Explicit points on the Legendre curve III

Douglas Ulmer

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 $\mathrm{III}(E/K_d)$ and a class number formula: $[E(K_d) : V_d]^2 = |\mathrm{III}(E/K_d)|$. In this paper, we compute $E(K_d)/V_d$ and $\mathrm{III}(E/K_d)$ explicitly as modules over $\mathbb{Z}_p[\mathrm{Gal}(K_d/\mathbb{F}_p(t))]$.

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 $\mathrm{III}(E/K_d)$ is finite and its order satisfies $|\mathrm{III}(E/K_d)| = [E(K_d) : V_d]^2$. 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 $\mathrm{III}(E/K_d)$ as modules over the group ring $\mathbb{Z}_p[\mathrm{Gal}(K_d/K)]$. 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 $G = \mathrm{Gal}(K_d/K)$. 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 $\mathrm{III}(E/K_d)$ be the Tate–Shafarevich group of E over K_d. Then $E(K_d)/V_d$ and $\mathrm{III}(E/K_d)$ 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 $f \leq 2$.

(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 $\leq x$.

(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 $f \leq 4$. 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 $\text{Ш}(E/K_d)$. In Section 3, we state the more precise results on $E(K_d)$ and $\text{Ш}(E/K_d)$ 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 $\text{Ш}(E/K_d)$. 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 $o = \{i, pi, p^2 i, \dots\}$.

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 $1 \le j \le |o|/2$.

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 $1 \le j \le |o|/2$.

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

$$s_j = \begin{cases} O & \text{if } w_j = w_{j+1}, \\ X & \text{if } w_j \ne w_{j+1}. \end{cases}$$

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 $d_1 \le d_2 \le \cdots \le d_k$ 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*

$$d_k = \max\{e_{ij} \mid 1 \leq i \leq j \leq 2k - 1, \ i \text{ and } j \text{ odd}\}.$$

Choose $i \leq j$ 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 $e_{ij} \geq e_{ij+2}, \ldots,$ $e_{ij} \geq e_{i,2k-1}$ 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 $d_k = e_{1k} = \text{ht}(o)$. 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 $\widetilde{O}$ 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*

$$\Gamma = \bigoplus_{o \in \widetilde{O}} \Gamma_o,$$

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*

$$(E(K_d) \otimes \mathbb{Z}_p)^o \cong \begin{cases} \Gamma_o & \text{if } \gcd(o, d) < d/2 \text{ and } p \text{ is balanced modulo } d/\gcd(o, d), \\ 0 & \text{otherwise.} \end{cases}$$

(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*

$$\mathrm{III}(E/\mathbb{F}_q(u))[p^{\infty}] \xrightarrow{\sim} \mathrm{Br}(\mathscr{S})[p^{\infty}]^{\Delta}.$$

Here Br($\mathscr{S}$) *is the* (*cohomological*) *Brauer group of* $\mathscr{S}$ *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 $\mathscr{S}$. To that end, recall the Weierstrass fibration $\mathscr{W} \to \mathbb{P}^1_u$ (whose fibers are the plane cubic reductions of E at places of $\mathbb{F}_q(u)$) and the Néron model $\mathscr{E} \to \mathbb{P}^1_u$, which is obtained from $\mathscr{W}$ 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, $\mathscr{E}$ has two points at infinity that we denote $P'_{\pm}$, where the sign corresponds to the limiting value of $x/z^{d/2}$. Similarly, $\mathscr{D}$ has two points at infinity, denoted $Q'_{\pm}$.

Let $\widetilde{\mathscr{S}} = \widetilde{\mathscr{C} \times \mathscr{D}}$ be the blow-up of $\mathscr{S}$ 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 $\widetilde{\mathscr{S}}$ and the exceptional fibers are fixed pointwise by the stabilizer of the corresponding point. The action of Δ on $\widetilde{\mathscr{S}}$ has other isolated fixed points, but we do not need to make them explicit.

