EXPLICIT POINTS ON THE LEGENDRE CURVE II

RICARDO P. CONCEIÇÃO, CHRIS HALL AND DOUGLAS ULMER

ABSTRACT. Let E be the elliptic curve $y^2 = x(x+1)(x+t)$ over the field $\mathbb{F}_p(t)$, where p is an odd prime. We study the arithmetic of E over extensions $\mathbb{F}_q(t^{1/d})$, where q is a power of p and d is an integer prime to p. The rank of E is given in terms of an elementary property of the subgroup of $(\mathbb{Z}/d\mathbb{Z})^\times$ generated by p. We show that for many values of d the rank is large. For example, if d divides $2(p^f - 1)$ and $2(p^f - 1)/d$ is odd, then the rank is at least $d/2$. When $d = 2(p^f - 1)$, we exhibit explicit points generating a subgroup of $E(\mathbb{F}_q(t^{1/d}))$ of finite index in the "2-new" part, and we bound the index as well as the order of the "2-new" part of the Tate–Shafarevich group.

1. Introduction

Fix an odd prime p and consider the elliptic curve

$$(1.1) \qquad E: \qquad y^2 = x(x+1)(x+t)$$

defined over the rational function field $\mathbb{F}_p(t)$. We call E the Legendre curve. In [9], the third author considered the arithmetic of E over extensions of the form $\mathbb{F}_q(t^{1/d})$, where q is a power of p and d is a positive integer prime to p, proving in particular that the Birch and Swinnerton–Dyer conjecture holds for E over each of these fields.

Most of [9] emphasizes the case when d divides $p^f + 1$ for some f. (These integers d can also be described as those such that -1 is in the cyclic subgroup of $(\mathbb{Z}/d\mathbb{Z})^\times$ generated by p.) The emphasis on this case is natural because the integers $p^f + 1$ are known to play a special role in arithmetic geometry in characteristic p. For example, the Jacobian of the Fermat curve of degree d is supersingular if and only if d divides $p^f + 1$ for some $f \geq 1$ [6].

One of our aims in this note is to point out that that there are many other values of d such that the curve E has interesting arithmetic (e.g., large Mordell–Weil rank) over $\mathbb{F}_q(t^{1/d})$. To that end, we calculate the Hasse–Weil L-function of E over the extensions $\mathbb{F}_q(t^{1/d})$ for all q and d, and we give a simple and explicit formula for the rank of $E(\mathbb{F}_q(t^{1/d}))$. Our formula for the rank is in terms of a new, elementary notion of "balanced subgroup of the multiplicative group."

Using the notion of balanced subgroup, we prove that if 4 divides d, $p^f \equiv d/2 + 1$ (mod d) for some f, and $q \equiv 1$ (mod d), then $\operatorname{ord}_{s=1} L(E/\mathbb{F}_q(t^{1/d}), s) \geq d/2$ and $E(\mathbb{F}_q(t^{1/d}))$ has rank at least $d/2$. These integers d can also be described as those dividing $2(p^f - 1)$ for some f with $2(p^f - 1)/d$ odd. Note that such integers $d > 4$ do not divide $p^g + 1$ for any value of g, so this is indeed a class of integers distinct from

those studied in [9]. In [4], it is shown that this class of integers is, in a precise sense, more numerous than the class of divisors of elements of $\{p^g + 1 | g \geq 1\}$.

The statement of our rank formula is in Section 2. In Section 3, we calculate the L-function of E over $\mathbb{F}_q(t^{1/d})$ for all d and all q in terms of Jacobi sums, and in Section 4, we make these Jacobi sums explicit for those values of d where the L-function has zeroes. This leads to the proof of the rank formula stated in Section 2.

In Section 5, we make several comments on the condition that p is balanced modulo d, and in Section 5.5, we prove the rank assertion made above for values d where some power of p is congruent to $d/2 + 1$ modulo d.

In Sections 6–9, we study the case $d = 2(p^f - 1)$ in more detail, exhibiting explicit points which generate a finite index subgroup of the "2-new" part of the Mordell–Weil group of E. We also obtain bounds on the "2-new" part of the Tate–Shafarevich group of E, showing in particular that it is a p-group.

In Section 10, we show how certain endomorphisms of curves "explain" the explicit points of [9] and this paper, in the style of [8]. Finally, in Section 11, we explain how many of the results of this paper can be extended to a context where $p = 2$ is relevant.

1.1. Notation. For the convenience of the reader, we gather here notation which is used in several parts of the paper.

- For a finite set S, we write $|S|$ for the cardinality of S.
- We assume that p is an odd prime number and q is a power of p. We write $\mathbb{F}_p$ and $\mathbb{F}_q$ for the fields of cardinality p and q, respectively. See Section 11 for a situation where $p = 2$ is relevant.
- Throughout, d will be an integer >2 and relatively prime to p. See [9, Remark 12.2] for the case when p divides d.
- Let K be the function field $\mathbb{F}_q(t^{1/d}) = \mathbb{F}_q(u)$, where $u^d = t$.
- Throughout, E will denote the elliptic curve over $\mathbb{F}_p(t)$ defined by equation (1.1). We write $L(E/K, T)$ and $L(E/K, s)$ for the Hasse–Weil L-function of E over the extension K of $\mathbb{F}_p(t)$. Here T and s are related by $T = q^{-s}$. We write $Ш(E/K)$ for the Tate–Shafarevich group of E over K.
- Let $G = (\mathbb{Z}/d\mathbb{Z})^\times$ and let A (resp. B) be the subset of G consisting of classes whose least positive residue lies in $(0, d/2)$ (resp. $(d/2, d)$).
- For an integer a prime to d, let $\langle a \rangle_d$ be the cyclic subgroup of G generated by a. We will only use this notation when $a = p$ or $a = q$. We write $\phi(d)$ for $|G|$ and $o_d(q)$ for $|\langle q \rangle_d|$, i.e., for the order of q modulo d. We will also write $\phi(e) = |(\mathbb{Z}/e\mathbb{Z})^\times|$ and $o_e(q) = |\langle q \rangle_e|$ for divisors e of d.
- We write $o \subset \mathbb{Z}/d\mathbb{Z}$ for an orbit of the action of $\langle p \rangle_d$ on $\mathbb{Z}/d\mathbb{Z}$. We always assume that $o \neq \{0\}$ and that $o \neq \{d/2\}$ when d is even.
- For an orbit $o \subset \mathbb{Z}/d\mathbb{Z}$ as above, we define a certain Jacobi sum J_o in Section 3.1.
- We write μ_e and ζ_e for the group of roots of unity of order e and a fixed primitive root of unity of order e, respectively. Depending on the context, these are to be taken in $\overline{\mathbb{Q}}$, the algebraic closure of $\mathbb{Q}$, or $\overline{\mathbb{F}}_p$, the algebraic closure of $\mathbb{F}_p$. In particular, $\mathbb{Q}(\mu_e)$ denotes the splitting field of $x^e - 1$ over $\mathbb{Q}$.
- In Sections 6–9, we take $d = 2(p^f - 1)$ and $q \equiv 1 \pmod{d}$ and write down explicit points $R_i \in E(\mathbb{F}_q(t^{1/d}))$. The subgroup they generate is denoted W_d.

2. The rank of E over $\mathbb{F}_q(t^{1/d})$

We are going to compute the rank of the Mordell–Weil group of E over $K = \mathbb{F}_q(t^{1/d})$ in terms of a certain property of the subgroup $\langle p \rangle_e$ of $(\mathbb{Z}/e\mathbb{Z})^\times$ for divisors e of d.

Consider the multiplicative group $G = (\mathbb{Z}/d\mathbb{Z})^\times$, and recall that $A \subset G$ is the subset of classes whose least positive residue lies in $(0, d/2)$, and $B \subset G$ is the subset whose least positive residue lies in $(d/2, d)$, so that G is the disjoint union of A and B.

Definition 2.1. We say "p is balanced modulo d" if every coset C of $\langle p \rangle_d$ in G satisfies $|C \cap A| = |C \cap B|$. In other words, the cosets of $\langle p \rangle_d$ are all evenly divided between the two halves A and B of G. In this case, we also say that "$\langle p \rangle_d$ is a balanced subgroup of G."

For example, it is easy to see that p is balanced modulo d if $d > 2$ and $-1 \in \langle p \rangle_d$, in other words, if d divides $p^f + 1$ for some $f > 0$. See Section 5 for several elementary properties of the balanced condition. See also [4] for further analysis of this condition.

One of our main results is the following calculation of the rank of the Legendre curve E over the fields $\mathbb{F}_q(t^{1/d})$.

Theorem 2.2. *Let p be an odd prime number, let q be a power of p, and let d be a positive integer not divisible by p. Let K be the field $\mathbb{F}_q(t^{1/d})$ and let E be the elliptic curve defined by equation* (1.1). *Then the order of vanishing at $s = 1$ of $L(E/K, s)$ and the rank of the Mordell–Weil group $E(K)$ are both equal to*

$$\sum_{\substack{e \mid d \\ e > 2}} \begin{cases} \frac{\phi(e)}{o_e(q)} & \text{if } p \text{ is balanced modulo } e, \\ 0 & \text{if not,} \end{cases}$$

where ϕ is Euler's function and $o_e(q)$ is the order of q in $(\mathbb{Z}/e\mathbb{Z})^\times$.

The proof will be given at the end of Section 4 below. The case when d divides $p^f + 1$ was already treated in [9, Corollary 5.3].

3. The L-function

Our goal in this section is to calculate the L-function of E in terms of Jacobi sums.

3.1. Jacobi sums. We review some elementary facts about Jacobi sums to set notation. These facts can all be found, for example, in [2] although our notations are not identical to those of [2].

