V(\pi_{A^\vee}, \chi^{-1})$, ϕ^0 the normalized new vector of π_A^{JL}, and $U = \mathscr{R}^\times$ as in Theorem 1.5. By Lemma 3.13 and Lemma 3.14, we have

$$L'^{(\Sigma)}\left(\tfrac{1}{2}, \pi, \chi\right) = 2^{-\#\Sigma_D+2}(4\pi^3)^d \frac{\langle \phi^0, \overline{\phi}^0 \rangle_{U_0(N)}}{v_{c_1}^2 \sqrt{|D_K| \|c_1^2\|}} \frac{\langle P_\chi^0(f_1), P_{\chi^{-1}}^0(f_2) \rangle_{K,L}}{(f_1, f_2)_U} .$$

Then the explicit Gross–Zagier formula follows again by noting facts (i) and (ii) above. $\square$

Proof of Theorems 1.9 and 1.6. We now show that the variations of the explicit Waldspurger formula in Theorem 1.9 follow from the Waldspurger formula (2-1) and its explicit form in Theorem 1.8, and similarly for the variation of the explicit Gross–Zagier formula in Theorem 1.6.

Let $f_1' = \bigotimes_v f_{1,v}' \in \pi$, $f_2' = \bigotimes_v f_{2,v}' \in \widetilde{\pi}$ be forms different from the test vectors $f_1 = \bigotimes_v f_{1,v} \in V(\pi, \chi)$, $f_2 = \bigotimes_v f_{2,v} \in V(\widetilde{\pi}, \chi^{-1})$ at a finite set S of places of F, respectively, such that $\langle f_{1,v}', f_{2,v}' \rangle_v \neq 0$ and $\beta(f_{1,v}', f_{2,v}') \neq 0$ for any $v \in S$. By the Waldspurger formula (2-1), we have the formulas

$$\frac{P_\chi^0(f_1) \cdot P_{\chi^{-1}}^0(f_2)}{\langle f_1, f_2 \rangle_U} = \mathscr{L}(\pi, \chi) \prod_v \beta(f_{1,v}, f_{2,v}),$$

$$\frac{P_\chi^0(f_1') \cdot P_{\chi^{-1}}^0(f_2')}{\langle f_1', f_2' \rangle_U} = \mathscr{L}(\pi, \chi) \prod_v \beta(f_{1,v}', f_{2,v}'),$$

where

$$\mathscr{L}(\pi, \chi) = \left(\frac{\#\operatorname{Pic}_{K/F}(\mathbb{O}_{c_1})}{2L(1, \eta)}\right)^2 \cdot \frac{2}{\operatorname{Vol}(X_U)} \cdot \frac{L\left(\tfrac{1}{2}, \pi, \chi\right)}{2L(1, \pi, \mathrm{ad})L(2, 1_F)^{-1}} .$$

It follows that

$$\frac{P_\chi^0(f_1) \cdot P_{\chi^{-1}}^0(f_2)}{\langle f_1, f_2 \rangle_U} = \frac{P_\chi^0(f_1') \cdot P_{\chi^{-1}}^0(f_2')}{\langle f_1', f_2' \rangle_U} \cdot \prod_{v \in S} \frac{\beta(f_{1,v}, f_{2,v})}{\beta(f_{1,v}', f_{2,v}')} .$$

The variation formula follows immediately. $\square$

3. Local theory

Notations. In this section, we denote by F a local field of characteristic zero, i.e., a finite field extension of $\mathbb{Q}_v$ for some place v of $\mathbb{Q}$. Denote by $|\cdot|$ the absolute value of F such that $d(ax) = |a| \, dx$ for a Haar measure dx on F. Take an element $\delta \in F^\times$ such that $\delta\mathbb{O}$ is the different of F over $\mathbb{Q}_v$ for v finite and $\delta = 1$ for v infinite. For F nonarchimedean, denote by $\mathbb{O}$ the ring of integers in F, ϖ a uniformizer, $\mathfrak{p}$ its

maximal ideal, and q the cardinality of its residue field. Let $v : F \to \mathbb{Z} \cup \{\infty\}$ be the additive valuation on F such that $v(\varpi) = 1$. For μ a (continuous) character on $F^\times$, denote by $n(\mu)$ the conductor of μ, that is, the minimal nonnegative integer n such that μ is trivial on $(1 + \varpi^n \mathbb{O}) \cap \mathbb{O}^\times$. We will always use the additive character ψ on F and the Haar measure da on F as in Section 2, so that da is self-dual to ψ.

Denote by K a separable quadratic extension of F and, for any $t \in K$, write $t \mapsto \bar{t}$ for the nontrivial automorphism of K over F. We use similar notations as those for F with a subscript K. If F is nonarchimedean and K is nonsplit, denote by e the ramification index of K/F. Denote by $\mathrm{tr}_{K/F}$ and $\mathrm{N}_{K/F}$ the trace and norm maps from K to F, and let $D \in \mathbb{O}$ be an element such that $D\mathbb{O}$ is the relative discriminant of K over F. For an integer $c \geq 0$, denote by $\mathbb{O}_c$ the order $\mathbb{O} + \varpi^c \mathbb{O}_K$ in K. Let $\eta : F^\times \to \{\pm 1\}$ be the character associated to the extension K over F. Let B be a quaternion algebra over F. Let $\epsilon(B) = +1$ and $\delta(B) = 0$ if $B \cong M_2(F)$ is split, and $\epsilon(B) = -1$ and $\delta(B) = 1$ if B is division. Denote by G the algebraic group $B^\times$ over F, and we also write G for $G(F)$. We take the Haar measure on $F^\times$, $K^\times$ and $K^\times / F^\times$ as in Section 2. In particular, $\mathrm{Vol}(\mathbb{O}^\times, d^\times a) = \mathrm{Vol}(\mathbb{O}, da) = |\delta|^{1/2}$ and

$$\mathrm{Vol}(K^\times / F^\times) = \begin{cases} 2 & \text{if } F = \mathbb{R} \text{ and } K = \mathbb{C}, \\ |\delta|^{1/2} & \text{if } K \text{ is the unramified extension field of } F, \\ 2|D\delta|^{1/2} & \text{if } K/F \text{ is ramified.} \end{cases}$$

For F nonarchimedean and n a nonnegative integer, define the following subgroups of $\mathrm{GL}_2(\mathbb{O})$:

$$U_0(n) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{O}) \,\middle|\, c \in \mathfrak{p}^n \right\}, \quad U_1(n) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in U_0(n) \,\middle|\, d \in 1 + \varpi^n \mathbb{O} \right\}.$$

Let π be an irreducible admissible representation of G, which is always assumed to be generic if $G \cong \mathrm{GL}_2$. Denote by ω the central character of π and by $\sigma = \pi^{\mathrm{JL}}$ the Jacquet–Langlands correspondence of π to $\mathrm{GL}_2(F)$. Let χ be a character on $K^\times$ such that

$$\chi|_{F^\times} \cdot \omega = 1.$$

For F nonarchimedean, let n be the conductor of σ, i.e., the minimal nonnegative integer such that the invariant subspace $\sigma^{U_1(n)}$ is nonzero, and let c be the minimal nonnegative integer such that χ is trivial on $(1 + \varpi^c \mathbb{O}_K) \cap \mathbb{O}_K^\times$.

Denote by

$$L(s, \pi, \chi) := L(s, \sigma \times \pi_\chi) \quad \text{and} \quad \epsilon(s, \pi, \chi) := \epsilon(s, \sigma \times \pi_\chi, \psi)$$

the Rankin–Selberg L-factor and ϵ-factor of $\sigma \times \pi_\chi$, where π_χ is the representation on $\mathrm{GL}_2(F)$ constructed from χ via Weil representation. Denote by π_K the base

change lifting of σ to $\mathrm{GL}_2(K)$; then we have

$$L(s, \pi, \chi) = L(s, \pi_K \otimes \chi), \quad \epsilon(s, \pi, \chi) = \eta(-1)\epsilon(s, \pi_K \otimes \chi, \psi_K)$$

Note that $\epsilon(\pi, \chi) := \epsilon\left(\frac{1}{2}, \pi, \chi\right)$ equals ± 1 and is independent of the choice of ψ. In the following, we denote by $L(s, \pi, \mathrm{ad}) := L(s, \sigma, \mathrm{ad})$ the adjoint L-factor of σ.

3A. *Local toric integrals.* Let $\mathscr{P}(\pi, \chi)$ denote the functional space

$$\mathscr{P}(\pi, \chi) := \mathrm{Hom}_{K^\times}(\pi, \chi^{-1}).$$

By a theorem of Tunnell [1983] and Saito [1993], the space $\mathscr{P}(\pi, \chi)$ has dimension at most one, and equals one if and only if

$$\epsilon(\pi, \chi) = \chi\eta(-1)\epsilon(B).$$

Lemma 3.1. *Let the pair (π, χ) be as above with $\epsilon(\pi, \chi) = \chi\eta(-1)\epsilon(B)$.*

(1) *If K is split or π is a principal series, then B is split.*

(2) *If $K/F = \mathbb{C}/\mathbb{R}$, σ is the discrete series of weight k, and $\chi(z) = |z|_{\mathbb{C}}^s (z/\sqrt{|z|_{\mathbb{C}}})^m$ with $s \in \mathbb{C}$ and $m \equiv k \pmod 2$, then B is split if and only if $m \geq k$.*

Furthermore, assume F is nonarchimedean. Then:

(3) *If K/F is nonsplit and σ is the special representation $\mathrm{sp}(2) \otimes \mu$ with μ a character of $F^\times$, then B is division if and only if $\mu_K \chi = 1$ with $\mu_K := \mu \circ N_{K/F}$.*

