Algebra & Number Theory

Volume 8
2014
No. 5

Tetrahedral elliptic curves and the local-global principle for isogenies

Barinder S. Banwait and John E. Cremona

msp

ALGEBRA AND NUMBER THEORY 8:5 (2014)
dx.doi.org/10.2140/ant.2014.8.1201

msp

Tetrahedral elliptic curves and the local-global principle for isogenies

Barinder S. Banwait and John E. Cremona

We study the failure of a local-global principle for the existence of l-isogenies for elliptic curves over number fields K. Sutherland has shown that over $\mathbb{Q}$ there is just one failure, which occurs for $l = 7$ and a unique j-invariant, and has given a classification of such failures when K does not contain the quadratic subfield of the l-th cyclotomic field. In this paper we provide a classification of failures for number fields which do contain this quadratic field, and we find a new "exceptional" source of such failures arising from the exceptional subgroups of $\mathrm{PGL}_2(\mathbb{F}_l)$. By constructing models of two modular curves, $X_s(5)$ and $X_{S_4}(13)$, we find two new families of elliptic curves for which the principle fails, and we show that, for quadratic fields, there can be no other exceptional failures.

1. Introduction

Let E be an elliptic curve defined over a number field K, and l a prime. It is easy to show that if E possesses a K-rational l-isogeny, then the reduction $\widetilde{E}_{\mathfrak{p}}/\mathbb{F}_{\mathfrak{p}}$, for all primes $\mathfrak{p}$ of K of good reduction and not dividing l, likewise possesses an $\mathbb{F}_{\mathfrak{p}}$-rational l-isogeny.

Andrew Sutherland [2012] asked a converse question: if $\widetilde{E}_{\mathfrak{p}}/\mathbb{F}_{\mathfrak{p}}$ admits an $\mathbb{F}_{\mathfrak{p}}$-rational l-isogeny for a density-one set of primes $\mathfrak{p}$, then does E/K admit a K-rational l-isogeny? Sutherland showed that while the answer to this question is usually "yes", there nevertheless exist pairs $(E/K, l)$ for which the answer is "no".

Whether an elliptic curve over a field possesses a rational l-isogeny or not depends only on its j-invariant, provided that the j-invariant is neither 0 nor 1728; thus, if the answer is "no" for one elliptic curve E/K for the prime l, it is also "no" for every elliptic curve over K with the same j-invariant $j(E)$ (with the same exceptions). Following Sutherland, we thus define a pair (l, j_0), consisting of a prime l and an element $j_0 \neq 0, 1728$ of a number field K, to be *exceptional for* K if there exists an elliptic curve E over K, with $j(E) = j_0$, such that the answer to

The first author was supported by an EPSRC Doctoral Training Award at the University of Warwick.
MSC2010: primary 11G05; secondary 11G18.
Keywords: elliptic curves, local-global, isogeny, exceptional modular curves.

the above question at l is "no". We will refer to the prime in the exceptional pair as an *exceptional prime for* K, and any elliptic curve E over K with $j(E) = j_0$ as a *Hasse at* l *curve over* K.

Sutherland gives a necessary condition for the existence of an exceptional pair, under a certain assumption. To state Sutherland's result, recall that the absolute Galois group $G_K := \mathrm{Gal}(\overline{K}/K)$ acts on the l-torsion subgroup $E(\overline{K})[l]$, yielding the mod-l representation

$$\bar{\rho}_{E,l} : G_K \to \mathrm{GL}_2(\mathbb{F}_l),$$

whose image $G_{E,l} := \mathrm{Im}\,\bar{\rho}_{E,l}$ is well-defined up to conjugacy; we refer to $G_{E,l}$ as *the mod-*l *image of* E. We let $H_{E,l} := G_{E,l}$ modulo scalars, and observe that $H_{E,l}$ depends only upon $j(E)$, provided that $j(E) \neq 0$ or 1728; we refer to $H_{E,l}$ as *the projective mod-*l *image of* E.

It is easy to show that $l = 2$ is not an exceptional prime for any number field, so henceforth we assume that l is odd. We now define $l^* := \pm l$, where the plus sign is taken if $l \equiv 1 \pmod 4$, and the minus sign otherwise.

Sutherland's result may now be stated as follows; by D_{2n} we mean the dihedral group of order $2n$:

Proposition 1.1 (Sutherland). *Assume* $\sqrt{l^*} \notin K$. *If* (l, j_0) *is exceptional for* K, *then for all elliptic curves* E/K *with* $j(E) = j_0$:

(1) *The projective mod-*l *image of* E *is isomorphic to* D_{2n}, *where* $n > 1$ *is an odd divisor of* $(l-1)/2$.

(2) $l \equiv 3 \pmod 4$.

(3) *The mod-*l *image of* E *is contained in the normaliser of a split Cartan subgroup of* $\mathrm{GL}_2(\mathbb{F}_l)$.

(4) E *obtains a rational* l*-isogeny over* $K(\sqrt{l^*})$.

(In fact, the converse is also true, as may be shown by applying the proof of the converse part of Proposition 1.3 below; see Section 7.)

Sutherland used this result for $K = \mathbb{Q}$ to determine the exceptional pairs for $\mathbb{Q}$ (where the assumption $\sqrt{l^*} \notin \mathbb{Q}$ is trivially satisfied for all l). If $(l, j(E))$ is exceptional for $\mathbb{Q}$, then (3) above says that E corresponds to a $\mathbb{Q}$-point on the modular curve $X_{\mathrm{s}}(l)$. By the recent work of Bilu, Parent and Rebolledo [Bilu et al. 2013], it follows that l must be 2, 3, 5, 7 or 13. Of these, only 3 and 7 are 3 (mod 4), and 3 can easily be ruled out as a possible exceptional prime (for all number fields). Thus, 7 is the only possible exceptional prime for $\mathbb{Q}$, and (1) above tells us that the projective mod-7 image of a Hasse at 7 curve over $\mathbb{Q}$ must be isomorphic to D_6, the dihedral group of order 6. The modular curve parametrising elliptic curves with this specific level-7 structure turns out to be the rational elliptic curve with

label 49a3 in [Cremona 1997], which has precisely two noncuspidal rational points. Evaluating j at these points yields the same value, and hence gives Sutherland's second result.

Theorem 1.2 [Sutherland 2012, Theorem 2]. *The only exceptional pair for $\mathbb{Q}$ is*

$$\left(7, \tfrac{2268945}{128}\right).$$

In this paper we would like to investigate what happens in the case where $\sqrt{l^*} \in K$. In Section 7 we will prove the following using Sutherland's methods:

Proposition 1.3. *Assume $\sqrt{l^*} \in K$. Then (l, j_0) is exceptional for K if and only if one of the following holds for elliptic curves E/K with $j(E) = j_0$:*

- *$H_{E,l} \cong A_4$ and $l \equiv 1 \pmod{12}$.*
- *$H_{E,l} \cong S_4$ and $l \equiv 1 \pmod{24}$.*
- *$H_{E,l} \cong A_5$ and $l \equiv 1 \pmod{60}$.*
- *$H_{E,l} \cong D_{2n}$ and $l \equiv 1 \pmod 4$, where $n > 1$ is a divisor of $(l-1)/2$, and $G_{E,l}$ lies in the normaliser of a split Cartan subgroup.*

Thus, in the case $\sqrt{l^*} \in K$, there are two sorts of exceptional pairs: the *dihedral ones* and the *nondihedral ones*.

Let us now consider each of these two cases over $K = \mathbb{Q}(\sqrt{l^*})$, the smallest field containing $\sqrt{l^*}$. Regarding the dihedral pairs, we may ask the following question:

Question 1.4. For which $l \equiv 1 \pmod 4$ is there an elliptic curve E over $\mathbb{Q}(\sqrt{l})$ such that $H_{E,l} \cong D_{2n}$, for $n > 1$ a divisor of $(l-1)/2$?

A positive answer to the Serre uniformity problem for number fields would imply that there should be only finitely many such l, but we are unable to prove this. Instead, we show that the set of l asked for by the above question is not empty; $l = 5$ gives a positive answer.

Theorem 1.5. *An elliptic curve E over $\mathbb{Q}(\sqrt{5})$ has $H_{E,5} \cong D_4$ if and only if its j-invariant is given by the formula*

$$j(E) = \frac{\left((s+5)(s^2-5)(s^2+5s+10)\right)^3}{(s^2+5s+5)^5} \tag{1-1}$$

for some $s \in \mathbb{Q}(\sqrt{5})$, together with the condition that $s^2 - 20$ is not a square in $\mathbb{Q}(\sqrt{5})$ for all $s \in \mathbb{Q}(\sqrt{5})$ satisfying (1-1).

Thus, the exceptional pairs at 5 over $\mathbb{Q}(\sqrt{5})$ are given by $(5, j(E))$ for $j(E)$ as above, and, in particular, there are infinitely many exceptional pairs at 5 over $\mathbb{Q}(\sqrt{5})$.

The proof of this theorem considers the modular curve $X_{\mathrm{s}}(5)$ corresponding to the normaliser of a split Cartan subgroup, whose $\mathbb{Q}(\sqrt{5})$-points (as we will see) correspond to elliptic curves E over $\mathbb{Q}(\sqrt{5})$ with $H_{E,5} \subseteq D_4$. This curve is defined over $\mathbb{Q}$ and has genus 0; writing the j-map

$$X_{\mathrm{s}}(5) \xrightarrow{j} X(1)$$

as a rational function yields the parametrisation (1-1); the further condition stated in the theorem is needed to force the corresponding elliptic curve to have $H_{E,5} \cong D_4$ (and not merely a subgroup of D_4); see Section 3 for the full proof.

Regarding the nondihedral pairs, we prove the following in Section 8:

Proposition 1.6. *The only nondihedral exceptional prime l over any quadratic field is* 13 *over* $\mathbb{Q}(\sqrt{13})$, *where the projective mod-*13 *image is isomorphic to* A_4.

This leads to the following question:

Question 1.7. Find all elliptic curves E over $\mathbb{Q}(\sqrt{13})$ such that $H_{E,13} \cong A_4$.

By Proposition 1.6, such elliptic curves are the only nondihedral Hasse curves over quadratic fields.

We take a similar approach to this question as we did for Theorem 1.5, by studying the relevant modular curve $X_{S_4}(13)$; this is the modular curve over $\mathbb{Q}$ corresponding to the pullback to $\mathrm{GL}_2(\mathbb{F}_{13})$ of $S_4 \subset \mathrm{PGL}_2(\mathbb{F}_{13})$; the earliest reference to this curve we are aware of is in [Mazur 1977b]. This modular curve is geometrically connected, and over the complex numbers has the description $\Gamma_{A_4}(13)\backslash\mathcal{H}^*$, where $\Gamma_{A_4}(13)$ is the pullback to $\mathrm{PSL}_2(\mathbb{Z})$ of $A_4 \subset \mathrm{PSL}_2(\mathbb{F}_{13})$. A $\mathbb{Q}$-point on $X_{S_4}(13)$ corresponds to an elliptic curve $E/\mathbb{Q}$ such that $H_{E,13} \subseteq S_4$. A $\mathbb{Q}(\sqrt{13})$-point corresponds to an elliptic curve $E/\mathbb{Q}(\sqrt{13})$ such that $H_{E,13} \subseteq A_4$. Thus, the elliptic curves we seek in Question 1.7 correspond to certain $\mathbb{Q}(\sqrt{13})$-points on the modular curve $X_{S_4}(13)$.

