



ELSEVIER

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt



Explicit points on the Legendre curve [☆]

Douglas Ulmer

School of Mathematics, Georgia Institute of Technology, Atlanta, GA 30332, United States

ARTICLE INFO

Article history:

Received 6 May 2013

Received in revised form 19

September 2013

Accepted 20 September 2013

Available online xxxx

Communicated by David Goss

MSC:

11G05

11G40

Keywords:

Elliptic curves

Ranks

Conjecture of Birch and

Swinnerton-Dyer

ABSTRACT

We study the elliptic curve E given by $y^2 = x(x+1)(x+t)$ over the rational function field $k(t)$ and its extensions $K_d = k(\mu_d, t^{1/d})$. When k is finite of characteristic p and $d = p^f + 1$, we write down explicit points on E and show by elementary arguments that they generate a subgroup V_d of rank $d-2$ and of finite index in $E(K_d)$. Using more sophisticated methods, we then show that the Birch and Swinnerton-Dyer conjecture holds for E over K_d , and we relate the index of V_d in $E(K_d)$ to the order of the Tate–Shafarevich group $\text{III}(E/K_d)$. When k has characteristic 0, we show that E has rank 0 over K_d for all d .

© 2013 Elsevier Inc. All rights reserved.

1. Introduction

Throughout the paper, $p > 2$ is a prime number, \mathbb{F}_p is the field of p elements, \mathbb{F}_q is a finite extension of \mathbb{F}_p of cardinality q , and $\overline{\mathbb{F}}_p$ is an algebraic closure of \mathbb{F}_p . We write $\mathbb{F}_p(t)$, $\mathbb{F}_q(t)$, and $\overline{\mathbb{F}}_p(t)$ for the rational function fields over \mathbb{F}_p , \mathbb{F}_q , and $\overline{\mathbb{F}}_p$ respectively.

There are now several constructions of elliptic curves (and higher-dimensional Jacobians) of large rank over $\mathbb{F}_p(t)$ or $\overline{\mathbb{F}}_p(t)$. The first results in this direction are due to Shafarevich and Tate [TS67], and their arguments as well as more recent results

[☆] This paper is based upon work partially supported by the National Science Foundation under Grant No. DMS 0701053.

E-mail address: ulmer@math.gatech.edu.

on large ranks are discussed in [Ulm11]. Most of these constructions rely on relatively sophisticated mathematics, such as the theory of algebraic surfaces, cohomology, and L -functions.

Our first aim in this note is to give an explicit, elementary construction of points on a certain non-isotrivial elliptic curve over $\mathbb{F}_p(t)$, the Legendre curve. We then show that the rank of the group these points generate can be arbitrarily large. The arguments are elementary and could have been given fifty years ago.¹ It is remarkable that such a classical and well-studied object as the Legendre curve still has a few surprises.

Further pleasant surprises appear when we look deeper into the arithmetic of the Legendre curve. Specifically, we find that the index of the points we have constructed in the full Mordell–Weil group is a power of p , and the square of this index is the order of a Tate–Shafarevich group. This “class number formula” is reminiscent of formulas appearing in the contexts of cyclotomic units and of Heegner points. See Theorem 12.1 for a precise statement of our main results.

Here is an outline of the paper: In Sections 2 and 3, we write down the relevant curve and a collection of points on it, and in Section 4 we prove that the rank of the group they generate is large. The arguments require only elementary aspects of the theory of elliptic curves and Galois theory. Using slightly more advanced ideas, (namely Galois cohomology), in Section 5 we then calculate the exact rank of the Mordell–Weil group and see that our points generate a subgroup of finite index. The tools used up to this point will be familiar to anyone who has studied Silverman’s book [Sil09]. In Section 6 we compute the torsion subgroup, and in Sections 7 through 10, we use more sophisticated techniques (heights, L -functions, and the Birch and Swinnerton-Dyer formula) to bound the index and relate it to the Tate–Shafarevich group of E . Finally, in Section 11 we make a connection with our paper [Ulm13] and Berger’s construction, which yields strong results on the Birch and Swinnerton-Dyer conjecture for E .

There are several avenues for further exploration of the arithmetic of the Legendre curve, including a more general rank formula, more explicit points, and a full calculation of the Tate–Shafarevich group. These are stated more precisely at the end of Section 12 and will be taken up in subsequent publications.

This note came about as a result of conversations with Dick Gross at the 2009 IAS/Park City Mathematics Institute. It is a pleasure to thank the organizers of the meeting for the opportunity to give a course, the audience for their attention and comments, and Gross for his interest and incisive questions. Thanks are also due to Chris Hall for thought-provoking data on L -functions and stimulating conversations on questions related to the topics of this paper, and to Lisa Berger and Alice Silverberg for several useful comments.

The exposition of the final version of the paper was influenced by the possibility of generalizations to higher genus. These were worked out with an energetic group of

¹ We note that in [Ca09], Conceição gives an equally simple construction of polynomial points on certain isotrivial elliptic curves over $\mathbb{F}_p(t)$ and uses them to show that the rank is large.

mathematicians starting at an AIM workshop on “Cohomological methods in abelian varieties” in March, 2012. It is a pleasure to thank AIM, the organizers, and the participants for their collaboration, the fruits of which will appear in a future paper.

2. The elliptic curve E

We refer to [Ulm11] and the references there for basic results on elliptic curves over function fields. Throughout the paper, p will be an odd prime number and E will be the elliptic curve

$$E: y^2 = x(x + 1)(x + t) \tag{2.1}$$

over $\mathbb{F}_p(t)$ or one of its extensions. The j -invariant of E is

$$j(E) = \frac{256(t^2 - t + 1)^3}{t^2(t - 1)^2}$$

and the discriminant of the model (2.1) is

$$\Delta = 16t^2(t - 1)^2.$$

A word on the $+$ signs in the definition of E is in order. The term “Legendre curve” usually refers to the elliptic curve

$$E_L: y^2 = x(x - 1)(x - t).$$

The curve E is isomorphic to the quadratic twist

$$(-1)y^2 = x(x - 1)(x - t)$$

of E_L (via the change of coordinates $x \mapsto -x$). Whenever the ground field has a primitive 4-th root of unity i , there is an isomorphism $E \cong E_L$ which sends y to iy . In most of our work, the fourth roots of unity will be in the ground field. Even when they are not, it turns out that E is more convenient than E_L , and so we use E throughout and refer to it as “the Legendre curve.”

We will consider E and its arithmetic over various extensions of $K = \mathbb{F}_p(t)$. Specifically, for each power q of p and each integer d relatively prime to p , we have the extension field $\mathbb{F}_q(t^{1/d})$. We will also consider $\bar{\mathbb{F}}_p(t^{1/d})$ where $\bar{\mathbb{F}}_p$ is an algebraic closure of \mathbb{F}_p . When d is fixed, we sometimes simplify notation by setting $u = t^{1/d}$. The most important extensions for our study will be the fields $K_d = \mathbb{F}_p(\mu_d, t^{1/d})$ where μ_d denotes the d -th roots of unity in $\bar{\mathbb{F}}_p$. Note that if d divides $q - 1$, then $\mathbb{F}_q(t^{1/d})$ is a Galois extension of $K_1 = \mathbb{F}_p(t)$ whose Galois group is a semidirect product of two cyclic groups. We fix a primitive d -th root of unity in $\bar{\mathbb{F}}_p$ and denote it ζ_d .

Note that as an abstract field, $\mathbb{F}_q(t^{1/d}) = \mathbb{F}_q(u)$ is a rational function field over \mathbb{F}_q and so is isomorphic to $\mathbb{F}_q(t)$. Thus instead of fixing our curve E and varying the ground field, we could fix the ground field $\mathbb{F}_q(t)$ and vary the curve E . The former point of view will be more convenient for our purposes.

As an aside for experts, very little of what we do requires that d be relatively prime to p , but we assume this throughout for simplicity.

3. Several points on E

In this section we write down several points on E rational over various extensions of $\mathbb{F}_p(t)$.

First we have the points of order 2 visible immediately from the Weierstrass equation (2.1): let $Q_0 = (0, 0)$, $Q_1 = (-1, 0)$, and $Q_t = (-t, 0)$.

Next assume that d is an integer of the form $d = p^f + 1$ with f a non-negative integer. Over $K_d = \mathbb{F}_p(\mu_d, u)$ with $u^d = t$, E has the Weierstrass equation

$$y^2 = x(x + 1)(x + u^{p^f + 1})$$

and the rational point $P(u) = (u, u(u + 1)^{d/2})$. Indeed, evaluating the right hand side of (2.1) at $x = u$, we have

$$u(u + 1)(u + u^{p^f + 1}) = u^2(u + 1)(1 + u^{p^f}) = u^2(u + 1)^{p^f + 1} = u^2(u + 1)^d.$$

Since E is defined over $K = \mathbb{F}_p(t) \subset K_d$, applying elements of $\text{Gal}(K_d/K)$ to $P(u)$ we get a collection of points

$$P_i = P(\zeta_d^i u) = (\zeta_d^i u, \zeta_d^i u(\zeta_d^i u + 1)^{d/2}) \quad (i \in \mathbb{Z}/d\mathbb{Z}). \tag{3.1}$$

Occasionally we will want to discuss more than one value of d at a time, and when we do so we label the points above $P_i^{(d)}$ to emphasize that they are defined over K_d . It is not yet evident what connections there are between the $P_i^{(d)}$ for varying values of d .

We will see by elementary means in the next section that the points P_i ($i \in \mathbb{Z}/d\mathbb{Z}$) are almost independent—they generate a subgroup of $E(K_d)$ of rank $d - 2$. Using somewhat more technology, we will see in the following sections that they generate a subgroup of finite index, i.e., that the rank of $E(K_d)$ is $d - 2$.

One case can be dealt with immediately: Suppose that $f = 0$ so that $d = 2$. Then it is easy to see using the explicit formulas for addition on E that $P_0^{(2)}$ and $P_1^{(2)}$ have order 4. In fact, we find that $2P_0^{(2)} = Q_0$, and four points of order exactly 4 on $E(K_d)$ are:

$$P_0^{(2)}, \quad -P_0^{(2)} = P_0^{(2)} + Q_0, \quad P_1^{(2)} = P_0^{(2)} + Q_1, \quad \text{and} \quad -P_1^{(2)} = P_0^{(2)} + Q_t.$$

We will see later (Proposition 6.1) that the torsion in $E(\overline{\mathbb{F}}_p(t^{1/d}))$ is generated by Q_0 and Q_1 when d is odd, and by $P_0^{(2)}$ and Q_1 when d is even.

Using the points $P_i^{(2)}$, we can see by elementary means certain relations among the $P_i^{(d)}$.

Proposition 3.2. *Suppose that $f \geq 1$ and $d = p^f + 1$. Then we have the following equalities in the Mordell–Weil group $E(K_d)$:*

$$\sum_{i=0}^{d-1} P_i^{(d)} = Q_t \quad \text{and} \quad \sum_{i=0}^{d-1} (-1)^i P_i^{(d)} = Q_1.$$

Proof. Consider the rational function $f = y - x(x+1)^{d/2}$ on E . Because f is a polynomial in x and y , it is regular away from O , the origin of E , and it has a pole there of order $d + 2$. It is easy to see that f vanishes at each P_i ($i \in \mathbb{Z}/d\mathbb{Z}$) and at Q_0 and Q_1 . (Here and below, we write P_i for $P_i^{(d)}$.) Since the degree of the divisor of f is zero, f must vanish simply at each of these points. Thus we have

$$\text{div}(f) = \sum_{i \in \mathbb{Z}/d\mathbb{Z}} [P_i] + [Q_0] + [Q_1] - (d + 2)[O].$$

Abel’s theorem then yields

$$\sum_{i \in \mathbb{Z}/d\mathbb{Z}} P_i = -Q_0 - Q_1 = Q_t$$

in $E(K_d)$.