We let $\widetilde{\mathscr{S}}/\Delta$ denote the quotient of $\widetilde{\mathscr{S}}$ 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 $\mathscr{S} \dashrightarrow \mathscr{W}$ 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 $\mathscr{W}$ as in [Ulmer 2014b, §7]. This induces a rational map $\phi \colon \widetilde{\mathscr{S}} \dashrightarrow \mathscr{W}$ that is obviously equivariant for the Δ action, where Δ acts trivially on $\mathscr{W}$. Thus, ϕ descends to a map on the quotient that we denote $\psi \colon \widetilde{\mathscr{S}}/\Delta \dashrightarrow \mathscr{W}$.

The following diagram shows the surfaces under consideration and various morphisms between them:

$$
\begin{array}{ccc}
\mathscr{C} \times \mathscr{D} = \mathscr{S} & \xleftarrow{\ \rho\ } & \widetilde{\mathscr{S}} \\
& & \Big\downarrow{\scriptstyle\phi} \\
\pi \Big\downarrow & & \searrow \\
\widetilde{\mathscr{S}}/\Delta & \dashrightarrow[\psi] & \mathscr{W} \xleftarrow{\ \sigma\ } \mathscr{E}
\end{array}
$$

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 $\widetilde{\mathcal{F}} \to \widetilde{\mathcal{F}}/\Delta$, 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 straight-forward but tedious exercise in coordinates that we omit. Since ϕ is a morphism, it follows that ψ is also a morphism. $\square$

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. ≥ 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 $\mathcal{G} = \mathcal{C} \times_{\mathbb{F}_q} \mathcal{D}$ "antidiagonally". Arguments parallel to those in the proof of Proposition 4.3.1 show that $\mathcal{X}$ is birationally isomorphic to $\mathcal{G}/\Delta$. Using this, the arguments proving Theorem 4.2 generalize readily to give isomorphisms

$$J(\mathbb{F}_q(u))[1/rd] \cong \text{NS}'(\mathcal{G})[1/rd]^\Delta$$

and

$$\text{III}(J/\mathbb{F}_q(u))[p^\infty] \cong \text{Br}(\mathcal{G})[p^\infty]^\Delta.$$

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

$$H^i(\mathcal{X}) := H^i_{\mathrm{crys}}(\mathcal{X}/W)$$

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 $H^1(\mathcal{X}, \mathbb{G}_m) \cong \mathrm{Pic}(\mathcal{X})$ and that we define the Brauer group of $\mathcal{X}$ by

$$\mathrm{Br}(\mathcal{X}) := H^2(\mathcal{X}, \mathbb{G}_m).$$

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 $\mathrm{NS}(\mathcal{C} \times_k \mathcal{D})$ of $P \times \mathcal{D}$ and $\mathcal{C} \times Q$ are independent of the choices of P and Q. We define $\mathrm{NS}'(\mathcal{C} \times_k \mathcal{D})$ as the orthogonal complement in $\mathrm{NS}(\mathcal{C} \times_k \mathcal{D})$ 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*

$$\mathrm{NS}'(\mathcal{C} \times_k \mathcal{D}) \otimes \mathbb{Z}_p \xrightarrow{\sim} (H^1(\mathcal{C}) \otimes_W H^1(\mathcal{D}))^{F=p}.$$

(2) *There is a functorial exact sequence*

$$0 \to ((H^1(\mathcal{C}) \otimes_W H^1(\mathcal{D}))^{F=p})/p^n \to (H^1(\mathcal{C})/p^n \otimes_W H^1(\mathcal{D})/p^n)^{F=V=p}$$
$$\to \mathrm{Br}(\mathcal{C} \times_k \mathcal{D})_{p^n} \to 0.$$

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 $\mathrm{Aut}(\mathcal{C}) \times \mathrm{Aut}(\mathcal{D})$.