(4) *If K/F is inert and $c = 0$, then B is split if and only if n is even.*

(5) *If K is nonsplit with $c \geq n$, then B is split.*

Proof. See [Tunnell 1983, Propositions 1.6, 1.7] for (1), (3), and [Gross 1988, Propositions 6.5, 6.3(2)] for (2), (4). We now give a proof of (5). If π is a principal series then, by (1), B is split. If σ is a supercuspidal representation then, by [Tunnell 1983, Lemma 3.1], B is split if $n(\chi) \geq ne/2 + (2 - e)$. It is then easy to check that, if $c \geq n$, this condition always holds. Finally, assume $\sigma = \mathrm{sp}(2) \otimes \mu$ with μ a character of $F^\times$. By (2), B is division if and only if $\mu_K \chi = 1$. If μ is unramified, then $n = 1$ and χ is ramified, which implies that B must be split. Assume μ is ramified; then $n = 2n(\mu)$ and, by [Tunnell 1983, Lemma 1.8], $fn(\mu_K) = n(\mu) + n(\mu\eta) - n(\eta)$, where f is the residue degree of K/F. If K/F is unramified and $\mu_K \chi = 1$, then $c = n(\mu_K) = n(\mu) = n/2$, a contradiction. If K/F is ramified and $\mu_K \chi = 1$, then $2c - 1 \leq n(\mu_K) < 2n(\mu) = n$, a contradiction again. Hence, if $c \geq n$, B is always split. $\square$

Assume that the pair (π, χ) is *essentially unitary*, in the sense that there exists a character $\mu = |\cdot|^s$ on $F^\times$ with $s \in \mathbb{C}$ such that both $\pi \otimes \mu$ and $\chi \otimes \mu_K^{-1}$ are unitary. In particular, if π is a local component of some global cuspidal representation, then (π, χ) is essentially unitary. Under such an assumption, we study the space

$\mathcal{P}(\pi, \chi)$ via the toric integral

$$\int_{F^\times \backslash K^\times} \langle \pi(t) f_1, f_2 \rangle \chi(t) \, dt,$$

where $f_1 \in \pi$, $f_2 \in \widetilde{\pi}$, and $\langle \cdot, \cdot \rangle$ is any invariant pairing on $\pi \times \widetilde{\pi}$. The following basic properties for this toric integral are established in [Waldspurger 1985]:

- It is absolutely convergent for any $f_1 \in \pi$ and $f_2 \in \widetilde{\pi}$.

- $\mathcal{P}(\pi, \chi) \neq 0$ if and only if $\mathcal{P}(\pi, \chi) \otimes \mathcal{P}(\widetilde{\pi}, \chi^{-1}) \neq 0$, and in this case the above integral defines a generator of $\mathcal{P}(\pi, \chi) \otimes \mathcal{P}(\widetilde{\pi}, \chi^{-1})$.

- For $f_1 \in \pi$, $f_2 \in \widetilde{\pi}$ such that $\langle f_1, f_2 \rangle \neq 0$, define the toric integral

$$\beta(f_1, f_2) := \frac{L(1, \eta) L(1, \pi, \mathrm{ad})}{L(2, 1_F) L(\frac{1}{2}, \pi, \chi)} \int_{F^\times \backslash K^\times} \frac{\langle \pi(t) f_1, f_2 \rangle}{\langle f_1, f_2 \rangle} \chi(t) \, dt.$$

  Then $\beta(f_1, f_2) = 1$ in the case that $B = M_2(F)$, K is an unramified extension of F, both π and χ are unramified, dt is normalized such that $\mathrm{Vol}(\mathbb{O}_K^\times / \mathbb{O}^\times) = 1$, and f_1, f_2 are spherical.

For any pair (π, χ), β is invariant if we replace (π, χ) by $(\pi \otimes \mu, \chi \otimes \mu_K^{-1})$ for any character μ of $F^\times$. Therefore, we may assume π and χ are both unitary from now on and identify $(\widetilde{\pi}, \chi^{-1})$ with $(\overline{\pi}, \overline{\chi})$. Let $(\,,\,): \pi \times \pi \to \mathbb{C}$ be the Hermitian pairing defined by $(f_1, f_2) = \langle f_1, \overline{f_2} \rangle$.

Let $\beta(f) := \beta(f, \overline{f})$. Then the functional space $\mathcal{P}(\pi, \chi)$ is nontrivial if and only if β is nontrivial. Assume $\mathcal{P}(\pi, \chi)$ is nonzero in the following. A nonzero vector f of π is called a *test vector* for $\mathcal{P}(\pi, \chi)$ if $\ell(f) \neq 0$ for some (thus any) nonzero $\ell \in \mathcal{P}(\pi, \chi)$ or, equivalently, if $\beta(f)$ is nonvanishing.

The notion of new vectors in an irreducible smooth admissible representation of $\mathrm{GL}_2(F)$ (see [Casselman 1973a] for F nonarchimedean and [Popa 2008] for F archimedean) can be viewed as a special case of test vectors. Let π be an irreducible admissible representation of $\mathrm{GL}_2(F)$. Recall the definition of *new vector line* in π, as follows. Denote by $T = K^\times$ the diagonal torus in $\mathrm{GL}_2(F)$. Write $T = ZT_1$ with $T_1 = \{ \left(\begin{smallmatrix} * & \\ & 1 \end{smallmatrix} \right) \}$.

- If F is nonarchimedean, then the new vector line is the invariant subspace $\pi^{U_1(n)}$.

- If F is archimedean, take U to be $O_2(\mathbb{R})$ if $F = \mathbb{R}$ and U_2 if $F = \mathbb{C}$. The new vector line consists of vectors $f \in \pi$ which are invariant under $T_1 \cap U$ with weight minimal.

It is known that new vectors satisfy the following properties:

(1) For any $s \in \mathbb{C}$, denote by ω_s the character on T such that $\omega_s|_Z = \omega$ and $\omega_s|_{T_1} = |\cdot|^{s-1/2}$. Then any nonzero f in the new vector line is a test vector for $\mathcal{P}(\pi, \omega_s^{-1})$.

(2) If $\mathcal{W}(\pi, \psi)$ is the Whittaker model of π with respect to ψ, then there is a vector W_0 in the new vector line, called the *normalized new vector* of π, such that the local zeta integral $|\delta|^{s-1/2} Z(s, W_0)$ equals $L(s, \pi)$.

3B. *Local orders of quaternions.* Assume F is nonarchimedean in this subsection.

First, in the case that the quaternion algebra B is split, given nonnegative integers m and k we want to classify all the $K^\times$ conjugacy classes of Eichler orders R in B with discriminant m such that $R \cap K = \mathbb{O}_k$. For this, identify B with the F-algebra $\mathrm{End}_F(K)$ which contains K as an F-subalgebra by multiplication. Recall that an Eichler order in B is the intersection of two maximal orders in B. Then, any Eichler order must be of the form $R(L_1, L_2) := R(L_1) \cap R(L_2)$, where L_i, $i = 1, 2$, are two $\mathbb{O}$-lattices in K and $R(L_i) := \mathrm{End}_\mathbb{O}(L_i)$. Denote by $d(L_1, L_2)$ the discriminant of $R(L_1, L_2)$. For any maximal order $R(L)$, there exists a unique integer $j \geq 0$ such that $L = t\mathbb{O}_j$ for some $t \in K^\times$. In fact, $\mathbb{O}_j = \{x \in K \mid xL \subset L\}$. Thus, any $K^\times$-conjugacy class of Eichler order contains an order of the form $R(\mathbb{O}_j, t\mathbb{O}_{j'})$ with $0 \leq j' \leq j$ and $t \in K^\times$ and the conjugacy class is exactly determined by the integers $j' \leq j$ and the class of $t \in K^\times$ modulo $F^\times \mathbb{O}_{j'}^\times$. The question is reduced to solving the equation with variables k' and $[t]$,

$$d(\mathbb{O}_k, t\mathbb{O}_{k'}) = m, \quad 0 \leq k' \leq k, \quad [t] \in K^\times / F^\times \mathbb{O}_{k'}^\times.$$

If $(k', [t])$ is a solution, then so is $(k', [\bar{t}])$. A complete representative system (k', t) with $t \in K^\times$ of solutions to the above equation corresponds to a complete system $R(\mathbb{O}_k, t\mathbb{O}_{k'})$ for $K^\times$-conjugacy classes of Eichler orders R with discriminant m and $R \cap K = \mathbb{O}_k$.

Lemma 3.2. *Let m, k be nonnegative integers. Let $\tau \in K^\times$ be such that $\mathbb{O}_K = \mathbb{O}[\tau]$, if K is split then $\tau^2 - \tau = 0$, and if K is nonsplit then $v(\tau) = (e - 1)/2$. Let $d := k + k' - m$. Then a complete representative system of (k', t) is the following*:

- *For $0 \leq m \leq 2k$, $k' \in [|m - k|, k]$ with d even, so $d \in 2 \cdot [0, k']$, and*

$$t = 1 + \varpi^{d/2} \tau u, \quad u \in (\mathbb{O}/\varpi^{k'-d/2}\mathbb{O})^\times.$$

  In the case $k' = k - m \geq 0$, the unique class of t is also represented by 1.