The second equality in the statement of the proposition follows similarly from a consideration of the rational function $g = x^{d/2-1}y - t^{1/2}(x + 1)^{d/2}$ whose divisor is

$$\text{div}(g) = \sum_{i \in \mathbb{Z}/d\mathbb{Z}} [(-1)^i P_i] + [Q_1] - (d + 1)[O].$$

We leave the details of this case as an exercise for the reader. \square

Remark 3.3. Adding and subtracting the two relations above, we find that

$$2 \sum_{i \in 2\mathbb{Z}/d\mathbb{Z}} P_i = 2 \sum_{i \in 2\mathbb{Z}/d\mathbb{Z}} P_{i+1} = Q_0.$$

Thus the two sums are points of order 4. We will see below (Proposition 8.4) that

$$\sum_{i \in 2\mathbb{Z}/d\mathbb{Z}} P_i = P_{1+d/2}^{(2)} \quad \text{and} \quad \sum_{i \in 2\mathbb{Z}/d\mathbb{Z}} P_{i+1} = P_{d/2}^{(2)}.$$

These will turn out to be the only relations among the P_i (for a fixed value of d).

4. A lower bound on the rank

In this section we give a very simple proof that the rank of $E(K_d)$ is unbounded as d varies. Experts will see that the argument uses a coboundary map in Galois cohomology, but to make this section as accessible as possible we argue from first principles.

Proposition 4.1. *Let d be a positive integer not divisible by p and write ζ_d for a fixed primitive d -th root of unity in \mathbb{F}_p . Let $F = \mathbb{F}_q(t^{1/d}) = \mathbb{F}_q(u)$. Then the map $E(F) \rightarrow (\mathbb{Z}/2\mathbb{Z})^d$ which sends*

$$P = (x, y) \mapsto \begin{cases} (\text{ord}_{u=\zeta_d^j}(x+1) \pmod{2})_{j=0,\dots,d-1} & \text{if } P \neq (-1, 0) \text{ and } P \neq O, \\ (1, \dots, 1) & \text{if } P = (-1, 0), \\ (0, \dots, 0) & \text{if } P = O \end{cases}$$

induces a homomorphism $\nu : E(F)/2E(F) \rightarrow (\mathbb{Z}/2\mathbb{Z})^d$. Suppose further that $d = p^f + 1$ and let q be a power of p such that d divides $q - 1$. Then the homomorphism ν maps the subgroup of $E(F)$ generated by the points P_i ($i \in \mathbb{Z}/d\mathbb{Z}$) surjectively onto $(\mathbb{Z}/2\mathbb{Z})^d$.

Proof. Suppose we are given an elliptic curve E' in Weierstrass form

$$Y^2 = X^3 + a_2X^2 + a_4X$$

over a field k of characteristic $\neq 2$. Note that the point $(0, 0)$ on E' is of order 2. We claim that the map $E'(k) \rightarrow k^\times$ that sends

$$P = (X, Y) \mapsto \begin{cases} X & \text{if } X \neq 0 \text{ and } P \neq O, \\ a_4 & \text{if } X = 0, \\ 1 & \text{if } P = O \end{cases}$$

induces a homomorphism $E'(k)/2E'(k) \rightarrow k^\times/k^{\times 2}$ (where $k^\times/k^{\times 2}$ denotes the multiplicative group of k modulo squares). Indeed, if we have three points in $E'(k)$ with $P_1 + P_2 = P_3$, then P_1, P_2 , and $-P_3$ lie on a line $Y = \lambda X + \nu$, and the X -coordinates $X_i = X(P_i)$ are the three roots of

$$(\lambda X + \nu)^2 = X^3 + a_2X^2 + a_4X$$

or equivalently of

$$0 = X^3 + (a_2 - \lambda^2)X^2 + (a_4 - 2\lambda\nu)X - \nu^2.$$

If none of the X_i are 0, it follows that $X_1X_2X_3 = \nu^2$ and so $X_3 = X_1X_2$ in $k^\times/k^{\times 2}$. If one of the $X_i = 0$, say $X_1 = 0$ for concreteness, then we have $X_2X_3 = a_4$ and so $X_3 = a_4X_2$ in $k^\times/k^{\times 2}$. The cases where $X_2 = 0$ or $X_3 = 0$ are similar. This shows that

we have a homomorphism $E'(k) \rightarrow k^\times/k^{\times 2}$. Since the target is a group of exponent 2, we get an induced homomorphism $E'(k)/2E'(k) \rightarrow k^\times/k^{\times 2}$ as claimed.

Now we apply this observation to the Legendre curve over $k = F$ with the change of coordinates $X = x + 1, Y = y$. We get a homomorphism $E(F)/2E(F) \rightarrow F^\times/F^{\times 2}$ defined by

$$P = (x, y) \mapsto \begin{cases} x + 1 & \text{if } x \neq -1, \\ 1 - t & \text{if } x = -1. \end{cases}$$

Next we compose with the homomorphism $F^\times/F^{\times 2} \rightarrow (\mathbb{Z}/2\mathbb{Z})^d$ that sends the class of $z \in F^\times$ to $(\text{ord}_{u=\zeta_d^j}(z) \pmod{2})_{j=0,\dots,d-1}$. Noting that $1 - t = 1 - u^d$ vanishes simply at each of the points $u = \zeta_d^j$, we see that we have a homomorphism $\nu : E(F)/2E(F) \rightarrow (\mathbb{Z}/2\mathbb{Z})^d$ given by the formula in the statement of the proposition.

Now assume that $d = p^f + 1$ and d divides $q - 1$ so that the points P_i lie in $E(F)$. Then it is easy to see that the point $P_i = (\zeta_d^i u, \zeta_d^i u (\zeta_d^i u + 1)^{d/2})$ maps to the vector in $(\mathbb{Z}/2\mathbb{Z})^d$ with a 1 in the position labeled by j with $j \equiv (d/2) - i \pmod{d}$ and zeroes elsewhere. Thus the subgroup of $E(F)$ generated by the P_i maps surjectively onto $(\mathbb{Z}/2\mathbb{Z})^d$.

This completes the proof of the proposition. \square

For the statement of the next result, suppose that $d = p^f + 1$ and let G be the quotient of the free abelian group \mathbb{Z}^d by the subgroup generated by the vectors

$$(2, -2, 2, -2, \dots, 2, -2)$$

(with 2s and -2 s alternating) and

$$(2, 2, \dots, 2)$$

(all entries equal to 2). We have

$$G \cong \mathbb{Z}^{d-2} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}. \tag{4.2}$$

By Proposition 3.2, the map $\mathbb{Z}^d \rightarrow E(K_d), (a_0, \dots, a_{d-1}) \mapsto \sum_i a_i P_i$ factors through G . Moreover, the 2-torsion points of $E(K_d)$ are all images of 2-torsion elements of G .

Corollary 4.3. *For $d = p^f + 1$ and $K_d = \mathbb{F}_p(\mu_d, t^{1/d})$, we have $\text{Rank } E(K_d) \geq d - 2$. More precisely, the subgroup of $E(K_d)$ generated by the P_i ($i \in \mathbb{Z}/d\mathbb{Z}$) is isomorphic to G .*

Proof. By definition, the subgroup of $E(K_d)$ generated by the P_i is the image of the homomorphism $G \rightarrow E(K_d)$. On the other hand, since $d = p^f + 1$ and K_d contains the d -th roots of unity, Proposition 4.1 shows that the composed map $G/2G \rightarrow E(K_d)/2E(K_d) \xrightarrow{\nu} (\mathbb{Z}/2\mathbb{Z})^d$ is surjective, and therefore an isomorphism. Thus $G/2G \rightarrow E(K_d)/2E(K_d)$ is injective. If $a = (a_0, \dots, a_{d-1}) \in \mathbb{Z}^d$ maps to zero in $E(K_d)$, i.e., if $\sum_i a_i P_i = O$, then it follows that a is zero in $G/2G$, i.e., $a = 2a'$ for some element

$a' \in G$. Now a' maps to a 2-torsion point in $E(K_d)$, and since the 2-torsion of G maps onto the 2-torsion of $E(K_d)$, we may modify a' so that we still have $a = 2a'$ and a' goes to zero in $E(K_d)$. But now $a' = 2a''$ for some a'' in G . Iterating the argument, we see that a is divisible in G by arbitrarily large powers of 2. But we see from Eq. (4.2) that G has no non-trivial elements divisible by arbitrarily large powers of 2. This implies that $a = 0$. Thus $G \rightarrow E(K_d)$ is injective and this finishes the proof of the corollary. \square

Using Galois theory, we can estimate the rank of $E(\mathbb{F}_q(t^{1/d}))$ for any q and any divisor d of $p^f + 1$.

Corollary 4.4. *If d divides $p^f + 1$ for some f , q is any power of p , and $F = \mathbb{F}_q(t^{1/d})$, we have*

$$\text{Rank } E(F) \geq \sum_{\substack{e|d \\ e > 2}} \frac{\varphi(e)}{o_q(e)}$$

where the sum is over divisors e of d greater than 2, φ is Euler’s function, and $o_q(e)$ is the order of q in $(\mathbb{Z}/e\mathbb{Z})^\times$.

Remark 4.5. The corollary gives an elementary and constructive proof that for every odd p there is a non-isotrivial elliptic curve over the rational function field $\mathbb{F}_p(u)$ with arbitrarily large rank. Indeed, if we take $d = p^f + 1$ and $q = p$, then $o_q(e) \leq 2f$ for all divisors e of d . Thus over $F = \mathbb{F}_p(t^{1/d}) \cong \mathbb{F}_p(u)$, we have $\text{Rank } E(F) \geq (p^f - 1)/(2f)$. The same result is also known for $p = 2$; see [Ulm13, 8.1 and 8.2].

Proof of Corollary 4.4. Choose an f such that d divides $d' = p^f + 1$ and q divides $|\mathbb{F}_p(\mu_{d'})| = p^{2f}$. Then F is a subfield of $K_{d'} = \mathbb{F}_p(\mu_{d'}, t^{1/d'})$ and $K_{d'}/F$ is a Galois extension with Galois group $G = \text{Gal}(K_{d'}/F)$. We have rational points $P_i \in E(K_{d'})$ for $i \in \mathbb{Z}/d'\mathbb{Z}$. We will take the trace of these points down to $E(F)$ and see that they give the desired lower bound on the rank. More precisely we will compute the rank of the subgroup of $E(F) = E(K_{d'})^G$ generated by certain Galois invariant elements of the subgroup of $E(K_{d'})$ generated by the P_i .