Let $\mathcal{O}_{\overline{\mathbb{Q}}}$ be the ring of algebraic numbers and fix a prime $\mathfrak{p} \subset \mathcal{O}_{\overline{\mathbb{Q}}}$ over p. Then $\mathcal{O}_{\overline{\mathbb{Q}}}/\mathfrak{p}$ is an algebraic closure of $\mathbb{F}_p$ which we denote $\overline{\mathbb{F}}_p$. All finite fields of characteristic p will be taken to be subfields of this $\overline{\mathbb{F}}_p$.

Reduction modulo $\mathfrak{p}$ defines an isomorphism from the group of roots of unity in $\overline{\mathbb{Q}}$ of order prime to p to $\overline{\mathbb{F}}_p^\times$. Let $t : \overline{\mathbb{F}}_p^\times \to \overline{\mathbb{Q}}^\times$ be the inverse of this homomorphism. The restriction of t to any finite field $k^\times \subset \overline{\mathbb{F}}_p^\times$ is a character of order $|k^\times|$. We extend any character χ of $k^\times$ to k by setting $\chi(0) = 0$ if χ is non-trivial and $\chi_{\text{triv}}(0) = 1$.

If k is a finite field and χ_1 and χ_2 are multiplicative characters $k^\times \to \overline{\mathbb{Q}}^\times$, we define a Jacobi sum as follows:

$$J(\chi_1, \chi_2) = \sum_{u+v+1=0} \chi_1(u)\chi_2(v),$$

where the sum is over elements u and $v \in k$. The sum is an algebraic integer, and when χ_1, χ_2, and $\chi_1\chi_2$ are all non-trivial, it has absolute value $|k|^{1/2}$ in every complex embedding, i.e., it is a Weil integer of size $|k|^{1/2}$.

Let q be a fixed power of p, and let d be a positive integer not divisible by p. Multiplication by q defines a permutation of $\mathbb{Z}/d\mathbb{Z}$ and we consider the orbits of this action. Let $o \subset \mathbb{Z}/d\mathbb{Z}$ be such an orbit; we always assume that $o \neq \{0\}$ and, if d is even, that $o \neq \{d/2\}$.

We are going to define a Jacobi sum J_o. To that end, let $|o|$ be the cardinality of the orbit o and let $i \in o$. Note that if $e = d/\gcd(d, i)$, then $|o|$ is the smallest positive integer f such that $q^f \equiv 1 \pmod{e}$. We set

$$\chi_i = t^{\frac{q^{|o|}-1}{d}i},$$

which we view by restriction as a character of $\mathbb{F}_{q^{|o|}}^{\times}$. Also, we denote by λ the non-trivial quadratic character of $\mathbb{F}_{q^{|o|}}^{\times}$. With these notations, we set

$$J_o = J(\lambda, \chi_i) = \sum_{u \in \mathbb{F}_{q^{|o|}}} \lambda(u)\chi_i(-1-u).$$

This is independent of the choice of i because $J(\lambda, \chi_{qi}) = J(\lambda^q, \chi_i^q) = J(\lambda, \chi_i)$. Since we assumed $o \neq \{0\}$ and $\{d/2\}$, the character χ_i has order > 2 and so the Jacobi sum J_o is a Weil integer of size $q^{|o|/2}$.

The reader may wonder why we write χ_i rather than χ^i, and also why we introduce e. The reasons are that J_o is naturally an element of $\mathbb{Q}(\mu_e)$, and that χ_i is not in general the ith power of a character of $\mathbb{F}_{q^{|o|}}^{\times}$.

3.2. The L-function. In this subsection, we give an elementary calculation of the Hasse–Weil L-function of E over $\mathbb{F}_q(t)$.

Theorem 3.1. *Let O be the set of orbits for multiplication by q on $\mathbb{Z}/d\mathbb{Z}$ with the orbits $\{0\}$ and (when d is even) $\{d/2\}$ omitted. For each $o \in O$, let J_o be the Jacobi sum defined above, and let $|o|$ be the cardinality of o. Then the Hasse–Weil L-function of E over the field $K = \mathbb{F}_q(t^{1/d})$ is*

$$L(E/K, T) = \prod_{o \in O} \left(1 - J_o^2 T^{|o|}\right).$$

In particular, when $q \equiv 1 \pmod{d}$ we have

$$L(E/K, T) = \prod_{\substack{i=1 \\ i \neq d/2}}^{d-1} \left(1 - J(\lambda, \chi_i)^2 T\right).$$

Proof. By definition,

$$L(E/K, T) = \prod_{\text{good } v} \left(1 - a_v T^{\deg(v)} + q_v T^{2\deg(v)}\right)^{-1} \prod_{\text{bad } v} \left(1 - a_v T^{\deg(v)}\right)^{-1},$$

where the products are over places of K where E has good or bad reduction, q_v is the cardinality of the residue field at v, and a_v is defined by counting the number of points on the plane cubic model of E at v: $|E(\mathbb{F}_{q_v})| = q_v + 1 - a_v$. We note in

particular that $a_v = 1, -1, 0$ in the case when E has split multiplicative, non-split multiplicative, or additive reduction respectively.

Expanding $\log L(E/K, T)$ as a series in T and rearranging, we find that

$$(3.2) \qquad \log L(E/K, T) = \sum_{n=1}^{\infty} \frac{T^n}{n} \sum_{\beta \in \mathbb{P}^1(\mathbb{F}_{q^n})} a_{\beta, q^n},$$

where the sum is over the $\mathbb{F}_{q^n}$-valued points of $\mathbb{P}^1$ and a_{β, q^n} is defined by requiring that $q^n + 1 - a_{\beta, q^n}$ is the number of $\mathbb{F}_{q^n}$-valued points on the reduction of E at β.

Now focus on a particular value of n. We group the points $\beta \in \mathbb{P}^1(\mathbb{F}_{q^n})$ by their images under the morphism $\rho : \mathbb{P}^1 \to \mathbb{P}^1$, $\beta \mapsto \alpha = \beta^d$ corresponding to the field extension $\mathbb{F}_q(t^{1/d})/\mathbb{F}_q(t)$. Let $g = \gcd(q^n - 1, d)$ and let ψ be the character $\psi = t^{(q^n-1)/g}$ of $\mathbb{F}_{q^n}^{\times}$. Then the number of $\mathbb{F}_{q^n}$-valued points β over a fixed $\alpha \neq 0, \infty$ is either 0 or g depending on whether α is an gth power or not. This value is equal to the character sum $\sum_{i=0}^{g} \psi^i(\alpha)$. Assuming that $\alpha \neq 0, \infty$ so that ρ is unramified over α, we have that $a_{\beta, q^n} = a_{\alpha, q^n}$. Thus,

$$\sum_{\beta \in \mathbb{P}^1(\mathbb{F}_{q^n})} a_{\beta, q^n} = a_{0, q^n} + a_{\infty, q^n} + \sum_{\substack{\alpha \in \mathbb{P}^1(\mathbb{F}_{q^n}) \\ \alpha \neq 0, \infty}} \sum_{i=0}^{g-1} \psi^i(\alpha) a_{\alpha, q^n}.$$

Now we write a_{α, q^n} as a character sum. Let λ be the non-trivial character of $\mathbb{F}_{q^n}^{\times}$ of order 2. Then by a standard calculation, for all finite α we have

$$a_{\alpha, q^n} = - \sum_{\gamma \in \mathbb{F}_{q^n}} \lambda(\gamma(\gamma + 1)(\gamma + \alpha)).$$

Combining the last two paragraphs, we have

$$\sum_{\beta \in \mathbb{P}^1(\mathbb{F}_{q^n})} a_{\beta, q^n} = a_{\infty, q^n} - \sum_{\alpha \in \mathbb{F}_{q^n}} \sum_{i=0}^{g-1} \psi^i(\alpha) \sum_{\gamma \in \mathbb{F}_{q^n}} \lambda(\gamma(\gamma + 1)(\gamma + \alpha)).$$

Changing the order of summation and replacing α with $\gamma \alpha$, we have

$$\sum_{\beta \in \mathbb{P}^1(\mathbb{F}_{q^n})} a_{\beta, q^n} = a_{\infty, q^n} - \sum_{i=0}^{g-1} \sum_{\gamma \in \mathbb{F}_{q^n}} \lambda(\gamma + 1) \psi^i(\gamma) \sum_{\alpha \in \mathbb{F}_{q^n}} \lambda(\alpha + 1) \psi^i(\alpha).$$

Now since $\lambda(-1)^2 = 1$, we may change $\lambda(\alpha + 1)$ and $\lambda(\gamma + 1)$ to $\lambda(-\alpha - 1)$ and $\lambda(-\gamma - 1)$. We find that

$$\sum_{\beta \in \mathbb{P}^1(\mathbb{F}_{q^n})} a_{\beta, q^n} = a_{\infty, q^n} - \sum_{i=0}^{g-1} J(\lambda, \psi^i)^2.$$

Finally, we note that $J(\lambda, \psi^0) = 0$ and, if g is even, $J(\lambda, \psi^{g/2})^2 = 1$. On the other hand, using the reduction types of E [9, Section 7] and what we said above about a_v at places of bad reduction, we have that

$$a_{\infty, q^n} = \begin{cases} 1 & \text{if } d \text{ is even,} \\ 0 & \text{if } d \text{ is odd.} \end{cases}$$

Thus,

$$
(3.3) \qquad \sum_{\beta \in \mathbb{P}^1(\mathbb{F}_{q^n})} a_{\beta, q^n} = - \sum_{\substack{i=1 \\ i \neq g/2}}^{g-1} J(\lambda, \psi^i)^2.
$$