- *For split $K \cong F^2$ and $k + 1 \leq m$, $k' \in [0, \min(m - k - 1, k)]$, so $d \in [k - m, 0)$, and*

$$t = (\varpi^{\pm d} u, 1), \quad u \in (\mathbb{O}/\varpi^{k'}\mathbb{O})^\times.$$

- *For nonsplit K and $k + 1 \leq m \leq 2k + e - 1$, $k' = m - k - e + 1$, i.e., $d = 1 - e$, and*

$$t = \varpi x + \tau, \quad x \in \mathbb{O}/\varpi^{k'+e-2}\mathbb{O}.$$

Proof. The discriminant $d(L_1, L_2)$ of the Eichler order $R(L_1, L_2)$ can be computed as follows. Let e_i, e'_i be an $\mathbb{O}$-basis of L_i, $i = 1, 2$, and let $A = (a_{ij}) \in \mathrm{GL}_2(F)$ so that $A\left(\begin{smallmatrix} e_1 \\ e'_1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} e_2 \\ e'_2 \end{smallmatrix}\right)$. Let $v : F \to \mathbb{Z} \cup \{\infty\}$ be the additive valuation on F such that $v(\varpi) = 1$. Let $\alpha = \min_{i,j} v(a_{ij})$ and $\beta = v(\det A)$. Then $d(L_1, L_2) = |2\alpha - \beta|$. Now solve the equation

$$d(\mathbb{O}_k, t\mathbb{O}_{k'}) = m, \quad k' \in [0, k], \quad t \in K^\times / F^\times \mathbb{O}_{k'}^\times. \qquad \square$$

Define

$$c_1 = \begin{cases} 0 & \text{if } K \text{ is nonsplit and } c < n, \\ c & \text{otherwise.} \end{cases}$$

Lemma 3.3. *There exists an order R of discriminant n and $R \cap K = \mathbb{O}_{c_1}$ satisfying the condition that, if $nc_1 \neq 0$, then R is the intersection of two maximal orders R' and R'' of B such that $R' \cap K = \mathbb{O}_{c_1}$, $R'' \cap K = \mathbb{O}_{\max\{0, c_1 - n\}}$. Such an order is unique up to $K^\times$-conjugacy unless $0 < c_1 < n$. In the case $0 < c_1 < n$, there are exactly two $K^\times$-conjugacy classes which are conjugate to each other by a normalizer of $K^\times$.*

Proof. If $nc_1 = 0$, this is proved in [Gross 1988, Propositions 3.2, 3.4]. Now assume that $nc_1 \neq 0$; then B is split and one can apply Lemma 3.2. $\qquad \square$

Let R be an $\mathbb{O}$-order of B of discriminant n such that $R \cap K = \mathbb{O}_{c_1}$. Such an order R is called admissible for (π, χ) if the following conditions are satisfied:

(1) If $nc_1 \neq 0$ (thus B is split), then R is the intersection of two maximal orders R' and R'' of B such that $R' \cap K = \mathbb{O}_{c_1}$ and $R'' \cap K = \mathbb{O}_{\max\{0, c_1 - n\}}$.

(2) If $0 < c_1 < n$, fix an F-algebra isomorphism $K \cong F^2$ and identify B with $\mathrm{End}_F(K)$. The two $K^\times$-conjugacy classes of $\mathbb{O}$-orders in B satisfying the above condition (1) contain, respectively, the orders $R_i = R'_i \cap R''_i$, $i = 1, 2$ with $R'_1 = R'_2 = \mathrm{End}_\mathbb{O}(\mathbb{O}_c)$, $R''_1 = \mathrm{End}_\mathbb{O}((\varpi^{n-c}, 1)\mathbb{O}_K)$ and $R''_2 = \mathrm{End}_\mathbb{O}((1, \varpi^{n-c})\mathbb{O}_K)$. Let $\chi_1(a) = \chi(a, 1)$ and $\chi_2(b) = \chi(1, b)$. Then R is $K^\times$-conjugate to some R_i such that the conductor of χ_i is c_1.

Lemma 3.4. *If K is nonsplit, $n > 0$ and $c = 0$, then there is a unique admissible order R for (π, χ).*

Proof. Let $\mathbb{O}_B$ be a maximal order containing $\mathbb{O}_K$; then, by [Gross 1988, (3.3)], any admissible order for (π, χ) is $K^\times$-conjugate to $R := \mathbb{O}_K + I\mathbb{O}_B$, where I is a nonzero ideal of $\mathbb{O}_K$ such that $n = \delta(B) + \mathrm{length}_\mathbb{O}(\mathbb{O}_K / I)$. If B is nonsplit, then $\mathbb{O}_B$ is invariant under $B^\times$-conjugations and R is unique. Assume B is split. As $\mathbb{O}_K^\times \subset \mathbb{O}_B^\times$, $\mathbb{O}_B$ is invariant under $F^\times \mathbb{O}_K^\times$-conjugations. In particular, if K is unramified, then $K^\times = F^\times \mathbb{O}_K^\times$ and R is unique. Consider the case that K is ramified. Then $K^\times = F^\times \mathbb{O}_K^\times \cup \varpi_K F^\times \mathbb{O}_K^\times$ and it suffices to show that ϖ_K normalizes R. For this, embed K into $B = M_2(F)$ by $\varpi_K \mapsto \left(\begin{smallmatrix} \mathrm{tr}\,\varpi_K & 1 \\ -N\varpi_K & 0 \end{smallmatrix}\right)$ and take $\mathbb{O}_B = M_2(\mathbb{O})$. Then $R = \mathbb{O}_K + \varpi_K^n M_2(\mathbb{O})$. Note that $R_0(1) = \mathbb{O}_K + \varpi_K M_2(\mathbb{O})$ with $R_0(1) = \left(\begin{smallmatrix} \mathbb{O} & \mathbb{O} \\ \mathfrak{p} & \mathbb{O} \end{smallmatrix}\right)$ the

Iwahori order in $M_2(F)$. Denote by m the maximal integer such that $2m \leq n$. Then $R = \mathbb{O}_K + \varpi^{m-1} \varpi_K R_0(1)$ if n is even, and $R = \mathbb{O}_K + \varpi^m R_0(1)$ if n is odd. As ϖ_K normalizes $R_0(1)$, it also normalizes R and R is unique. $\qquad\square$

In the following, take an admissible $\mathbb{O}$-order R of B. Let $U = R^\times$ and define

$$\gamma := \frac{\mathrm{Vol}(U)}{\mathrm{Vol}(U_0(n))},$$

where the Haar measure is taken, so that $\mathrm{Vol}(\mathrm{GL}_2(\mathbb{O})) = L(2, 1_F)^{-1}|\delta|^2$ and $\mathrm{Vol}(\mathbb{O}_B^\times) = L(2, 1_F)^{-1}(q-1)^{-1}|\delta|^2$ if B is division.

Lemma 3.5. *If either R is not maximal or B is nonsplit, then*

$$\gamma = L(1, 1_F)(1 - e(R)q^{-1})$$

where $e(R)$ is the Eichler symbol of R, defined as follows: Let $\kappa(R) = R/\mathrm{rad}(R)$ with $\mathrm{rad}(R)$ the Jacobson radical of R and let κ be the residue field of F. Then

$$e(R) = \begin{cases} 1 & \text{if } \kappa(R) = \kappa^2, \\ -1 & \text{if } \kappa(R) \text{ is a quadratic field extension of } \kappa, \\ 0 & \text{if } \kappa(R) = \kappa. \end{cases}$$

Proof. Let R_0 be a maximal order of B containing R. Then we have the formula (for example, see [Yu 2013])

$$\frac{[R_0^\times : R^\times]}{[R_0 : R]} = \frac{|\kappa(R_0)^\times|/|\kappa(R^\times)|}{|\kappa(R_0)|/|\kappa(R)|}.$$

If B is split and R is not maximal, then

$$[R_0 : R] = q^n, \quad \frac{|\kappa(R_0)^\times|}{|\kappa(R_0)|} = (1 - q^{-2})(1 - q^{-1}),$$

$$\frac{|\kappa(R)|}{|\kappa(R)^\times|} = (1 - q^{-1})^{-1}(1 - e(R)q)^{-1},$$

while, if B is division, then

$$[R_0 : R] = q^{n-1}, \quad \frac{|\kappa(R_0)^\times|}{|\kappa(R_0)|} = 1 - q^{-2}, \quad \frac{|\kappa(R)|}{|\kappa(R)^\times|} = (1 - q^{-1})^{-1}(1 - e(R)q)^{-1}.$$

Summing up,

$$[R_0^\times : R^\times] = (q-1)^{-\delta(B)} q^n (1 - q^{-2})(1 - e(R)q^{-1})^{-1},$$

where $\delta(B)$ equals 0 if B is split and 1 if B is ramified. Thus

$$\gamma^{-1} = \frac{\mathrm{Vol}(U_0(n))}{\mathrm{Vol}(U)} = \frac{\mathrm{Vol}(\mathrm{GL}_2(\mathbb{O}))}{\mathrm{Vol}(R_0^\times)} \frac{[R_0^\times : U]}{[\mathrm{GL}_2(\mathbb{O}) : U_0(n)]}$$

$$= \frac{L(2,1)^{-1}}{(q-1)^{-\delta(B)} L(2,1)^{-1}} \frac{(q-1)^{-\delta(B)} q^n (1-q^{-2})(1-e(R)q^{-1})^{-1}}{q^n (1-q^{-2})(1-q^{-1})^{-1}}$$

$$= L(1, 1_F)^{-1} (1 - e(R)q^{-1})^{-1}. \qquad\qquad \square$$

3C. *Test vector spaces.*

Definition 3.6. Define $V(\pi, \chi) \subset \pi$ to be the subspace of vectors f satisfying the following conditions:

- For nonarchimedean F, K split or $c \geq n$, let $U \subset G$ be the compact subgroup defined before Lemma 3.5, then f is an ω-eigenform under U. Here, write $U = (U \cap Z)U'$ so that $U' = U$ if $cn = 0$ and $U' \cong U_1(n)$ otherwise, and view ω as a character on $U \cap Z$ that extends to U by making it trivial on U'.

- For nonarchimedean F, K nonsplit and $c < n$, f is a χ^{-1}-eigenform under the action of $K^\times$.

- For archimedean F, let U be a maximal compact subgroup of G such that $U \cap K^\times$ is the maximal compact subgroup of $K^\times$; then f is a χ^{-1}-eigenform under $U \cap K^\times$ with weight minimal.