Theorem 1.8. *The modular curve $X_{S_4}(13)$ is a genus-*3 *curve, whose canonical embedding in $\mathbb{P}^2_{\mathbb{Q}}$ has the model*

$$\mathcal{C} : 4X^3Y - 3X^2Y^2 + 3XY^3 - X^3Z + 16X^2YZ - 11XY^2Z + 5Y^3Z + 3X^2Z^2 + 9XYZ^2 + Y^2Z^2 + XZ^3 + 2YZ^3 = 0.$$

On this model, the j-map $X_{S_4}(13) \xrightarrow{j} X(1)$ is given by

$$j(X, Y, Z) = \frac{n(X, Y, Z)}{d(X, Y, Z)^{13}},$$

where

$$d(X, Y, Z) = 5X^3 - 19X^2Y - 6XY^2 + 9Y^3 + X^2Z - 23XYZ - 16Y^2Z + 8XZ^2 - 22YZ^2 + 3Z^3$$

and $n(X, Y, Z)$ is an explicit degree-39 polynomial.

The proof of this theorem will occupy Sections 4 and 5 of the paper.

We have not been able to provably determine the $\mathbb{Q}(\sqrt{13})$-points on the curve. The method of Chabauty does not apply in this case, and this is likely to be a difficult problem; see Section 9 for more about the Jacobian of $\mathscr{C}$ and the difficulty of determining the $\mathbb{Q}$ and $\mathbb{Q}(\sqrt{13})$-rational points.

We have, however, the following six points[1] in $\mathscr{C}(\mathbb{Q}(\sqrt{13}))$, four of which are in $\mathscr{C}(\mathbb{Q})$:

$$\big\{(1:3:-2),\ (0:0:1),\ (0:1:0),\ (1:0:0),\ (3\pm\sqrt{13}:0:2)\big\}.$$

By evaluating the j-map at these points, we obtain the j-invariants of elliptic curves over $\mathbb{Q}(\sqrt{13})$ whose projective mod-13 image is contained in A_4; in fact, apart from $(0:0:1)$, whose corresponding j-invariant is 0, these points have projective mod-13 image isomorphic to A_4.

Corollary 1.9. *Elliptic curves over $\mathbb{Q}$ with j-invariants*

$$\frac{11225615440}{1594323} = \frac{2^4\cdot 5\cdot 13^4\cdot 17^3}{3^{13}},$$

$$-\frac{160855552000}{1594323} = -\frac{2^{12}\cdot 5^3\cdot 11\cdot 13^4}{3^{13}},$$

$$\frac{9061636498563792450559037262116207748 7104}{19765049735370209430 8570556640625} = \frac{2^{18}\cdot 3^3\cdot 13^4\cdot 127^3\cdot 139^3\cdot 157^3\cdot 283^3\cdot 929}{5^{13}\cdot 61^{13}}$$

have projective mod-13 images isomorphic to S_4. Elliptic curves over $\mathbb{Q}(\sqrt{13})$ with these j-invariants have projective mod-13 images isomorphic to A_4, as do elliptic curves over $\mathbb{Q}(\sqrt{13})$ with j-invariant

$$j = \frac{4096000}{1594323}(15996230 \pm 4436419\sqrt{13}).$$

Thus, elliptic curves over $\mathbb{Q}(\sqrt{13})$ with these j-invariants are Hasse at 13 curves over $\mathbb{Q}(\sqrt{13})$.

Remark 1.10. It is known that, for $l > 13$, there are no elliptic curves E over $\mathbb{Q}$ with $H_{E,l} \cong S_4$; in fact, Serre proved that $X_{S_4}(l)(\mathbb{Q})$ is empty for $l > 13$. Mazur [1977a, p. 36] reports that Serre has constructed a $\mathbb{Q}$-point on $X_{S_4}(13)$ corresponding to elliptic curves with complex multiplication by $\sqrt{-3}$; this point that Serre found corresponds to the point $(0:0:1)$ on the curve $\mathscr{C}$ above.

[1] These are all the points in $\mathscr{C}(\mathbb{Q}(\sqrt{13}))$ of logarithmic height less than 5.24, according to [Turner 2013].

Remark 1.11. The rational points on $X_{S_4}(l)$ for $l \leq 11$ have already been determined. The most interesting case is $l = 11$, where Ligozat [1977] proved that the curve $X_{S_4}(11)$ is the elliptic curve with Cremona label 121c1.

We conclude this introduction by considering the following problem, which we would like to solve at least for every quadratic field. This may be viewed as a generalisation of Sutherland's theorem 2 (see 1.2).

Problem 1.12. Fix a number field K. Find all exceptional pairs over K.

Samuele Anni [2014] has proved that there can be only finitely many exceptional primes for a given number field K. In the quadratic case, his result gives the following:

Proposition 1.13 (Anni). *A quadratic field K admits at most* 3 *exceptional primes. If $K = \mathbb{Q}(\sqrt{l})$ for l a prime $\equiv 1 \pmod 4$, then the only possible exceptional primes are* 7, 11, *and l. If $K \neq \mathbb{Q}(\sqrt{l})$, then only* 7 *and* 11 *are possible exceptional primes.*

It is straightforward to determine, for a given quadratic field K, the exceptional pairs of the form $(7, j_0)$; in principle all one needs to do is determine the j-invariants of the K-points on the elliptic curve 49a3.

In the case where $K = \mathbb{Q}(\sqrt{l})$ and the prime is l, Problem 1.12 reduces to Question 1.4 above, which essentially asks for quadratic points on the modular curves $X_{\mathrm{s}}(l)$; this is known to be a difficult problem.

Regarding 11 as a possible exceptional prime, we make the following conjecture:

Conjecture 1.14. 11 is not an exceptional prime for any quadratic field.

In Section 10, we will explain our evidence for this conjecture.

2. Preliminaries

Let l be an odd prime. We define $\mathrm{PSL}_2(\mathbb{F}_l)$ to be the kernel of the map det : $\mathrm{PGL}_2(\mathbb{F}_l) \to \mathbb{F}_l^*/(\mathbb{F}_l^*)^2 \cong \{\pm 1\}$. It is isomorphic to $\mathrm{SL}_2(\mathbb{F}_l)/\{\pm I\}$. By $\mathrm{GL}_2^+(\mathbb{F}_l)$ we mean the subgroup of matrices with square determinant.

Lemma 2.1. *Let E/K be an elliptic curve. The following are equivalent*:

(1) $H_{E,l} \subseteq \mathrm{PSL}_2(\mathbb{F}_l)$.

(2) $\sqrt{l^*} \in K$.

(3) $G_{E,l} \subseteq \mathrm{GL}_2^+(\mathbb{F}_l)$.

Proof. The equivalence of (1) and (3) is clear. The equivalent of (2) and (3) follows from standard Galois theory upon observing that the determinant of $\bar{\rho}_{E,l}$ is equal to the mod-l cyclotomic character over K. □

In particular, if $E/\mathbb{Q}$ is an elliptic curve with $H_{E,13} \cong S_4$, then after base-changing to $\mathbb{Q}(\sqrt{13})$ the projective image is intersected with $\mathrm{PSL}_2(\mathbb{F}_{13})$, and becomes isomorphic to A_4. This argument uses the fact that $13 \equiv 5 \pmod 8$.

We would like to briefly mention the Cartan subgroups of $\mathrm{GL}_2(\mathbb{F}_l)$; for a complete treatment see [Lang 2002, Chapter XVIII, §12]. There are two sorts of Cartan subgroup, *split* and *nonsplit*. A split Cartan subgroup is conjugate to the group of diagonal matrices, and hence is isomorphic to $\mathbb{F}_l^* \times \mathbb{F}_l^*$. Its normaliser is then conjugate to the group C_{s}^+ of diagonal and antidiagonal matrices. A nonsplit Cartan subgroup is isomorphic to $\mathbb{F}_{l^2}^*$, and is conjugate to the group C_{ns} defined as follows:

$$C_{\mathrm{ns}} = \left\{ \begin{pmatrix} x & \delta y \\ y & x \end{pmatrix} : x, y \in \mathbb{F}_l,\ (x, y) \neq (0, 0) \right\},$$

where δ is any fixed quadratic nonresidue in $\mathbb{F}_l^*$. It also has index two in its normaliser C_{ns}^+.

Associated to the groups C_{s}^+ and C_{ns}^+ are modular curves $X_{\mathrm{s}}(l)$ and $X_{\mathrm{ns}}(l)$ respectively; these serve as coarse moduli spaces for elliptic curves E whose mod-l Galois image $G_{E,l}$ is contained in (a conjugate of) C_{s}^+ and C_{ns}^+ respectively. Both curves are geometrically connected and defined over $\mathbb{Q}$. Over the complex numbers each curve has the description of being the quotient of the extended upper half-plane $\mathscr{H}^*$ by an appropriate congruence subgroup. The curve $X_{\mathrm{s}}(l)$ is $\mathbb{Q}$-isomorphic to the quotient $X_0^+(l^2)$ of the modular curve $X_0(l^2)$ by the Fricke involution. Over $\mathbb{C}$, this isomorphism is established by mapping τ on $X_0^+(l^2)$ to $l\tau$ on $X_{\mathrm{s}}(l)$.

One of Sutherland's insights was that the notion of Hasse at l curve E over K depends only on the projective mod-l image $H_{E,l}$. Given a subgroup H of $\mathrm{PGL}_2(\mathbb{F}_l)$, we say that H is *Hasse* if its natural action on $\mathbb{P}^1(\mathbb{F}_l)$ satisfies the following two properties:

- Every element $h \in H$ fixes a point in $\mathbb{P}^1(\mathbb{F}_l)$.
- There is no point in $\mathbb{P}^1(\mathbb{F}_l)$ fixed by the whole of H.

Proposition 2.2 (Sutherland). *An elliptic curve E/K is Hasse at l if and only if $H_{E,l}$ is Hasse.*

This allows us to reduce the study of exceptional pairs largely to group theory.

3. Proof of Theorem 1.5

Throughout this proof, $K = \mathbb{Q}(\sqrt{5})$.

Let E/K have $H_{E,5} \cong D_4$. It follows from Dickson's classification of subgroups of $\mathrm{GL}_2(\mathbb{F}_l)$ [1901] that $G_{E,5}$ is contained in the normaliser of a Cartan subgroup. If this Cartan subgroup were nonsplit, then $G_{E,5}$ would be contained in $C_{\mathrm{ns}}^+ \cap \mathrm{GL}_2^+(\mathbb{F}_5)$ (we take the intersection by Lemma 2.1), and so $H_{E,5}$ would be contained in

$(C_{\mathrm{ns}}^+ \cap \mathrm{GL}_2^+(\mathbb{F}_5))/\mathrm{scalars}$, which is a group of size 6, and hence cannot contain a subgroup isomorphic to D_4; thus $G_{E,5} \subseteq C_{\mathrm{s}}^+$, and so E/K corresponds to a K-point on $X_{\mathrm{s}}(5)$. The converse is not quite true; a K-point on $X_{\mathrm{s}}(5)$ corresponds to an elliptic curve E' over K with $H_{E',5} \subseteq D_4$, but not necessarily equal to D_4.