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

$$\mathrm{NS}(\mathcal{X}) \otimes \mathbb{Z}_p \cong H^2(\mathcal{X})^{F=p}.$$

Decomposing $\mathrm{NS}(\mathcal{X})$ as $\mathbb{Z}^2 \oplus \mathrm{NS}'(\mathcal{X})$ and $H^2(\mathcal{X})$ via the Künneth formula leads to the statement in part (1).

For part (2), we may assume that $\mathscr{C}$ and $\mathscr{D}$ 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 $\mathscr{C}$ and $\mathscr{D}$ 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 $\mathscr{C}$ and $\mathscr{D}$ 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 $\mathscr{X}$. Taking flat cohomology yields

$$0 \to \mathrm{Pic}(\mathscr{X})/p^n \to H^2(\mathscr{X}, \mu_{p^n}) \to \mathrm{Br}(\mathscr{X})_{p^n} \to 0.$$

Let $T = \mathrm{Pic}(\mathscr{C})/p^n \oplus \mathrm{Pic}(\mathscr{D})/p^n$. The natural map $T \to \mathrm{Pic}(\mathscr{X})/p^n$ is an injection with cokernel $\mathrm{NS}'(\mathscr{X})/p^n$. Thus, we have a commutative diagram with exact rows and columns:

$$
\begin{array}{ccccccccc}
& & 0 & & 0 & & & & \\
& & \downarrow & & \downarrow & & & & \\
& & T & = & T & & & & \\
& & \downarrow & & \downarrow & & & & \\
0 & \to & \mathrm{Pic}(\mathscr{X})/p^n & \to & H^2(\mathscr{X}, \mu_{p^n}) & \to & \mathrm{Br}(\mathscr{X})_{p^n} & \to & 0 \\
& & \downarrow & & \downarrow & & \| & & \\
0 & \to & \mathrm{NS}'(\mathscr{X})/p^n & \to & H^2(\mathscr{X}, \mu_{p^n})/T & \to & \mathrm{Br}(\mathscr{X})_{p^n} & \to & 0 \\
& & \downarrow & & \downarrow & & & & \\
& & 0 & & 0 & & & &
\end{array}
$$

Using part (1), we have

$$\mathrm{NS}'(\mathscr{X})/p^n \cong ((H^1(\mathscr{C}) \otimes_{W(k)} H^1(\mathscr{D}))^{F=p})/p^n,$$

so to complete the proof, we must show that

$$H^2(\mathscr{X}, \mu_{p^n})/T \cong (H^1(\mathscr{C})/p^n \otimes H^1(\mathscr{D})/p^n)^{F=V=p}.$$

Let $\pi : \mathscr{C} \times \mathscr{D} \to \mathscr{D}$ be the projection on the second factor. We will compute $H^2(\mathscr{X}, \mu_{p^n})$ via the Leray spectral sequence for π. By a theorem of Artin proven

in [Grothendieck 1968b],

$$R^i \pi_* \mathbb{G}_m = \begin{cases} \mathbb{G}_m & \text{if } i = 0, \\ \underline{\mathrm{Pic}}_{\mathscr{X}/\mathscr{D}} = \underline{\mathrm{Pic}}_{\mathscr{C}/k} \times_k \mathscr{D} & \text{if } i = 1, \\ 0 & \text{if } i > 1. \end{cases}$$

It follows that

$$R^i \pi_* \mu_{p^n} = \begin{cases} \mu_{p^n} & \text{if } i = 0, \\ \underline{\mathrm{Pic}}_{\mathscr{X}/\mathscr{D}}[p^n] = J_{\mathscr{C}}[p^n] & \text{if } i = 1, \\ \underline{\mathrm{Pic}}_{\mathscr{X}/\mathscr{D}} / p^n = \mathbb{Z}/p^n\mathbb{Z} & \text{if } i = 2, \\ 0 & \text{if } i > 2. \end{cases}$$