Proposition 3.7. *The dimension of $V(\pi, \chi)$ is one, and any nonzero vector in $V(\pi, \chi)$ is a test vector for $\mathscr{P}(\pi, \chi)$.*

Proof. If F is nonarchimedean, the claim that $\dim V(\pi, \chi) = 1$ follows from local newform theory [Casselman 1973a]. Assume F is archimedean. If K is nonsplit, then $V(\pi, \chi)$ is the χ^{-1}-eigenline of $K^\times$. If K is split, then without loss of generality embed $K^\times$ into $G \cong \mathrm{GL}_2(F)$ as the diagonal matrices and decompose $K^\times = F^\times K^1$ so that the image of K^1 in G is $\left(\begin{smallmatrix} * & \\ & 1 \end{smallmatrix}\right)$. Then $V(\pi, \chi)$ is the new vector line for $\pi \otimes \chi_1$ with $\chi_1 := \chi|_{K^1}$.

   We shall prove any nonzero vector in $V(\pi, \chi)$ is a test vector in the next subsection by computing the toric integral β. $\qquad\qquad \square$

Proposition 3.8. *Assume K/F is a quadratic extension of nonarchimedean fields with $n > 0$ and $c = 0$. Then $V(\pi, \chi) \subseteq \pi^{R^\times}$ and $\dim \pi^{R^\times} = \dim \pi^{\mathbb{O}_K^\times} \leq 2$. The dimension of $\pi^{R^\times}$ is one precisely when K/F is inert or K/F is ramified and $\epsilon(\pi, \chi_1) \neq \epsilon(\pi, \chi_2)$, where χ_i, $i = 1, 2$, are unramified characters of $K^\times$ with $\chi_i|_{F^\times} \cdot \omega = 1$.*

   The proof of this proposition is in [Gross 1988; Gross and Prasad 1991] except for the case that π is a supercuspidal representation on $G = \mathrm{GL}_2(F)$. For this case, the proof in [Gross 1988, §7] is based on a character formula for odd residue characteristic. We next prove this case with arbitrary residue characteristic.

Let $R_0 = M_2(\mathbb{O})$ if $e = 1$ and the Iwahori order $\begin{pmatrix} \mathbb{O} & \mathbb{O} \\ \mathfrak{p} & \mathbb{O} \end{pmatrix}$ if $e = 2$. Fix an embedding of K into $M_2(F)$ such that $R_0 \cap K = \mathbb{O}_K$. Consider the filtration of open compact subgroups of G and $K^\times$

$$\mathcal{K}(r) := (1 + \varpi^r R_0) \cap \mathrm{GL}_2(\mathbb{O}), \quad \mathcal{E}(r) := \mathcal{K}(r) \cap K^\times, \quad r \geq 0.$$

Denote by m the minimal integer such that $2m + 1 \geq n$. The proof is based on:

Proposition 3.9. *For any integer $r \geq m$, $\pi^{\mathcal{K}(r)} = \pi^{\mathcal{E}(r)}$.*

Proof. Firstly, note that it is enough to prove Proposition 3.9 for the case π is minimal, that is, π has minimal conductor among its twists. In fact, assume that π is not minimal. Denote by n_0 the minimal conductor of π. Take a character μ so that $\pi_0 := \pi \otimes \mu$ has conductor n_0. Then, by [Tunnell 1978, Proposition 3.4], $n_0 \leq \max(n, 2n(\mu))$ with equality if π is minimal or $n \neq 2n(\mu)$. In particular, $n = 2m$ with $n(\mu) = m$. Hence, for any $r \geq m$, $\pi^{\mathcal{K}(r)} = \pi_0^{\mathcal{K}(r)}$ and $\pi^{\mathcal{E}(r)} = \pi_0^{\mathcal{E}(r)}$. Since $r \geq n_0/2$, one can apply the proposition to the minimal representation π_0.

Assume π is minimal in the following. Since $\mathcal{K}(r) \supset \mathcal{E}(r)$, $\pi^{\mathcal{K}(r)} \subset \pi^{\mathcal{E}(r)}$. It remains to prove that $\pi^{\mathcal{K}(r)}$ and $\pi^{\mathcal{E}(r)}$ have the same dimension. Denote by π_D the representation on $D^\times$, where D is the division quaternion algebra over F, so that the Jacquet–Langlands lifting of π_D to G is π. Then π_D has conductor n, that is, $\pi_D^{1 + \varpi_D^{n-1} \mathbb{O}_D} = \pi_D$ and $\pi_D^{1 + \varpi_D^{n-2} \mathbb{O}_D} = 0$, where ϖ_D is a uniformizer of D. Moreover, by [Carayol 1984, Proposition 6.5],

$$\dim \pi_D = \begin{cases} 2q^{m-1} & \text{if } n \text{ is even,} \\ q^m + q^{m-1} & \text{if } n \text{ is odd.} \end{cases}$$

For any $r \geq m$, $\mathcal{E}(r) \subset (1 + \varpi_D^{n-1} \mathbb{O}_D) \cap \mathbb{O}_K^\times$. Therefore, by the Tunnell–Saito theorem, if we denote by $\mathcal{X}(r)$ the set of all the characters μ on $K^\times$ such that $\mu|_{F^\times} \omega = 1$ and $\mu|_{\mathcal{E}(r)} = 1$, then

$$\dim \pi^{\mathcal{E}(r)} + \dim \pi_D = \sum_{\mu \in \mathcal{X}(r)} \dim \pi^\mu + \sum_\mu \dim \pi_D^\mu = \sum_{\mu \in \mathcal{X}(r)} (\dim \pi^\mu + \dim \pi_D^\mu) = \#\mathcal{X}(r)$$

and, on the other hand, the lemma below implies that

$$\dim \pi^{\mathcal{K}(r)} + \dim \pi_D = \#\mathcal{X}(r),$$

and then the equality $\dim \pi^{\mathcal{E}(r)} = \dim \pi^{\mathcal{K}(r)}$ holds. $\square$

Lemma 3.10. *Let π be minimal. For any integer $r \geq m$, we have the dimension formula*

$$\dim \pi^{\mathcal{K}(r)} = \begin{cases} q^r + q^{r-1} - 2q^{m-1} & \text{if } n \text{ is even and } e = 1, \\ q^r + q^{r-1} - (q^{m-1} + q^{m-2}) & \text{if } n \text{ is odd and } e = 1, \\ 2q^r - (q^m + q^{m-1}) & \text{if } n \text{ is odd and } e = 2, \\ 2q^r - 2q^{m-1} & \text{if } n \text{ is even and } e = 2. \end{cases}$$

Proof. For $r = m$ and $e = 1$, this formula occurs in [Casselman 1973b, Theorem 3]. We now use the method in [Casselman 1973b] to prove the dimension formula for the case n is even and $e = 1$, while the other cases are similar. Firstly, recall some basics about the Kirillov model. Let ψ be an unramified additive character of F. Associated to ψ, we can realize π on the space $C_c^\infty(F^\times)$ of Schwartz functions on the multiplicative group. For any $f \in C_c^\infty(F^\times)$ and any character μ of $\mathbb{O}^\times$, define

$$f_k(\mu) = \int_{\mathbb{O}^\times} f(u\varpi^k)\mu(u)\,du,$$

where we choose the Haar measure on $\mathbb{O}^\times$ so that the total measure is 1. Define further the formal power series

$$\hat{f}(\mu, t) = \sum_{k \in \mathbb{Z}} f_k(\mu)t^k,$$

which is actually a Laurent polynomial in t as f has compact support on $F^\times$. Because f is locally constant, this vanishes identically for all but a finite number of μ. By Fourier duality for $F^\times$, knowing $f(\mu, t)$ for all μ is equivalent to knowing f. For each μ, there is a formal power series $C(\mu, t)$ such that, for all $f \in C_c^\infty(F^\times)$,

$$(\pi(w)f)\hat{}(\mu, t) = C(\mu, t)\hat{f}(\mu^{-1}\omega_0^{-1}, t^{-1}z_0^{-1}),$$

$$C(\mu, t) = C_0(\mu)t^{n_\mu}, \quad w = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

where $\omega_0 = \omega|_{\mathbb{O}^\times}$, $z_0 = \omega(\varpi)$ and n_μ is an integer, $n_\mu \leq -2$. Moreover, if $\mu = 1$, then $-n_1 = n$. For any character μ of $\mathbb{O}^\times$,

$$-n_\mu = \begin{cases} n & \text{if } n(\mu) \leq m, \\ 2n(\mu) & \text{if } n(\mu) > m. \end{cases}$$

In fact, if we take any character Ω on $F^\times$ such that $\Omega|_{\mathbb{O}^\times} = \mu$, denote $\pi' = \pi \otimes \Omega$ and $C'(\cdot, \cdot)$ the monomial that occurs in the above functional equation, then for any character ν on $\mathbb{O}^\times$, $C'(\nu, t) = C(\nu\mu, \Omega(\varpi)t)$. Therefore, $-n_\mu = n(\pi') = \max(n, 2n(\mu))$.

On the other hand, by [Casselman 1973b, Corollary to Lemma 2], for any $r \geq m$, the subspace $\pi^{\mathcal{H}(r)}$ is isomorphic to the space of all functions $\hat{f}(\mu, t)$ such that

(1) $\hat{f}(\mu, t) = 0$ unless $n(\mu) \leq r$;

(2) for each μ, $f_k(\mu) = 0$ unless $-r \leq k \leq n_\mu + r$.