We now give an expression for the j-map $X_{\mathrm{s}}(5) \xrightarrow{j} X(1)$. Since $X_0^+(25)$ is isomorphic to $X_{\mathrm{s}}(5)$ under the map $\tau \mapsto 5\tau$, it suffices to write down the function $j(5\tau)$ in terms of a Hauptmodul s for $X_0^+(25)$.

Let t_N be a Hauptmodul for $X_0(N)$. Klein found the following formula in 1879:

$$j(5\tau) = \frac{(t_5^2 + 250t_5 + 3125)^3}{t_5^5}.$$

We can look up an expression for t_5 in terms of t_{25} from [Maier 2009]:

$$t_5 = t_{25}(t_{25}^4 + 5t_{25}^3 + 15t_{25}^2 + 25t_{25} + 25).$$

We also know that the Fricke involution w_{25} maps t_{25} to $5/t_{25}$. Hence a Hauptmodul for $X_0^+(25)$ is $s := t_{25} + 5/t_{25}$. It follows that

$$j(5\tau) = \frac{((s+5)(s^2-5)(s^2+5s+10))^3}{(s^2+5s+5)^5}.$$

Inserting a K-value for s in this expression yields the j-invariant of an elliptic curve E over K with $H_{E,5} \subseteq D_4$. The condition on $s^2 - 20$ in the statement of the theorem ensures that we have equality here, by ensuring that the image is not contained in any one of the three subgroups of order 2 in D_4, as we now demonstrate.

Let E be a curve in $X_{\mathrm{s}}(5)(K)$ corresponding to a choice of s in K, so that $H_{E,5} \subseteq D_4$. The following statements are readily seen to be equivalent to $H_{E,5} \neq D_4$:

- $H_{E,5}$ is cyclic.
- $G_{E,5}$ is contained in (a conjugate of) $C_{\mathrm{s}}(\mathbb{F}_5)$.
- E has a pair of independent K-rational 5-isogenies.
- E pulls back to a K-point on $X_0(25)$.
- $t_{25} \in K$.

Since t_{25} is a root of the polynomial $x^2 - sx + 5$ of discriminant $s^2 - 20$, we have $t_{25} \in K$ if and only if $s^2 - 20$ is a square in K. Thus the statement that $s^2 - 20$ is not a square in K is equivalent to $H_{E,5}$ not being cyclic, and hence $H_{E,5} \cong D_4$.

We have, however, overlooked an issue above. For a given $j = j(E) \in K$ satisfying (1-1), there are two other values of $s \in K$ also satisfying (1-1). This is because the field extension $K(s)/K(j)$, which has degree 15 and is not Galois, has

automorphism group of order 3, generated by $s \mapsto ((\sqrt{5}-5)s-20)/(2s+5+\sqrt{5})$. We must ensure that for none of the Galois conjugate values is s^2-20 square in K, so that $H_{E,5}$ is not contained in any of the three cyclic subgroups of D_4. This explains the final condition in the statement of the theorem.

Example 3.1. To illustrate this theorem, we input $s = 3\sqrt{5}+1$ to obtain

$$j = \frac{337876318862280\sqrt{5}+741305345279328}{41615795893};$$

we check that s^2-20 is not a square for the other two values of $s \in K$, namely $(\sqrt{5}-15)/7$ and $(-22\sqrt{5}-30)/19$, and hence any elliptic curve over $\mathbb{Q}(\sqrt{5})$ with this j has $H_{E,5} \cong D_4$. Equivalently, the pair $(5, j)$ is exceptional for $\mathbb{Q}(\sqrt{5})$.

However, if we input $s = (3\sqrt{5}-80)/41$, we get

$$j = \frac{277374956280053760\sqrt{5}+622630488102469632}{18658757027251},$$

and whilst $(3\sqrt{5}-80)/41$ does satisfy s^2-20 not being a square, this is not the case for $s = 3\sqrt{5}+2$, which yields the same j-value. One therefore has to be careful of these "pretenders", hence the last paragraph of the above proof.

We can even insert rational values of s, such as $s = 1$, to obtain elliptic curves over $\mathbb{Q}$ whose base-change to $\mathbb{Q}(\sqrt{5})$ are Hasse at 5, e.g.,

$$j = \frac{-56623104}{161051}.$$

4. Proof of Theorem 1.8: the model

Let G be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ for some N, and consider the modular curve $X_G(N)$ over $\mathbb{Q}$; let us assume $\det G = (\mathbb{Z}/N\mathbb{Z})^*$, so that this curve is geometrically connected. As a curve over $\mathbb{C}$, the curve depends only on the intersection of G with $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. Therefore, if $N = 13$, and G is the pullback to $\mathrm{GL}_2(\mathbb{F}_{13})$ of $S_4 \subset \mathrm{PGL}_2(\mathbb{F}_{13})$, then the modular curve $X_{S_4}(13) := X_G(13)$, when considered over $\mathbb{C}$, depends only on $G \cap \mathrm{SL}_2(\mathbb{F}_{13})$, which modulo scalar matrices becomes $A_4 \subset \mathrm{PSL}_2(\mathbb{F}_{13})$, and has the description $\Gamma_{A_4}(13)\backslash\mathcal{H}^*$, where $\Gamma_{A_4}(13)$ is the pullback of $A_4 \subset \mathrm{PSL}_2(\mathbb{F}_{13})$ to $\mathrm{PSL}_2(\mathbb{Z})$, and $\mathcal{H}^*$ is the extended upper half-plane.

Steven Galbraith [1996, Chapter 3] has described a method to compute the canonical model of any modular curve $X(\Gamma)$, provided one can compute explicitly and to some precision the q-expansions of a basis of $S_2(\Gamma)$, the weight-2 cuspforms of level Γ (a congruence subgroup). Hence, to compute the desired equation, we are reduced to computing explicitly a basis of the finite-dimensional $\mathbb{C}$-vector space $S_2(\Gamma_{A_4}(13))$. A standard application of the Riemann–Hurwitz genus formula gives

that the genus of the desired curve is 3; this is also the dimension of $S_2(\Gamma_{A_4}(13))$. We will proceed with the exposition in a series of steps.

Step 1. *Identifying our desired space as the set of invariant vectors of a representation.* Since $\Gamma(13) \subset \Gamma_{A_4}(13)$, we obtain

$$S_2(\Gamma_{A_4}(13)) \subset S_2(\Gamma(13)),$$

a 3-dimensional subspace of a 50-dimensional space. On this latter 50-dimensional space there is a right action — the "weight 2 slash operator" — of $\mathrm{PSL}_2(\mathbb{Z})$ (since $\Gamma(13)$ is normal in $\mathrm{PSL}_2(\mathbb{Z})$) which, by definition of $S_2(\Gamma(13))$, factors through the quotient $\mathrm{PSL}_2(\mathbb{F}_{13})$, which we recall contains a unique (up to conjugacy) subgroup isomorphic to A_4. Our desired 3-dimensional space is then the subspace of $S_2(\Gamma(13))$ fixed by A_4:

$$S_2(\Gamma_{A_4}(13)) = S_2(\Gamma(13))^{A_4},$$

that is, the A_4-invariant subspace of the $\mathrm{PSL}_2(\mathbb{F}_{13})$-representation $S_2(\Gamma(13))$.

When we carry out the computation, we will work with an explicit subgroup of $\mathrm{PSL}_2(\mathbb{F}_{13})$ isomorphic to A_4, namely that generated by the two matrices

$$A = \begin{pmatrix} -5 & 0 \\ 0 & 5 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} -2 & -2 \\ -3 & 3 \end{pmatrix}.$$

A different choice of A_4 will yield an isomorphic space of cuspforms, which for our application (in computing an equation for $X_{S_4}(13)$) makes no difference. However, the present choice of A_4 is favourable for computational reasons, since it is normalised by the matrix $\left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$; the congruence subgroup is then said to be of *real type* (see [Cremona 1997, Section 2.1.3]).

Step 2. *The conjugate representation.* Given a congruence subgroup Γ of level 13, denote by $\widetilde{\Gamma}$ the conjugate subgroup of level 13^2:

$$\widetilde{\Gamma} := \begin{pmatrix} 13 & 0 \\ 0 & 1 \end{pmatrix}^{-1} \Gamma \begin{pmatrix} 13 & 0 \\ 0 & 1 \end{pmatrix} \supseteq \Gamma_0(13^2) \cap \Gamma_1(13).$$

In general, $\widetilde{\Gamma}$ has level 13^2; in particular we have

$$\widetilde{\Gamma(13)} = \Gamma_0(13^2) \cap \Gamma_1(13).$$

Then we have the important isomorphism

$$\begin{aligned} S_2(\Gamma) &\to S_2(\widetilde{\Gamma}), \\ f(z) &\mapsto f(13z), \end{aligned}$$

which on q-expansions takes $q := e^{2\pi iz}$ to q^{13}. The point is that we may work with $S_2(\widetilde{\Gamma})$ instead of $S_2(\Gamma)$ if we like, as we can easily pass between the two; the two spaces are only superficially different.

This is exactly our plan for $\Gamma(13) \subset \Gamma_{A_4}(13)$. We have $S_2(\widetilde{\Gamma_{A_4}(13)}) \subset S_2(\widetilde{\Gamma(13)})$. This latter space is also a representation of $\mathrm{PSL}_2(\mathbb{F}_{13})$; for $g \in \mathrm{PSL}_2(\mathbb{F}_{13})$, we let γ be a pullback to $\mathrm{PSL}_2(\mathbb{Z})$ of g, and define, for $F \in S_2(\widetilde{\Gamma(13)})$,

$$g \cdot F := F|_2\tilde{\gamma} := F|_2 \begin{pmatrix} 13 & 0 \\ 0 & 1 \end{pmatrix}^{-1} \gamma \begin{pmatrix} 13 & 0 \\ 0 & 1 \end{pmatrix}.$$

We then obtain

$$S_2(\widetilde{\Gamma_{A_4}(13)}) = S_2(\widetilde{\Gamma(13)})^{A_4}.$$

Working inside the conjugated space $S_2(\widetilde{\Gamma(13)})$ is better, since its alternative description as $S_2(\Gamma_0(169) \cap \Gamma_1(13))$ is more amenable to the explicit computations we wish to carry out using the computer algebra systems Sage and Magma.

Step 3. *The three relevant subrepresentations.* Inside $S_2(\Gamma_0(169) \cap \Gamma_1(13))$, we have $S_2(\Gamma_0^+(169))$, the subspace of w_{169}-invariants of $S_2(\Gamma_0(169))$. We can compute this space explicitly in Sage. Let $q := e^{2\pi iz}$, $\zeta_7 := e^{2\pi i/7}$, $\zeta_7^+ := \zeta_7 + \zeta_7^{-1}$, and σ a nontrivial Galois automorphism of the field $\mathbb{Q}(\zeta_7^+) = \mathbb{Q}(\zeta_7)^+$. Then an explicit Sage computation yields

$$S_2(\Gamma_0^+(169)) = \langle g, g^\sigma, g^{\sigma^2} \rangle,$$

where

$$g(z) = q - (\zeta_7^+ + 1)q^2 + (1 - \zeta_7^{+2})q^3 + (\zeta_7^{+2} + 2\zeta_7^+ - 1)q^4 + \cdots.$$

These three forms are Galois-conjugate newforms. We will denote by a_n the Fourier coefficients of g.