Now we turn to the expression on the right-hand side of the formula of the theorem. Expanding its log as a series in T and rearranging, we have

$$
(3.4) \qquad \log \prod_{\substack{o \subset \mathbb{Z}/d\mathbb{Z} \\ o \neq \{0\}, \{d/2\}}} \left(1 - J_o^2 T^{|o|} \right) = - \sum_{n=1}^{\infty} \frac{T^n}{n} \sum_{\substack{o \subset \mathbb{Z}/d\mathbb{Z} \\ o \neq \{0\}, \{d/2\} \\ |o| \text{ divides } n}} J_o^{2n/|o|} |o|.
$$

The union of the orbits which appear here (namely those where $|o|$ divides n) is the set of elements $j \in \mathbb{Z}/d\mathbb{Z}$, such that $(q^n - 1)j \equiv 0 \pmod{d}$, or equivalently, those divisible by $e = d/\gcd(q^n - 1, d)$. For such an orbit,

$$
J_o^{2n/|o|} |o| = \sum_{j \in o} J\left(\lambda_{q^{|o|}}, \chi_j\right)^{2n/|o|} = \sum_{j \in o} J\left(\lambda_{q^{|o|}}, t^{\frac{q^{|o|}-1}{d} j}\right)^{2n/|o|},
$$

where we write $\lambda_{q^{|o|}}$ to emphasize that in this formula λ is the quadratic character of $\mathbb{F}_{q^{|o|}}$. Summing over the orbits with $|o|$ dividing n, we have

$$
\sum_{\substack{o \subset \mathbb{Z}/d\mathbb{Z} \\ o \neq \{0\}, \{d/2\} \\ |o| \text{ divides } n}} J_o^{2n/|o|} |o| = \sum_{\substack{i=1 \\ i \neq g/2}}^{g-1} J\left(\lambda_{q^{|o|}}, t^{\frac{q^{|o|}-1}{g} i}\right)^{2n/|o|}.
$$

Now the Hasse–Davenport relation [2, 3.7.4] shows that

$$
J\left(\lambda_{q^{|o|}}, t^{\frac{q^{|o|}-1}{g} i}\right)^{2n/|o|} = J\left(\lambda_{q^n}, t^{\frac{q^n-1}{g} i}\right)^2 = J\left(\lambda_{q^n}, \psi^i\right)^2.
$$

Thus we have

$$
(3.5) \qquad \sum_{\substack{o \subset \mathbb{Z}/d\mathbb{Z} \\ o \neq \{0\}, \{d/2\} \\ |o| \text{ divides } n}} J_o^{2n/|o|} |o| = \sum_{\substack{i=1 \\ i \neq g/2}}^{g-1} J\left(\lambda_{q^n}, \psi^i\right)^2.
$$

Comparing equations (3.2) and (3.3) with (3.4) and (3.5) completes the proof of the theorem. $\qquad \square$

4. Explicit Jacobi sums

In this section, we will make the Jacobi sums of the previous section sufficiently explicit to calculate the order of vanishing of the L-function at $s = 1$ (i.e., at $T = q^{-1}$).

Proposition 4.1. *Let $o \subset \mathbb{Z}/d\mathbb{Z}$ be an orbit for multiplication by q with $o \neq \{0\}$ and $o \neq \{d/2\}$. Let $e = d/\gcd(d, i)$ for any $i \in o$. Then $J_o^2/q^{|o|}$ is a root of unity if and only if p is balanced modulo e. Moreover, if p is balanced modulo e then $J_o^2 = q^{|o|}$.*

Proof. We first show that $J_o^2/q^{|o|}$ is a root of unity if and only if p is balanced modulo e.

Note that $J_o \in \mathbb{Q}(\mu_e)$. For $a \in (\mathbb{Z}/e\mathbb{Z})^\times$, let $\sigma_a \in \mathrm{Gal}(\mathbb{Q}(\mu_e)/\mathbb{Q})$ be the automorphism with $\sigma_a(\zeta_e) = \zeta_e^a$. Recall that we fixed a prime $\mathfrak{p}$ of $\overline{\mathbb{Q}}$ over p. We write $\mathfrak{p}$ also for the prime of $\mathbb{Q}(\mu_e)$ that it induces.

For a rational number r, write $\langle r \rangle$ for the fractional part of r, i.e., the number in $[0,1)$ such that $r - \langle r \rangle \in \mathbb{Z}$.

We set $e = d/\gcd(d,i)$ and $i' = i/\gcd(d,i)$. Stickelberger's theorem (e.g., [2, Theorem 3.6.6 and Proposition 2.5.14]) gives the valuation of

$$J_o = J(\lambda, \chi_i) = J\left(t^{(q^f-1)/2}, t^{(q^f-1)i/d}\right)$$

at the prime $\sigma_a(\mathfrak{p})$ as

$$-\nu + \sum_{j=0}^{\nu-1} \left\langle \frac{ap^j}{2} \right\rangle + \left\langle \frac{ai'p^j}{e} \right\rangle + \left\langle \frac{a(-i'-e/2)p^j}{e} \right\rangle,$$

where ν satisfies $q^{|o|} = p^\nu$ and the valuation of p is 1.

Since $J_o^2/q^{|o|}$ is a unit away from primes over p, it is a root of unity if and only if its valuation at every prime over p is 0, or equivalently, if and only the displayed quantity is equal to $\nu/2$ for all a.

Now we note that if $ai'p^j$ has least positive residue modulo e in the interval $(0, e/2)$, then the sum of the three fractional parts in the display above is 1; on the other hand, if $ai'p^j$ has least positive residue modulo e in $(e/2, e)$, then the sum is 2. Thus the displayed quantity is $\nu/2$ if and only if exactly half of the elements of the coset $ai'\langle p \rangle_e \subset (\mathbb{Z}/e\mathbb{Z})^\times$ have least positive residue in $(0, e/2)$ and the other half have least positive residue in $(e/2, e)$. This holds for all $a \in (\mathbb{Z}/e\mathbb{Z})^\times$ if and only if p is balanced modulo e. This completes the proof that $J_o^2/q^{|o|}$ is a root of unity if and only if p is balanced modulo e.

Now we assume that p is balanced modulo e and we check that the root of unity $J_o^2/q^{|o|}$ is in fact 1. To that end, consider $\sum_{u+v+1=0}(\lambda(u)-1)(\chi_i(v)-1)$ (cf. [2, 2.5.11 (2)]). Since $\sum_u \lambda(u) = \sum_v \chi_i(v) = 0$, we have

$$\sum_{u+v+1=0} (\lambda(u)-1)(\chi_i(v)-1) = J(\lambda, \chi_i) + q^{|o|}.$$

Since λ takes values in $\{\pm 1\}$, the sum is zero modulo 2. Thus, $J_o = J(\lambda, \chi_i) \equiv 1$ (mod $2\mathbb{Z}[\mu_e]$). But it is easy to see that the only roots of unity in $\mathbb{Z}[\mu_e]$ congruent to 1 (mod 2) are ± 1. Thus, $J_o = \pm q^{|o|/2}$ and $J_o^2 = q^{|o|}$. $\qquad\square$

Corollary 4.2. *Let $K = \mathbb{F}_q(t^{1/d})$. The order of vanishing of $L(E/K, s)$ at $s = 1$ is*

$$\sum_{\substack{e|d \\ e>2}} \begin{cases} \frac{\phi(e)}{o_e(q)} & \text{if } p \text{ is balanced modulo } e, \\ 0 & \text{otherwise,} \end{cases}$$

where ϕ is Euler's function and $o_e(q)$ is the order of q in $(\mathbb{Z}/e\mathbb{Z})^\times$.

Proof. As in Theorem 3.1, let O be the set of orbits $o \neq \{0\}, \{d/2\}$ for multiplication by q on $\mathbb{Z}/d\mathbb{Z}$. Write O_e for the subset of orbits o where $\gcd(i,d) = e$ for $i \in o$, so

that O is the disjoint union of the O_e as e runs through the divisors of d. Then by Theorem 3.1, we have

$$L(E/K, T) = \prod_{e|d} \prod_{o \in O_e} (1 - J_o^2 T^{|o|}).$$

Since $T = q^{-s}$, for $o \in O_e$ the factor $(1 - J_o^2 T^{|o|})$ contributes a simple zero at $s = 1$ if and only if p is balanced modulo e. On the other hand, the cardinality of the orbits in O_e is $o_e(q)$, so the number of orbits in O_e is $\phi(e)/o_e(q)$. Summing over e gives the asserted order of vanishing. $\qquad\square$

Proof of Theorem 2.2. It is proven in [9, Corollary 11.3] that the Birch and Swinnerton–Dyer conjecture holds for E/K, i.e., we have

$$\operatorname{ord}_{s=1} L(E/K, s) = \operatorname{Rank} E(K).$$

Thus Theorem 2.2 follows immediately from Corollary 4.2. $\qquad\square$

5. Comments on balanced subgroups

In this section, we make several remarks on the condition that p be balanced modulo d.

5.1. First, we note that the cyclicity of $\langle p \rangle_d$ plays no role in the definition of balanced. We may thus define the notion of a balanced subgroup of $G = (\mathbb{Z}/d\mathbb{Z})^\times$. Namely, we say a subgroup H "is balanced in G" or "is balanced modulo d" if for every coset gH of H, the sets $gH \cap A$ and $gH \cap B$ have the same cardinality.

5.2. Next we note that if H and H' are subgroups of G with $H \subset H'$ and if H is balanced, then so is H'. Indeed, the cosets of H' are unions of cosets of H, so are equally distributed between A and B.

5.3. We call a balanced subgroup "minimal" if it does not properly contain another balanced subgroup. Since $\{1\}$ is never balanced, a balanced subgroup of order 2 is automatically minimal. Examples show that there can be distinct minimal balanced subgroups for a fixed d, or equivalently, that the intersection of two balanced subgroups need not be balanced. For example, if $d = 39$, the cyclic subgroups generated by 7 and 29 are balanced, but their intersection (which is generated by 16) is not balanced.