The Galois group of $K_{d'}$ over F is a semidirect product. More precisely, choosing a primitive d' -th root of unity ζ , we have an identification:

$$\text{Gal}(K_{d'}/F) \cong (d\mathbb{Z}/d'\mathbb{Z}) \rtimes \langle \text{Fr}_q \rangle.$$

Here $\langle \text{Fr}_q \rangle$ is the cyclic group of order $[\mathbb{F}_q(\mu_{d'}) : \mathbb{F}_q]$ generated by the q -power Frobenius acting trivially on $t^{1/d'}$ and as usual on $\mathbb{F}_q(\mu_{d'}) \subset K_{d'}$, and $jd \in d\mathbb{Z}/d'\mathbb{Z}$ acts trivially on $\mathbb{F}_q(\mu_{d'}) \subset K_{d'}$ and sends $t^{1/d'}$ to $\zeta^{jd}t^{1/d'}$.

Looking back at the definition of P_i , it is clear that the orbit of P_i under $\text{Gal}(K_{d'}/F)$ consists of all points P_j where $j \equiv q^a i \pmod{d}$ for some power q^a of q . Summing all the

points in the orbit yields a rational point in $E(F)$. If $o \subset \mathbb{Z}/d'\mathbb{Z}$ is an orbit, we write P_o for the corresponding sum.

To estimate the rank, we first note that the number of orbits is

$$r = \sum_{e|d} \frac{\varphi(e)}{o_q(e)}.$$

(The orbit through P_i is counted in the term corresponding to $e = d/\gcd(d, i)$.) It is easy to see, using Proposition 4.1, that the points just constructed are linearly independent in $E(K)/2E(K) \cong (\mathbb{Z}/2\mathbb{Z})^{d'}$. Thus the rank of the subgroup of $E(F)$ they generate is $r - s$ where 2^s is the number of 2-torsion points in the span of the P_o .

By Proposition 3.2, the 2-torsion point Q_t is the sum over all orbits o of P_o . Again using Proposition 3.2, it is easy to see that the 2-torsion point Q_0 is in the span of the P_o if and only if d is even. Thus $s = 1$ if d is odd and $s = 2$ if d is even. This gives the formula for the rank of $E(F)$ in the statement of the corollary. \square

Examples 4.6.

- (1) Suppose that $p \equiv 3 \pmod{4}$, $d = 4$, and $q = p$. Let $d' = p + 1$, $F = \mathbb{F}_p(t^{1/4})$, and $K = K_{d'}$. We have points $P_i \in E(K)$ ($i \in \mathbb{Z}/d'\mathbb{Z}$). There are three orbits of $\text{Gal}(K/F)$ on the P_i :

$$\begin{aligned} o_0 &= \{P_i \mid i \in \mathbb{Z}/d'\mathbb{Z} \text{ and } i \equiv 0 \pmod{4}\}, \\ o_{13} &= \{P_i \mid i \in \mathbb{Z}/d'\mathbb{Z} \text{ and } i \equiv 1 \pmod{4} \text{ or } i \equiv 3 \pmod{4}\}, \\ o_2 &= \{P_i \mid i \in \mathbb{Z}/d'\mathbb{Z} \text{ and } i \equiv 2 \pmod{4}\}. \end{aligned}$$

We have $P_{o_0} + P_{o_{13}} + P_{o_2} = Q_t$ and $P_{o_0} - P_{o_{13}} + P_{o_2} = Q_0$, and the subgroup of $E(F)$ generated by P_{o_0} , $P_{o_{13}}$, and P_{o_2} has rank 1.

- (2) Now suppose that $p \equiv 3 \pmod{4}$, $d = 4$, and $q = p^2$. The situation is similar to the previous example, except that the orbit o_{13} breaks up into two orbits

$$\begin{aligned} o_1 &= \{P_i \mid i \in \mathbb{Z}/d'\mathbb{Z} \text{ and } i \equiv 1 \pmod{4}\}, \\ o_3 &= \{P_i \mid i \in \mathbb{Z}/d'\mathbb{Z} \text{ and } i \equiv 3 \pmod{4}\} \end{aligned}$$

and the subgroup of $E(F)$ generated by P_{o_0}, \dots, P_{o_3} has rank 2.

- (3) Suppose now that $d = d' = p + 1$ and $q = p$. Let $K = K_{d'} = \mathbb{F}_{p^2}(t^{1/(p+1)})$ and $F = \mathbb{F}_p(t^{1/(p+1)})$. Then $\text{Gal}(K/F)$ has order 2, generated by the Frobenius Fr_p . The orbits of Galois on the P_i are $\{P_0\}$, $\{P_{d/2}\}$, and $\{P_i, P_{-i}\}$ for $1 \leq i \leq (p-1)/2$. We find that the subgroup of $E(F)$ generated by the P_o has rank $(p-1)/2$.
- (4) We can make the previous example more explicit. For an integer i in the range $1 \leq i \leq (p-1)/2$, let $b = \zeta_d^i + \zeta_d^{pi} = \zeta_d^i + \zeta_d^{-i} \in \mathbb{F}_p$ so that the roots of $x^2 - bx + 1$ are ζ_d^i and ζ_d^{pi} . Then computing with the standard formulas leads to an expression

for $P_{\{i,-i\}} = P_i + P_{-i}$ in terms of b . More precisely, we find that the x coordinate of $P_{\{i,-i\}}$ is

$$\frac{2u^{p+1} + bu^p + bu + 2 - 2(u^2 + ub + 1)^{d/2}}{b^2 - 4}.$$

(We omit the y coordinate, which is even more unwieldy.) This example suggests that the coordinates of the points P_o may in general be rather complicated.

5. An upper bound on the rank

In this section we compute the Selmer group of E for multiplication by 2 and complete the calculation of the rank of E when d divides $p^f + 1$ for some f .

Throughout, we fix a value of d (prime to p as always) and a power q of p . Let $F = \mathbb{F}_q(t^{1/d}) = \mathbb{F}_q(u)$ and let F^{sep} be a separable closure of F . Write G_F for $\text{Gal}(F^{sep}/F)$.

We have an exact sequence of G_F -modules:

$$0 \rightarrow E[2] \rightarrow E(F^{sep}) \xrightarrow{2} E(F^{sep}) \rightarrow 0 \tag{5.1}$$

where “2” denotes the multiplication-by-2 homomorphism and $E[2] \subset E(F) \subset E(F^{sep})$ is its kernel.

Taking Galois cohomology leads to an injection

$$0 \rightarrow E(F)/2E(F) \xrightarrow{\lambda} H^1(G_F, E[2]).$$

For each place v of F , we have the completion F_v , its separable closure F_v^{sep} , and the Galois group $G_{F_v} = \text{Gal}(F_v^{sep}/F_v)$. There is a short exact sequence analogous to (5.1) yielding an injection

$$0 \rightarrow E(F_v)/2E(F_v) \xrightarrow{\lambda_v} H^1(G_{F_v}, E[2]).$$

The field inclusion $F \subset F_v$ and the induced restriction maps of Galois groups $G_{F_v} \hookrightarrow G_F$ lead to a diagram

$$\begin{array}{ccccc} 0 & \longrightarrow & E(F)/2E(F) & \xrightarrow{\lambda} & H^1(G_F, E[2]) \\ & & \downarrow & & \downarrow r \\ 0 & \longrightarrow & \prod_v E(F_v)/2E(F_v) & \xrightarrow{\prod_v \lambda_v} & \prod_v H^1(G_{F_v}, E[2]) \end{array}$$

We define the 2-Selmer group $\text{Sel}_2(E/F)$ to be $r^{-1}(\text{Im}(\prod_v \lambda_v))$. In other words, $\text{Sel}_2(E/F)$ consists of classes $c \in H^1(G_F, E[2])$ such that for all v , the component of $r(c)$

indexed by v lies in the image of $E(F_v)/2E(F_v) \rightarrow H^1(G_{F_v}, E[2])$. Since the diagram above is commutative, we have an injection

$$0 \rightarrow E(F)/2E(F) \xrightarrow{\lambda} \text{Sel}_2(E/F).$$

Choosing a basis of $E[2]$ yields an identification $E[2] \cong \mu_2^2$ of G_F -modules. In the calculations below, we always use the basis $\{Q_0, Q_1\}$. Kummer theory yields an isomorphism $H^1(G_F, \mu_2) \cong F^\times/F^{\times 2}$ and so the Selmer group $\text{Sel}_2(E/F)$ is a subgroup of $(F^\times/F^{\times 2})^2$.

We define a homomorphism

$$\lambda' : \text{Sel}_2(E/F) \rightarrow (\mathbb{Z}/2\mathbb{Z})^d$$

as the composition of the inclusion $\text{Sel}_2(E/F) \subset (F^\times/F^{\times 2})^2$ and the map

$$(F^\times/F^{\times 2})^2 \rightarrow (\mathbb{Z}/2\mathbb{Z})^d$$

$$[a, b] \mapsto (\text{ord}_{u=\zeta_d^j} b \pmod{2})_{j=0, \dots, d-1}.$$

Proposition 5.2. *Recall that $F = \mathbb{F}_q(t^{1/d}) = \mathbb{F}_q(u)$ and E is the elliptic curve given by Eq. (2.1). Assume that d divides $q - 1$.*

(1) *The composed homomorphism*

$$E(F)/2E(F) \xrightarrow{\lambda} \text{Sel}_2(E/F) \xrightarrow{\lambda'} (\mathbb{Z}/2\mathbb{Z})^d$$

is equal to the map ν appearing in Proposition 4.1.

- (2) *If d is even then λ' is injective. Its image has order 2^d if $2d$ divides $q - 1$, order 2^{d-2} if $(q - 1)/d$ is odd and $q \equiv 1 \pmod{4}$, and order 4 if $q \equiv 3 \pmod{4}$.*
- (3) *If d is odd and $q \equiv 1 \pmod{4}$ then λ' is surjective with kernel of order 2. If d is odd and $q \equiv 3 \pmod{4}$ then λ' is injective with image of order 4.*

Before proving the proposition, we state several corollaries.

Corollary 5.3.

- (1) *If d is even, then $\text{Rank } E(F) \leq d - 2$.*
- (2) *If d is odd, then $\text{Rank } E(F) \leq d - 1$.*
- (3) *If $d = p^f + 1$ and d divides $q - 1$, then $\text{Rank } E(F) = d - 2$.*
- (4) *More generally, if d divides $p^f + 1$ for some f , then*

$$\text{Rank } E(F) = \sum_{\substack{e|d \\ e > 2}} \frac{\varphi(e)}{o_q(e)}$$

where the sum is over divisors e of d greater than 2, φ is Euler’s function, and $o_q(e)$ is the order of q in $(\mathbb{Z}/e\mathbb{Z})^\times$.

Proof. For the upper bounds, we may extend the finite field q and so we may assume that $2d$ divides $q - 1$ when d is even and $4d$ divides $q - 1$ when d is odd. Proposition 5.2 then shows that $\text{Sel}_2(E/F)$ has cardinality 2^d when d is even and 2^{d+1} when d is odd. Since E has two independent points of order 2 defined over $\mathbb{F}_p(t) \subset F$, it follows that $\text{Rank } E(F)$ is bounded above by $d - 2$ when d is even and by $d - 1$ when d is odd. This establishes the first two claims. The third claim is immediate from the first and the lower bound in Corollary 4.3.