Summing up, for a given μ with conductor $n(\mu) \leq r$, the dimension of the space consisting of those $\hat{f}(\mu, t)$ with $f \in \pi^{\mathcal{H}(r)}$ is

$$\begin{cases} 2(r - m) + 1 & \text{if } n(\mu) \leq m, \\ 2(r - n(\mu)) + 1 & \text{if } n(\mu) > m. \end{cases}$$

Therefore,

$$\dim \pi^{\mathcal{K}(r)} = (q^m - q^{m-1})(2(r-m)+1) + \sum_{m<k\leq r}(q^k - 2q^{k-1} + q^{k-2})(2(r-k)+1)$$

$$= q^r + q^{r-1} - 2q^{m-1}. \qquad \square$$

Proof of Proposition 3.8. Note that $R^\times = \mathbb{O}_K^\times \mathcal{K}(m)$ unless K is ramified with n even and, once this equation holds, Proposition 3.8 follows directly from Proposition 3.9. So consider the case K is ramified with n even. Here, $R^\times = \mathbb{O}_K^\times \mathcal{K}'(m)$ with $\mathcal{K}'(m) = 1 + \varpi_K^{2m-1} R_0$. We want to show $\pi^{\mathcal{K}'(m)} = \pi^{\mathcal{E}'(m)}$ with $\mathcal{E}'(m) = \mathcal{K}'(m) \cap K^\times$, and Proposition 3.8 then holds. By [Tunnell 1983, Proposition 3.5], π is not minimal. Take a character μ such that $\pi_0 = \pi \otimes \mu$ has minimal conductor n_0. Then $n(\mu) = m$. Apply Proposition 3.9:

$$\pi^{\mathcal{K}'(m)} = \pi_0^{\mathcal{K}'(m)} \supset \pi_0^{\mathcal{K}(m-1)} = \pi_0^{\mathcal{E}(m-1)}.$$

We claim that $\pi_0^{\mathcal{E}(m-1)} = \pi_0^{\mathcal{E}'(m)}$. If so, $\pi_0^{\mathcal{E}(m-1)} = \pi^{\mathcal{E}'(m)}$ and then $\pi^{\mathcal{K}'(m)} = \pi^{\mathcal{E}'(m)}$. To prove this, note that $\mathcal{E}'(m) \subset \mathcal{E}(m-1) \subset 1 + \varpi_D^{n_0-1}\mathbb{O}_D$. Using the Tunnell–Saito theorem,

$$\dim \pi_0^{\mathcal{E}(m-1)} + \dim \pi_{0,D} = \#\mathcal{X}(m-1), \quad \dim \pi_0^{\mathcal{E}'(m)} + \dim \pi_{0,D} = \#\mathcal{X}'(m),$$

where the set $\mathcal{X}(m-1)$ consists of characters Ω of $K^\times$ such that $\Omega|_{F^\times} \cdot \omega_{\pi_0} = 1$ with $\Omega|_{\mathcal{E}(m-1)} = 1$, and the set $\mathcal{X}'(m)$ is defined similarly. As they are nonempty,

$$\#\mathcal{X}(m-1) = \#K^\times / F^\times \mathcal{E}(m-1) = \#K^\times / F^\times \mathcal{E}'(m) = \#\mathcal{X}'(m).$$

Thus, $\pi_0^{\mathcal{E}(m-1)} = \pi_0^{\mathcal{E}'(m)}$ and the proof is complete. $\qquad \square$

3D. *Local computations.* Let $\mathcal{W}(\sigma, \psi)$ be the Whittaker model of σ with respect to ψ and recall that we have an invariant Hermitian form on $\mathcal{W}(\sigma, \psi)$ defined by

$$(W_1, W_2) := \int_{F^\times} W_1\left[\begin{pmatrix} a & \\ & 1 \end{pmatrix}\right] \overline{W_2\left[\begin{pmatrix} a & \\ & 1 \end{pmatrix}\right]} \, d^\times a.$$

For any $W \in \sigma$, denote

$$\alpha(W) = \frac{(W, W)}{L(1, \sigma, \mathrm{ad})L(1, 1_F)L(2, 1_F)^{-1}}.$$

Proposition 3.11. *Denote by W_0 the normalized new vector of σ. If F is non-archimedean, then*

$$\alpha(W_0)|\delta|^{1/2} = \begin{cases} 1 & \text{if } \sigma \text{ is unramified,} \\ L(2, 1_F)L(1, 1_F)^{-1}L(1, \sigma, \mathrm{ad})^{-\delta_\sigma} & \text{otherwise,} \end{cases}$$

where $\delta_\sigma \in \{0, 1\}$ and equals 0 precisely when σ is a subrepresentation of the induced representation $\mathrm{Ind}(\mu_1, \mu_2)$ with at least one μ_i unramified. If $F = \mathbb{R}$ and σ is the discrete series $\mathscr{D}_\mu(k)$, then $\alpha(W_0) = 2^{-k}$.

The proposition follows from the explicit form of W_0. If F is nonarchimedean, W_0 is the one in the new vector line such that

$$W_0\left[\begin{pmatrix} \delta^{-1} & \\ & 1 \end{pmatrix}\right] = |\delta|^{-1/2}$$

and we have the following list (see [Schmidt 2002, p. 23]):

(1) If $\sigma = \pi(\mu_1, \mu_2)$ is a principal series, then

$$W_0\left[\begin{pmatrix} y & \\ & 1 \end{pmatrix}\right] = \begin{cases} |y|^{1/2} \displaystyle\sum_{\substack{k+l=v(y\delta) \\ k,l \geq 0}} \mu_1(\varpi)^k \mu_2(\varpi)^l 1_{\mathbb{O}}(\delta y) & \text{if } n(\mu_1) = n(\mu_2) = 0, \\ |y|^{1/2} \mu_1(\delta y) 1_{\mathbb{O}}(\delta y) & \text{if } n(\mu_1) = 0, n(\mu_2) > 0, \\ |\delta|^{-1/2} 1_{\mathbb{O}^\times}(\delta y) & \text{if } n(\mu_1) > 0, n(\mu_2) > 0. \end{cases}$$

(2) If $\sigma = \mathrm{sp}(2) \otimes \mu$ is a special representation, then

$$W_0\left[\begin{pmatrix} y & \\ & 1 \end{pmatrix}\right] = \begin{cases} |\delta|^{-1/2} \mu(\delta y) |\delta y| 1_{\mathbb{O}}(\delta y) & \text{if } n(\mu) = 0, \\ |\delta|^{-1/2} 1_{\mathbb{O}^\times}(\delta y) & \text{if } n(\mu) > 0. \end{cases}$$

(3) If σ is supercuspidal, then

$$W_0\left[\begin{pmatrix} y & \\ & 1 \end{pmatrix}\right] = |\delta|^{-1/2} 1_{\mathbb{O}^\times}(\delta y).$$

If $F = \mathbb{R}$ and σ is the discrete series $\mathscr{D}_\mu(k)$, then

$$W_0\left[\begin{pmatrix} y & \\ & 1 \end{pmatrix}\right] = |y|^{k/2} e^{-2\pi|y|}$$

and, in general, for archimedean cases it is expressed by the Bessel function [Popa 2008]. For $F = \mathbb{R}$ and σ a unitary discrete series of weight k, let $W \in \mathcal{W}(\sigma, \psi)$ be the vector satisfying

$$W\left[\begin{pmatrix} y & \\ & 1 \end{pmatrix}\right] = |y|^{k/2} e^{-2\pi|y|} 1_{\mathbb{R}_+^\times}(y).$$

Then W can be realized as a local component of a Hilbert newform and

$$(W_0, W_0) = 2(W, W), \quad Z(s, W) = \tfrac{1}{2} L(s, \sigma).$$

Proposition 3.12. *If F is nonarchimedean, let f be a nonzero vector in the one-dimensional space $V(\pi, \chi)$; then $\beta(f)|D\delta|^{-1/2}$ equals:*

$$
\begin{cases}
1 & \text{if } n = c = 0, \\[4pt]
L(1, \eta)^2 |\varpi^c| & \text{if } n = 0 \text{ and } c > 0, \\[4pt]
\dfrac{L(1, 1_F)}{L(2, 1_F)} L(1, \pi, \mathrm{ad})^{\delta_\pi} & \text{if } n > 0, \ c = 0 \text{ and } K \text{ is split,} \\[8pt]
\dfrac{L(1, 1_F)}{L(2, 1_F)} L(1, \eta)^2 |\varpi^c| \dfrac{L(1, \pi, \mathrm{ad})^{\delta_\pi}}{L(\frac{1}{2}, \pi, \chi)} & \text{if } nc > 0, \text{ either } K \text{ is split or } c \geq n, \\[8pt]
e(1 - q^{-e}) \dfrac{L(1, \pi, \mathrm{ad})}{L(\frac{1}{2}, \pi, \chi)} & \text{if } n > c \text{ and } K \text{ is nonsplit,}
\end{cases}
$$

which is independent of the choice of $f \in V(\pi, \chi)$.

The proof of Proposition 3.12 is reduced to computing the integral

$$
\beta^0 = \int_{F^\times \backslash K^\times} \frac{(\pi(t)f, f)}{(f, f)} \chi(t) \, dt,
$$

where f is any nonzero vector in $V(\pi, \chi)$.

In the case that $n > c$ and K is nonsplit, f is a χ^{-1}-eigenform and it is easy to see that $\beta^0 = \mathrm{Vol}(F^\times \backslash K^\times)$.

From now on assume $n \leq c$ or K is split. Then $B = M_2(F)$ by Lemma 3.1(5). Recall that the space $V(\pi, \chi)$ depends on a choice of an admissible order R for (π, χ). Let f be a test vector in $V(\pi, \chi)$ defined by R. For any $t \in K^\times$, $f' := \pi(t)f$ is a test vector defined by the admissible order $R' = tRt^{-1}$. It is easy to check that $\beta(f') = \beta(f)$. Thus, for a $K^\times$-conjugacy class of admissible orders, we can pick a particular order to compute β^0. There is a unique $K^\times$-conjugacy class of admissible orders except for the exceptional case $0 < c_1 < n$ and $n(\chi_1) = n(\chi_2) = c$. In this case, there are exactly two $K^\times$-conjugacy classes of admissible orders, which are conjugate to each other by a normalizer of $K^\times$ in $B^\times$.