For each $r \in \mathbb{F}_{13}^*$, define the *isotypical component* g_r *of* g as

$$g_r := \sum_{j \equiv r \bmod 13} a_j q^j,$$

and consider the $\mathbb{C}$-span V_0 of these components. Similarly define V_1 and V_2 by replacing g with g^σ and g^{σ^2} respectively. We will show in the coming sections that each V_i is a 12-dimensional subrepresentation of $S_2(\widetilde{\Gamma(13)})$ which is irreducible as $\mathbb{Q}[\mathrm{PSL}_2(\mathbb{F}_{13})]$-module. We may focus on these three subrepresentations, because, as we compute later, each one contains a unique (up to scaling) A_4-invariant cuspform.

Since we already know that we are looking for three forms, we need not concern ourselves with the other irreducible components of $S_2(\widetilde{\Gamma(13)})$. In fact, the sum $V_0 \oplus V_1 \oplus V_2$, of dimension 36, is the subspace of $S_2(\Gamma_0(169) \cap \Gamma_1(13))$ spanned by the Galois conjugates of the newform g together with their twists by characters

of conductor 13. The complementary subspace of dimension 14 is spanned by oldforms from level 13 and their twists. Each of these two subspaces is the base-change of a vector space over $\mathbb{Q}$ which is irreducible as a $\mathbb{Q}[\mathrm{PSL}_2(\mathbb{F}_{13})]$-module, while the 36-dimensional piece splits as a $\mathbb{Q}(\zeta_7^+)[\mathrm{PSL}_2(\mathbb{F}_{13})]$-module into three irreducible 12-dimensional subspaces.

Although we discovered these facts computationally, there is an alternative representation-theoretic explanation of these spaces in [Baran 2013], whose Propositions 3.6 and 5.2 show that the spaces V_i are irreducible cuspidal representations of $\mathrm{PSL}_2(\mathbb{F}_{13})$.

Step 4. *Computing the action of* $\mathrm{PSL}_2(\mathbb{F}_{13})$ *on each subrepresentation.* $\mathrm{PSL}_2(\mathbb{F}_{13})$ is generated by the two matrices

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

However, since we have conjugated the congruence subgroup, the action we need to consider must also be conjugated by the matrix $\left(\begin{smallmatrix} 13 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Hence, $\mathrm{PSL}_2(\mathbb{F}_{13})$ acts on $S_2(\widetilde{\Gamma(13)})$ via the matrices $\widetilde{S}$ and $\widetilde{T}$:

$$\widetilde{S} = \frac{1}{13}\begin{pmatrix} 0 & -1 \\ 169 & 0 \end{pmatrix} \quad \text{and} \quad \widetilde{T} = \begin{pmatrix} 1 & 1/13 \\ 0 & 1 \end{pmatrix}.$$

Observe that the action of $\widetilde{S}$ is, up to a scaling that we may ignore, the same as the Fricke involution w_{169}.

Thus, to describe the action of $\mathrm{PSL}_2(\mathbb{F}_{13})$ on each V_i, we will express the action of $\widetilde{S}$ and $\widetilde{T}$ on each V_i, explicitly as 12×12 matrices.

Step 5. *Computing the action of* $\widetilde{S}$ *and* $\widetilde{T}$. We fix $i = 0$; the other two cases are completely analogous and can be obtained by Galois conjugation (see Lemma 4.4 below).

To compute the action of $\widetilde{T}$ on V_0, we use the definition directly:

$$\left(g|_2 \begin{pmatrix} 1 & 1/13 \\ 0 & 1 \end{pmatrix}\right)(z) = g\big(z + \tfrac{1}{13}\big).$$

Recall that a_i is the i-th coefficient of g. We then get

$$g\big(z + \tfrac{1}{13}\big) = \zeta_{13} q - (\zeta_7^+ + 1)\zeta_{13}^2 q^2 + \cdots,$$

which we can rearrange as

$$\zeta_{13}(a_1 q + a_{14} q^{14} + a_{27} q^{27} + \cdots) + \zeta_{13}^2 (a_2 q^2 + a_{15} q^{15} + \cdots) + \cdots.$$

Thus, in the isotypical basis for V_0, the action of $\widetilde{T}$ is given simply by the 12×12 diagonal matrix

$$\begin{pmatrix} \zeta & & & \\ & \zeta^2 & & \\ & & \ddots & \\ & & & \zeta^{12} \end{pmatrix},$$

where we write ζ for ζ_{13}. In particular, this shows that V_0 is indeed invariant under the action of $\widetilde{T}$.

Computing $\widetilde{S}$ directly on the isotypical basis is not so easy, so what we do is change to a basis upon which we can compute it. Instead of the isotypical basis, we take the *twist basis*

$$\langle g \otimes \chi^j : 0 \le j \le 11 \rangle,$$

where $\chi : 2 \mapsto \zeta_{12}$ is a fixed generator of the group of Dirichlet characters of conductor 13, and $g \otimes \chi$ denotes the usual twist of g by χ. Note that this twist basis consists entirely of newforms (see [Atkin and Li 1978]). Since twisting by χ preserves V_0 and the change of basis matrix is $(\chi^j(i))$ (for $0 \le j \le 11$ and $1 \le i \le 12$), which has nonzero determinant, we have shown the following:

Lemma 4.1. *Both the isotypical and twist bases are* $\mathbb{C}$*-bases for the* 12*-dimensional subspace* V_0 *of* $S_2(\widetilde{\Gamma(13)})$:

$$\langle g \otimes \chi^j : 0 \le j \le 11 \rangle = \langle g_j : 1 \le j \le 12 \rangle.$$

Recall that the action of $\widetilde{S}$ is the same as the Fricke involution w_{169}. It is known (see [loc. cit.]) that w_N acts on newforms F of level N as

$$F|_2 w_N = \lambda_N(F) \cdot \overline{F},$$

where $\overline{F}$ is the newform obtained from the Fourier expansion of F by complex conjugation, and $\lambda_N(F)$ is the Atkin–Lehner pseudoeigenvalue, an algebraic number of absolute value 1 [loc. cit., Theorem 1.1]. In our twist basis, we have

$$\overline{g \otimes \chi^j} = g \otimes \chi^{12-j},$$

so we only need to compute the pseudoeigenvalues associated to $g \otimes \chi^j$ for $0 \le j \le 6$; the others may be obtained from these by complex conjugation. Also, the pseudoeigenvalues for $j = 0$ and $j = 6$ are actually eigenvalues, and may be computed directly (for example in Sage); we find that the eigenvalue for $j = 0$ is $+1$, and for $j = 6$ is -1.

Step 6. *Computing the Atkin–Lehner pseudoeigenvalues.* In order to stay consistent with the notation of [Atkin and Li 1978], we relabel g to F, and we let $q = 13$. By $a(q)$ we mean the q-th Fourier coefficient of F, which we may check is 0. We may also check that F is not a twist of an oldform of $S_2(\widetilde{\Gamma(13)})$; thus, in the language of [loc. cit.], F is *13-primitive*. We let χ_0 be the trivial character modulo 13, so $\chi_0 = \chi^0$, and we write $\lambda(\chi)$ for the Atkin–Lehner pseudoeigenvalue of $F \otimes \chi$, for χ any character. We let $g(\chi)$ be the Gauss sum of the character χ, with the convention that $g(\chi_0) = -1$.

The main tool to compute $\lambda(\chi^j)$, for $0 \le j \le 11$, is this:

Theorem 4.2 (special case of Theorem 4.5 of [Atkin and Li 1978]). *With the above notation and assumptions, we have, for* $0 \le j \le 11$,

$$(-1)^j 12 g(\chi^{12-j})\lambda(\chi^j) = \sum_{k=0}^{11} g(\chi^k) g(\chi^{j+k}) \overline{\lambda(\chi^k)}.$$

This theorem gives us, for each $0 \le j \le 11$, a linear relation among the $\lambda(\chi^k)$. Although there are twelve $\lambda(\chi^k)$, we have in the previous paragraph computed two of them, leaving us with ten. But actually, we have $\lambda(\chi^j) = \overline{\lambda(\chi^{12-j})}$ for $0 \le j \le 5$, so we really only have five independent unknowns. However, our strategy is, at first, to consider that we indeed have ten unknowns (namely, $\lambda(\chi^j)$ for $1 \le j \le 5$ and $7 \le j \le 11$) and use the theorem to derive as many linear relations between these ten unknowns as we can.

Doing this yields six independent equations, whose coefficients lie in $\mathbb{Q}(\zeta_{156})$ (the field over which the Gauss sums are defined). One is, however, able to obtain two more independent equations, by applying Theorem 4.5 of Atkin and Li starting not with $F = g$ (as we did previously), but rather with $F = g \otimes \chi^6$. Thus we get:

Theorem 4.3 (another special case of Theorem 4.5 of [Atkin and Li 1978]). *For* $0 \le j \le 11$, *we have*

$$(-1)^{j+1} 12 g(\chi^{12-j})\lambda(\chi^{6+j}) = \sum_{k=0}^{11} g(\chi^k) g(\chi^{j+k}) \overline{\lambda(\chi^{6+k})}.$$

As previously stated, this yields two more independent equations, giving us a linear system of eight independent equations in ten unknowns.

Let $x = \lambda(\chi)$ and $y = \lambda(\chi^2)$. We obtain the following two linear equations in the unknowns $x, \bar{x}, y, \bar{y}$:

$$c_1\bar{y} + c_2 y + c_3 x + c_4 \bar{x} = c_5, \tag{4-1}$$

$$c_6 y + c_7 x + c_8 \bar{x} = c_9; \tag{4-2}$$

here the c_i are explicit elements of $\mathbb{Q}(\zeta_{156})$. We now use the relations $x\bar{x} = y\bar{y} = 1$. We use (4-2) to eliminate y and $\bar{y}$ from (4-1) to obtain a linear relation between

x and $\bar{x}$; now, using $x\bar{x} = 1$, we obtain a quadratic in x. This quadratic has no root in $\mathbb{Q}(\zeta_{156})$; we need to adjoin $\sqrt{-7}$, so in fact we work in the field $\mathbb{Q}(\zeta_{1092})$; this might seem excessive, but the coefficients of g are anyway in $\mathbb{Q}(\zeta_7)^+$. This quadratic in x tells us that x is one of two values, and x determines all other $\lambda(\chi^j)$.

In order to determine which of the two values x really is, we computed two competing $\widetilde{S}$ matrices, and took the one which satisfied the correct relations with $\widetilde{T}$ to be the generators of $\mathrm{PSL}_2(\mathbb{F}_{13})$, namely,

$$\widetilde{S}^2 = \widetilde{T}^{13} = (\widetilde{S}\widetilde{T})^3 = 1.$$

Step 7. *The cuspforms.* We now have matrices giving the action of $\widetilde{S}$ on the twist basis, and the action of $\widetilde{T}$ on the isotypical basis; a change of basis matrix applied to either of these gives the action of both matrices in terms of the same basis. Write $\rho(S)$ and $\rho(T)$ for the 12×12 matrices giving the action of $\widetilde{S}$ and $\widetilde{T}$ respectively with respect to the twist basis.