To establish the last claim, choose a value of f so that d divides $d' = p^f + 1$ and q divides p^{2f} , in which case F is a subfield of $K_{d'} = \mathbb{F}_p(\mu_{d'}, t^{1/d'})$. Then $K_{d'}$ is Galois over F and we write G for $\text{Gal}(K_{d'}/F)$. Write $V_{d'}$ for the subgroup of $E(K_{d'})$ generated by $P_i^{(d')}$ ($i \in \mathbb{Z}/d'\mathbb{Z}$). The lower bound of Corollary 4.3 together with Proposition 5.2 shows that $V_{d'}$ has finite index in $E(K_{d'})$. Taking Galois invariants, we find that $V_{d'}^G$ has finite index in $E(F) = E(K_{d'})^G$. On the other hand, the proof of the lower bound of Corollary 4.4 constructs a submodule of $V_{d'}^G$ of finite index and rank equal to $\sum_{\substack{e|d \\ e>2}} \frac{\varphi(e)}{o_q(e)}$. This gives the rank asserted in the corollary. \square

Proof of Proposition 5.2. We use [BK77] as a general reference for 2-descent; it has fairly complete results on the 2-Selmer group for elliptic curves over local and global fields of characteristic $\neq 2$.

To prove the first part of the proposition, we note from [BK77, §2] that under the identification $H^1(F, E[2]) \cong (F^\times/F^{\times 2})^2$, the coboundary homomorphism $E(F) \rightarrow H^1(F, E[2])$ becomes the map

$$E(F) \rightarrow (F^\times/F^{\times 2})^2$$

$$P = (x, y) \mapsto \begin{cases} [x, x + 1] & \text{if } P \neq Q_0, Q_1, O, \\ [t, 1] & \text{if } P = Q_0, \\ [-1, 1 - t] & \text{if } P = Q_1, \\ [1, 1] & \text{if } P = O. \end{cases}$$

(Here and below we use square brackets to denote the class of an element $a \in F^\times$ or a pair $(a, b) \in (F^\times)^2$ in a quotient group.) It is immediate from this formula that the composition $\lambda'\lambda$ is equal to ν .

For the second and third parts of the proposition, we need to compute the Selmer group explicitly. For each place v of F , we write $\text{Sel}_2(E/F_v)$ for the local Selmer group, i.e., for the image of the coboundary map

$$E(F_v) \rightarrow H^1(F_v, E[2]) \cong (F_v^\times/F_v^{\times 2})^2.$$

Recall that the ambient group $(F_v^\times/F_v^{\times 2})^2$ has order 16. By [BK77, Lemma 3.1], the local Selmer group has order 4.

In order to apply the local results of [BK77], we need to know the reduction types of E at the places of F . Using Tate’s algorithm [Tat75], we find that E has good reduction away from $u = 0$, $u \in \mu_d$, and $u = \infty$. At $u = 0$ the reduction is split multiplicative for any value of q . At places with $u \in \mu_d$, the reduction is split multiplicative when $q \equiv 1 \pmod{4}$, and non-split multiplicative when $q \equiv 3 \pmod{4}$. At $u = \infty$, the reduction is additive when d is odd and split multiplicative (for any q) when d is even.

To describe $\text{Sel}_2(E/F_v)$ explicitly, let \mathcal{O}_v be the ring of integers of F_v and let π_v be a uniformiser at v . At places where E has good reduction [BK77, Cor. 3.3] says that the local Selmer group is

$$\text{Sel}_2(E/F_v) = (\mathcal{O}_v^\times/\mathcal{O}_v^{\times 2})^2 \subset (F_v^\times/F_v^{\times 2})^2.$$

The local Selmer group at places of split multiplicative reduction is given by [BK77, Prop. 4.1]. That result tells us that at $u = 0$ the local group is $(F_v^\times/F_v^{\times 2}) \times \{1\}$, at places with $u \in \mu_d$, when $q \equiv 1 \pmod{4}$ the local group is $\{1\} \times (F_v^\times/F_v^{\times 2})$, and at $u = \infty$, when d is even the local group is

$$\{[a, b] \in (F_v^\times/F_v^{\times 2})^2 \mid a = b\}.$$

The local Selmer group at places of non-split multiplicative reduction is given by [BK77, Prop. 4.3]. That result tells us that at places with $u \in \mu_d$, when $q \equiv 3 \pmod{4}$ the local group is generated by $[-1, \pi_v]$ and $[-1, -\pi_v]$ where π_v is a uniformiser at v .

Unfortunately, [BK77] does not give the local Selmer group in general for places of additive reduction. However, we can determine it by exhibiting explicit classes. Namely, if we apply the coboundary map

$$E(F) \rightarrow (F^\times/F^{\times 2})^2 \rightarrow (F_\infty^\times/F_\infty^{\times 2})^2$$

at the place $u = \infty$ to the points Q_0 and Q_1 , we obtain non-trivial elements $[t, 1] = [\pi_\infty, 1]$ and $[-1, 1 - t] = [-1, -\pi_\infty]$. (Here the square brackets indicate classes in $(F_\infty^\times/F_\infty^{\times 2})^2$.) Since the local Selmer group has order 4, it must be generated by these classes. Note that if $q \equiv 1 \pmod{4}$ then -1 is a square in \mathbb{F}_q and $[-1, -\pi_\infty] = [1, \pi_\infty]$.

We can now describe the global Selmer group when d is even. First assume that $2d$ divides $q - 1$. We use crucially that the Picard group of \mathbb{P}^1 is trivial, so that every divisor of degree 0 is the divisor of a function. If $[a, b]$ is in the Selmer group, then the divisor of b has the form $D_1 + 2D_2$ where D_1 is supported on the places $u \in \mu_d$ and $u = \infty$. Modifying b by a square, we may assume that b is a polynomial in u whose zeroes are all in μ_d and that these zeroes have order 0 or 1. The local condition at $u = 0$ then requires that the value of b at $u = 0$ should be a square; modifying by the square of an element

of \mathbb{F}_q^\times , we may assume that the value of b at $u = 0$ is 1. We have thus put b in the standard form

$$b = \prod_{j=0, \dots, d-1} (1 - u\zeta_d^j)^{e_j}$$

where (e_0, \dots, e_{d-1}) is an arbitrary tuple in $\{0, 1\}^d$. Now consider the local conditions on a . Modifying a by a square, we may assume that a is regular away from 0 and ∞ , so it has the form cu^f where $c \in \mathbb{F}_q$ and where we may take $f = 0$ or $f = 1$. Since the value of a must be a square at places where $u \in \mu_d$, and since our hypotheses imply that a d -th root ζ_d is a square in \mathbb{F}_q , we must have that c is a square; modifying a by the square of a scalar, we may take c to be 1. Finally, the local condition at ∞ implies that $f \equiv \sum_j e_j \pmod{2}$. Summarizing, we have that when d is even and $2d$ divides $q - 1$, $\text{Sel}_2(E/F)$ consists of classes $[a, b] \in (F^\times/F^{\times 2})^2$ represented by pairs (a, b) of the form

$$a = u^f, \quad b = \prod_{j=0, \dots, d-1} (1 - u\zeta_d^j)^{e_j}$$

where $(e_0, \dots, e_{d-1}) \in \{0, 1\}^d$ is arbitrary and $f \in \{0, 1\}$ satisfies $f \equiv \sum_j e_j \pmod{2}$. It is immediate that the map

$$\begin{aligned} \text{Sel}_2(E/F) &\xrightarrow{\lambda'} (\mathbb{Z}/2\mathbb{Z})^d \\ [a, b] &\mapsto (\text{ord}_{u=\zeta_d^j} b \pmod{2})_{j=0, \dots, d-1} \end{aligned}$$

is an isomorphism.

The argument when d is even, $(q - 1)/d$ is odd, and $q \equiv 1 \pmod{4}$ is very similar, except in this case ζ_d is not a square in \mathbb{F}_q . We find that f must be even and c must be a square above (i.e., we may take $a = 1$). The local conditions at $u = \infty$ then imply that the allowable tuples (e_0, \dots, e_{d-1}) are those that satisfy $\sum_j e_j \equiv \sum_j j e_j \equiv 0 \pmod{2}$. Thus in this case λ' is injective and its image has order 2^{d-2} .

Now we assume that $q \equiv 3 \pmod{4}$. The argument is the same whether d is even or odd. Considering the projection of the local Selmer group to the first factor $F_v^\times/F_v^{\times 2}$, we see that a must be equivalent mod squares to cu^f where $c \in \{\pm 1\}$ and $f \in \{0, 1\}$. Considering the projection to the second factor, we see that we may again take b of the form $\prod_j (1 - u\zeta_d^j)^{e_j}$. On the other hand, the local conditions at $u \in \mu_d$, where we have non-split multiplicative reduction, link a and b . More precisely, they require that $\text{ord}_v(b)$ be odd exactly when the value of a at v is a non-square. Thus a determines b . It follows that the order of the global Selmer group is at most 4. One may argue directly that it is exactly 4, or note that the images of Q_0 and Q_1 already generate a subgroup of order 4. We note that the image of λ' in this case is the subgroup of $(\mathbb{Z}/2\mathbb{Z})^d$ generated by $(1, 0, 1, 0, \dots, 1, 0)$ and $(0, 1, 0, 1, \dots, 0, 1)$, and λ' is again injective.

The last case to be dealt with is when d is odd and $q \equiv 1 \pmod{4}$. This case is very similar to the case where d is even and $2d$ divides $q - 1$, the only difference being the

local conditions at $u = \infty$. By an argument similar to that above, we see that a class $[a, b]$ in $\text{Sel}_2(E/F)$ can be represented by a pair (a, b) with

$$a = u^f, \quad b = \prod_{j=0, \dots, d-1} (1 - u\zeta_d^j)^{e_j}$$

where $(e_0, \dots, e_{d-1}) \in \{0, 1\}^d$ and $f \in \{0, 1\}$ are arbitrary. It is immediate that λ' is surjective with kernel of order 2.

This completes the proof of the proposition. \square

6. Torsion

To complete the elementary part of our analysis of the arithmetic of E , we compute the torsion subgroup of $E(\mathbb{F}_q(t^{1/d}))$.

Proposition 6.1. *Let d be a positive integer not divisible by p . If d is odd, then*

$$E(\mathbb{F}_p(t^{1/d}))_{\text{tor}} = E(\overline{\mathbb{F}}_p(t^{1/d}))_{\text{tor}} \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}).$$

If d is even, then

$$E(\mathbb{F}_p(t^{1/d}))_{\text{tor}} = E(\overline{\mathbb{F}}_p(t^{1/d}))_{\text{tor}} \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z}).$$

Proof. We have already seen in Section 3 that the torsion subgroup of $E(\mathbb{F}_p(t^{1/d}))$ is at least as large as what is asserted in the proposition. Thus it will suffice to prove that the torsion subgroup of $E(\overline{\mathbb{F}}_p(t^{1/d}))$ is no larger than what is asserted.

We work one prime at a time, starting with 2-power torsion. If d is odd, then the subgroup of $E(\overline{\mathbb{F}}_p(t^{1/d}))$ generated by the 2-torsion points Q_0 and Q_1 maps injectively to $(\mathbb{Z}/2\mathbb{Z})^d$ under the map in the display in Proposition 4.1 (for any value of q). Thus no non-trivial combination of these points is divisible by 2 in $E(\overline{\mathbb{F}}_p(t^{1/d}))$ and so the 2-power-torsion subgroup of $E(\overline{\mathbb{F}}_p(t^{1/d}))$ is generated by Q_0 and Q_1 . Similarly, when d is even, we have a subgroup of $E(\overline{\mathbb{F}}_p(t^{1/d}))$ isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ generated by Q_1 and $P_0^{(2)}$, call it H . Under the displayed map in Proposition 4.1, $H/2H$ maps injectively to $(\mathbb{Z}/2\mathbb{Z})^d$ (for any value of q), so again we find that the 2-power torsion of $E(\overline{\mathbb{F}}_p(t^{1/d}))$ is generated by Q_1 and $P_0^{(2)}$.