(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

$$H^2(\mathscr{D}, \mu_{p^n}) \cong \mathrm{Pic}(\mathscr{D})/p^n,$$

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 $\mathrm{Spec}\, k$ represented by the finite flat group scheme $J_{\mathscr{C}}[p^n] = \mathrm{Pic}_{\mathscr{C}/k}[p^n]$. Let σ be the structure map $\mathscr{D} \to \mathrm{Spec}\, k$ (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

$$R^1 \sigma_* \sigma^* N \cong \underline{\mathrm{Hom}}_k(N', \underline{\mathrm{Pic}}_{\mathscr{D}/k}) \cong \underline{\mathrm{Hom}}_k(N, \underline{\mathrm{Pic}}_{\mathscr{D}/k}).$$

Here $\underline{\mathrm{Hom}}_k$ means the sheaf of homomorphisms of sheaves on the flat site of k, and we have used that $\mathrm{Pic}_{\mathscr{C}/k}[p^n]$ 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

$$0 \to H^1(k, N) \to H^1(\mathscr{D}, \sigma^* N) \to H^0(k, \underline{\mathrm{Hom}}_k(N, \underline{\mathrm{Pic}}_{\mathscr{D}/k})) \to 0.$$

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

$$f_{12}^i = \frac{x}{z^i} \in \mathcal{O}_{\mathscr{C}/\mathbb{Z}_p}(U_1 \cap U_2),$$

$$\omega_1^i = \left(1 - \frac{2i}{d}\right) \frac{dx}{z^i} \in \Omega_{\mathscr{C}/\mathbb{Z}_p}^1(U_1),$$

$$\omega_2^i = \frac{ix\, dz}{z^{i+1}} - \frac{2i}{d} \frac{dx}{z^i} \in \Omega_{\mathscr{C}/\mathbb{Z}_p}^1(U_2)$$

satisfies $df_{12}^i = \omega_1^i - \omega_2^i$ and so defines a class in $H_{\mathrm{dR}}^1(\mathscr{C}/\mathbb{Z}_p)$ 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 $H_{\mathrm{dR}}^1(\mathscr{C}/\mathbb{Z}_p)$ and have the following properties*:

(1) *The cup product $H_{\mathrm{dR}}^1(\mathscr{C}/\mathbb{Z}_p) \times H_{\mathrm{dR}}^1(\mathscr{C}/\mathbb{Z}_p) \to \mathbb{Z}_p$ 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 $1 \le i \le \lfloor (d-1)/2 \rfloor$ form a $\mathbb{Z}_p$-basis of the submodule $H^0(\mathscr{C}/\mathbb{Z}_p, \Omega_{\mathscr{C}/\mathbb{Z}_p}^1)$ of $H_{\mathrm{dR}}^1(\mathscr{C}/\mathbb{Z}_p)$, and the classes e_i with $\lfloor (d+1)/2 \rfloor \le i \le d - 1$ 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 $H_{\mathrm{crys}}^1(\mathscr{C}/W(\mathbb{F}_q)) \cong H_{\mathrm{dR}}^1(\mathscr{C}/\mathbb{Z}_p) \otimes_{\mathbb{Z}_p} W(\mathbb{F}_q)$ is given by*

$$[\zeta]e_i = \zeta^i e_i.$$

Also, $-1 \in \mu_2$ acts on $H_{\mathrm{crys}}^1(\mathscr{C}/W(\mathbb{F}_q))$ 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 $H_{\mathrm{dR}}^1(\mathscr{C}/\mathbb{F}_p)$ 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 $H_{\mathrm{dR}}^1(\mathscr{C}/\mathbb{Z}_p)$.