5.4. It is clear that $\{\pm 1\} \subset \mathbb{Z}/d\mathbb{Z}$ is balanced since $-A = B$. Therefore, if a subgroup H contains -1, then H is balanced. For the case $H = \langle p \rangle_d$, this means that p is balanced modulo d if some power of p is congruent to -1 modulo d, or equivalently, if d divides $p^f + 1$ for some f. This is the case that is studied in [9].

5.5. It is equally clear that if $4|d$ then $\{1, d/2 + 1\}$ is balanced, again because $(d/2 + 1)A = B$. Therefore, $\langle p \rangle_d$ is balanced when some power of p is congruent to $d/2 + 1$. This case occurs when p is odd and $d = 2(p^f - 1)$, or more generally when p is odd, and there is an f, such that d divides $2(p^f - 1)$ with an odd quotient.

Note that if d divides $2(p^f - 1)$ with odd quotient, then the same is true of d/e for every odd e dividing d. Thus p is balanced modulo d/e for every odd e dividing d. Applying Theorem 2.2 yields the following result.

Proposition 5.1. *Suppose that p is odd, d divides $2(p^f - 1)$ with an odd quotient, $u^d = t$, and $q \equiv 1 \pmod{d}$. Then*

$$\mathrm{Rank}\, E(\mathbb{F}_q(u))) = \mathrm{Rank}\, E(\mathbb{F}_q(u^2)) + d/2.$$

We will study the arithmetic of E over $\mathbb{F}_q(u)$ in the case when $d = 2(p^f - 1)$ and $q \equiv 1 \pmod{d}$ in more detail in Sections 6–9 below.

5.6. In [4], it is shown that the case where $4 | d$ and $d/2 + 1 \in \langle p \rangle_d$ is more common than the "supersingular" case where $-1 \in \langle p \rangle_d$. More precisely, for a fixed odd prime p, the number of integers $d < X$ satisfying $4 | d$ and $d/2 + 1 \in \langle p \rangle_d$ grows faster than the number of integers $d < X$ with $-1 \in \langle p \rangle_d$.

5.7. Machine calculation shows that there are many pairs (p, d) such that p is balanced modulo d but $-1 \notin \langle p \rangle_d$ and $d/2 + 1 \notin \langle p \rangle_d$. However, it is conjectured in [4] and proven in [3] that these "sporadic" cases are less common than the case $-1 \in \langle p \rangle_d$. In other words, for a fixed odd prime p, the number of integers $d < X$ such that p is balanced modulo d, but $-1 \notin \langle p \rangle_d$ and $d/2 + 1 \notin \langle p \rangle_d$ grows more slowly than the number of $d < X$ such that $-1 \in \langle p \rangle_d$.

5.8. If $H = \langle p \rangle_d$ is balanced, then it has even cardinality. In other words, the order of p in $(\mathbb{Z}/d\mathbb{Z})^\times$ must be even.

5.9. If $d = \ell^a$ is an odd prime power, then $\langle p \rangle_d$ is balanced if and only if $-1 \in \langle p \rangle_e$. Indeed, if p is balanced, then $\langle p \rangle_d$ has even cardinality, so contains an element of order exactly 2. But $(\mathbb{Z}/\ell^a\mathbb{Z})^\times$ is cyclic and so contains a unique element of order exactly 2, namely -1. Conversely, we noted above that p is balanced if $-1 \in \langle p \rangle_d$. The same argument applies when $e = 2\ell^a$ is twice an odd prime power.

5.10. If p is odd and does not divide d, then for all sufficiently large j, p is balanced modulo $2^j d$. Indeed, suppose that $p^g \equiv 1 \pmod{d}$. If j is large, then p^g has order 2^e modulo 2^j for some $e > 1$. The elements of $(\mathbb{Z}/2^j\mathbb{Z})^\times$ of order 2 are -1, $2^{j-1} - 1$, and $2^{j-1} + 1$. Of these, only $2^{j-1} + 1$ is the square of another element of $(\mathbb{Z}/2^j\mathbb{Z})^\times$. This implies that

$$p^{g 2^{e-1}} \equiv 2^{j-1} d + 1 \pmod{2^j d}$$

and so p is balanced modulo $2^j d$.

Using Theorem 2.2, we find that for any odd p, any power q of p, and any d not divisible by p, the rank of $E(K)$ is unbounded as K runs through the (2-adic) tower of fields $\mathbb{F}_q(t^{1/(2^j d)})$, $j = 1, 2, \ldots$.

5.11. When d is odd, it makes sense to speak of 2 being balanced modulo d. We will discuss arithmetic consequences of this case in Section 11 below.

5.12. Examining the first part of the proof of Proposition 4.1, the reader will note that our balanced condition is equivalent to a certain condition on sums of fractional parts which arises from considering valuations of Jacobi sums and Stickelberger's theorem. Similar conditions arise in the study of Fermat varieties, and there is a large literature on these conditions and the related notion of "purity of Gauss sums." We mention only [1, 6, 7].

6. Explicit points for $d = 2(p^f - 1)$

We observed above that when a power of p is $-1 \pmod d$ then $\langle p \rangle_d$ is balanced. In [9, Section 3], explicit points are exhibited on E when $d = p^f + 1$ and $q \equiv 1 \pmod d$. Indeed, if ζ_d denotes a fixed primitive dth root of unity in $\mathbb{F}_q$ and $u^d = t$, then we have points $P_i = (\zeta_d^i u, \zeta_d^i u (\zeta_d^i u + 1)^{d/2})$ for $i = 0, \ldots, d-1$ in $E(\mathbb{F}_q(u))$. We write V_d for the subgroup of $E(\mathbb{F}_q(u))$ generated by the P_i. It is shown in [9, 4.3 and 5.3] that V_d has finite index in $E(\mathbb{F}_q(t^{1/d}))$. More generally when d divides $p^f + 1$ for some f, the traces down to $E(\mathbb{F}_q(t^{1/d}))$ of the P_i generate a finite index subgroup of the Mordell–Weil group.

Our goal in this section is to do something similar for $d = 2(p^f - 1)$. We work over $\mathbb{F}_q(u)$ where $u^d = t$. Let

$$R(u) = \left(u^{-2}, u^{-3}(u^2 + 1)^{(p^f+1)/2} \right).$$

A simple calculation shows that $R(u)$ is a rational point on E defined over $\mathbb{F}_p(u)$.

Next, fix a dth root of unity ζ_d in $\overline{\mathbb{F}}_p$. We define $R_i = R(\zeta_d^i u)$ for $i = 0, \ldots, d-1$. Since E is defined over $\mathbb{F}_p(t)$, the R_i are rational points on E defined over $\mathbb{F}_q(u)$ where $\mathbb{F}_q = \mathbb{F}_p(\mu_d) = \mathbb{F}_{p^{2f}}$.

Note that $\zeta_d^{d/2} = -1$ and that $R_{i+d/2} = -R_i$, so the group generated by the R_i has rank at most $d/2$. Because of this relation we will consider R_i only for $i = 0, \ldots, d/2 - 1$. We write W_d for the subgroup of $E(\mathbb{F}_q(u))$ generated by R_i for $i = 0, \ldots, d/2 - 1$.

In the next section, we will prove the following results.

Theorem 6.1. *Suppose that $d = 2(p^f - 1)$, $u^d = t$, and $q \equiv 1 \pmod d$. Let W_d be the subgroup of $E(\mathbb{F}_q(u))$ generated by the points R_i defined above. Then W_d is free abelian of rank $d/2$. The natural homomorphism*

$$E(\mathbb{F}_q(u^2)) \oplus W_d \to E(\mathbb{F}_q(u))$$

is injective, and its image has finite index.

We will show that the index is independent of q and give bounds on it in Theorem 8.1 below.

Note that if we trace the points R_i down to level $d/2$ (i.e., to $\mathbb{F}_q(u^2)$), we get zero. On the other hand, it follows from the height calculation in the next subsection that if e is a odd divisor of $p^f + 1$ and if we trace from level $d = 2(p^f + 1)$ to level d/e (i.e., to $\mathbb{F}_q(u^e)$), the resulting points generate a group of rank $d/(2e)$.

7. Heights for $d = 2(p^f - 1)$

In this section, we compute the heights of the points R_i and use the result to prove Theorem 6.1. As in [9, Section 8], we write $\langle \cdot, \cdot \rangle$ for the canonical height pairing without the factor $\log q$.

Proposition 7.1. *Let R_i be the points exhibited in Section 6. For $0 \leq i, j \leq d/2 - 1$, the height pairing has values*

$$\langle R_i, R_j \rangle = \begin{cases} p^f & \text{if } i = j, \\ 0 & \text{if } i \neq j. \end{cases}$$

If $P \in E(\mathbb{F}_q(u^2))$, then $\langle P, R_i \rangle = 0$ for all i.

Proof. The general strategy for calculating heights is discussed in [5]. The case of the Legendre curve and the construction of the Néron model needed to carry out the calculation are discussed in detail in [9, Sections 7 and 8]. Since the case $d = p^f + 1$ treated there is similar to the case $d = 2(p^f - 1)$ discussed here, we will not give many details.

Using the Galois invariance of the height pairing and the equality $R_{i+d/2} = -R_i$, we may assume that $j = 0$. As in the proof of [9, Theorem 8.2], we conflate the points R_i and O with the corresponding sections of π.