We now compute the A_4-invariant subspace of V_0. Recall that our generators of $A_4 \subset \mathrm{PSL}_2(\mathbb{F}_{13})$ are

$$A = \begin{pmatrix} -5 & 0 \\ 0 & 5 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} -2 & -2 \\ -3 & 3 \end{pmatrix}.$$

Writing each generator as a word in S and T,

$$A = T^5 S T^{-2} S T^2 S T^3 S T^{-5},$$
$$B = T^4 S T^3 S T^{-3} S,$$

the action of A_4 on $S_2(\widetilde{\Gamma(13)})$ is given by the same words in the matrices $\widetilde{S}, \widetilde{T}$:

$$\widetilde{A} = \widetilde{T}^5 \widetilde{S} \widetilde{T}^{-2} \widetilde{S} \widetilde{T}^2 \widetilde{S} \widetilde{T}^3 \widetilde{S} \widetilde{T}^{-5},$$
$$\widetilde{B} = \widetilde{T}^4 \widetilde{S} \widetilde{T}^3 \widetilde{S} \widetilde{T}^{-3} \widetilde{S}.$$

The action of $\widetilde{A}$ and $\widetilde{B}$ on our vector space V_0 is given by taking the same words as above, but in $\rho(S)$ and $\rho(T)$; we call the resulting matrices $\rho(A)$ and $\rho(B)$.

The intersection of the kernels of $\rho(A) - I$ and $\rho(B) - I$ is one-dimensional, spanned by a vector of the coefficients, in the twist basis, of an A_4-invariant cuspform in V_0. These coefficients lie in the degree-9 field $\mathbb{Q}(\zeta_7^+, \zeta_{13}^{++})$, where by $\mathbb{Q}(\zeta_{13}^{++})$ we denote the unique cubic subfield of $\mathbb{Q}(\zeta_{13})$. We call this A_4-invariant form f.

We do not have to repeat the calculation for V_1 and V_2, because of the following fact. Here we regard V_i as $\overline{\mathbb{Q}}[\mathrm{PSL}_2(\mathbb{F}_{13})]$-modules.

Lemma 4.4. *Let γ be an element of* $\mathrm{PSL}_2(\mathbb{F}_{13})$. *The following diagram commutes*:

$$\begin{array}{ccc} V_0 & \xrightarrow{\sigma} & V_1 \\ {\scriptstyle\gamma}\downarrow & & \downarrow{\scriptstyle\gamma} \\ V_0 & \xrightarrow{\sigma} & V_1 \end{array}$$

Proof. Each V_i admits a twist basis, corresponding to g^{σ^i} and its twists under powers of χ. Fixing this twist basis for each V_i, we find that the actions of $\widetilde{S}$ and $\widetilde{T}$ are exactly the same; this is because the coefficients in $\widetilde{S}$ and $\widetilde{T}$ we found for V_0 are invariant under the action of σ. □

The lemma allows us to conclude that for $i = 0, 1, 2$, the conjugate f^{σ^i} spans the A_4-invariant subspace of V_i, and hence that $\{f, f^\sigma, f^{\sigma^2}\}$ is a basis of $S_2(\widetilde{\Gamma_{A_4}(13)})$. Next we replace this basis with one defined over a smaller field, namely $\mathbb{Q}(\zeta_{13}^{++})$.

Write f as

$$f = F + \zeta_7^+ G + \zeta_7^{+2} H,$$

where F, G, H have coefficients in $\mathbb{Q}(\zeta_{13}^{++})$. The forms F, G, H form a basis for the same space, with coefficients in the smaller field:

Lemma 4.5. *The following two $\mathbb{C}$-spans are the same*:

$$\langle f, f^\sigma, f^{\sigma^2}\rangle = \langle F, G, H\rangle.$$

Proof. We have

$$\begin{pmatrix} f \\ f^\sigma \\ f^{\sigma^2} \end{pmatrix} = \begin{pmatrix} 1 & \zeta_7^+ & \zeta_7^{+2} \\ 1 & \sigma(\zeta_7^+) & \sigma(\zeta_7^{+2}) \\ 1 & \sigma^2(\zeta_7^+) & \sigma^2(\zeta_7^{+2}) \end{pmatrix} \begin{pmatrix} F \\ G \\ H \end{pmatrix},$$

where the matrix has nonzero determinant. □

As a final flourish, we apply the nonsingular transformation

$$\begin{pmatrix} 1 & 4 & 3 \\ -4 & -3 & 1 \\ 6 & -2 & 5 \end{pmatrix}$$

to obtain the following cuspforms (where again $\zeta = \zeta_{13}$), which are a basis for $S_2(\widetilde{\Gamma_{A_4}(13)})$:

$$\begin{aligned} f = {} & -q \\ & + (-\zeta^{11} - \zeta^{10} - \zeta^3 - \zeta^2) q^2 \\ & + (\zeta^{11} + \zeta^{10} - \zeta^9 - \zeta^7 - \zeta^6 - \zeta^4 + \zeta^3 + \zeta^2 - 2) q^3 + \cdots, \end{aligned}$$

$$\begin{aligned} g = {} & (-\zeta^{11}-\zeta^{10}-\zeta^9-\zeta^7-\zeta^6-\zeta^4-\zeta^3-\zeta^2-1)q \\ & + (-\zeta^{11}-\zeta^{10}-\zeta^9-\zeta^7-\zeta^6-\zeta^4-\zeta^3-\zeta^2-2)q^2 \\ & \qquad + (-\zeta^{11}-\zeta^{10}-\zeta^3-\zeta^2-1)q^3 + \cdots, \\ h = {} & (\zeta^{11}+\zeta^{10}+\zeta^3+\zeta^2+3)q \\ & + (-\zeta^{11}-\zeta^{10}-\zeta^9-\zeta^7-\zeta^6-\zeta^4-\zeta^3-\zeta^2-3)q^2 \\ & \qquad + q^3 + \cdots. \end{aligned}$$

The final transformation was chosen retrospectively, solely for cosmetic reasons; it moves three of the rational points on the curve to $[1:0:0]$, $[0:1:0]$, $[0:0:1]$.

Having obtained the q-expansions, we may proceed with the canonical embedding algorithm of Galbraith, to obtain the smooth quartic equation for the model $\mathscr{C}$ given in the introduction. In practice this simply amounts to finding a linear relation between the q-expansions of the fifteen monomials of degree 4 in f, g, h. Although these q-expansions have coefficients defined over a cubic field (and there is no basis with rational q-expansions), the relation we find has rational coefficients.

Remark 4.6. Burcu Baran [2013] uses a different method to compute the equation of the modular curve $X_{\mathrm{ns}}(13)$; her method would also work for the present curve $X_{S_4}(13)$; one would need an analogue of her Proposition 6.1 for the subgroup at hand, which can be proved using her formulae in §3.

Remark 4.7. We also implemented a variation of the approach detailed here, using a modular symbol space of level 169, dual to the spaces V_i above. This second approach saved us from having to find the pseudoeigenvalues, since the matrices of both S and T on modular symbols are easily computed. This variation is also easy to adapt to find models for the curves $X_{\mathrm{s}}(13)$ and $X_{\mathrm{ns}}(13)$. Full details (including the cases $X_{\mathrm{s}}(13)$ and $X_{\mathrm{ns}}(13)$) may be found in the annotated Sage code [Banwait and Cremona 2013] and Sage worksheet [Cremona 2014].

5. Proof of Theorem 1.8: the j-map

In this section we explicitly determine the j-map

$$X_{S_4}(13) \xrightarrow{j} X(1) \cong \mathbb{P}^1_{\mathbb{Q}}$$

as a rational function on $X_{S_4}(13)$. This is a function of degree 91, which we seek to express in the form

$$j(X,Y,Z) = \frac{n(X,Y,Z)}{d_0(X,Y,Z)},$$

where n and d_0 are polynomials of the same degree over $\mathbb{Q}$. We first find a suitable denominator $d_0(X,Y,Z)$. The poles of j are all of order 13 and are at the seven cusps of $X_{S_4}(13)$, so we will find these, as $\overline{\mathbb{Q}}$-rational points on $X_{S_4}(13)$. Then

we find a cubic d in $\mathbb{Q}[X, Y, Z]$ which passes through these seven points (there is no quadratic which does), and set $d_0 = d^{13}$. Having found d_0 we determine the numerator n using linear algebra on q-expansions.

Remark 5.1. It would also be possible, in principal, to follow [Baran 2013] by computing the zeros of j numerically to sufficient precision to be able to recognise them as algebraic points, as then we would have the full divisor of the function j from which j itself could be recovered using an explicit Riemann–Roch space computation. Our method has the advantage of not requiring any numerical approximations.

We first need to find which points on our model $\mathscr{C}$ for $X_{S_4}(13)$ are the seven cusps. It turns out that there are three which are defined and conjugate over the degree-3 subfield $\mathbb{Q}(\alpha)$ of $\mathbb{Q}(\zeta)$, where $\zeta = \zeta_{13}$ and $\alpha = \zeta + \zeta^5 + \zeta^8 + \zeta^{12}$, and the other four are defined and conjugate over the degree-4 subfield $\mathbb{Q}(\beta)$ of $\mathbb{Q}(\zeta)$, where $\beta = \zeta + \zeta^3 + \zeta^9$.

Proposition 5.2. *On the model $\mathscr{C}$ for $X_{S_4}(13)$, the seven cusps are given by the three Galois conjugates of*

$$[-3\alpha^2 - 7\alpha + 1 : 4\alpha^2 + 11\alpha - 3 : 5]$$

and the four conjugates of

$$[3\beta^3 + 6\beta^2 + 6\beta - 15 : \beta^3 + \beta^2 - 4\beta - 4 : 9],$$

where α and β have minimal polynomials x^3+x^2-4x+1 and $x^4+x^3+2x^2-4x+3$ respectively.

The degree-3 cusps are easy to obtain; the cusp corresponding to the point $i\infty$ on the extended upper half-plane $\mathscr{H}^*$ has coordinates given by the leading coefficients of the three basis cuspforms f, g, h; denoting by φ the map

$$\begin{aligned} \varphi : \Gamma_{A_4}(13)\backslash\mathscr{H}^* &\xrightarrow{\sim} X_{S_4}(13), \\ \Gamma_{A_4}(13)\cdot z &\longmapsto [f(z) : g(z) : h(z)], \end{aligned}$$

we see that $\varphi(i\infty) = [a_1(f) : a_1(g) : a_1(h)]$. Expressing these coordinates in terms of α gives the degree-3 cusp given in the proposition.

It is possible to determine in advance the Galois action on the cusps, as in the following lemma. However, note that in practice our method to compute the cusps algebraically, given below, does not require this knowledge.

Lemma 5.3. *The absolute Galois group of $\mathbb{Q}$ acts on the seven cusps with two orbits, of sizes* 3 *and* 4.

Proof. We know *a priori* that the cusps are all defined over $\mathbb{Q}(\zeta_{13})$. Theorem 1.3.1 in [Stevens 1982] explains how to compute the action of $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \cong (\mathbb{Z}/N\mathbb{Z})^*$ on the cusps of a modular curve X of level N, provided that the field of rational functions on X is generated by rational functions whose q-expansions have rational coefficients. This does not apply here, since the field of modular functions for $\Gamma_{A_4}(13)$ is not generated by functions with rational q-expansions, but rather by functions with q-expansions in the cubic field $\mathbb{Q}(\alpha)$. But following Stevens' method we can compute the action of the absolute Galois group of $\mathbb{Q}(\alpha)$, which acts through the cyclic subgroup of order 4 of $(\mathbb{Z}/13\mathbb{Z})^*$ fixing α. We find that it fixes three cusps (which we already know from above, as they are defined over $\mathbb{Q}(\alpha)$), and permutes the remaining four cyclically. It follows that the other four cusps are also permuted cyclically by the full Galois group, and hence have degree 4 as claimed. □

It remains to find the coordinates of one cusp of degree 4.