Since the j -invariant of E is visibly not a p -th power in $\overline{\mathbb{F}}_p(t^{1/d})$, Proposition I.7.3 of [Ulm11] implies that E has no non-trivial p -torsion points over that field.

To finish, we must show that for all primes ℓ not dividing $2p$, E has no non-trivial ℓ -torsion points defined over $\overline{\mathbb{F}}_p(t^{1/d})$ for any d . For this we may assume that d is even, and we assume so for the rest of the proof. Suppose then that we had a point of order ℓ . Then we would have an injection $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\ell\mathbb{Z} \hookrightarrow E(\overline{\mathbb{F}}_p(t^{1/d}))$. This would lead to a morphism $\mathbb{P}^1 \rightarrow X(2, 4\ell)$ where \mathbb{P}^1 is the curve over $\overline{\mathbb{F}}_p$ whose function field is $\overline{\mathbb{F}}_p(t^{1/d}) \cong \overline{\mathbb{F}}_p(u)$ and $X(2, 4\ell)$ is the modular curve over $\overline{\mathbb{F}}_p$ parameterizing elliptic curves equipped with an

injection $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\ell\mathbb{Z} \hookrightarrow E$. Since the j -invariant of E is non-constant, the morphism $\mathbb{P}^1 \rightarrow X(2, 4\ell)$ would also be non-constant. But that is impossible by the lemma below. Thus $E(\overline{\mathbb{F}}_p(t^{1/d}))$ has no non-trivial ℓ -torsion. \square

Lemma 6.2. *If ℓ is a prime number not dividing $2p$, then the modular curve $X(2, 4\ell)$ over $\overline{\mathbb{F}}_p$ parameterizing elliptic curves equipped with a subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\ell\mathbb{Z}$ has positive genus.*

Proof. The curve $X(2, 4\ell)$ covers $X(1, 4\ell) = X_1(4\ell)$ and it is well known that $X_1(n)$ has positive genus for $n \geq 13$ or $n = 11$. (See, for example, [Shi94, 1.6] or [Miy06, 4.2] for formulas for the genus of a modular curve and the ramification assertions just below.) This suffices to prove the lemma for $\ell > 3$. For $\ell = 3$ we consider the covering $X(2, 12) \rightarrow X_1(12)$. It has degree 2 and is branched over 4 cusps of the rational curve $X_1(12)$, so $X(2, 12)$ has genus 1. \square

Remark 6.3. There are at least two other ways to bound the prime-to- p torsion on E , both perhaps better for generalizations to higher genus. One uses an integrality result, namely Proposition 9.1 below. Another proceeds by considering the monodromy group of the finite-coefficient cohomology of the family $\mathcal{E} \rightarrow \mathbb{P}^1$ associated to $E/\overline{\mathbb{F}}_p(u)$.

7. The Néron model

Fix a positive integer d , let $F = \mathbb{F}_q(t^{1/d}) = \mathbb{F}_q(u)$, and consider E over F . In order to compute heights on $E(K_d)$ we will need a nice model for E over \mathbb{P}^1 , specifically, a smooth proper surface \mathcal{E}_d over \mathbb{F}_q equipped with a relatively minimal, generically smooth morphism $\pi : \mathcal{E}_d \rightarrow \mathbb{P}^1$ whose generic fiber is E .

Using Tate’s algorithm [Tat75] we find that E has reduction type I_{2d} at $u = 0$ and type I_2 at the places dividing $u^d - 1$. At $u = \infty$, the reduction type is I_{2d} if d is even and I_{2d}^* if d is odd. At all other places, E has good reduction. The reduction at $u = 0$ and at ∞ when d is even is split multiplicative, while the reduction at the d -th roots of unity is split if and only if 4 divides $q - 1$.

We only need the Néron model when $d = p^f + 1$, which is even, so for the rest of this section, we assume that d is even. We also assume for convenience of exposition that d divides $q - 1$, i.e., that \mathbb{F}_q contains the d -th roots of unity.

We start by constructing a fibered projective surface $\mathcal{W}_d \rightarrow \mathbb{P}^1$ whose fibers are plane cubics which are the reductions of E at places of F . To that end, let $\mathcal{W}_{d,0}$ be the closed subset of $\mathbb{P}^3 \times \mathbb{A}^1$ (with homogeneous coordinates X, Y, Z , on \mathbb{P}^3 and coordinate u on \mathbb{A}^1) defined by

$$Y^2Z - X(X + Z)(X + u^dZ) = 0$$

and let $W_{d,0}^0$ be the open subset where $u \neq 0$. Also, let $W_{d,1}$ be the closed subset of $\mathbb{P}^3 \times \mathbb{A}^1$ (with homogeneous coordinates X', Y', Z' , on \mathbb{P}^3 and coordinate v on \mathbb{A}^1) defined by

$$Y'^2 Z' - X'(X' + Z')(X' + v^d Z') = 0$$

and let $W_{d,1}^0$ be the open subset where $v \neq 0$. We glue $W_{d,0}$ and $W_{d,1}$ along their open subsets $W_{d,0}^0$ and $W_{d,1}^0$ via the identification

$$([X', Y', Z'], v) = ([u^{-d} X, u^{-3d/2} Y, Z], u^{-1}).$$

We write W_d for the resulting surface. It is equipped with a canonical morphism $W_d \rightarrow \mathbb{P}^1$ which is projective and generically smooth and whose fibers are plane cubics.

Applying the Jacobian criterion, we find that W_d is regular away from $d+2$ points. In the coordinates above, they are located at $u = 0, [X, Y, Z] = [0, 0, 1]; u \in \mu_d, [X, Y, Z] = [-1, 0, 1];$ and at $v = 0, [X', Y', Z'] = [0, 0, 1]$. The Néron model $\mathcal{E}_d \rightarrow \mathbb{P}^1$ is obtained by blowing up each of these singular points so that \mathcal{E}_d is smooth and relatively minimal over \mathbb{P}^1 .

We first focus attention on the fiber over $u = 0$. The blow-ups required to desingularize this fiber were discussed in some detail in [Ulm11, Lecture 3, §3], and we will not repeat all the details here. However, to establish notation to be used later, we will quickly review what is needed. We work in the affine open subset of $W_{d,0}$ where $Z \neq 0$ and set $x = X/Z, y = Y/Z,$ so that our surface is given by

$$y^2 - x(x + 1)(x + u^d)$$

in the affine 3-space with coordinate x, y, u . The interesting patch of the blow-up at $x = y = u = 0$ has coordinates x_1, y_1, u satisfying $x = ux_1, y = uy_1,$ and in those coordinates, the proper transform of our surface has equation

$$y_1^2 - x_1(ux_1 + 1)(x_1 + u^{d-1})$$

and the exceptional divisor is the reducible curve $u = y_1^2 - x_1^2 = 0$. The point $u = x_1 = y_1 = 0$ is the unique singular point of the proper transform, and we continue by blowing it up. The new interesting patch has coordinates $x_2, y_2, u,$ with $x_1 = ux_2$ and $y_1 = uy_2;$ two new components are introduced; and there is a unique singular point, which we again blow up. At each of the first $d - 1$ blow-ups, two new components are introduced. At the d -th blow-up, one component is introduced and we arrive at a smooth surface mapping to \mathbb{P}^1 with fiber over $u = 0$ consisting of a chain of $2d$ \mathbb{P}^1 s meeting transversally. We label the components cyclically by $i \in \mathbb{Z}/2d\mathbb{Z}$ so that the original fiber over $u = 0$ is labeled 0 and the component introduced in the first blow up with $u = y_1 - x_1 = 0$ is labeled 1. (Thus the component $u = y_1 + x_1 = 0$ is labeled $2d - 1$.)

The situation over $v = 0$ is essentially identical to that over $u = 0$, and we employ similar notation and conventions there.

Now consider the fiber over $u = \zeta_d^i$. We set $x' = x + 1 = X/Z + 1$, $u' = u - \zeta_d^i$, and $f = (u^d - 1)/(u - \zeta_d^i)$, so that f is a unit in the local ring at $u' = 0$. An affine patch of \mathcal{W}_d is given by

$$y^2 - (x' - 1)x'(x' + u'f) = 0.$$

The singular point is at $u' = x' = y = 0$ and the projectivized tangent cone is the irreducible curve with projective equation $y^2 + x'^2 + x'u'f = 0$. Blowing up once introduces a single component and the proper transform of \mathcal{W}_d is regular in a neighborhood of $u' = 0$. This is consistent with our earlier observation that the fibers over the points with $u \in \mu_d$ are of type I_2 .

The end result is a fibered surface $\pi : \mathcal{E}_d \rightarrow \mathbb{P}^1$ such that \mathcal{E}_d is regular and proper, and π is generically smooth over \mathbb{P}^1 with generic fiber E/F .

The following result follows from our construction of \mathcal{E}_d ; see [Ulm11, Lecture 3, §2] and especially Exercise 2.2 in that section. The quantity δ defined here is sometimes called the *height* of \mathcal{E}_d .

Lemma 7.1. *Assume that d is even. Let $\pi : \mathcal{E}_d \rightarrow \mathbb{P}^1$ be the model of $E/\mathbb{F}_q(t^{1/d})$ just constructed, with zero section $s : \mathbb{P}^1 \rightarrow \mathcal{E}_d$, and let ω be the invertible sheaf $s^*\Omega_{\mathcal{E}_d/\mathbb{P}^1}^1 \cong (R^1\pi_*\mathcal{O}_{\mathcal{E}_d})^{-1}$. Then δ , the degree of ω , is $d/2$.*

8. Heights

Our next task is to compute the height pairing on the subgroup of $E(F)$ generated by the points P_i . This will give another proof that the subgroup they generate has rank at least $d - 2$ and it will give us some control on the index in $E(F)$ of this subgroup.

Throughout this section, we assume that $F = \mathbb{F}_q(t^{1/d})$ where $d = p^f + 1$ and d divides $q - 1$, and that $\pi : \mathcal{E}_d \rightarrow \mathbb{P}^1$ is the Néron model of E/F discussed in the preceding section.

Both the height pairing and the discussion of discriminants in the next section are based heavily on the Shioda–Tate isomorphism. We refer to [Ulm12, Chap. 4] for a discussion of this in a somewhat more general context. In particular, the definition of the height pairing on $E(F)$ and the proof that it is closely related to the canonical height is discussed in [Ulm12, Prop. 4.3.1].

We quickly review the definition of the height pairing here. For a point $P \in E(F)$, we write $[P]$ for the corresponding curve in \mathcal{E}_d , namely the image of the section $\mathbb{P}^1 \rightarrow \mathcal{E}_d$ whose generic fiber is P . For each P there is a unique \mathbb{Q} -linear combination D_P of non-identity components of reducible fibers of π such that the divisor $[P] - [0] + D_P$ is orthogonal to all components of fibers of π under the intersection pairing on \mathcal{E}_d .