We write $\pi : \mathcal{E}_d \to \mathbb{P}^1$ for the Néron model of $E/\mathbb{F}_q(u)$. We recall from [9, Section 7] that E has reduction type I_{2d} at $u = 0$ and type I_2 at the places dividing $u^d - 1$. Since d is even, the reduction type is I_{2d} at $u = \infty$. At all other places, E has good reduction.

By [9, Lemma 7.1], the height (or degree) of $\mathcal{E}_d \to \mathbb{P}^1$ is $d/2 = p^f - 1$. Therefore, the self-intersections O^2 and R_i^2 are $-d/2 = -(p^f - 1)$. The intersection number $R_0.O$ is equal to 1. (There is a simple intersection over $u = 0$.) Therefore, the "geometric" part of the height pairing $\langle R_0, R_0 \rangle$ is

$$-(R_0 - O)(R_0 - O) = d + 2 = 2p^f.$$

For the "correction factors," one checks that R_0 meets the identity component at $u = 0$, the non-identity component at $u = \zeta_d^j$ where $j = \pm d/4$, the identity component at $u = \zeta_d^j$ for other values of j, and the component labelled d at $u = \infty$. Thus the correction factor is

$$-2 \left(\frac{1 \cdot 1}{2} \right) - \left(\frac{d \cdot d}{2d} \right) = -1 - d/2$$

and the height $\langle R_0, R_0 \rangle = d/2 + 1 = p^f$.

For $0 < i \le d/2 - 1$, the intersection number $R_i.R_0$ is 2. (There are simple intersections over $u = 0$ and $u = \infty$.) Thus the "geometric" part of the height pairing $\langle R_i, R_0 \rangle$ is

$$-(R_i - O)(R_0 - O) = -2 + 2 + d/2 = d/2.$$

The only place where both R_i and R_0 meet a non-identity component is at $u = \infty$, where they both meet the component labeled d. The local contribution is thus $-d/2$, and the height pairing is zero.

This verifies the formula for the heights $\langle R_i, R_j \rangle$.

If $P \in E(\mathbb{F}_q(u^2))$, then P is fixed by $\mathrm{Gal}(\mathbb{F}_q(u)/\mathbb{F}_q(u^2))$. But the automorphism σ with $\sigma(u) = -u$ satisfies $\sigma(R_i) = -R_i$ for all i. Thus

$$\langle P, R_i \rangle = \langle \sigma(P), \sigma(R_i) \rangle = -\langle P, R_i \rangle$$

and it follows that $\langle P, R_i \rangle = 0$ for all i as desired.

This completes the proof of the proposition. $\square$

Proof of Theorem 6.1. It follows immediately from Proposition 7.1 that the points R_i for $i = 0, \dots, d/2 - 1$ are independent, in other words that W_d is free abelian of rank $d/2$.

If P is a point in the intersection of W_d and $E(\mathbb{F}_q(u))$ then by the Proposition we have $\langle P, P \rangle = 0$, so that P is torsion. But we just saw that W_d is torsion-free, so $P = 0$. This proves that $E(\mathbb{F}_q(u^2)) \oplus W_d \to E(\mathbb{F}_q(u))$ is injective.

By Proposition 5.1, the rank of $E(\mathbb{F}_q(u))$ is $d/2$ plus the rank of $E(\mathbb{F}_q(u^2))$, so the index of $E(\mathbb{F}_q(u^2)) \oplus W_d$ in $E(\mathbb{F}_q(u))$ is finite.

This completes the proof of Theorem 6.1. $\square$

8. Bounds on the index for $d = 2(p^f - 1)$

Throughout this section, we assume that $d = 2(p^f - 1)$, $u^d = t$, and $q \equiv 1 \pmod{d}$. Since p is odd, this implies that $q \equiv 1 \pmod 4$.

We begin by recalling several points from [9, Section 3]: we have 2-torsion points $Q_0 = (0,0)$, $Q_1 = (-1,0)$, and $Q_t = (-t,0)$, as well as the 4-torsion points $P_i^{(2)}$ with $i \in \mathbb{Z}/2\mathbb{Z}$ defined by $P_0^{(2)} = (t^{1/2}, t^{1/2}(t^{1/2}+1))$ and $P_1^{(2)} = (-t^{1/2}, -t^{1/2}(-t^{1/2}+1))$.

Next we recall some results on $\mathrm{Sel}_2(E/\mathbb{F}_q(u))$, the 2-Selmer group of E over $\mathbb{F}_q(u)$. This group is defined in [9, Section 5], and it is shown there that when d is even there is an injection
$$\mathrm{Sel}_2(E/\mathbb{F}_q(u)) \hookrightarrow (\mathbb{Z}/2\mathbb{Z})^d$$
and the composed map
$$E(\mathbb{F}_q(u))/2E(\mathbb{F}_q(u)) \hookrightarrow \mathrm{Sel}_2(E/\mathbb{F}_q(u)) \hookrightarrow (\mathbb{Z}/2\mathbb{Z})^d$$
sends a point $(x, y) \notin \{O, Q_1\}$ to the tuple $(e_0, \ldots, e_{d-1})$ where
$$e_j = \mathrm{ord}_{u = \zeta^j}(x + 1) \pmod 2.$$
It follows immediately from this that if q' is a power of q, then the natural map of 2-Selmer groups
$$\mathrm{Sel}_2(E/\mathbb{F}_q(u)) \to \mathrm{Sel}_2(E/\mathbb{F}_{q'}(u))$$
is injective.

There is also an explicit calculation of $\mathrm{Sel}_2(E/\mathbb{F}_q(u))$ in [9, Section 5]. In terms of the injection $\mathrm{Sel}_2(E/\mathbb{F}_q(u)) \hookrightarrow (\mathbb{Z}/2\mathbb{Z})^d$, we have that $\mathrm{Sel}_2(E/\mathbb{F}_q(u)) \cong (\mathbb{Z}/2\mathbb{Z})^d$ if $q \equiv 1 \pmod{2d}$, whereas if $(q-1)/d$ is odd, $\mathrm{Sel}_2(E/\mathbb{F}_q(u))$ consists of those tuples $(e_0, \ldots, e_{d-1})$ satisfying
$$\sum_{i=0}^{d/2-1} e_{2i} = \sum_{i=0}^{d/2-1} e_{2i+1} = 0.$$
Recall that W_d is the subgroup of $E(\mathbb{F}_q(u))$ generated by the points R_i, $i = 0, \ldots, d/2 - 1$ defined in Section 6. Now we turn to the main topic of this section, namely the index of $E(\mathbb{F}_q(u^2)) \oplus W_d$ in $E(\mathbb{F}_q(u))$.

Theorem 8.1. *Suppose that $d = 2(p^f - 1)$, $u^d = t$, and $q \equiv 1 \pmod d$. Let I be the index of $E(\mathbb{F}_q(u^2)) \oplus W_d$ in $E(\mathbb{F}_q(u))$. Then for a fixed p and f, I is independent of q and is a power of 2 times a power of p. The p part of I divides $p^{f(p^f-1)/2}$, and I is divisible by 4.*

Proof. Note that the index I can only increase with q. We argue that it does not increase. Since the rank of $E(\mathbb{F}_q(u))$ is independent of q (for q satisfying our hypotheses), if I increased going from $\mathbb{F}_q(u)$ to $\mathbb{F}_{q'}(u)$, there would be a point $P \in E(\mathbb{F}_{q'}(u)) \setminus E(\mathbb{F}_q(u))$ with $nP \in E(\mathbb{F}_q(u))$. In this case, $\mathrm{Fr}_q(P) - P$ would be n-torsion. By [9, Proposition 6.1] we may assume $n = 2$. But the injectivity of $\mathrm{Sel}_2(E/\mathbb{F}_q(u)) \to \mathrm{Sel}_2(\mathbb{F}_{q'}(u))$ noted above implies that a basis of $E(\mathbb{F}_q(u))/2E(\mathbb{F}_q(u))$ is also a basis of

$E(\mathbb{F}_{q'}(u))/2E(\mathbb{F}_{q'}(u))$, and this implies that the 2 part of the index cannot increase. This proves that I is independent of q.

We can also use Selmer groups to see that the index I is divisible by 4 as follows. An easy calculation shows that the image of W_d in $\mathrm{Sel}_2(\mathbb{F}_q(u))$ has dimension $d/2$ and it contains the image of the 4-torsion points $P_0^{(2)}$ and $P_1^{(2)}$. More explicitly, we find that

$$\sum_{i=0}^{d/4-1} R_{2i} + P_{1+d/4}^{(2)} \quad \text{and} \quad \sum_{i=0}^{d/4-1} R_{2i+1} + P_{d/4}^{(2)}$$

are divisible by 2 in $E(\mathbb{F}_q(u))$. On the other hand, they are are not divisible by 2 in $E(\mathbb{F}_q(u)) \oplus W_d$ since Theorem 6.1 shows the sums $\sum R_{2i}$ and $\sum R_{2i+1}$ are not divisible by 2 in W_d.

To further control the index of $E(\mathbb{F}_q(u^2)) \oplus W_d$ in $E(\mathbb{F}_q(u))$, we use a relative version of the integrality result [9, Proposition 9.1]. To state the result, we first introduce some notation. If M is a finitely generated $\mathbb{Z}$-module, we write $M[1/2]$ for $M \otimes \mathbb{Z}[1/2]$. If M is also equipped with an automorphism of order 2, we have a direct sum decomposition

$$M[1/2] = M^+ \oplus M^-,$$

where M^+ denotes the fixed subgroup of $M[1/2]$ and M^- denotes the subgroup of $M[1/2]$ where the automorphism acts as -1. If M is equipped with a symmetric, bilinear, $\mathbb{Q}$-valued pairing, we may canonically extend the pairing to $M[1/2]$. If M (resp. M') is a finitely generated $\mathbb{Z}$-module (resp. a finitely generated $\mathbb{Z}[1/2]$-module) equipped with a symmetric, bilinear, $\mathbb{Q}$-valued pairing, we define $\mathrm{Disc}(M)$ and $\mathrm{Disc}(M')$ in the usual way: choose a basis of M modulo torsion (resp. a basis of M' modulo $\mathbb{Z}[1/2]$-torsion) and let Disc be the absolute value of the determinant of the matrix of pairings of basis elements. Then $\mathrm{Disc}(M)$ is a well-defined element of $\mathbb{Q}$, and $\mathrm{Disc}(M')$ is well defined up to multiplication by the square of an element of $\mathbb{Z}[1/2]^\times$, i.e., up to a power of 4.