Any admissible order (in the case $n \leq c$ or K is split) is an Eichler order of discriminant n, i.e., conjugate to $R_0(n) := \left(\begin{smallmatrix} \mathbb{O} & \mathbb{O} \\ \mathfrak{p}^n & \mathbb{O} \end{smallmatrix}\right)$. Choose an embedding of K into $M_2(F)$ as follows, so that $R_0(n)$ is an admissible order for (π, χ):

(1) If K is split, fix an F-algebra isomorphism $K \cong F^2$. If $c \geq n$ or $n(\chi_1) = c$, embed K into $M_2(F)$ by

$$
\iota_1 : (a, b) \longmapsto \gamma_c^{-1} \begin{pmatrix} a & \\ & b \end{pmatrix} \gamma_c, \quad \gamma_c = \begin{pmatrix} 1 & \varpi^{-c} \\ & 1 \end{pmatrix}.
$$

If $n(\chi_1) < c < n$, embed K into $M_2(F)$ by

$$
\iota_2 : (a, b) \longmapsto \gamma_c^{-1} \begin{pmatrix} b & \\ & a \end{pmatrix} \gamma_c.
$$

Note that, for any $t \in K^\times$, $\iota_1(t) = j\iota_2(t)j^{-1}$ with $j = \gamma_c^{-1}w\gamma_c$ and $w = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

(2) If K is a field, take $\tau \in \mathbb{O}_K$ such that $\mathbb{O}_K = \mathbb{O}[\tau]$ and, if K/F is ramified, then τ is a uniformizer. Embed K into $M_2(F)$ by

$$a + b\tau \longmapsto \gamma_c^{-1} \begin{pmatrix} a + b\,\mathrm{tr}\,\tau & b\mathrm{N}\tau \\ -b & a \end{pmatrix} \gamma_c, \quad \text{where } \gamma_c = \begin{pmatrix} \varpi^c \mathrm{N}\tau & \\ & 1 \end{pmatrix}.$$

Assume $K \cong F^2$. If $n(\chi_1) < c < n$,

$$\beta^0 = \int_{F^\times \backslash K^\times} \frac{(\pi(\iota_2(t))W_0, W_0)}{(W_0, W_0)} \chi(t)\,dt = \int_{F^\times \backslash K^\times} \frac{(\pi(\iota_1(t))W_0, W_0)}{(W_0, W_0)} \bar{\chi}(t)\,dt,$$

where $\bar{\chi}_1 = \chi_2$, $\bar{\chi}_2 = \chi_1$ and $n(\bar{\chi}_1) = n(\chi_2) = c$. We reduce to the case $c \geq n$ or $n(\chi_1) = c$. For the exceptional case, if we take $\pi(j)W_0$ as a test vector, then

$$\beta^0 = \int_{F^\times \backslash K^\times} \frac{(\pi(\iota_1(t)j)W_0, \pi(j)W_0)}{(W_0, W_0)} \chi(t)\,dt = \int_{F^\times \backslash K^\times} \frac{(\pi(\iota_1(t))W_0, W_0)}{(W_0, W_0)} \chi(\bar{t})\,dt$$

with $n(\bar{\chi}_1) = n(\chi_2) = c$. Thus, even for the exceptional case, we only need to consider W_0 as a test vector. Thus,

$$\beta^0 = (W_0, W_0)^{-1} \iint_{(F^\times)^2} \pi(\gamma_c)W_0\left[\begin{pmatrix} ab & \\ & 1 \end{pmatrix}\right] \overline{\pi(\gamma_c)W_0\left[\begin{pmatrix} b & \\ & 1 \end{pmatrix}\right]} \chi_1(a)\,d^\times b\,d^\times a$$

$$= (W_0, W_0)^{-1} \left| Z\left(\tfrac{1}{2}, \pi(\gamma_c)W_0, \chi_1\right) \right|^2.$$

If $c = 0$, $Z\left(\tfrac{1}{2}, W_0, \chi_1\right) = \chi_1(\delta)^{-1}L\left(\tfrac{1}{2}, \pi \otimes \chi_1\right)$ and so $\beta^0 = (W_0, W_0)^{-1}L\left(\tfrac{1}{2}, \pi, \chi\right)$. If $c > 0$, then

$$Z\left(\tfrac{1}{2}, \pi(\gamma_c)W_0, \chi_1\right) = \int_{F^\times} W_0\left[\begin{pmatrix} a & \\ & 1 \end{pmatrix}\right] \psi(a\varpi^{-c})\chi_1(a)\,d^\times a$$

$$= \sum_{k \in \mathbb{Z}} W_0\left[\begin{pmatrix} \varpi^k & \\ & 1 \end{pmatrix}\right] \int_{\varpi^k \mathbb{O}^\times} \psi(a\varpi^{-c})\chi_1(a)\,d^\times a.$$

Assume $n(\chi_1) = c$; then the integral $\int_{\varpi^k \mathbb{O}^\times} \psi(a\varpi^{-c})\chi_1(a)\,d^\times a$ vanishes unless $k = -v(\delta)$, while

$$\left| \int_{\delta^{-1}\mathbb{O}^\times} \psi(a\varpi^{-c})\chi_1(a)\,d^\times a \right| = L(1, 1_F)|\delta|^{1/2}q^{-c/2}.$$

Thus,

$$\beta^0 = (W_0, W_0)^{-1}L(1, 1_F)^2 q^{-c}.$$

Assume $c \geq n$ and $n(\chi_1) < c$. Let j be a normalizer of $K^\times$ with $jt = \bar{t}j$ for any $t \in K^\times$. As $c \geq n$, there exists some $t_0 \in K^\times$ such that $t_0 U_0(n)t_0^{-1} = jU_0(n)j^{-1}$

and $\pi(t_0)W_0, \pi(j)W_0$ are in the same line. Thus,

$$\beta^0 = \int_{F^\times \backslash K^\times} \frac{(\pi(t)W_0, W_0)}{(W_0, W_0)} \overline{\chi}(t)\, dt = (W_0, W_0)^{-1} L(1, 1_F)^2 q^{-c}$$

as $n(\overline{\chi}_1) = n(\chi_2) = c$.

Remark. Assume $n(\chi_1) < c < n$ and R is the intersection of two maximal orders R' and R'' with $R' \cap K = \mathbb{O}_c$ and $R'' \cap K = \mathbb{O}_K$. If R is not admissible, then the toric integral for ω-eigenforms f under $R^\times$ must vanish if $c > 1$. In the case $c = 1$, so that $n(\chi_1) = 0$,

$$\int_{F^\times \backslash K^\times} \frac{(\pi(\iota_1(t))W_0, W_0)}{(W_0, W_0)} \chi(t)\, dt = (W_0, W_0)^{-1} L(1, 1_F)^2 q^{-2}.$$

It remains to consider the case K is a field and $c \geq n$. Let $\Psi(g)$ denote the matrix coefficient:

$$\Psi(g) := \frac{(\pi(g)W_0, W_0)}{(W_0, W_0)}, \quad g \in \mathrm{GL}_2(F).$$

Then

$$\beta^0 = \frac{\mathrm{Vol}(K^\times/F^\times)}{\#K^\times/F^\times \mathbb{O}_c^\times} \sum_{t \in K^\times/F^\times \mathbb{O}_c^\times} \Psi(t)\chi(t).$$

In the case $c = 0$, π is unramified. Furthermore, if K/F is unramified, then $\beta^0 = \mathrm{Vol}(K^\times/F^\times) = |\delta|^{1/2}$ and, if K/F is ramified, $\beta^0 = |D\delta|^{1/2}(1 + \Psi(\tau)\chi(\tau))$, where $\Psi(\tau)$ is expressed by the MacDonald polynomial and one has $\beta(f) = |D\delta|^{1/2}$. It remains to consider the case $c > 0$. Denote

$$S_i = \{1 + b\tau \mid b \in \mathbb{O}/\mathfrak{p}^c, v(b) = i\}, \quad 0 \leq i \leq c - 1,$$

and

$$S' = \begin{cases} \{a + \tau \mid a \in \mathfrak{p}/\mathfrak{p}^c\} & \text{if } e = 1, \\ \{a\varpi + \tau \mid a \in \mathbb{O}/\mathfrak{p}^c\} & \text{if } e = 2. \end{cases}$$

Then a complete representatives of $K^\times/F^\times \mathbb{O}_c^\times$ can be taken as

$$\{1\} \sqcup \bigsqcup_i S_i \sqcup S'.$$

Note that Ψ is a function on $U_1(n)\backslash G/U_1(n)$. The following observation is key to our computation: the images of S_i, $0 \leq i \leq c - 1$, and S' under the natural map

$$\mathrm{pr} : K^\times \to U_1(n)\backslash G/U_1(n)$$

are constant. Precisely,

$$\mathrm{pr}(S_i) = \left[\begin{pmatrix} 1 & \varpi^{i-c} \\ & 1 \end{pmatrix} \right], \quad \mathrm{pr}(S') = \left[\begin{pmatrix} & \varpi^{-c} \\ -\varpi^{c+e-1} & \end{pmatrix} \right].$$

From this, it follows that

$$\sum_{t \in K^\times/F^\times \mathbb{O}_c^\times} \Psi(t)\chi(t) = 1 + \sum_{i=0}^{c-1} \Psi_i \sum_{t \in S_i} \chi(t) + \Psi' \sum_{t \in S'} \chi(t),$$

where Ψ_i (resp. Ψ') are the valuations of $\Psi(t)$ on S_i (resp. S').