It is clear from the definition that the e_i with $0 < i < d/2$ are in the submodule $H^0(\mathscr{C}/\mathbb{Z}_p, \Omega^1_{\mathscr{C}/\mathbb{Z}_p})$, 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 $H^1(\mathscr{C}/\mathbb{Z}_p, \mathcal{O}_{\mathscr{C}/\mathbb{Z}_p})$. 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 $H^1(\mathscr{C}/W(k))$ 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 $H^1_{\mathrm{crys}}(\mathscr{C}/\mathbb{Z}_p)$. 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 $\pm p^{|o|/2}$. $\qquad\square$

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 $H^0(\mathscr{C}/\mathbb{Z}_p, \Omega^1_{\mathscr{C}/\mathbb{Z}_p})$, 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 $\mathscr{C}_r$ 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 $\mathscr{C}_r$ has an obvious lift to $\mathbb{Z}_p$ that we denote $\mathscr{C}_r/\mathbb{Z}_p$. This yields an identification $H^1_{\mathrm{crys}}(\mathscr{C}_r/\mathbb{Z}_p) \cong H^1_{\mathrm{dR}}(\mathscr{C}_r/\mathbb{Z}_p)$.

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 $H^1_{\mathrm{dR}}(\mathscr{C}_r/\mathbb{Z}_p)$ 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 $H^0(\mathscr{C}_r/\mathbb{Z}_p, \Omega^1_{\mathscr{C}_r/\mathbb{Z}_p})$, and the $e_{i,j}$ with $(i, j) \in B$ project to a basis of $H^1(\mathscr{C}_r/\mathbb{Z}_p, \mathcal{O}_{\mathscr{C}_r/\mathbb{Z}_p})$.

(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 $H^1_{\operatorname{crys}}(\mathscr{C}_r / \mathbb{Z}_p)$. 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 $\Sha(E/\mathbb{F}_q(u))$ 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 $H^1_{\text{crys}}(\mathscr{C}/W)$, and $H^1(\mathscr{D})$ for $H^1_{\text{crys}}(\mathscr{D}/W)$, 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 $G = \mu_d \rtimes \text{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ 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_n^o 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

$$f_{ip^j} = \left(\prod_{\ell=1}^{j} d_{p^i\ell}^2 \right) e_{ip^j} \otimes e_{ip^j}.$$

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_n^o 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_n^o):

$$c = \sum_{j=0}^{|o|-1} \alpha_j f_{ip^j},$$

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

$$(\sigma p)^{e_1} \beta_0 = (\sigma^{-1} p)^{e_2} \beta_1,$$
$$(\sigma p)^{e_3} \beta_1 = (\sigma^{-1} p)^{e_4} \beta_2,$$
$$\vdots$$
$$(\sigma p)^{e_{2k-1}} \beta_{k-1} = (\sigma^{-1} p)^{e_{2k}} \beta_k. \qquad (7.4.2)$$

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 $c \mapsto (\beta_j)_{j=1,\dots,k}$ 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

$$\beta_1 = \sigma^{e_1 + e_2} p^{e_{1,2}} \beta_0,$$
$$\beta_2 = \sigma^{e_3 + e_4} p^{e_3 - e_4} \beta_1 = \sigma^{e_1 + \cdots + e_4} p^{e_{1,4}} \beta_0,$$
$$\vdots$$
$$\beta_k = \sigma^{e_1 + \cdots + e_{2k}} p^{e_{1,2k}} \beta_0 = \sigma^{|o|} p^{e_{1,2k}} \beta_0 = \sigma^{|o|} \beta_0, \qquad (7.5.1)$$

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:

$$
\begin{array}{ccccccccc}
 & & 0 & & 0 & & & & \\
 & & \downarrow & & \downarrow & & & & \\
0 & \longrightarrow & \dfrac{p^{n-\mathrm{ht}(o)}\,H^o}{p^n\,H^o} & \longrightarrow & p^{n-\mathrm{ht}(o)}\,H^o_n & \longrightarrow & \mathrm{Br}^o[p^n] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \| & & \\
0 & \longrightarrow & \dfrac{H^o}{p^n\,H^o} & \longrightarrow & H^o_n & \longrightarrow & \mathrm{Br}^o[p^n] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & & & \\
 & & \dfrac{H^o}{p^{n-\mathrm{ht}(o)}\,H^o} & \overset{\cong}{\longrightarrow} & \dfrac{H^o_n}{p^{n-\mathrm{ht}(o)}\,H^0_n} & & & & \\
 & & \downarrow & & \downarrow & & & & \\
 & & 0 & & 0 & & & &
\end{array}
$$