To compute D_P , one need only determine the component of the fiber through which $[P]$ passes at each reducible fiber. The height pairing is then defined by

$$\langle P, Q \rangle = -([P] - [0] + D_P) \cdot ([Q] - [0]). \tag{8.1}$$

Here the dot signifies the intersection pairing on \mathcal{E}_d .

This pairing is known to be symmetric and positive definite modulo torsion. It makes $E(F)$ into a lattice in the real vector space $E(F) \otimes_{\mathbb{Z}} \mathbb{R}$. The Néron–Tate canonical height is $\log q$ times this height.

The “correction factor” $D_P.[Q]$ is symmetric in P and Q and depends only on the components through which $[P]$ and $[Q]$ pass at each reducible fiber. A table of values is given in [CZ79, 1.19].

For any elliptic surface $\pi : \mathcal{E} \rightarrow \mathbb{P}^1$, the self-intersection of any section is equal to $-\delta$ where δ is the degree of the invertible sheaf $\omega = (R^1\pi_*\mathcal{O}_{\mathcal{E}})^{-1}$. We computed in Lemma 7.1 that for \mathcal{E}_d we have $\delta = d/2$.

We apply the above to the elliptic surface $\mathcal{E}_d \rightarrow \mathbb{P}^1$ associated to E over F and the points P_i and obtain the following.

Theorem 8.2. *The height pairing (8.1) of the points P_i ($i \in \mathbb{Z}/d\mathbb{Z}$) on E given by (3.1) is*

$$\langle P_i, P_j \rangle = \begin{cases} \frac{(d-1)(d-2)}{2d} & \text{if } i = j, \\ \frac{(1-d)}{d} & \text{if } i - j \text{ is even and } \neq 0, \\ 0 & \text{if } i - j \text{ is odd.} \end{cases}$$

Proof. Throughout, we conflate the point P_i with the section of $\mathcal{E}_d \rightarrow \mathbb{P}^1$ determined by P_i .

Let us first examine the reduction of $P_i = (\zeta_d^i u, \zeta_d^i u(\zeta_d^i u + 1)^{d/2})$ in the various reducible fibers. At $u = 0$ it is clear that P_i reduces to the singular point in the fiber of \mathcal{W}_d . In the first blow up, P_i has coordinates $(x_1, y_1) = (\zeta_d^i, \zeta_d^i(\zeta_d^i u + 1)^{d/2})$ and so reduces to a smooth point on the component labeled 1. At $u = \zeta_d^j$, we see that P_i reduces to a point on the identity component if and only if $\zeta_d^{i+j} \neq -1$, i.e., if and only if $i + j \not\equiv d/2 \pmod{d}$.

To examine the reduction at $u = \infty$ (i.e., over $v = 0$ in the coordinates used to construct \mathcal{W}_d and \mathcal{E}_d), we introduce $x' = X'/Z'$ and $y' = Y'/Z'$. In these coordinates, we have that $x'(P_i) = \zeta_d^i v^{d-1}$ and $y'(P_i) = \zeta_d^i v^{d-1}(\zeta_d^i + v)^{d/2}$. Thus in the model \mathcal{W}_d , P_i reduces to the singular point in the fiber over $v = 0$ and we have to follow its behavior in the blow ups used to construct \mathcal{E}_d . Using notation analogous to that in the last section, we see that for $1 \leq a \leq d - 1$, $x'_a(P_i) = \zeta_d^i v^{d-1-a}$ and so P_i continues to reduce to a singular point until the $(d - 1)$ st blow up. At that stage, P_i has coordinates

$$(x'_{d-1}, y'_{d-1}) = (\zeta_d^i, \zeta_d^i(\zeta_d^i + v)^{d/2}).$$

If i is even, then $(\zeta_d^i)^{d/2} = 1$ and so P_i reduces to the component labeled $d - 1$, whereas if i is odd, then $(\zeta_d^i)^{d/2} = -1$ and so P_i reduces to the component labeled $d + 1$.

This calculation allows us to determine the “correction factors” $D_{P_i} \cdot [P_j]$, using the table [CZ79, 1.19]. At $u = 0$, both points reduce to the component labeled 1, so the contribution is $(2d - 1)/(2d)$. At places with $u \in \mu_d$, if $i \neq j$ then at least one of P_i or P_j lands on the identity component, so the contribution is always 0. If $i = j$, then at exactly one root of unity (namely at $u = \zeta_d^{d/2-i} = -\zeta_d^{-i}$), P_i lands on the non-identity component, and we get a local contribution of $1/2$. Finally, at $u = \infty$, P_i and P_j land on components $d \pm 1$ and we find a local contribution of

$$\begin{cases} \frac{(d - 1)(d + 1)}{2d} & \text{if } i - j \text{ is even,} \\ \frac{(d - 1)^2}{2d} & \text{if } i - j \text{ is odd.} \end{cases}$$

The above calculations also show that the intersection numbers $[P_i] \cdot [P_j]$ ($i \neq j$) and $[P_i] \cdot [O]$ are 0. Indeed, it is evident from inspecting the x -coordinates that P_i and P_j do not meet except possibly at $u = 0$ or $u = \infty$. But at $u = 0$, P_i reduces to $(x_1, y_1) = (\zeta_d^i, \zeta_d^i)$; thus P_i and P_j do not meet in that fiber. At $u = \infty$, P_i reduces to $(\zeta_d^i, \pm \zeta_d^i)$, and so again P_i and P_j do not meet in that fiber. To see that $[P_i] \cdot [O] = 0$ we note that the coordinates of P_i are polynomials in u , so P_i cannot meet the zero section except at $u = \infty$. But near $u = \infty$ (i.e., near $v = 0$) we just saw that the coordinates of P_i are polynomials in v and so P_i does not meet O in that fiber either. Thus we have that

$$(P_i - O) \cdot (P_j - O) = \begin{cases} P_i^2 + O^2 = -d & \text{if } i = j, \\ O^2 = -d/2 & \text{if } i \neq j. \end{cases}$$

Combining the “geometric” contribution $-(P_i - O) \cdot (P_j - O)$ with the “correction factor” $-D_{P_i} \cdot P_j$ leads, after a small bout of arithmetic, to the stated result. This completes the proof of the theorem. \square

We could have simplified the calculation slightly by noting that since E is defined over $K_1 = \mathbb{F}_p(t)$ and $\text{Gal}(F/K_1)$ permutes the P_i cyclically, the pairing $\langle P_i, P_j \rangle$ depends only on $i - j$ modulo d .

Remark 8.3. We write V_d for the subgroup of $E(K_d)$ generated by the P_i . It is easy to see that the lattice V_d modulo torsion is isomorphic to the direct sum of two copies of a scaling of the lattice $A_{d/2-1}^*$ where A_n^* is the dual of the A_n lattice, as in [CS99, 4.6.6]. The points P_i are root vectors; perhaps this explains why it is so easy to write them down.

We note that the height calculation provides a second proof that V_d has rank $d - 2$. We finish this section by tying up a loose end from Section 3.

Proposition 8.4. *Suppose that $d = p^f + 1$. Then for $j \in \mathbb{Z}/2\mathbb{Z}$, we have the following equality in $E(K_d)$:*

$$\sum_{\substack{i \in \mathbb{Z}/d\mathbb{Z} \\ i \equiv j+1+d/2 \pmod{2}}} P_i^{(d)} = P_j^{(2)}.$$

Proof. We saw in Section 3 that the sum on the left hand side is a 4-torsion point. Applying the map ν of Proposition 5.2, we see that both sides of the equality above map to either $(1, 0, \dots, 1, 0)$ or $(0, 1, \dots, 0, 1)$ in $(\mathbb{Z}/2\mathbb{Z})^d$ (depending on the parity of j). This shows that the equality above holds in $E(K_d)/2E(K_d)$ and therefore holds in $E(K_d)$ up to a sign. (The kernel of $E(K_d)_{\text{tor}} \rightarrow E(K_d)/2E(K_d)$ is generated by Q_0 , and we have $P_j^{(2)} + Q_0 = -P_j^{(2)}$.) To pin down the sign, we consider the images of the two sides in the component group of E at $u = 0$. We saw in the proof of Theorem 8.2 that $P_i^{(d)}$ reduces to the component labeled 1, so the sum reduces to the component labeled $d/2$. To finish, one checks that $P_j^{(2)}$ reduces to component $d/2$ while $-P_j^{(2)}$ reduces to component $2d - d/2$. This completes the proof of the proposition. \square

9. The index $[E(F) : V_d]$

We start by proving a result that is probably well-known to experts. There is a closely related discussion in a more general context in [Gor79, §5], but I do not know a convenient reference for the result we need.

Suppose that $F = \mathbb{F}_q(\mathcal{C})$ is the function field of a curve over \mathbb{F}_q and E/F is an elliptic curve with Néron model $\pi : \mathcal{E} \rightarrow \mathcal{C}$. For each place v if F , let f_v be the number of irreducible components in the fiber of π over v . One of these components meets the zero section and we let N_v be the subgroup of $\text{NS}(\mathcal{E})$ generated by the other components of the fiber. This is known to be a free abelian group of rank $f_v - 1$ (e.g., [Ulm11, Lecture 2, 8.6]). We write Disc_v for the discriminant of the intersection form on \mathcal{E} restricted to N_v . If $f_v = 1$, we set $\text{Disc}_v = 1$. We write $\langle \cdot, \cdot \rangle$ for the height pairing on $E(F)$ discussed in the previous section, so that $\langle \cdot, \cdot \rangle \log q$ is the Néron–Tate canonical height. Let R_1, \dots, R_r be a basis for $E(F)_{\text{tor}}$ and let

$$R(E/F) = \left| \det(\langle R_i, R_j \rangle)_{i,j=1,\dots,r} \right|.$$

This is the usual regulator of E/F divided by $(\log q)^r$.

The result we have in mind gives an *a priori* bound on the denominator of the rational number $R(E/F)$.

Proposition 9.1. *Suppose that E is non-constant, i.e., not defined over the constant field $\mathbb{F}_q \subset F$. Then the rational number*

$$\frac{R(E/F) \prod_v \text{Disc}_v}{|E(F)_{\text{tor}}|^2}$$

is an integer.

Proof. Let $L^1 \text{NS}(\mathcal{E})$ be the subgroup of the Néron–Severi group $\text{NS}(\mathcal{E})$ generated by classes of divisors which meet the generic fiber in a divisor of degree 0, and let $L^2 \text{NS}(\mathcal{E})$ be the subgroup generated by components of fibers of π . The Shioda–Tate isomorphism says that restriction to the generic fiber induces an isomorphism $L^1 \text{NS}(\mathcal{E})/L^2 \text{NS}(\mathcal{E}) \rightarrow E(F)$. (Here we use that E is non-constant, so its F/\mathbb{F}_q -trace is zero.) See [Ulm11, Lecture 3, §5] for a discussion in our context, as well as [Ulm12, Chap. 4] for a proof of a more general result and several results used below.

The intersection form restricted to $L^1 \text{NS}(\mathcal{E})$ is degenerate—by definition it is orthogonal to F , the class of a fiber of π . We define \bar{L}^1 as $L^1 \text{NS}(\mathcal{E})$ modulo $\mathbb{Z}F$. Since $\text{NS}(\mathcal{E})$ is torsion-free [Mir89, VII.1.2] and F is primitive, \bar{L}^1 is torsion free. The intersection form induces a non-degenerate integral pairing on \bar{L}^1 . For any subgroup $L \subset \bar{L}^1$, we write $\text{Disc}(L)$ for the discriminant of the intersection pairing restricted to L . (By discriminant, we mean the *absolute value* of the determinant of the matrix of pairings.)