Assume the central character ω is unramified; then we may take $\omega = 1$. If $e = c = 1$, we have

$$\sum_{t \in S_0} \chi(t) = -\chi(\tau) - 1 \quad \text{and} \quad \sum_{t \in S'} \chi(t) = \chi(\tau).$$

Otherwise,

$$\sum_{t \in S_i} \chi(t) = \begin{cases} 0 & \text{if } c > 1 \text{ and } 0 \le i \le c-2, \\ -1 & \text{if } i = c-1, \end{cases} \quad \text{and} \quad \sum_{t \in S'} \chi(t) = 0.$$

Therefore,

$$\sum_{t \in K^\times/F^\times \mathbb{O}_c^\times} \Psi(t)\chi(t) = \begin{cases} 1 + (-\chi(\tau) - 1)\Psi_0 + \chi(\tau)\Psi' & \text{if } e = c = 1, \\ 1 - \Psi_{c-1} & \text{otherwise.} \end{cases}$$

Note that, if $e = 1$, then $\left(\begin{smallmatrix} & \varpi^{-c} \\ -\varpi^c & \end{smallmatrix}\right)$ equals $\left(\begin{smallmatrix} 1 & \varpi^{-c} \\ & 1 \end{smallmatrix}\right)$ in $ZU_1(n)\backslash G/U_1(n)$ and, since $\omega = 1$, $\Psi' = \Psi_0$. We obtain

$$\sum_{t \in K^\times/F^\times \mathbb{O}_c^\times} \Psi(t)\chi(t) = 1 - \Psi_{c-1}$$

and reduce to the evaluation of Ψ_{c-1}. If $n = 0$, the matrix coefficient Ψ_{c-1} is expressed by the MacDonald polynomial. In particular, if the Satake parameter of π is (α, α^{-1}), then

$$1 - \Psi_{c-1} = \frac{(1 - \alpha^2 q^{-1})(1 - \alpha^{-2}q^{-1})}{1 + q^{-1}}.$$

If $n = 1$, then $\pi = \mathrm{sp}(2) \otimes \mu$ with μ an unramified quadratic character on $F^\times$. By definition,

$$\Psi_{c-1} = |\delta|^{1/2} L(1, \pi, \mathrm{ad})^{-1} \int_{F^\times} W_0\left[\begin{pmatrix} a & \\ & 1 \end{pmatrix}\begin{pmatrix} 1 & \varpi^{-1} \\ & 1 \end{pmatrix}\right] \overline{W_0\left[\begin{pmatrix} a & \\ & 1 \end{pmatrix}\right]} d^\times a$$

$$= |\delta|^{3/2} L(1, \pi, \mathrm{ad})^{-1} \int_{\varpi^{-n(\psi)}\mathbb{O}} \psi(a\varpi^{-1})|a|^2 d^\times a$$

$$= |\delta|^{3/2} L(1, \pi, \mathrm{ad})^{-1}(-q^{-1})L(1, \pi, \mathrm{ad})|\delta|^{-3/2} = -q^{-1}.$$

If $n \ge 2$, then

$$\Psi_{c-1} = |\delta|^{-1/2} \int_{\varpi^{-1-n(\psi)}\mathbb{O}^\times} \psi(x) d^\times x = -q^{-1} L(1, 1_F).$$

With these results, we obtain

$$\beta^0 = \frac{\mathrm{Vol}(K^\times/F^\times)}{\#K^\times/F^\times\mathbb{O}_c^\times} \times \begin{cases} \dfrac{L(1, 1_F)}{L(1, \pi, \mathrm{ad})(1+q^{-1})} & \text{if } n = 0, \\ 1+q^{-1} & \text{if } n = 1, \\ L(1, 1_F) & \text{if } n \geq 2. \end{cases}$$

Finally, we deal with the case that ω is ramified. As above, it is routine to check that Ψ_i for $i < c - 1$ and Ψ' are vanishing. Moreover, $\Psi_{c-1} = 0$ if and only if $\delta_\pi = 0$ and, for $\delta_\pi = 1$,

$$\Psi_{c-1} = -q^{-1}L(1, 1_F).$$

By the definition of δ_π, if $\delta_\pi = 1$ then $c \geq 2$ and $n(\omega) < n \leq c$. Thus, for $\delta_\pi = 1$,

$$0 = \sum_{t \in 1+\varpi^{c-1}\mathbb{O}_K/1+\varpi^c\mathbb{O}_K} \chi(t)$$

$$= \sum_{t \in 1+\varpi^{c-1}\mathbb{O}_K/(1+\varpi^{c-1}\mathbb{O})(1+\varpi^c\mathbb{O}_K)} \chi(t) \sum_{a \in 1+\varpi^{c-1}\mathbb{O}/1+\varpi^c\mathbb{O}} \omega^{-1}(a)$$

$$= q \sum_{b \in \mathfrak{p}^{c-1}/\mathfrak{p}^c} \chi(1+b\tau).$$

Therefore, if $\delta_\pi = 1$, then $\sum_{t \in S_{c-1}} \chi(t) = -1$ and

$$\beta^0 = \frac{\mathrm{Vol}(K^\times/F^\times)}{\#K^\times/F^\times\mathbb{O}_c^\times} \times \begin{cases} 1 & \text{if } \delta_\pi = 0, \\ L(1, 1_F) & \text{if } \delta_\pi = 1. \end{cases}$$

The proof of Proposition 3.12 is now complete. □

We finish our discussions of $\alpha(W_0)$, $\beta(f)$ and γ with Lemmas 3.13 and 3.14.

Lemma 3.13. *Let F be nonarchimedean and f a nonzero element in $V(\pi, \chi)$; then*

$$\alpha(W_0)\beta(f)\gamma|D|^{-1/2} = 2^{\delta(\Sigma_D)}L\left(\tfrac{1}{2}, \pi, \chi\right)^{-\delta(\Sigma)}L(1, \eta)^{2\delta(c_1)}q^{-c_1},$$

where these $\delta \in \{0, 1\}$ are given by:

- $\delta(\Sigma_D) = 1$ *if and only if K is ramified, $n > 0$ and $c < n$;*
- $\delta(\Sigma) = 1$ *if and only if $n > 0$, K is either ramified or $c > 0$ and, if $n = 1$, then $c \geq n$;*
- $\delta(c_1) = 1$ *if and only if $c_1 \neq 0$.*

Proof. We have computed $\alpha(W_0)$ in Proposition 3.11 and $\beta(f)$ in Proposition 3.12. When $n > 0$, by Lemma 3.5, $\gamma = L(1, 1_F)(1 - e(R)q^{-1})$ and it suffices to compute $e(R)$:

(i) $e(R) = 1$ and $\gamma = 1$ if K is split, or if K is ramified, $n = 1$ and B is split, or if K is nonsplit and $c \geq n$;

(ii) $e(R) = -1$ and $\gamma = L(1, 1_F)(1 + q^{-1})$ if K is inert and $c < n$, or if K is ramified, $n = 1$, B is division and $c = 0$;

(iii) $e(R) = 0$ and $\gamma = L(1, 1_F)$ if K is ramified, $n \geq 2$ and $c < n$. $\qquad \square$

For archimedean places, using Barnes' lemma we have the following list for (W_0, W_0) (see [Tadić 2009] for the classification of unitary dual of $GL_2(F)$):

(1) Assume $F = \mathbb{R}$, σ is the infinite-dimensional subquotient of the induced representation $\text{Ind}(\mu_1, \mu_2)$, where $\mu_i(a) = |a|^{s_i} \text{sgn}(a)^{m_i}$ with $s_i \in \mathbb{C}$ and $m_i \in \{0, 1\}$. Let $k = s_1 - s_2 + 1$, $\mu = s_1 + s_2$.

(a) If $\sigma = \mathcal{D}_\mu(k)$ is the discrete series with $k \geq 2$, then (W_0, W_0) equals

$$2(4\pi)^{-k} \Gamma(k).$$

(b) If $\sigma = \pi(\mu_1, \mu_2)$ is a principal series, then (W_0, W_0) equals

$$\pi^{-1-m_1-m_2} \Gamma\left(\tfrac{1}{2}(1+2m_1)\right) \Gamma\left(\tfrac{1}{2}(1+2m_2)\right) B\left(\tfrac{1}{2}(k+m_1+m_2), \tfrac{1}{2}(2-k+m_1+m_2)\right),$$

where $B(x, y) := \Gamma(x)\Gamma(y)\Gamma(x+y)^{-1}$ is the beta function.

(2) Assume $F = \mathbb{C}$, $\sigma = \pi(\mu_1, \mu_2)$ is a principal series with $\mu_i(z) = |z|^{s_i} \left(\dfrac{z}{\sqrt{|z|_\mathbb{C}}}\right)^{m_i}$ and $s_i \in \mathbb{C}$ and $m_i \in \mathbb{Z}$; then (W_0, W_0) equals

$$8(2\pi)^{-1-|m_1|-|m_2|} \Gamma(1+|m_1|)\Gamma(1+|m_2|)$$
$$\times B\left(1 + s_1 - s_2 + \tfrac{1}{2}(|m_1| + |m_2|), 1 - s_1 + s_2 + \tfrac{1}{2}(|m_1| + |m_2|)\right).$$

For a pair (π, χ), define

$$C(\pi, \chi) = \begin{cases} 2^{-1}\pi(W_0, W_0)^{-1} & \text{if } K/F = \mathbb{C}/\mathbb{R}, \\ (W_0', W_0')(W_0, W_0)^{-1} & \text{if } K = F^2. \end{cases}$$

In the split case, W_0' is the new vector of $\pi \otimes \chi_1$, where K is embedded into $M_2(F)$ diagonally and $\chi_1(a) = \chi\left(\begin{pmatrix} a & \\ & 1 \end{pmatrix}\right)$.