Now returning to elliptic curves, we let $\pi : \mathcal{E} \to \mathbb{P}^1$ be the Néron model of $E/\mathbb{F}_q(u)$, and we let N be the subgroup of the Néron–Severi group of $\mathcal{E}$ generated by components of fibers of π that do not meet the zero section. This is known to be a finitely generated free abelian group. With these notations, [9, Proposition 9.1] says that the rational number

$$\frac{\mathrm{Disc}(E(\mathbb{F}_q(u)))\,\mathrm{Disc}(N)}{|E(\mathbb{F}_q(u))_{\mathrm{tor}}|^2}$$

is in fact an integer. If we take the proof of this result, tensor all the groups appearing in it with $\mathbb{Z}[1/2]$, and then take the minus part for $\mathrm{Gal}(\mathbb{F}_q(u)/\mathbb{F}_q(u^2)) = \{1, \sigma\}$, we find that the rational number

$$\frac{\mathrm{Disc}(E(\mathbb{F}_q(u))^-)\,\mathrm{Disc}(N^-)}{|E(\mathbb{F}_q(u))_{\mathrm{tor}}^-|^2}$$

(well-defined up to squares of elements of $\mathbb{Z}[1/2]^\times$) is in fact an element of $\mathbb{Z}[1/2]$.

Since $E(\mathbb{F}_q(u))_{\mathrm{tor}}$ is a 2-group, $E(\mathbb{F}_q(u))_{\mathrm{tor}}^-$ is trivial. Using the Néron model calculations of [9, Section 7], we find that all components of the fibers of π over 0 and ∞ are fixed by σ and so do not contribute to N^-. The fibers over the dth roots of unity are permuted in pairs, so N^- is a free $\mathbb{Z}[1/2]$-module of rank $d/2$, and it has an orthogonal set of generators each of which has self-pairing -4. Thus $\mathrm{Disc}(N^-) = (-4)^{d/2} = 2^d$

which is a unit in $\mathbb{Z}[1/2]$. Our integrality result then yields that $\mathrm{Disc}(E(\mathbb{F}_q(u))^-)$ lies in $\mathbb{Z}[1/2]$.

Now the inclusion $E(\mathbb{F}_q(u^2)) \oplus W_d \hookrightarrow E(\mathbb{F}_q(u))$ yields an identification

$$\left(\frac{E(\mathbb{F}_q(u))}{E(\mathbb{F}_q(u^2)) \oplus W_d} \right)[1/2] \cong \frac{E(\mathbb{F}_q(u))^-}{W_d[1/2]}.$$

If J denotes the order of this group (which is the prime-to-2 part of the index of $E(\mathbb{F}_q(u^2)) \oplus W_d$ in $E(\mathbb{F}_q(u))$), then we have

$$\mathrm{Disc}(E(\mathbb{F}_q(u))^-) = \frac{\mathrm{Disc}(W_d[1/2])}{J^2}.$$

Proposition 7.1 shows that $\mathrm{Disc}(W_d[1/2])$ is $p^{f(p^f-1)}$, so our integrality result shows that J is a power of p. Therefore, the index of $E(\mathbb{F}_q(u^2)) \oplus W_d$ in $E(\mathbb{F}_q(u))$ is a power of 2 times a power of p. Moreover, the power of p divides $p^{f(p^f-1)/2}$. □

It follows from Theorem 9.1 below that the 2 part of I divides 2^{p^f+1}. We suspect that the 2 part of I is in fact always 4. We can prove this when $p^f \equiv 3 \pmod 4$ by comparing the trace down to level $d = 4$ of points R_i of this paper and the points P_i of [9, Section 3]. It is also true in several other examples we have checked, but we do not know how to prove it in general.

9. Bounds on Ш for $d = 2(p^f - 1)$

Recall that the second part of the conjecture of Birch and Swinnerton-Dyer relates the leading coefficient of the L-series of E at $s = 1$ to other invariants of E. More precisely, defining $L^*(E) := \frac{1}{r!} L^{(r)}(E, 1)$, we should have

$$L^*(E) = \frac{|\text{Ш}| \, R \, \tau}{|E_{\mathrm{tor}}|^2},$$

where r is the order of vanishing of the L-function, Ш is the Tate–Shafarevich group of E, R is a regulator, and τ is a Tamagawa number. See [10, Section 6] for definitions and a precise statement. The conjecture holds in our context by [9, Corollary 11.3].

Our goal in this section is to exploit the BSD formula to obtain information on $\text{Ш}(E/\mathbb{F}_q(u))$ when $d = 2(p^f - 1)$. In [9, Corollary 10.2] it is proven that when $d = p^f + 1$, $\text{Ш}(E/\mathbb{F}_q(u))$ is a p-group of order equal to the square of an index. The analog for $d = 2(p^f - 1)$ is necessarily more complicated because we have very little information in general on the arithmetic of E over $\mathbb{F}_q(u^2)$. Nevertheless, we can prove a strong relative statement.

To state the theorem, we write

$$Nm_q : \text{Ш}(E/\mathbb{F}_q(u)) \to \text{Ш}(E/\mathbb{F}_q(u^2))$$

for the norm map induced by the corestriction

$$H^1(\mathrm{Spec}\,\mathbb{F}_q(u), E) \to H^1(\mathrm{Spec}\,\mathbb{F}_q(u^2), E).$$

Theorem 9.1. *Suppose that $d = 2(p^f - 1)$, $u^d = t$, and $q \equiv 1 \pmod d$. Let I be the index of $E(\mathbb{F}_q(u^2)) \oplus W_d$ in $E(\mathbb{F}_q(u))$, as in Theorem 8.1.*

(1) *We have*

$$I^2 = 2^{p^f+1} \frac{p^{fd/2}}{q^{d/4}} \frac{|\text{Ш}(E/\mathbb{F}_q(u))|}{|\text{Ш}(E/\mathbb{F}_q(u^2))|} = 2^{p^f+1} \frac{p^{fd/2}}{q^{d/4}} \frac{|\operatorname{Ker} Nm_q|}{|\operatorname{Coker} Nm_q|}.$$

In particular, when $q = p^{2f}$, we have

$$I^2 = 2^{p^f+1} \frac{|\text{Ш}(E/\mathbb{F}_q(u))|}{|\text{Ш}(E/\mathbb{F}_q(u^2))|} = 2^{p^f+1} \frac{|\operatorname{Ker} Nm_q|}{|\operatorname{Coker} Nm_q|}.$$

(2) *The cokernel of Nm_q is a 2-group.*
(3) *The kernel of Nm_q is a p-group.*
(4) *For fixed p and f, the cokernel of Nm_q is independent of q. The cokernel of Nm_q is non-trivial if $p^f \equiv 1$ (mod 4). The order of $\operatorname{Ker} Nm_q$ goes to infinity with $\log_p q$.*

Proof. By Theorem 3.1, Proposition 4.1, and Section 5.5, we have

$$\frac{L(E/\mathbb{F}_q(u), s)}{L(E/\mathbb{F}_q(u^2), s)} = (1 - q^{1-s})^{d/2}$$

and so $L^*(E/\mathbb{F}_q(u)) = L^*(E/\mathbb{F}_q(u^2))$. Taking the ratio of the two BSD formulas, we find

$$1 = \frac{R(E/\mathbb{F}_q(u))}{R(E/\mathbb{F}_q(u^2))} \frac{|\text{Ш}(E/\mathbb{F}_q(u))|}{|\text{Ш}(E/\mathbb{F}_q(u^2))|} \frac{\tau(E/\mathbb{F}_q(u))}{\tau(E/\mathbb{F}_q(u^2))}.$$

Using the notation of Section 8 and Theorem 6.1, we have

$$R(E/\mathbb{F}_q(u)) = \operatorname{Disc}(E(\mathbb{F}_q(u))) = \operatorname{Disc}\left(E(\mathbb{F}_q(u^2)) \oplus W_d\right)/I^2.$$

On the other hand, $E(\mathbb{F}_q(u^2)) \oplus W_d$ is an orthogonal direct sum and $\operatorname{Disc}(W_d) = p^{fd/2}$ by Proposition 7.1. Thus

$$\frac{R(E/\mathbb{F}_q(u))}{R(E/\mathbb{F}_q(u^2))} = \frac{p^{fd/2}}{I^2}.$$

For the τ ratio, we have

$$\tau(E/\mathbb{F}_q(u)) = 2^{d+2} d^2 q^{1-d/2} \quad \text{and} \quad \tau(E/\mathbb{F}_q(u^2)) = 2^{d/2} d^2 q^{1-d/4},$$

so

$$\frac{\tau(E/\mathbb{F}_q(u))}{\tau(E/\mathbb{F}_q(u^2))} = 2^{d/2+2} q^{-d/4} = 2^{p^f+1} q^{-d/4}.$$

Substituting the last two displayed ratios into the ratio of BSD formulas yields part (1).

We saw in Theorem 6.1 that I is a power of 2 times a power of p, so part (1) shows that the same is true of $|\text{Ш}(E/\mathbb{F}_q(u))|/|\text{Ш}(E/\mathbb{F}_q(u^2))|$.