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., $U^2(p^\infty) = U^2(p^{\mathrm{ht}(o)}) = p^{n-\mathrm{ht}(o)} H^o_n$ and $D^2(p^{n-\mathrm{ht}(o)}) = H^o_n / p^{n-\mathrm{ht}(o)} H^o_n$. 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

$$i_{f-1} < (p-1)/2,$$

$$\text{or} \quad i_{f-1} = (p-1)/2 \qquad \text{and} \quad i_{f-2} < (p-1)/2,$$

$$\text{or} \quad i_{f-1} = i_{f-2} = (p-1)/2 \quad \text{and} \quad i_{f-3} < (p-1)/2,$$

$$\vdots$$

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

$$(E(K_d) \otimes \mathbb{Z}_p)^o \cong (H^1(\mathcal{C}) \otimes_W H^1(\mathcal{D}))^{\Delta, o, F=p}.$$

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

$$M^o := (H^1(\mathcal{C}) \otimes_W H^1(\mathcal{D}))^{\Delta, o}.$$

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 $\mathrm{Ш}(E/\mathbb{F}_q(u))[p^n]^o$ 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 $u^f l^f$ 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 $u^3 l^3$ 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 $u^4 l^4$ and $u^2 l u l^2 u l$. 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

$$I = \sum_{o \in O_{d,p}} \mathrm{inv}(o).$$

Recall that a word is "good" if it associated to a good base point of an orbit. Let $|\mathrm{Aut}(w)|$ be the number of automorphisms of w, i.e., the number of rotations leaving w invariant. Then since $\mathrm{inv}(o)$ only depends on the word associated to o,

$$I = \sum_{\text{good } w} \frac{|\{i \mid \text{the orbit through } i \text{ is } w\}|}{|\mathrm{Aut}(w)|} \mathrm{inv}(w).$$

Now $\mathrm{inv}(w)/|\mathrm{Aut}(w)|$ 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

$$I = \sum_{\text{full length, good } w} \frac{\mathrm{inv}(w)}{|\mathrm{Aut}(w)|} |\{i \mid \text{the pattern of } i \text{ is } w\}|.$$

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 $\mathrm{inv}(u^3 l^3) = 0$, $\mathrm{inv}(ululul) = 12$, and $\mathrm{inv}(ul) = 4$. 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 $\mathrm{III}(E/K_d)$ 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 $\mathrm{III}(E/K_d)$ 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 $\text{Ш}(E/K_d)$ 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

$$0 \to E(K_d)/pE(K_d) \to \text{Sel}(K_d, p_E) \to \text{Ш}(E/K_d)[p] \to 0.$$

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) $\text{Ш}(E/K_d) = 0$ *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 $I_{d,p} \to \mathbb{P}_u^1$ 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 $\psi : \mathbb{F}_p^\times \to k^\times$ 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 $I_{d,p} \to \mathbb{P}_u^1$ (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

$$\frac{dt}{\alpha^{p-2}} = (f_0^p + t f_1^p + \cdots + t^{p-1} f_{p-1}^p) \, dt,$$

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

$$\langle f_{(p-3)/2}, \ldots, f_0 \rangle = \langle f_{(p-5)/2}, \ldots, f_0, t f_{p-1} \rangle = \cdots = \langle f_0, t f_{p-1}, \ldots, t f_{(p+3)/2} \rangle.$$

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 $\mathrm{III}(E/K) = 0$. Thus, $\mathrm{Sel}(K, p_E) = 0$.