Let $c \in \Gamma_{A_4}(13)\backslash\mathbb{P}^1(\mathbb{Q})$ be any cusp. Then there exists $\gamma \in \mathrm{PSL}_2(\mathbb{Z})\backslash\Gamma_{A_4}(13)$ such that $\gamma(c) = \infty$, and hence,

$$\alpha(c) = [a_1(f|\gamma) : a_1(g|\gamma) : a_1(h|\gamma)].$$

Since we already computed in the previous section the action of $\mathrm{PSL}_2(\mathbb{Z})$ on the cuspforms f, g, h, we can compute the right-hand side of this equation for any γ. With some work one can show that the cubic cusps are obtained using $c = \infty, 1$ and $7/6$, while the quartic cusps are obtained from $c = 2, 3, 6$ and 9; or we can simply choose random $\gamma \in \mathrm{PSL}_2(\mathbb{Z})$ until we find a point which is not one of the three conjugates we already have. This proves Proposition 5.2.

Next we find a cubic curve passing through these seven points.

Proposition 5.4. *The following cubic passes through the seven cusps*:

$$5X^3-19X^2Y-6XY^2+9Y^3+X^2Z-23XYZ-16Y^2Z+8XZ^2-22YZ^2+3Z^3.$$

Proof. The full linear system of degree 3 associated to $\mathcal{O}_{\mathbb{P}^2}(1)$ has dimension 10, and the subsystem passing though the seven cusps has dimension 3 with a basis in $\mathbb{Q}[X, Y, Z]$. Using LLL-reduction we found a short element which does not pass through any rational points on $\mathcal{C}$ (to simplify the evaluation of the j-map at these points later). □

Since all cusps have ramification degree 13 under the j-map, a possible choice for the denominator of the j-map is to take the thirteenth power $d_0 = d^{13}$ of this cubic.

Next we turn to the numerator $n(X, Y, Z)$, which is a polynomial of degree 39. The idea is to consider an arbitrary degree-39 polynomial in the q-expansions of the cusp forms f, g, h, and compare it with the known q-expansion of $j \cdot d(f, g, h)^{13}$. This gives a system of linear equations which can be solved.

The full linear system of degree 39 has dimension 820, but modulo the defining quartic polynomial for $\mathscr{C}$ we can reduce the number of monomials needing to be considered to only 154. We chose those monomials in which either X does not occur, or else Y does not occur and X has exponent 1 or 2, but this is arbitrary.

Now we consider the equation

$$n(X,Y,Z) - j(X,Y,Z)\cdot d(X,Y,Z)^{13} = 0$$

as a q-expansion identity after substituting f, g, h for X, Y, Z. Using 250 terms in the q-expansions (giving a margin to safeguard against error) and comparing coefficients gives 250 equations for the unknown coefficients of $n(X,Y,Z)$. There is a unique solution, which has rational coefficients. Although we have apparently only shown that the equation holds modulo q^{250}, it must hold identically, since we know that there is exactly one solution.

The expression for $n(X,Y,Z)$ we obtain this way is too large to display here (it has 151 nonzero integral coefficients of between 46 and 75 digits), but can easily be used to evaluate the j-map at any given point on the curve $\mathscr{C}$. For the sake of completeness, however, we give here explicitly the zeros of the j-map from which (together with the poles) it may be recovered; the complete expression may be seen in [Cremona 2014].

The 91 zeros of j consist of 29 points with multiplicity 3 and four with multiplicity 1, all defined over the number field $M = \mathbb{Q}(\delta)$, where δ has minimal polynomial

$$x^8 - 9x^6 + 32x^4 - 9x^2 + 1,$$

which is Galois with group D_8. This field is the splitting field of the polynomial $P(t)$ defined in the next section, so is also the field of definition of the points in the fibre over $j = 0$ of the covering map $X_0(13) \to X(1)$. Some of the 33 zeros are defined over the quartic subfields $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\beta)$, where α and β have minimal polynomials $x^4 + 13x^2 - 39$ and $x^4 - 13x^2 + 52$ respectively. Their coordinates are as follows (together with all Galois conjugates): with multiplicity 1 we have

$$[3\beta^3 + 2\beta^2 - 15\beta - 14 : -3\beta^3 + 4\beta^2 + 29\beta - 22 : -3\beta^3 - 4\beta^2 + 25\beta + 46],$$

and with multiplicity 3 we have the rational point $[1:0:0]$, the degree-4 points

$$[2(-\alpha^2 + 5\alpha - 4) : -\alpha^3 - \alpha^2 + \alpha + 6 : \alpha^3 + 14\alpha - 35],$$
$$[\beta^3 - 2\beta^2 - 9\beta + 14 : 2(\beta^2 - \beta - 2) : 2(-\beta^3 - 2\beta^2 + 7\beta + 16)],$$
$$[4(\beta - 1) : \beta^3 - 7\beta - 10 : 2(\beta^3 + 2\beta^2 - 7\beta - 12)],$$

and the degree-8 points

$$[\delta^7+2\delta^6-8\delta^5-8\delta^4+36\delta^3+12\delta^2-5\delta-2 : 8(\delta^3+\delta^2) : \\ -\delta^7-2\delta^6+4\delta^5-28\delta^3-8\delta^2+5\delta+2]$$

and

$$[2(-\delta^6+4\delta^5-10\delta^3+4\delta-1) : -3\delta^7+2\delta^6+28\delta^5-32\delta^4-52\delta^3+16\delta^2+7\delta-2 : \\ \delta^7-2\delta^6-4\delta^5+4\delta^4+4\delta^3+8\delta^2-9\delta+2].$$

6. Proof of Corollary 1.9

Evaluating the j-map at the six points in $\mathscr{C}(\mathbb{Q}(\sqrt{13}))$ exhibited in the introduction yields the five j-invariants listed in the statement of Corollary 1.9, together with $j=0$, which is the image of $[1:0:0]$. We know that any elliptic curve E over $\mathbb{Q}(\sqrt{13})$ with one of these six j-invariants has $H_{E,13}\subseteq A_4$. Any elliptic curve with $j=0$ has complex multiplication, with mod-13 image contained in a split Cartan subgroup (split since $13\equiv 1 \pmod 3$). Hence what remains to prove in this section is that $H_{E,13}\cong A_4$ for the five nonzero j-invariants listed.

Lemma 6.1. *Let l be a prime for which $X_0(l)$ has genus 0 (that is, $l=2,3,5,7,13$). There is an explicit polynomial $F_l(X,Y)\in\mathbb{Z}[X,Y]$ such that, if E/K is an elliptic curve over a number field, then*

$$H_{E,l}\cong \mathrm{Gal}\big(F_l(X,j(E))\big).$$

Proof. The function field of $X_0(l)$ is generated by a single modular function t (the so-called "Hauptmodul"), and classically there is a canonical choice of such, for each l. The j-function is a rational function of t of degree $l+1$ of the form $P(t)/t$, where P is an explicit integral polynomial of degree $l+1$.

Define $F_l(X,Y)=P(X)-YX\in\mathbb{Z}[X,Y]$. Let E/K be an elliptic curve over a number field, and consider the set of roots of $F_l(X,j(E))\in K[X]$ over $\overline{\mathbb{Q}}$. As a set, this is in bijection with the set of preimages t of $j(E)$ under the j-map $X_0(l)\to X(1)$ (which is unramified away from $j=0$ and $j=1728$), and hence is in Galois-equivariant bijection with the l-isogenies on E. Hence the Galois action on the set of $l+1$ isogenies is isomorphic to the Galois action on the roots of $F_l(X,j(E))$. □

For $l=13$, we have

$$P(t)=(t^2+5t+13)\cdot(t^4+7t^3+20t^2+19t+1)^3,$$

and hence

$$F_{13}(X,Y)=(X^2+5X+13)\cdot(X^4+7X^3+20X^2+19X+1)^3-XY.$$

For each j-invariant listed in Corollary 1.9 we may verify that $F_{13}(X, j)$ has Galois group isomorphic to A_4 over $\mathbb{Q}(\sqrt{13})$, and for the rational j-values, isomorphic to S_4 over $\mathbb{Q}$.

7. Proof of Proposition 1.3

By Proposition 2.2 and Lemma 2.1, Proposition 1.3 is equivalent to the following purely group-theoretic statement.

Proposition 7.1. *Let $H \subseteq \mathrm{PSL}_2(\mathbb{F}_l)$. Then H is Hasse if and only if one of the following holds*:

(1) $H \cong A_4$ *and* $l \equiv 1 \pmod{12}$.

(2) $H \cong S_4$ *and* $l \equiv 1 \pmod{24}$.

(3) $H \cong A_5$ *and* $l \equiv 1 \pmod{60}$.

(4) $H \cong D_{2n}$ *and* $l \equiv 1 \pmod 4$, *where* $n > 1$ *is a divisor of* $(l-1)/2$, *and the pullback of* H *to* $\mathrm{GL}_2(\mathbb{F}_l)$ *is contained in the normaliser of a split Cartan subgroup.*

We begin the forward implication of this Proposition by quoting the following lemma of Sutherland, which is a small piece of his Lemma 1.

Lemma 7.2 (Sutherland). *If $H \subseteq \mathrm{PSL}_2(\mathbb{F}_l)$ is Hasse, then $l \nmid |H|$.*

We may now invoke the following classical result (see [Lang 1976, Theorem XI.2.3]).

Fact 7.3. *Let H be a subgroup of $\mathrm{PGL}_2(\mathbb{F}_l)$ with $l \nmid |H|$, and let G denote its pullback to $\mathrm{GL}_2(\mathbb{F}_l)$. Then one of the following occurs*:

- *H is cyclic, and G is contained in a Cartan subgroup.*
- *H is dihedral, and G is contained in the normaliser of a Cartan subgroup.*
- *H is isomorphic to A_4, S_4 or A_5.*

Clearly H being cyclic is incompatible with H being Hasse, so either $H \cong D_{2n}$ for $n > 1$, or H is one of A_4, S_4 or A_5.

Lemma 7.4. *Let $H \subseteq \mathrm{PSL}_2(\mathbb{F}_l)$ be Hasse, and let $h \in H$. Then the order of h must divide $(l-1)/2$.*

Proof. Write $H' := \langle h \rangle$, a cyclic group of order r say, prime to l. By Fact 7.3, the pullback G' of H' to $\mathrm{GL}_2(\mathbb{F}_l)$ is contained in a Cartan subgroup. If this Cartan subgroup were nonsplit, then the elements of G' would *not* be diagonalisable, and hence h would not fix an element of $\mathbb{P}^1(\mathbb{F}_l)$, contradicting the Hasse assumption. Thus the Cartan subgroup must be split, so the elements of G' are diagonalisable,

and thus h has two fixed points; the same is true for every nonidentity element of H'. We now apply the orbit counting lemma to H':

$$s := |\mathbb{P}^1(\mathbb{F}_l)/H| = 2 + \frac{l-1}{r}. \tag{7-1}$$

Note that this formula says that there are $(l-1)/r$ nontrivial orbits of $\mathbb{P}^1(\mathbb{F}_l)$ under h (a trivial orbit being a fixed point). The sizes of these $(l-1)/r$ nontrivial orbits all divide r and sum to $l-1$, and hence they are all equal to r.