Next we consider the pull-back and norm maps on the Tate–Shafarevich groups induced by the inclusion of fields $\mathbb{F}_q(u^2) \hookrightarrow \mathbb{F}_q(u)$:

$$\text{Ш}(E/\mathbb{F}_q(u^2)) \xrightarrow{j} \text{Ш}(E/\mathbb{F}_q(u)) \xrightarrow{Nm_q} \text{Ш}(E/\mathbb{F}_q(u^2)).$$

The composition $Nm_q \circ j$ is multiplication by 2, so is an isomorphism on the prime-to-2 part of $\text{Ш}(E/\mathbb{F}_q(u^2))$. Therefore, Nm_q is surjective on the prime-to-2 parts. This proves part (2), namely that $\operatorname{Coker} Nm_q$ is a 2-group. Bounds on its order will be proven below.

Since the prime-to-$2p$ parts of $\mathrm{III}(E/\mathbb{F}_q(u))$ and $\mathrm{III}(E/\mathbb{F}_q(u^2))$ have the same order, they are isomorphic via Nm_q. We will prove that the kernel of Nm_q has odd order and that the cokernel is non-trivial if $(q-1)/d$ is odd. For these assertions, we consider the diagram of descent sequences:

$$0 \longrightarrow E(\mathbb{F}_q(u))/2E(\mathbb{F}_q(u)) \longrightarrow \mathrm{Sel}_2(E(\mathbb{F}_q(u))) \longrightarrow \mathrm{III}(E/\mathbb{F}_q(u))_2 \longrightarrow 0$$

$$0 \longrightarrow E(\mathbb{F}_q(u^2))/2E(\mathbb{F}_q(u^2)) \longrightarrow \mathrm{Sel}_2(E(\mathbb{F}_q(u^2))) \longrightarrow \mathrm{III}(E/\mathbb{F}_q(u^2))_2 \longrightarrow 0,$$

where the vertical maps are norms.

Suppose that $(q-1)/d$ is even. The Selmer group calculations recalled above show that if r is the rank of $E(\mathbb{F}_q(u^2))$, then the diagram above is isomorphic to

$$0 \longrightarrow \mathbb{F}_2^{d/2+r+2} \longrightarrow \mathbb{F}_2^d \longrightarrow \mathrm{III}(E/\mathbb{F}_q(u))_2 \longrightarrow 0$$

$$0 \longrightarrow \mathbb{F}_2^{r+2} \longrightarrow \mathbb{F}_2^{d/2} \longrightarrow \mathrm{III}(E/\mathbb{F}_q(u^2))_2 \longrightarrow 0$$

and the middle vertical map is surjective. It follows that the right vertical map is also surjective. On the other hand, considering the rows shows that the right-hand groups have the same order, so they are isomorphic via the vertical map, in other words

$$Nm_q : \mathrm{III}(E/\mathbb{F}_q(u))_2 \to \mathrm{III}(E/\mathbb{F}_q(u^2))_2$$

is an isomorphism. A chase using the diagram

$$0 \longrightarrow \mathrm{III}(E/\mathbb{F}_q(u))_2 \longrightarrow \mathrm{III}(E/\mathbb{F}_q(u))_{2^n} \overset{2}{\longrightarrow} \mathrm{III}(E/\mathbb{F}_q(u))_{2^{n-1}}$$

$$0 \longrightarrow \mathrm{III}(E/\mathbb{F}_q(u^2))_2 \longrightarrow \mathrm{III}(E/\mathbb{F}_q(u^2))_{2^n} \overset{2}{\longrightarrow} \mathrm{III}(E/\mathbb{F}_q(u^2))_{2^{n-1}}$$

and induction on n shows that

$$Nm_q : \mathrm{III}(E/\mathbb{F}_q(u))_{2^\infty} \to \mathrm{III}(E/\mathbb{F}_q(u^2))_{2^\infty}$$

is injective.

Matters are slightly more complicated when we assume that $(q-1)/d$ is odd. In this case, the Selmer group calculations recalled above show that that the descent diagram is isomorphic to

$$0 \longrightarrow \mathbb{F}_2^{d/2+r+2} \longrightarrow \mathbb{F}_2^{d-2} \longrightarrow \mathrm{III}(E/\mathbb{F}_q(u))_2 \longrightarrow 0$$

$$0 \longrightarrow \mathbb{F}_2^{r+2} \longrightarrow \mathbb{F}_2^{d/2} \longrightarrow \mathrm{III}(E/\mathbb{F}_q(u^2))_2 \longrightarrow 0$$

and the middle vertical map has cokernel of order 4. This shows that the cokernel of the right vertical map has order at most 4. On the other hand, considering the rows shows that the orders of the right-hand groups have ratio 4, and we conclude that the

right-hand vertical map is injective. The same argument as in the case $(q-1)/d$ is even then shows that

$$Nm_q : \text{Ш}(E/\mathbb{F}_q(u))_{2^\infty} \to \text{Ш}(E/\mathbb{F}_q(u^2))_{2^\infty}$$

is injective. If it were surjective, it would be an isomorphism, and therefore induce an isomorphism on the 2-torsion subgroups, but we just saw this is not the case, so the cokernel is non-trivial.

Summarizing the last three paragraphs, we have that the 2 part of $\ker Nm_q$ is always trivial, and the 2 part of $\text{Coker}\, Nm_q$ is non-trivial when $(q-1)/d$ is odd. This completes the proof that $\text{Ker}\, Nm_q$ is a p-group, i.e., part (3).

We saw in Theorem 8.1 that for fixed p and f, I is independent of q. Since the kernel and cokernel of Nm_q are p-groups and 2-groups, respectively, it follows from parts (1), (2), and (3) that the cokernel of Nm_q is independent of q, and the order of the kernel goes to infinity with q. Finally, if $p^f \equiv 1 \pmod 4$ and we take $q = p^{2f}$, then $(q-1)/d = (p^f+1)/2$ is odd and the cokernel of Nm_q is non-trivial. This completes the proof of part (4) and the proof of the theorem. $\square$

10. Correspondences and points

It is proven in [9, Section 11] that the Néron model $\mathcal{E}_d \to \mathbb{P}^1$ of $E/\mathbb{F}_q(u)$ is birational to the quotient of a product of curves. This implies the BSD conjecture for $E/\mathbb{F}_q(u)$ and it allows us to compute the rank of $E(\mathbb{F}_q(u))$ in terms of Jacobians over finite fields. It also allows us to "explain" the explicit points of this paper and [9] via certain correspondences. In this section, we briefly explain how this plays out for $d = p^f + 1$ and $d = 2(p^f - 1)$.

Let $\mathcal{E}_d$ be the Néron model of $E/\mathbb{F}_q(u)$, so the function field of $\mathcal{E}_d$ is generated by x, y, u with relation $y^2 = x(x+1)(x+u^d)$.

Let $\mathcal{C}_d$ be the smooth projective curve with affine model

$$z^d + x^2 + 1 = 0$$

and let $\mathcal{D}_d$ be defined by

$$w^d + y^2 + 1 = 0.$$

There is an action of $\mu_d \times \mu_2$ on $\mathcal{C}_d \times \mathcal{D}_d$ given by

$$\zeta_d(x, y, z, w) = (x, y, \zeta_d z, \zeta_d^{-1} w) \qquad (-1)(x, y, z, w) = (-x, -y, z, w).$$

The quotient has function field generated by x^2, xy, and zw. It is birational to $\mathcal{E}_d$ with the quotient map $\phi : \mathcal{C}_d \times \mathcal{D}_d \to \mathcal{E}_d$ given by

$$\phi^*(x, y, u) = (-x^2 - 1, xy(x^2 + 1), zw).$$

The rational quotient map $\mathcal{C}_d \times \mathcal{D}_d \dashrightarrow \mathcal{E}_d$ can be used to compute the zeta-function of $\mathcal{E}_d$ and the L-function of $E/\mathbb{F}_q(u)$. The fact that $\mathcal{E}_d$ is dominated by a product of quotients of Fermat curves "explains" why the L-function of E is expressible in terms of the Jacobi sums $J(\lambda, \chi_i) = J(\chi_{d/2}, \chi_i)$.

Let $J = J_{\mathcal{C}_d}$ be the Jacobian of $\mathcal{C}_d$. The results of [8] use the rational map ϕ to prove that the rank of $E(\overline{\mathbb{F}}_p(t^{1/d})$ is equal to the rank of the group of endomorphisms of J which anti-commute with the action of μ_d. This group can also be identified with a certain group of correspondences on $\mathcal{C}_d \times \mathcal{D}_d$.

The geometry of this setup can be used to "explain" the explicit points of [9] and this paper. Namely, when $d = p^f + 1$, consider the graph of the p^f-power Frobenius $\mathrm{Fr}_{p^f} : \mathcal{C}_d \to \mathcal{D}_d$. This anti-commutes with the μ_d action. Pushing it down via ϕ yields the section corresponding to the point P_0 of [8, Theorem 8.1].

When d is even, we have an automorphism $\psi : \mathcal{C}_d \to \mathcal{C}_d$ given by

$$\psi^*(x, z) = (x/z^{d/2}, z^{-1}).$$

When $d = 2(p^f - 1)$, the composition of ψ and the p^f-power Frobenius gives a morphism $\mathcal{C}_d \to \mathcal{D}_d$ which induces a homomorphism $J_{\mathcal{C}_d} \to J_{\mathcal{D}_d}$ which anti-commutes with the μ_d actions. Pushing the graph of this morphism down to $\mathcal{E}_d$ via ϕ leads to the section associated to the point R_0 of Section 6.