Lemma 3.14. *For F archimedean, let f be a nonzero vector in $V(\pi, \chi)$; then*

$$\alpha(W_0)\beta(f) = C(\pi, \chi)^{-1} \begin{cases} L\left(\tfrac{1}{2}, \pi, \chi\right)^{-1} & \text{if } K/F = \mathbb{C}/\mathbb{R}, \\ 1 & \text{if } K = F^2. \end{cases}$$

In particular, if $\sigma = \mathcal{D}_\mu(k)$ is a discrete series with weight k, then

$$C(\pi, \chi) = \begin{cases} 4^{k-1}\pi^{k+1}\Gamma(k)^{-1} & \text{if } K = \mathbb{C}, \\ 1 & \text{if } K = \mathbb{R}^2. \end{cases}$$

Proof. By definition,

$$\alpha(W_0)\beta(f) = \frac{L(1, \eta)}{L(1, 1_F)} L\left(\tfrac{1}{2}, \pi, \chi\right)^{-1}(W_0, W_0)\beta^0$$

with

$$\beta^0 = \int_{F^\times \backslash K^\times} \frac{(\pi(t)f, f)}{(f, f)} \chi(t)\, dt, \quad f \in V(\pi, \chi).$$

If $K/F = \mathbb{C}/\mathbb{R}$, then $\beta^0 = \mathrm{Vol}(K^\times/F^\times) = 2$. If K is split, taking $f = W_0'$, then $\beta^0 = L\left(\frac{1}{2}, \pi, \chi\right)(W_0', W_0')^{-1}$. If $\sigma = \mathcal{D}_\mu(k)$, the value for (W_0, W_0) is given in (1a) in the above list and we note that, if $K = \mathbb{R}^2$, then $(W_0', W_0') = (W_0, W_0)$ as, for any χ_1, $\pi \otimes \chi_1$ and π have the same weight. $\qquad\square$

Acknowledgements

References

[Bertolini and Darmon 1997] M. Bertolini and H. Darmon, "A rigid analytic Gross–Zagier formula and arithmetic applications", *Ann. of Math.* (2) **146**:1 (1997), 111–147. MR 99f:11079 Zbl 1029.11027

[Cai et al. 2014] L. Cai, J. Shu, and Y. Tian, "Cube sum problem and an explicit Gross–Zagier formula", preprint, 2014. arXiv 1412.1950

[Carayol 1984] H. Carayol, "Représentations cuspidales du groupe linéaire", *Ann. Sci. École Norm. Sup.* (4) **17**:2 (1984), 191–225. MR 86f:22019 Zbl 0549.22009

[Casselman 1973a] W. Casselman, "On some results of Atkin and Lehner", *Math. Ann.* **201** (1973), 301–314. MR 49 #2558 Zbl 0239.10015

[Casselman 1973b] W. Casselman, "The restriction of a representation of $GL_2(k)$ to $GL_2(\mathfrak{o})$", *Math. Ann.* **206** (1973), 311–318. MR 49 #3040 Zbl 0253.20062

[Coates et al. 2014] J. Coates, Y. Li, Y. Tian, and S. Zhai, "Quadratic twists of elliptic curves", *Proc. London Math. Soc.* (3) (appeared online December 2014). arXiv 1312.3884

[Dasgupta and Voight 2009] S. Dasgupta and J. Voight, "Heegner points and Sylvester's conjecture", pp. 91–102 in *Arithmetic geometry* (Göttingen, 2006), edited by H. Darmon et al., Clay Math. Proc. **8**, Amer. Math. Soc., Providence, RI, 2009. MR 2010j:11088 Zbl 1250.11057

[Gross 1987] B. H. Gross, "Heights and the special values of L-series", pp. 115–187 in *Number theory* (Montreal, 1985), edited by H. Kisilevsky and J. Labute, CMS Conf. Proc. **7**, Amer. Math. Soc., Providence, RI, 1987. MR 89c:11082 Zbl 0623.10019

[Gross 1988] B. H. Gross, "Local orders, root numbers, and modular curves", *Amer. J. Math.* **110**:6 (1988), 1153–1182. MR 90b:11053 Zbl 0675.12011

[Gross and Prasad 1991] B. H. Gross and D. Prasad, "Test vectors for linear forms", *Math. Ann.* **291**:2 (1991), 343–355. MR 92k:22028 Zbl 0768.22004

[Gross and Zagier 1986] B. H. Gross and D. B. Zagier, "Heegner points and derivatives of L-series", *Invent. Math.* **84**:2 (1986), 225–320. MR 87j:11057 Zbl 0608.14019

[Jacquet and Chen 2001] H. Jacquet and N. Chen, "Positivity of quadratic base change L-functions", *Bull. Soc. Math. France* **129**:1 (2001), 33–90. MR 2003b:11048 Zbl 1069.11017

[Popa 2008] A. A. Popa, "Whittaker newforms for Archimedean representations", *J. Number Theory* **128**:6 (2008), 1637–1645. MR 2009c:22012 Zbl 1146.11030

[Saito 1993] H. Saito, "On Tunnell's formula for characters of GL(2)", *Compositio Math.* **85**:1 (1993), 99–108. MR 93m:22021 Zbl 0795.22009

[Satgé 1987] P. Satgé, "Un analogue du calcul de Heegner", *Invent. Math.* **87**:2 (1987), 425–439. MR 88d:11057 Zbl 0616.14023

[Schmidt 2002] R. Schmidt, "Some remarks on local newforms for GL(2)", *J. Ramanujan Math. Soc.* **17**:2 (2002), 115–147. MR 2003g:11056 Zbl 0997.11040

[Tadić 2009] M. Tadić, "GL$(n, \mathbb{C})^\wedge$ and GL$(n, \mathbb{R})^\wedge$", pp. 285–313 in *Automorphic forms and L-functions, II: Local aspects*, Contemp. Math. **489**, Amer. Math. Soc., Providence, RI, 2009. MR 2010j:22020 Zbl 1186.22021

[Tian 2014] Y. Tian, "Congruent numbers and Heegner points", *Cambridge J. Math.* **2**:1 (2014), 117–161. Zbl 06324779

[Tian et al. 2013] Y. Tian, X. Yuan, and S. Zhang, "Genus periods, genus points and congruent number problem", preprint, 2013. arXiv 1411.4728

[Tunnell 1978] J. B. Tunnell, "On the local Langlands conjecture for $GL(2)$", *Invent. Math.* **46**:2 (1978), 179–200. MR 57 #16262 Zbl 0385.12006

[Tunnell 1983] J. B. Tunnell, "Local ϵ-factors and characters of GL(2)", *Amer. J. Math.* **105**:6 (1983), 1277–1307. MR 86a:22018 Zbl 0532.12015

[Vignéras 1980] M.-F. Vignéras, *Arithmétique des algèbres de quaternions*, Lecture Notes in Mathematics **800**, Springer, Berlin, 1980. MR 82i:12016 Zbl 0422.12008

[Waldspurger 1985] J.-L. Waldspurger, "Sur les valeurs de certaines fonctions L automorphes en leur centre de symétrie", *Compositio Math.* **54**:2 (1985), 173–242. MR 87g:11061b Zbl 0567.10021

[Washington 1997] L. C. Washington, *Introduction to cyclotomic fields*, 2nd ed., Graduate Texts in Mathematics **83**, Springer, New York, 1997. MR 97h:11130 Zbl 0966.11047

[Yu 2013] C. Yu, "Variants of mass formulas for definite division algebras", preprint, 2013. arXiv 1304:6175

[Yuan et al. 2013] X. Yuan, S.-W. Zhang, and W. Zhang, *The Gross-Zagier formula on Shimura curves*, Annals of Mathematics Studies **184**, Princeton University Press, Princeton, NJ, 2013. MR 3237437 Zbl 1272.11082

lcai@math.tsinghua.edu.cn   *Mathematical Sciences Center, Tsinghua University, Jin Chun Yuan West Bldg. 248, Beijing, 100084, China*

shujie09@mails.gucas.ac.cn   *Academy of Mathematics and Systems Science, Morningside Center of Mathematics, Chinese Academy of Sciences, Beijing, 100190, China*

ytian@math.ac.cn   *Academy of Mathematics and Systems Science, Morningside Center of Mathematics, Chinese Academy of Sciences, Beijing, 100190, China*

Guidelines for Authors

Authors may submit manuscripts in PDF format on-line at the Submission page at the ANT website.

Originality. Submission of a manuscript acknowledges that the manuscript is original and and is not, in whole or in part, published or under consideration for publication elsewhere. It is understood also that the manuscript will not be submitted elsewhere while under consideration for publication in this journal.

Language. Articles in *ANT* are usually in English, but articles written in other languages are welcome.

Length There is no a priori limit on the length of an *ANT* article, but *ANT* considers long articles only if the significance-to-length ratio is appropriate. Very long manuscripts might be more suitable elsewhere as a memoir instead of a journal article.

Required items. A brief abstract of about 150 words or less must be included. It should be self-contained and not make any reference to the bibliography. If the article is not in English, two versions of the abstract must be included, one in the language of the article and one in English. Also required are keywords and subject classifications for the article, and, for each author, postal address, affiliation (if appropriate), and email address.

Format. Authors are encouraged to use LaTeX but submissions in other varieties of TeX, and exceptionally in other formats, are acceptable. Initial uploads should be in PDF format; after the refereeing process we will ask you to submit all source material.

References. Bibliographical references should be complete, including article titles and page ranges. All references in the bibliography should be cited in the text. The use of BibTeX is preferred but not required. Tags will be converted to the house format, however, for submission you may use the format of your choice. Links will be provided to all literature with known web locations and authors are encouraged to provide their own links in addition to those supplied in the editorial process.

Figures. Figures must be of publication quality. After acceptance, you will need to submit the original source files in vector graphics format for all diagrams in your manuscript: vector EPS or vector PDF files are the most useful.

Most drawing and graphing packages (Mathematica, Adobe Illustrator, Corel Draw, MATLAB, etc.) allow the user to save files in one of these formats. Make sure that what you are saving is vector graphics and not a bitmap. If you need help, please write to graphics@msp.org with details about how your graphics were generated.

White space. Forced line breaks or page breaks should not be inserted in the document. There is no point in your trying to optimize line and page breaks in the original manuscript. The manuscript will be reformatted to use the journal's preferred fonts and layout.

Proofs. Page proofs will be made available to authors (or to the designated corresponding author) at a Web site in PDF format. Failure to acknowledge the receipt of proofs or to return corrections within the requested deadline may cause publication to be postponed.