We claim that s must be even. This is clear if r is odd, by (7-1). If r is even, then

$$\operatorname{sign}(h) = (-1)^{s-2} = (-1)^s,$$

where sign means the sign as a permutation. The key observation, which proves the claim, is that $\operatorname{sign}(h)$ must be 1, because it coincides with $\det h$.

As s must be even, we look finally at (7-1) to conclude that r must divide $l-1$ with even quotient, and the lemma is proved. □

A part of the previous proof is worth framing, for it explains why the pullback of the dihedral group D_{2n} is contained in the normaliser of a *split* Cartan subgroup.

Lemma 7.5. *Let $H \subseteq \mathrm{PSL}_2(\mathbb{F}_l)$ be Hasse, and let $h \in H$. Let $H' := \langle h \rangle$, and let G' be the pullback of H' to $\mathrm{GL}_2(\mathbb{F}_l)$. Then G' is contained in a split Cartan subgroup.*

Lemma 7.4 implies that the n in D_{2n} divides $(l-1)/2$, and also the congruence restrictions for A_4, S_4 and A_5; indeed, since A_4 contains elements of order 1, 2 and 3, we must have that 2 and 3 divide $(l-1)/2$, or equivalently, $l \equiv 1 \pmod{12}$; the same argument works for S_4 and A_5. This proves the forward implication of the group-theoretic proposition above.

We now prove the converse; that is, if H is isomorphic to one of the four subgroups listed above, then it satisfies the Hasse condition.

The easier thing to prove is that every element h in H fixes a point of $\mathbb{P}^1(\mathbb{F}_l)$, so we address this first. Suppose, for a contradiction, that we have $h \in H$ which fixes no point of $\mathbb{P}^1(\mathbb{F}_l)$, let r be the order of this h, and let $s := |\mathbb{P}^1(\mathbb{F}_l)/h|$ be the number of orbits. Proposition 2 of [Sutherland 2012] says that $\operatorname{sign}(h) = (-1)^s$; in particular, s must be even. Applying the orbit counting lemma to the action of $\langle h \rangle$ on $\mathbb{P}^1(\mathbb{F}_l)$ yields the formula $s = (l+1)/r$, and hence r must divide $(l+1)/2$. We now do a case-by-case elimination. Suppose first that $H \cong D_{2n}$ with all the other conditions expressed above. The order of any element of this group must divide $(l-1)/2$. Since $(l-1)/2$ and $(l+1)/2$ are coprime, we obtain the desired contradiction. The argument in the other cases is similar.

We are left with proving that, in the four cases, no point of $\mathbb{P}^1(\mathbb{F}_l)$ is fixed by the whole of H. This follows from the following well-known fact from group theory; see for example Theorem 80.27 in [Curtis and Reiner 1987].

Lemma 7.6. *Let G be a group, S a transitive left G-set, and H a subgroup of G. Denote by $H\backslash S$ the set of orbits of S under H. Let B denote the G-stabiliser of any point of S. Then we have an isomorphism of H-sets*

$$S \cong \bigsqcup_g H/(H \cap B^g),$$

where g runs over a set of double coset representatives for $H\backslash G/B$; here we regard the S on the left as an H-set.

This allows us to prove that, in the four cases, there is no point of $\mathbb{P}^1(\mathbb{F}_l)$ fixed by all of H. We apply the lemma with $G = \mathrm{PSL}_2(\mathbb{F}_l)$, $S = \mathbb{P}^1(\mathbb{F}_l)$, and B the stabiliser of ∞, that is, the Borel subgroup. By the lemma, an orbit of size 1 corresponds to a double coset representative g for which $H \subseteq B^g$. But this inclusion is impossible, since each H contains D_4 and B does not. This finishes the proof.

8. Proof of Proposition 1.6

Let $E/\mathbb{Q}(\sqrt{l})$ be a nondihedral Hasse at l curve. Then $l \equiv 1 \pmod{12}$, $\pmod{24}$ or $\pmod{60}$, according as the projective image of $\bar{\rho}_{E,l}$ is A_4, S_4 or A_5, by Proposition 7.1. However, there is the following general result of David regarding the projective mod-p image, which we are grateful to Nicolas Billerey for bringing to our attention. For F a number field, and p a prime, let

$$e_p := \max_{\mathfrak{p}}\{e_{\mathfrak{p}}\},$$

where $e_{\mathfrak{p}}$ denotes the ramification index of the prime $\mathfrak{p} \mid p$.

Fact 8.1 [David 2011, Lemme 2.4]. *For an elliptic curve defined over a number field F, the projective mod-p image contains an element of order at least $(p-1)/(4e_p)$.*

Applying this with $F = \mathbb{Q}(\sqrt{l})$ and $p = l$, we see that:

- A_4 can occur only when $l \leq 25$ and $l \equiv 1 \pmod{12}$, so only for $l = 13$.
- S_4 can occur only when $l \leq 33$ and $l \equiv 1 \pmod{24}$, so cannot occur.
- A_5 can occur only when $l \leq 41$ and $l \equiv 1 \pmod{60}$, so cannot occur.

Thus only A_4 is possible, for the prime $l = 13$.

9. The Jacobian of $X_{S_4}(13)$

Over the complex numbers, there are precisely three modular curves of level 13 and genus 3; they are $X_{\mathrm{s}}(13)$, $X_{\mathrm{ns}}(13)$, and $X_{S_4}(13)$; see for example the table of

[Cummins and Pauli 2003]. Observe that all of these curves are defined over $\mathbb{Q}$ and are geometrically connected.

Baran [2013; 2012] proved in two different ways that the curves $X_{\mathrm{s}}(13)$ and $X_{\mathrm{ns}}(13)$ are in fact $\mathbb{Q}$-isomorphic. Her first proof [2013] was computational; she computed models of both curves and showed that they give isomorphic curves. Her second proof was more conceptual, establishing that the Jacobians $J_{\mathrm{s}}(13)$ and $J_{\mathrm{ns}}(13)$ are isomorphic, with an isomorphism preserving the canonical polarisation of both Jacobians; the Torelli theorem then gives the result.

The $\mathbb{Q}$-points on $X_{\mathrm{s}}(13)$ have not yet been determined; in fact, as discussed in the final section of [Bilu et al. 2013], $p = 13$ is the *only* prime p for which the $\mathbb{Q}$-points on $X_{\mathrm{s}}(p)$ have *not* yet been determined, and Baran's result, linking $X_{\mathrm{s}}(13)$ and $X_{\mathrm{ns}}(13)$, may give some reason for why this $p = 13$ case is so difficult: the determination of $\mathbb{Q}$-points on $X_{\mathrm{ns}}(p)$ is known to be a difficult problem.

Another reason for this difficulty is that $J_{\mathrm{s}}(13)(\mathbb{Q})$ is likely to have Mordell–Weil rank 3, which equals the genus, so the method of Chabauty to determine the rational points does not apply. By likely, we mean that the analytic rank of this Jacobian is 3, so under the Birch–Swinnerton-Dyer conjecture, we would have that the Mordell–Weil rank is also 3.

The curves $X_{\mathrm{s}}(13)$ and $X_{S_4}(13)$ are *not* isomorphic, even over $\mathbb{C}$; this may be verified using the explicit models of both curves, by computing certain invariants of genus-3 curves and observing that they are different — we are grateful to Jeroen Sijsling for carrying out this computation.

Nevertheless, their Jacobians are isogenous:

Proposition 9.1. *The Jacobians $J_{\mathrm{s}}(13)$ and $J_{S_4}(13)$ of the modular curves $X_{\mathrm{s}}(13)$ and $X_{S_4}(13)$ are $\mathbb{Q}$-isogenous.*

Proof. Let $G = \mathrm{GL}_2(\mathbb{F}_{13})$, B the Borel subgroup of G, and for K any subgroup of $\mathrm{PGL}_2(\mathbb{F}_{13})$, denote by $\pi^{-1}(K)$ the pullback of K to G. One first verifies (for example in Magma) that there is a $\mathbb{Q}[G]$-module isomorphism as follows:

$$2\mathbb{Q}[G/C_{\mathrm{s}}^{+}] \oplus \mathbb{Q}[G/\pi^{-1}(C_{13} \ltimes C_3)] \oplus \mathbb{Q}[G/\pi^{-1}(C_{13} \ltimes C_4)] \cong 2\mathbb{Q}[G/\pi^{-1}(S_4)] \oplus \mathbb{Q}[G/\pi^{-1}(D_{26})] \oplus \mathbb{Q}[G/B]. \quad (9\text{-}1)$$

For R any $\mathbb{Q}$-algebra, apply the contravariant functor $\mathrm{Hom}_{\mathbb{Q}[G]}(-, J(13)(R))$ to this formula; this yields, by a well-known method of Kani and Rosen ([1989], but see also [de Smit and Edixhoven 2000]), the following $\mathbb{Q}$-isogeny between Jacobians of modular curves of level 13:

$$J_{S_4}^2 \oplus J_{\pi^{-1}(D_{26})} \oplus J_B \quad \longrightarrow \quad J_{\mathrm{s}}^2 \oplus J_{\pi^{-1}(C_{13} \ltimes C_3)} \oplus J_{\pi^{-1}(C_{13} \ltimes C_4)}; \quad (9\text{-}2)$$

here we have, for simplicity, denoted the Jacobian of the modular curve $X_H(13)$ simply as J_H.

However, as may be checked by computing genera of these curves, most of these terms are zero, leaving us with a $\mathbb{Q}$-isogeny $J_{S_4}^2 \to J_{\mathrm{s}}^2$. Restricting this isogeny to the first component yields an isogeny between J_{S_4} and its image in J_{s}^2. This image must have dimension 3, and since J_{s} is simple over $\mathbb{Q}$ (as shown in Section 2 of [Baran 2012]), the image is isogenous to J_{s}. □

Remark 9.2. One may still wonder whether J_{s} is isomorphic to J_{S_4} or not. They are indeed not isomorphic; for if they were, then the arguments in Section 3 of [Baran 2012] would apply, and we would conclude that the curves X_{s} and X_{S_4} were isomorphic, which we know is not true.

Remark 9.3. With additional work one may show that there is a $\mathbb{Q}$-isogeny between J_{s} and J_{S_4} of degree a power of 13, and furthermore that 13 must divide the degree of any isogeny.

10. The evidence for Conjecture 1.14

There can be no Hasse at 11 curve over $\mathbb{Q}(\sqrt{-11})$, because 11 is not congruent to 1 (mod 4) (see Proposition 1.3). Thus, we let K be any other quadratic field. Sutherland's result (Proposition 1.1) tells us that, if E/K is a Hasse at 11 curve over K, then it corresponds to a K-point on the modular curve $X_{\mathrm{s}}(11)$. A model for this curve, as well as an expression for the j-map $X_{\mathrm{s}}(11) \to X(1)$, may be computed along the lines of that for $X_{S_4}(13)$; we obtain a singular projective model

$$X_{\mathrm{s}}(11) : y^2 = 4X^6 - 4X^4 - 2X^3 + 2X^2 + \tfrac{3}{2}X + \tfrac{1}{4}.$$

We used Magma to search for K-points on this curve, for every quadratic field with absolute discriminant up to 10^7, and evaluated the j-map at these points, giving many potential j-invariants of Hasse at 11 curves over quadratic fields.