Note that Theorem 2.2 shows that E has points of infinite order over many extensions $\mathbb{F}_q(t^{1/d})$, but we lack any explicit expression for their coordinates except when d divides $p^f + 1$ or $2(p^f - 1)$. It would be very interesting to find a direct connection between the balanced condition and special endomorphisms or correspondences on $\mathcal{C}_d \times \mathcal{D}_d$ which would provide explicit expressions for points of infinite order on E.

11. The case $p = 2$

The equation for the Legendre curve does not define an elliptic curve in characteristic 2. However, there is a curve E' defined uniformly for all p which is isogenous to the Legendre curve for all $p > 2$. Most of the results of this paper extend to E' and continue to hold in characteristic 2.

More precisely, let t' and u' be new indeterminates with $u'^d = t'$, and let E' be the elliptic curve

$$(11.1) \qquad\qquad y'^2 + x'y' + t'y' = x'^3 + t'x'^2$$

over $\mathbb{F}_p(t')$. It is proven in [9, Lemma 11.1] that if $p > 2$ and we identify $\mathbb{F}_p(t')$ and $\mathbb{F}_p(t)$ by sending t' to $t/16$, then E and E' are 2-isogenous. If 16 is a dth power in $\mathbb{F}_q$, then we may identify $\mathbb{F}_q(u)$ and $\mathbb{F}_q(u')$ (as extensions of $\mathbb{F}_p(t) = \mathbb{F}_p(t')$) and in this case E and E' have the same L-function over $\mathbb{F}_q(u)$ and the same rank because they are isogenous. We would like to make a more precise statement that holds over $\mathbb{F}_q(u')$ for all q.

To that end, we define a new Jacobi sum J'_o, where $o \subset \mathbb{Z}/d\mathbb{Z}$ is an orbit for multiplication by q. As before, we assume that $o \neq \{0\}$ and $o \neq \{d/2\}$ if d is even. We keep the notations of Section 3.1 and define

$$J'_o = J(\chi_i, \chi_i),$$

where i is any element of o. This is well defined because $J(\chi_{qi}, \chi_{qi}) = J(\chi_i, \chi_i)$.

The following theorem extends many of our results about E to E', where they continue to hold when $p = 2$.

Theorem 11.2. *Let p be an arbitrary prime number, q a power of p, and d an integer prime to p. Let $K' = \mathbb{F}_q(u')$ where $u'^d = t'$, and let E' be the elliptic curve over K' defined by (11.1).*

    (1) *The Hasse–Weil L-function of E' over K' is*

$$L(E'/K', T) = \prod_{o \in O} \left(1 - J'^2_o T^{|o|}\right).$$

Here the product is over the set O of orbits $o \subset \mathbb{Z}/d\mathbb{Z}$ for multiplication by q, omitting the orbits $\{0\}$ and $\{d/2\}$ (if d is even).

(2) Let $o \in O$ be an orbit and let $e = d/\gcd(d, i)$ for any $i \in o$. Then $J_o'^2/q^{|o|}$ is a root of unity if and only if p is balanced modulo e.

(3) If $p > 2$ and $i \in o$, then $J_o' = \chi^i(4)\lambda(-1)J_o$.

(4) Suppose $p = 2$ and $o \in O$. If $e = d/\gcd(d, i)$ for any $i \in o$ and 2 is balanced modulo e, then $J_o'^2 = q^{|o|}$. If $p = 2$, then the rank of $E'(\mathbb{F}_q(u'))$ is

$$\sum_{\substack{e|d \\ e>2}} \begin{cases} \frac{\phi(e)}{o_e(q)} & \text{if } 2 \text{ is balanced modulo } e, \\ 0 & \text{otherwise,} \end{cases}$$

where ϕ is Euler's function and $o_e(q)$ is the order of q in $(\mathbb{Z}/e\mathbb{Z})^\times$.

(5) Let $\mathcal{E}_d' \to \mathbb{P}^1$ be the Néron model of $E'/\mathbb{F}_q(u')$. Let $\mathcal{C}_d' = \mathcal{D}_d'$ be the smooth, projective (Fermat) curve over $\mathbb{F}_q$ defined by $z^d = x(1-x)$. Then $\mathcal{E}_d$ is birational to the quotient of $\mathcal{C}_d \times \mathcal{D}_d$ by the anti-diagonal action of μ_d.

Proof. The proofs are for the most part parallel to those of the corresponding statements for E, so we will omit many details.

For (1), one may give a direct, elementary argument along the lines of the proof of Theorem 3.1. Alternatively, one may use part (5) of this theorem and a geometric analysis of the morphism $(\mathcal{C}_d' \times \mathcal{D}_d')/\mu_d \dashrightarrow \mathcal{E}_d'$. Indeed, the inverse roots of the zeta function of $\mathcal{C}_d'$ are exactly the Jacobi sums J_o' and the inverse roots of the H^2 part of the zeta function of $(\mathcal{C}_d' \times \mathcal{D}_d')/\mu_d$ are the squares $J_o'^2$. In some sense this "explains" their appearance in the L-function of E'.

The proof of (2) is parallel to the first part of the proof of Proposition 4.1. Indeed, Stickelberger's theorem shows that the valuation of J_o' at the prime $\sigma_a(\mathfrak{p})$ is given by

$$-\nu + \sum_{j=0}^{\nu-1} \left\langle \frac{ai'p^j}{e} \right\rangle + \left\langle \frac{ai'p^j}{e} \right\rangle + \left\langle \frac{-2ai'p^j}{e} \right\rangle,$$

where $i' = i/\gcd(d, i)$, ν satisfies $q^{|o|} = p^\nu$, and the valuation of p is 1. It is then easy to see that the valuations are all $|o|/2$ if and only if p is balanced modulo e.

Part (3) is [2, Exer. 40 in Chapter 2].

For part (4), if $p = 2$ and 2 is balanced modulo e, then by part (2), $J_o'^2/q^{|o|}$ is a root of unity. To see that it is 1, we may use Stickelberger's congruence [2, Thm. 3.6.6] to see that $J_o'/q^{|o|/2} \equiv 1$ modulo any prime of $\mathbb{Q}(\mu_e)$ over 2, so that $J_o'/q^{|o|/2} = \pm 1$. The rest of part (4) then follows from parts (1) and (2).

For (5), let $\mathcal{C}_d'$ and $\mathcal{D}_d'$ be given by $z^d = x(1-x)$ and $w^d = y(1-y)$, so that the function field of the quotient $(\mathcal{C}_d' \times \mathcal{D}_d')/\mu_d$ is generated by x, y, and zw. The function field of $\mathcal{E}_d'$ is generated by u', x' and y' with relation $y'^2 + x'y' + t'y' = x'^3 + u'^d x'^2$. It is easy to see that the assignments $u' \mapsto zw$, $x' \mapsto -(zw)^d/y$, and $y' \mapsto (zw)^d x(1-y)/y$ yield a well-defined isomorphism between the two function fields. (This is essentially the example discussed in [8, Section 7].) $\square$

We note that part (3) is an arithmetic reflection of the fact that the Fermat curve $\mathcal{C}_d'$ in part (5) is a twisted form of the Fermat curve $\mathcal{C}_d$ of the previous section. It follows from part (3) that $J_o'^2 = \chi^i(16)J_o^2$. This relation between the inverse roots of the

L-functions of E and E' is an arithmetic reflection of the identification $\mathbb{F}_q(u) = \mathbb{F}_q(u')$ and the resulting isogeny between E and E' when 16 is a d-th power in $\mathbb{F}_q{}^\times$.

We also note that if $p > 2$, $d > 2$ divides $p^f + 1$, and $q \equiv 1 \pmod{d}$, then 16 (and indeed any integer) is a d-th power in $\mathbb{F}_q$. Thus the rank result of [8, Thm. 7.5] can be recovered from the theorem.

Acknowledgements

References

[1] N. Aoki, *Simple factors of the Jacobian of a Fermat curve and the Picard number of a product of Fermat curves*, Am. J. Math. **113** (1991), 779–833.

[2] H. Cohen, *Number theory. Vol. I. Tools and Diophantine equations*, Vol. 239 of Graduate Texts in Mathematics, Springer, New York (2007).

[3] Z. Engberg, *On the distribution of balanced subgroups*, J. Number Theory **136** (2014), 287–319.

[4] C. Pomerance and D. Ulmer, *On balanced subgroups of the multiplicative group*, in 'Number Theory and Related Fields: In Memory of Alf van der Poorten', 253–270, Springer, New York (2013).

[5] T. Shioda, *On the Mordell–Weil lattices*, Comment. Math. Univ. St. Paul. **39** (1990), 211–240.

[6] T. Shioda and T. Katsura, *On Fermat varieties*, Tôhoku Math. J. (2) **31** (1979), 97–115.

[7] D. Ulmer, *Jacobi sums, Fermat Jacobians, and ranks of abelian varieties over towers of function fields*, Math. Res. Lett. **14** (2007), 453–467.

[8] ———, *On Mordell–Weil groups of Jacobians over function fields*, J. Inst. Math. Jussieu **12** (2013), 1–29.

[9] ———, *Explicit points on the Legendre curve*, J. Number Theory **136** (2014), 165–194.

[10] ———, *Curves and Jacobians over function fields*, in 'Arithmetic Geometry over Global Function Fields' (G. Boeckle et al., ed.), Advanced Courses in Mathematics CRM Barcelona, 281–337, Springer, Basel, 2014.

Oxford College of Emory University, Oxford, GA 30054, USA
E-mail address: `rconcei@emory.edu`

Department of Mathematics, University of Wyoming, Laramie, WY 82071, USA
E-mail address: `chall14@uwyo.edu`

School of Mathematics, Georgia Institute of Technology, Atlanta, GA 30332, USA
E-mail address: `ulmer@math.gatech.edu`