We write \bar{L}^2 for the image of $L^2 \text{NS}(\mathcal{E})$ in \bar{L}^1 . We have an orthogonal direct sum decomposition

$$\bar{L}^2 = \prod_v N_v.$$

Recall that R_1, \dots, R_r form a basis for $E(F)/\text{tor}$. For each i we define the class

$$\widetilde{R}_i = [R_i] - [O]$$

(the class of the section of π attached to R_i minus the zero section). By the Shioda–Tate isomorphism, the subgroup N of \bar{L}^1 generated by $\widetilde{R}_1, \dots, \widetilde{R}_r$ and \bar{L}^2 has index equal to $|E(F)_{\text{tor}}|$. Thus we have

$$\text{Disc}(N) = |E(F)_{\text{tor}}|^2 \text{Disc}(\bar{L}^1).$$

Let t be the least common multiple of the exponents of the component groups over all place of F , so that for each i , the section associated to tR_i passes through the identity component at each place. Let \widetilde{tR}_i be the class of $[tR_i] - [O]$, and let N' be the subgroup of \bar{L}^1 generated by $\widetilde{tR}_1, \dots, \widetilde{tR}_r$ and \bar{L}^2 . The index of N' in N is clearly t^r and so $\text{Disc}(N') = t^{2r} \text{Disc}(N)$.

On the other hand, since each tR_i passes through the identity component at each place v , the \widetilde{tR}_i are orthogonal to \bar{L}^2 . Thus, we have an orthogonal direct sum decomposition

$$N' = \{\mathbb{Z}\widetilde{tR}_1 + \dots + \mathbb{Z}\widetilde{tR}_r\} \oplus \bar{L}^2.$$

Also, in the height pairing $\langle tR_i, tR_j \rangle$, no “correction factors” are required, i.e., we have

$$\langle tR_i, tR_j \rangle = -\widetilde{tR}_i \cdot \widetilde{tR}_j.$$

Taking discriminants, we find

$$\begin{aligned} \text{Disc}(N') &= t^{2r} R(E/F) \text{Disc}(\bar{L}^2) \\ &= t^{2r} R(E/F) \prod_v \text{Disc } N_v. \end{aligned}$$

But we saw above that

$$\text{Disc}(N') = t^{2r} \text{Disc}(N) = t^{2r} |E(F)_{\text{tor}}|^2 \text{Disc}(\bar{L}^1).$$

Thus

$$\frac{R(E/F) \prod_v \text{Disc}_v}{|E(F)_{\text{tor}}|^2} = \text{Disc}(\bar{L}^1)$$

which is an integer. \square

We now apply the proposition in the context of the Legendre curve E . Let $F = \mathbb{F}_q(t^{1/d})$ with $d = p^f + 1$ for some positive integer f and assume that d divides $q - 1$. Let V_d be the subgroup of $E(F)$ generated by the points P_0, \dots, P_{d-1} of Section 3. We saw in Section 5 that V_d has finite index in $E(F)$. Using the proposition, we find the following *a priori* bound on the index.

Theorem 9.2. *The index $[E(F) : V_d]$ divides $p^{f(d-2)/2} = p^{f(p^f-1)/2}$. In particular, it is a power of p .*

Proof. The lattice A_n^* has discriminant $(n + 1)^{n-1}$ [CS99, 4.6.6] and so Theorem 8.2 shows that the discriminant of V_d modulo torsion is $2^{4-d}(d - 1)^{d-2}d^{-2}$. Thus, we have that the regulator is

$$R(E/F) = \frac{2^{4-d}(d - 1)^{d-2}d^{-2}}{[E(K_d) : V_d]^2}. \tag{9.3}$$

The local factors Disc_v at $u = 0$ and $u = \infty$ are $2d$, at the d places where $u^d = 1$ they are 2, and elsewhere they are 1. (These are also the orders of the component groups at these places. This is of course not an accident—see [Gor79, Thm 5.2ff].) By Proposition 6.1, $|E(F)_{\text{tor}}| = 8$. Unwinding the integrality statement in the proposition, it follows that

$$\frac{p^{f(d-2)}}{[E(F) : V_d]^2}$$

is an integer. This completes the proof of the theorem. \square

Remarks 9.4. Let f and f' be positive integers such that f' divides f and f/f' is odd. Let $d = p^f + 1$ and $d' = p^{f'} + 1$ and note that d' divides d so that $K_{d'} \subset K_d$.

- (1) Writing $\langle \cdot, \cdot \rangle_d$ and $\langle \cdot, \cdot \rangle_{d'}$ for the height pairings on $E(K_d)$ and $E(K_{d'})$ respectively, we have that

$$\langle P_0^{(d')}, P_0^{(d')} \rangle_{d'} = \frac{(d' - 1)(d' - 2)}{2d'}$$

and so

$$\langle P_0^{(d')}, P_0^{(d')} \rangle_d = \left(\frac{d}{d'} \right) \frac{(d' - 1)(d' - 2)}{2d'}.$$

On the other hand, the root vectors $P_i^{(d)}$ of V_d satisfy

$$\langle P_i^{(d)}, P_i^{(d)} \rangle_d = \frac{(d - 1)(d - 2)}{2d}.$$

The ratio

$$\frac{\langle P_i^{(d)}, P_i^{(d)} \rangle_d}{\langle P_0^{(d')}, P_0^{(d')} \rangle_d} = \frac{(d - 1)}{(d - (d/d'))} \frac{(d - 2)}{(d - (2d/d'))}$$

is > 1 and so $P_0^{(d')}$ is not contained in V_d . This proves that if f is divisible by an odd prime, then $V_d \neq E(K_d)$.

- (2) In a future publication, we will compute the quotient group $E(K_d)/V_d$ as a module over $\mathbb{Z}_p[\text{Gal}(K_d/K_1)]$ and show that it is non-trivial precisely when $f > 2$. In general it is not generated by points in $V_{d'}$ as d' runs through divisors of d of the form $d' = p^{f'} + 1$.
- (3) With more work, one may compute the height pairings $\langle P_j^{(d')}, P_i^{(d)} \rangle_d$ and show that for every $j \in \mathbb{Z}/d'\mathbb{Z}$, we have the following equality in $E(K_d)$ modulo torsion:

$$\sum_{\substack{i \in \mathbb{Z}/d\mathbb{Z} \\ i \equiv j \pmod{d'}}} P_i^{(d)} = -p^{(f-f')/2} P_j^{(d')}.$$

(Note the surprising sign.)

10. The Tate–Shafarevich group

In this section we use the Birch and Swinnerton-Dyer formula to relate the order of the Tate–Shafarevich group to the index $[E(F) : V_d]$ of the preceding section. We refer to [Ulm11] and [Ulm12] for background on L -functions and the BSD conjecture.

First we calculate the L -function of E over $\mathbb{F}_q(t^{1/d})$ when $d = p^f + 1$.

Proposition 10.1. *Let $F = \mathbb{F}_q(t)(t^{1/d})$ where $d = p^f + 1$ and d divides $q - 1$. Then the Hasse–Weil L -function of E/F is*

$$L(E/F, s) = (1 - q^{1-s})^{d-2}.$$

Moreover, the Birch and Swinnerton-Dyer conjecture holds for E/F .

Proof. By [Ulm11, Lecture 1, Theorem 9.3], the L -function $L(E/F, s)$ is a polynomial in q^{-s} of the form $\prod_i (1 - \alpha_i q^{-s})$ where the α_i are Weil integers of size q . Its degree is $\deg n - 4$ where n is the conductor of E .

We saw in Section 7 that the curve E has multiplicative reduction at $d + 2$ places of F and good reduction elsewhere. It follows that its conductor has degree $d + 2$. Thus the degree of the L -function as a polynomial in q^{-s} is $d - 2$. Note that the order of vanishing of $L(E/F, s)$ at $s = 1$ is precisely the number of times q appears as an α_i .

Now we recall (e.g., from [Ulm12, Theorem 6.3.1]) that we have an inequality

$$\text{ord}_{s=1} L(E/F, s) \geq \text{Rank } E(F).$$

Since the degree of $L(E/F, s)$ is $d - 2$, the order of vanishing is certainly at most $d - 2$. On the other hand, we know from Corollary 5.3 that under the hypotheses of the proposition, the rank of $E(F)$ is $d - 2$. Thus all of the α_i must be equal to q , i.e., the L -function is as we have claimed. Moreover, we have the equality

$$\text{ord}_{s=1} L(E/F, s) = \text{Rank } E(F)$$

i.e., the basic BSD conjecture holds for E/F . \square

Using the refined BSD conjecture (on the leading term of the L -function) we get the following connection between the Tate–Shafarevich group $\text{III}(E/F)$ and the index.

Corollary 10.2. *Suppose that $d = p^f + 1$ and let $K_d = \mathbb{F}_p(\mu_d, t^{1/d})$. Recall that V_d is the subgroup of $E(K_d)$ generated by the points P_0, \dots, P_{d-1} . We have that $\text{III}(E/K_d)$ is finite and*

$$|\text{III}(E/K_d)| = [E(K_d) : V_d]^2.$$

More generally, if $F = \mathbb{F}_q(t^{1/d})$ with d dividing $q - 1$, we have

$$|\text{III}(E/F)| = [E(F) : V_d]^2 (q/p^{2f})^{(p^f - 1)/2}.$$

In particular, $\text{III}(E/F)$ is a p -group.

This result can be viewed as a class number formula, analogous to that relating the class number to the index of cyclotomic units or the index of a Heegner point to the order of a Tate–Shafarevich group (cf. [Was97, Thm. 8.2] and [GZ86, Conj. V.2.2]).

Proof of Corollary 10.2. It is known (see, e.g., [Ulm12, Theorem 6.3.1]) that the basic BSD conjecture implies the refined BSD conjecture. For E/F , writing $r = d - 2$ for the rank, we have that the leading coefficient is

$$(1/r!)L^{(r)}(E/F, 1) = (\log q)^r.$$

On the other hand, the regulator $\text{Reg}(E/F)$ (computed using the Néron–Tate canonical height) is equal to $(\log q)^r R(E/F)$ where $R(E/F)$ is the determinant appearing in Section 8. Thus the refined BSD conjecture leads to the equality

$$1 = \frac{|\text{III}(E/F)|R(E/F)\tau(E/F)}{|E(F)_{\text{tor}}|^2}$$

where $\tau(E/F)$ is the Tamagawa number.

To unwind this, recall (e.g., from [Ulm12, §6.2.3]) that

$$\tau(E/F) = q^{1-\delta} \prod_v c_v$$

where δ is the integer appearing in Lemma 7.1 and c_v is the order of the component group of the Néron model at v . Explicitly, we find that

$$\tau(E/F) = q^{1-d/2} 2^d (2d)^2 = q^{1-d/2} 2^{d+2} d^2.$$

Using the value of $R(E/F)$ from Eq. (9.3) and the order of the torsion subgroup from Proposition 6.1, a short calculation leads to

$$|\text{III}(E/F)| = [E(F) : V_d]^2 (q/p^{2f})^{(p^f-1)/2}.$$

Since we proved in Theorem 9.2 that the index $[E(F) : V_d]$ is a power of p , so is the order of $\text{III}(E/F)$. This completes the proof of the corollary. \square

Remark 10.3. Note that the upper bound on $[E(F) : V_d]$ of Theorem 9.2 gives an upper bound on the order of $\text{III}(E/F)$: it has order at most $q^{(d-2)/2}$. By the formula of the corollary, its order is bounded below by $(q/p^{2f})^{(d-2)/2}$. This lower bound suggests that there might be a construction of homogenous spaces for E with parameters with values in \mathbb{F}_q such that the homogenous space is trivial when the parameters lie in $\mathbb{F}_p(\mu_d)$.