Given such a j-invariant $j_0 \in K$, we considered the polynomial $\Phi_{11}(X, j_0) \in K[X]$, that is, the classical modular polynomial at 11, evaluated at $Y = j_0$.

Proposition 10.1. *The pair* $(11, j_0)$ *is exceptional for* K *if and only if the polynomial* $\Phi_{11}(X, j_0) \in K[X]$

- *has no linear factor over* K, *and*
- *modulo every prime* $\mathfrak{p}$ *in a density-one set, it has a linear factor.*

Proof. This is a direct consequence of the fact, proved in [Igusa 1959], that, for an elliptic curve E over any field F, and an integer N with char $F \nmid N$, the existence of a cyclic F-rational N-isogeny on E is equivalent to $\Phi_N(X, j(E)) \in F[X]$ having a linear factor. □

We found that, for all of our potential j-invariants, $\Phi_{11}(X, j_0)$ had many reductions with no linear factor — too many to be of density zero. This suggested to us that Conjecture 1.14 should be true.

The results of [Serre 1972] imply the following.

Proposition 10.2. *Let K be a quadratic field. If E/K is Hasse at* 11, *then either* 11 *ramifies in K, or E has additive reduction at all places v of K dividing* 11.

Proof. If 11 is unramified in K and E has a place v of good or multiplicative reduction above 11, then the results of [Serre 1972] (see in particular Section 4) give the image of the inertia subgroup at v of G_K under $\bar{\rho}_{E,11}$, which in all cases is incompatible with the projective image being isomorphic with D_{10}. □

We can also say, by part (a) of Proposition 1.1, that E/K is Hasse at 11 if and only if $H_{E,11} \cong D_{10}$, and so corresponds to a K-point on the modular curve $X_{D_{10}}(11)$ parametrising such elliptic curves. This modular curve is the $\mathbb{Q}(\sqrt{-11})$-twist of the more usual modular curve $X_0(121)$, which, by Theorem 4.9 of [Bars 2012], has only finitely many quadratic points. Thus, we can say that there are only finitely many quadratic fields over which a Hasse at 11 curve might exist. If we could determine exactly which quadratic fields K arise for the twist $X_{D_{10}}(11)$ of $X_0(121)$, we could prove the conjecture by determining the K-points on $X_{\mathrm{s}}(11)$, find the finite list of potential j-invariants, and show that none of them yield $H_{E,5} \cong D_{10}$ (this last step can be established by recent work of Sutherland, who has implemented an algorithm to determine the mod-p Galois image of any elliptic curve over any number field). The methods of Freitas, Le Hung and Siksek [Freitas et al. 2013] for determining the quadratic points on $X_0(N)$ for certain N may be of use here.

Acknowledgements

We are grateful to Jeroen Sijsling for helping us with the computation of the j-function in Theorem 1.8, as well as verifying that the genus-3 curves in Section 9 are not isomorphic. We would like to thank Damiano Testa for making interesting observations and suggestions regarding the curve $X_{S_4}(13)$ and its rational and quadratic points, Tim and Vladimir Dokchitser for their comments and suggestions regarding Theorem 1.5, Alex Bartel for finding the isomorphism (9-1), Martin Orr for communicating to us results about subvarieties of products of abelian varieties, and Andrew Sutherland for verifying the mod-13 Galois images of the elliptic curves in Corollary 1.9. Finally, we thank the anonymous referees for their careful reading and comments, and for verifying our results.

All computations in this paper were carried out using either Sage (see [Sage 2013]) or Magma (see [Bosma et al. 1997]), or both. Annotated Sage code which reproduces the computations in this paper concerning $X_{S_4}(13)$, together with similar computations for $X_{\mathrm{s}}(13)$ and $X_{\mathrm{ns}}(13)$, is available (see [Banwait and Cremona 2013]), as well as a Sage worksheet with the complete computation (see [Cremona 2014]).

References

[Anni 2014] S. Anni, "A local-to-global principle for isogenies of prime degree over number fields", *J. London Math. Soc.* **89**:3 (2014), 745–761.

[Atkin and Li 1978] A. O. L. Atkin and W. C. W. Li, "Twists of newforms and pseudo-eigenvalues of W-operators", *Invent. Math.* **48**:3 (1978), 221–243. MR 80a:10040 Zbl 0369.10016

[Banwait and Cremona 2013] B. Banwait and J. Cremona, "Computing the modular curves $X_{sp}(13)$, $X_{ns}(13)$ and $X_{A_4}(13)$ using modular symbols in Sage (annotated Sage code)", preprint, 2013, http://arxiv.org/src/1306.6818v3/anc/X13.pdf.

[Baran 2012] B. Baran, "An exceptional isomorphism between modular curves of level 13 via Torelli's theorem", preprint, 2012, http://www-personal.umich.edu/~bubaran/torelli.pdf.

[Baran 2013] B. Baran, "An exceptional isomorphism between modular curves of level 13", preprint, 2013, http://www-personal.umich.edu/~bubaran/bbaran.pdf.

[Bars 2012] F. Bars, "On quadratic points of classical modular curves", preprint, 2012, http://mat.uab.es/~francesc/surveyMomose.pdf.

[Bilu et al. 2013] Y. Bilu, P. Parent, and M. Rebolledo, "Rational points on $X_0^+(p^r)$", *Ann. Inst. Fourier* (*Grenoble*) **63**:3 (2013), 957–984. MR 3137477 Zbl 06227477

[Bosma et al. 1997] W. Bosma, J. Cannon, and C. Playoust, "The Magma algebra system, I: The user language", *J. Symbolic Comput.* **24**:3-4 (1997), 235–265. MR 1484478 Zbl 0898.68039

[Cremona 1997] J. Cremona, *Algorithms for modular elliptic curves*, 2nd ed., Cambridge University Press, 1997. MR 99e:11068 Zbl 0872.14041

[Cremona 2014] J. Cremona, "*X13* (Sage worksheet)", 2014, http://homepages.warwick.ac.uk/staff/J.E.Cremona/ftp/X13.sws.

[Cummins and Pauli 2003] C. J. Cummins and S. Pauli, "Congruence subgroups of $\mathrm{PSL}(2,\mathbb{Z})$ of genus less than or equal to 24", *Experiment. Math.* **12**:2 (2003), 243–255. MR 2004i:11037 Zbl 1060.11021

[Curtis and Reiner 1987] C. W. Curtis and I. Reiner, *Methods of representation theory, II: With applications to finite groups and orders*, Wiley, New York, 1987. MR 88f:20002 Zbl 0616.20001

[David 2011] A. David, "Borne uniforme pour les homothéties dans l'image de Galois associée aux courbes elliptiques", *J. Num. Theory* **131**:11 (2011), 2175–2191. MR 2012k:11075 Zbl 1246.11116

[Dickson 1901] L. E. Dickson, *Linear groups: With an exposition of the Galois field theory*, B. G. Teubner, Leipzig, 1901. JFM 32.0128.01

[Freitas et al. 2013] N. Freitas, B. V., L. Hung, and S. Siksek, "Elliptic curves over real quadratic fields are modular", preprint, 2013. arXiv 1310.7088

[Galbraith 1996] S. Galbraith, *Equations for modular curves*, Ph.D. thesis, University of Oxford, 1996, https://www.math.auckland.ac.nz/~sgal018/thesis.pdf.

[Igusa 1959] J.-i. Igusa, "Kroneckerian model of fields of elliptic modular functions", *Amer. J. Math.* **81** (1959), 561–577. MR 21 #7214 Zbl 0093.04502

[Kani and Rosen 1989] E. Kani and M. Rosen, "Idempotent relations and factors of Jacobians", *Math. Ann.* **284**:2 (1989), 307–327. MR 90h:14057 Zbl 0652.14011

[Lang 1976] S. Lang, *Introduction to modular forms*, Grundlehren Math. Wiss. **222**, Springer, New York, 1976. MR 55 #2751 Zbl 0344.10011

[Lang 2002] S. Lang, *Algebra*, 3rd ed., Graduate Texts in Mathematics **211**, Springer, New York, 2002. MR 2003e:00003 Zbl 0984.00001

[Ligozat 1977] G. Ligozat, "Courbes modulaires de niveau 11", pp. 149–237 in *Modular functions of one variable, V* (Bonn, 1976), edited by J. P. Serre and D. B. Zagier, Lecture Notes in Math. **601**, Springer, Berlin, 1977. MR 57 #3079 Zbl 0357.14006

[Maier 2009] R. S. Maier, "On rationally parametrized modular equations", *J. Ramanujan Math. Soc.* **24**:1 (2009), 1–73. MR 2010f:11060 Zbl 1214.11049

[Mazur 1977a] B. Mazur, "Modular curves and the Eisenstein ideal", *Inst. Hautes Études Sci. Publ. Math.* 47 (1977), 33–186. MR 80c:14015 Zbl 0394.14008

[Mazur 1977b] B. Mazur, "Rational points on modular curves", pp. 107–148 in *Modular functions of one variable, V* (Bonn, 1976), edited by J. P. Serre and D. B. Zagier, Lecture Notes in Math. **601**, Springer, Berlin, 1977. MR 56 #8579 Zbl 0357.14005

[Sage 2013] The Sage Development Team, Sage Mathematics Software (Version 5.10), 2013, http://www.sagemath.org.

[Serre 1972] J.-P. Serre, "Propriétés galoisiennes des points d'ordre fini des courbes elliptiques", *Invent. Math.* **15**:4 (1972), 259–331. MR 52 #8126 Zbl 0235.14012

[de Smit and Edixhoven 2000] B. de Smit and B. Edixhoven, "Sur un résultat d'Imin Chen", *Math. Res. Lett.* **7**:2-3 (2000), 147–153. MR 2001j:11043 Zbl 0968.14024

[Stevens 1982] G. Stevens, *Arithmetic on modular curves*, Progress in Mathematics **20**, Birkhäuser, Boston, 1982. MR 87b:11050 Zbl 0529.10028

[Sutherland 2012] A. V. Sutherland, "A local-global principle for rational isogenies of prime degree", *J. Théor. Nombres Bordeaux* **24**:2 (2012), 475–485. MR 2950703 Zbl 1276.11095

[Turner 2013] C. L. Turner, *Lattice methods for finding rational points on varieties over number fields*, Ph.D. thesis, University of Warwick, 2013, http://webcat.warwick.ac.uk/record=b2715884~S1.

Communicated by Joseph Silverman
Received 2013-09-03 Revised 2014-03-25 Accepted 2014-04-26

Barinder.Banwait@math.u-bordeaux1.fr
Institut de Mathématiques de Bordeaux, Université de Bordeaux I, 351 Cours de la Libération, 33405 Talence, France

J.E.Cremona@warwick.ac.uk *Mathematics Institute, University of Warwick, Zeeman Building, Coventry CV4 7AL, United Kingdom*

Algebra & Number Theory

msp.org/ant

See inside back cover or msp.org/ant for submission instructions.

The subscription price for 2014 is US $225/year for the electronic version, and $400/year (+$55, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscribers address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

ANT peer review and production are managed by EditFLOW® from Mathematical Sciences Publishers.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

Algebra & Number Theory

Volume 8 No. 5 2014

1937-0652(2014)8:5;1-6