On the other hand, as we noted above, $\mathrm{Sel}(K, p_E)$ is isomorphic to the kernel of the Cartier operator on

$$\left\{ \frac{f(t) \, dt}{\alpha^{p-2}} \; \middle| \; \deg(f) \leq (p-5)/2 \right\}.$$

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 $i \geq 0$. 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 $\mathscr{C}(g_0 dt/\alpha^{p-2}) = 0$ 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). $\square$

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,

$$R := \dim_{\mathbb{F}_q} \mathscr{C}\left(\left\{ \frac{f(u) \, du}{\alpha^{p-2}} \,\middle|\, \deg(f) \leq (p-2)(p^f+1)/2 - 2 \right\}\right).$$

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 $0 \leq i \leq p-1$ and

$$0 \leq j \leq \begin{cases} \frac{1}{2}(p-3)p^{f-1} + \frac{1}{2}(p^{f-1}-1) & \text{if } i \leq p-3, \\ \frac{1}{2}(p-3)p^{f-1} + \frac{1}{2}(p^{f-1}-3) & \text{if } i = p-2, p-1. \end{cases}$$

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 $\{t^j f_i \mid 0 \leq i \leq p-1, \ j \in \mathbb{Z}\}$, 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 $0 \leq i \leq (p-3)/2$ and $0 \leq j \leq (p^{f-1}-1)/2$ 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 $\mathrm{III}(E/K_d)$ 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

$$\bigoplus_{\substack{0 \leq i \leq (p-3)/2 \\ 0 \leq j \leq (p^{f-1}-1)/2}} \mathbb{F}_q u^{i+pj}.$$

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 $0 \leq i \leq (p-3)/2$ and $0 \leq j \leq (p^{f-1}-1)/2$. 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 $\text{III}(E/K_d)$ 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.) $\qquad\qquad\qquad\qquad\square$

We need one more result from [Ulmer 1991]. To state it, recall that the Selmer group for the isogeny $\text{Fr} : E \to E^{(p)}$ 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:

$$\text{Sel}(F_{p,d}, \text{Fr}_E) = \mathbb{F}_p \frac{dq}{q}.$$

Proof. The same argument as in [Ulmer 1991, Theorem 7.6] shows that the Selmer group $\text{Sel}(F_{p,d}, \text{Fr}_E)$ 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. $\qquad\qquad\qquad\qquad\square$

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*

$$\ker(p : E(K_d)/V_d \to E(K_d)/V_d)^o = \begin{cases} \Gamma_o/p & \textit{if the word of } o \textit{ is not } u^f l^f, \\ 0 & \textit{if the word of } o \textit{ is } u^f l^f. \end{cases}$$

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

$$E(K_d)/p \hookrightarrow \mathrm{Sel}(K_d, p_E), \tag{9.2.1}$$

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

$$(x(x+1)(x+t))^{(p-1)/2} = x^p M(x) + A x^{p-1} + \text{lower-order terms}$$

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 $0 \leq i \leq (p-3)/2$ and $0 \leq j \leq (p^{f-1}-1)/2$. 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 $u^f l^f$. $\qquad\square$

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 $\mathcal{C}'$ 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

$$(E'(K'_d)/\text{tor}) \otimes \mathbb{Z}[1/d] \xrightarrow{\sim} (\text{NS}'(\mathcal{C} \times \mathcal{C}) \otimes \mathbb{Z}[1/d])^{\mu_d},$$

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 $\mathcal{C}$ in Section 6 works for $\mathcal{C}'$ 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. $\geq$ 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 $\mathcal{X} \to \mathbb{P}^1_u$ of X/K_d is birational to the quotient of a product of curves by a finite group. The product is $\mathcal{S} = \mathcal{C} \times \mathcal{C}$, where $\mathcal{C}$ 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 $\mathcal{S}$ 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 $\mathcal{C}$ 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 $H^0(\mathcal{C}/\mathbb{Z}_p, \Omega^1_{\mathcal{C}/\mathbb{Z}_p})$ 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*

Algebra & Number Theory

msp.org/ant

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

Algebra & Number Theory