Remark 10.4. We computed the L -function when $d = p^f + 1$ by using the BSD inequality and a lower bound on the rank. We could also deduce the L -function from [Ulm07, 4.7] or from the Artin formalism and a root number calculation without knowing anything about points on $E(F)$.

11. Connection with Berger’s construction

In this section, we let k be any field of characteristic $\neq 2$, and we relate the Legendre curve over $k(t)$ to a curve studied in [Ulm13]. This leads to strong consequences for the arithmetic of E at every layer of the tower of fields $k(t^{1/d})$.

Let E' over $k(t')$ be the elliptic curve studied in Section 7 of [Ulm13]:

$$E': \quad y'^2 + x'y' + t'y' = x'^3 + t'x'^2.$$

We identify the fields $k(t)$ and $k(t')$ by setting $t' = t/16$ and view E' as an elliptic curve over $k(t)$.

Lemma 11.1. *The elliptic curve E' over $k(t)$ is 2-isogenous to the Legendre curve (2.1).*

Proof. This follows from a simple computation. On E' , changing coordinates

$$(x', y') \mapsto \left(\frac{x' - t}{16}, \frac{y' - 2x'}{64} \right)$$

leads to the equation

$$y'^2 = x'^3 + (4 - 2t)x'^2 + t^2x'.$$

Dividing by the 2-torsion point $(0, 0)$ yields the curve

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

(See, e.g., [Hus04, Chap. 4, §5].) Finally, the change of coordinates $(x, y) \mapsto (4x + 4, 8y)$ yields the Legendre curve

$$y^2 = x(x + 1)(x + t). \quad \square$$

Remark 11.2. Let $\psi : E \rightarrow E'$ be the isogeny dual to the one of the lemma (which we have only specified up to a sign). Writing ψ^* for the pull back of functions, we have

$$\psi^*(x') = \frac{x^2 - t}{16(x + 1)}$$

and

$$\psi^*(y') = \pm \left(\frac{y(x^2 + 2x + t)}{64(x + 1)^2} - \frac{x(x + t)}{32(x + 1)} \right).$$

Under this isogeny, the point P_0 of this paper maps to the sum of $(-t', 0)$ and the point $-P(u')$ in [Ulm13, Theorem 8.1(3)]. In particular, the group V_d of this paper is mapped to the group V_d of [Ulm13, Remark 8.10(3)].

The lemma allows us to transfer strong results about E' to E .

Corollary 11.3. *If k is a field of characteristic zero, then the rank of $E(k(t^{1/d}))$ is zero for all d . If k is a finite field of characteristic $p > 2$, then the Birch and Swinnerton-Dyer conjecture holds for E over $k(t^{1/d})$ for all d prime to p .*

Proof. The conclusions (rank zero or BSD) both “descend” under finite extensions of k , i.e., if they hold for E over $k'(t^{1/d})$ with k' a finite extension of k , then they hold over $k(t^{1/d})$. So for a fixed d we may assume that k contains a d -th root of 16. In this case, we may take $k(t^{1/d})$ and $k(t'^{1/d}) = k((t/16)^{1/d})$ to be the same field inside an algebraic closure of $k(t)$. The lemma shows that E and E' are 2-isogenous over this field and we proved the claims of the lemma for E' in [Ulm13, Section 7]. This shows that these claims also hold for E . \square

12. Summary and future directions

For the convenience of the reader, we summarize the main results of the paper.

Theorem 12.1. *Let k be a field of characteristic $\neq 2$ and let $k(t)$ be the rational function field over k . Let E be the elliptic curve over $k(t)$ given by*

$$y^2 = x(x + 1)(x + t).$$

- (1) *If the characteristic of k is zero, then for all positive integers d , the rank of $E(k(t^{1/d}))$ is zero.*
- (2) *If k is finite of characteristic p , then for all positive integers d not divisible by p , the Birch and Swinnerton-Dyer conjecture holds for E over $k(t^{1/d})$. In particular, the Tate–Shafarevich group $\text{III}(E/k(t^{1/d}))$ is finite.*
- (3) *Suppose that k is finite of characteristic p and cardinality q , and that d divides $p^f + 1$ for some f . Then*

$$\text{Rank } E(k(t^{1/d})) = \sum_{\substack{e|d \\ e > 2}} \frac{\varphi(e)}{o_q(e)}$$

where the sum is over divisors e of d greater than 2, φ is Euler’s function, and $o_q(e)$ is the order of q in $(\mathbb{Z}/e\mathbb{Z})^\times$.

- (4) *Suppose further that $d = p^f + 1$, $k = \mathbb{F}_p(\mu_d)$, and $K_d = k(t^{1/d})$. Let P_0, \dots, P_{d-1} be the points in $E(K_d)$ defined by Eq. (3.1), and let V_d be the subgroup of $E(K_d)$ generated by the P_i . Then V_d has rank $d - 2$, its index in $E(K_d)$ is a power of p , and we have*

$$[E(K_d) : V_d]^2 = |\text{III}(E/K_d)|.$$

Parts (1) and (2) of the theorem were proven in Corollary 11.3, part (3) is Corollary 5.3(4), and part (4) is the conjunction of Corollary 5.3(4), Theorem 9.2, and Corollary 10.2.

Remark 12.2. The claim in part (2) of the theorem in fact holds for all d . Indeed, if $d = pd'$, then $E/k(t^{1/d'})$ is isogenous to $E^{(p)}/k(t^{1/d'})$ and the latter is isomorphic to

$E/k(t^{1/d})$ after identifying $k(t^{1/d}) \cong k(u)$ with $k(u') \cong k(t^{1/d'})$. Since the truth of the BSD conjecture is invariant under isogeny, we can reduce to the case where d is not divisible by p .

For k finite and d dividing $p^f + 1$ for some f , we have calculated the rank of $E(k(t^{1/d}))$ now in three different ways: via cohomology in [Ulm07], using Berger’s construction and endomorphisms of Jacobians in [Ulm13], and “by hand” in this paper.

The theorem suggests (at least) two further directions for research that we will address in future publications. First, what is the rank of E/K_d for values of d that do not divide $p^f + 1$ for any f ? Surprisingly, there are many other “interesting” values of d [CHU13] and, in a sense made precise in [PU13], those dividing $p^f + 1$ are less numerous than the others.

Second, what can be said about the index $[E(K_d) : V_d]$ and the Tate–Shafarevich group, say when $d = p^f + 1$? In a future publication we will use flat cohomology and crystalline cohomology to show that the index is 1 if and only if $f \leq 2$ and to compute the quotient $E(K_d)/V_d$ and the Tate–Shafarevich group $\text{III}(E/K_d)$ as modules for the group ring $\mathbb{Z}_p[\text{Gal}(K_d/K_1)]$.

References

- [BK77] A. Brumer, K. Kramer, The rank of elliptic curves, *Duke Math. J.* 44 (1977) 715–743.
- [Ca09] R. Conceição, Twists of Elliptic curves with a large set of integral points over $\mathbf{F}_q(t)$, PhD thesis, The University of Texas at Austin, 2009.
- [CHU13] R. Conceição, C. Hall, D. Ulmer, Explicit points on the Legendre curve II, preprint, arXiv: 1307.4251, 2013.
- [CS99] J.H. Conway, N.J.A. Sloane, Sphere Packings Lattices and Groups, third edition, *Grundlehren Math. Wiss. (Fundamental Principles of Mathematical Sciences)*, vol. 290, Springer-Verlag, New York, 1999. With additional contributions by E. Bannai, R.E. Borcherds, J. Leech, S.P. Norton, A.M. Odlyzko, R.A. Parker, L. Queen and B.B. Venkov.
- [CZ79] D.A. Cox, S. Zucker, Intersection numbers of sections of elliptic surfaces, *Invent. Math.* 53 (1979) 1–44.
- [Gor79] W.J. Gordon, Linking the conjectures of Artin–Tate and Birch–Swinnerton-Dyer, *Compos. Math.* 38 (1979) 163–199.
- [GZ86] B.H. Gross, D.B. Zagier, Heegner points and derivatives of L -series, *Invent. Math.* 84 (1986) 225–320.
- [Hus04] D. Husemöller, Elliptic Curves, second edition, *Grad. Texts in Math.*, vol. 111, Springer-Verlag, New York, 2004. With appendices by Otto Forster, Ruth Lawrence and Stefan Theisen.
- [Mir89] R. Miranda, The Basic Theory of Elliptic Surfaces, *Dottorato di Ricerca in Matematica (Doctorate in Mathematical Research)*, ETS Editrice, Pisa, 1989.
- [Miy06] T. Miyake, Modular Forms, English edition, *Springer Monogr. Math.*, Springer-Verlag, Berlin, 2006. Translated from the 1976 Japanese original by Yoshitaka Maeda.
- [PU13] C. Pomerance, D. Ulmer, On balanced subgroups of the multiplicative group, in: *Number Theory and Related Fields: In Memory of Alf van der Poorten*, Springer, New York, 2013, pp. 253–270.
- [Shi94] G. Shimura, Introduction to the Arithmetic Theory of Automorphic Functions, *Publ. Math. Soc. Japan*, vol. 11, Princeton University Press, Princeton, NJ, 1994. Reprint of the 1971 original, Kanô Memorial Lectures, 1.
- [Sil09] J.H. Silverman, The Arithmetic of Elliptic Curves, second edition, *Grad. Texts in Math.*, vol. 106, Springer, Dordrecht, 2009.
- [Tat75] J.T. Tate, Algorithm for determining the type of a singular fiber in an elliptic pencil, in: *Modular Functions of One Variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, in: *Lecture Notes in Math.*, vol. 476, Springer, Berlin, 1975, pp. 33–52.

- [TS67] J.T. Tate, I.R. Shafarevich, The rank of elliptic curves, *Soviet Math. Dokl.* 8 (1967) 917–920.
- [Ulm07] D. Ulmer, *L*-functions with large analytic rank and abelian varieties with large algebraic rank over function fields, *Invent. Math.* 167 (2007) 379–408.
- [Ulm11] D. Ulmer, Elliptic curves over function fields, in: *Arithmetic of L-Functions*, Park City, UT, 2009, in: *IAS/Park City Math. Ser.*, vol. 18, Amer. Math. Soc., Providence, RI, 2011, pp. 211–280.
- [Ulm13] D. Ulmer, On Mordell–Weil groups of Jacobians over function fields, *J. Inst. Math. Jussieu* 12 (2013) 1–29.
- [Ulm12] D. Ulmer, *Curves and Jacobians over Function Fields*, *Adv. Courses Math. CRM Barcelona*, Birkhäuser, 2013, in press, arXiv:1203.5573.
- [Was97] L.C. Washington, *Introduction to Cyclotomic Fields*, second edition, *Grad. Texts in Math.*, vol. 83, Springer-Verlag, New York, 1997.