FAMILIES OF LARGE RANK ELLIPTIC CURVES OVER $\mathbb{F}_q(t)$

Srijan Sundar
Master of Mathematics
Hilary Term 2026

Abstract. The *rank* of an elliptic curve is an important non-negative integer associated to an elliptic curve. Ranks of elliptic curves have been studied for at least 75 years but remain an elusive quantity. We investigate the question: is the rank of an elliptic curve bounded? Over $\mathbb{Q}$, this is not known and is a major open problem. We investigate the analogous question over $\mathbb{F}_q(t)$ and answer it in the negative. More specifically, we give examples of families of elliptic curves over $\mathbb{F}_q(t)$ due to Ulmer and Conceição that have arbitrarily large rank. We also detail original progress towards generalising the ideas of Ulmer and Conceição to the Hessian family of elliptic curves.

Contents

1 Introduction and Preliminaries

Given a field K with algebraic closure $\overline{K}$, recall that the *projective plane* $\mathbb{P}\overline{K}^2$ is the set of equivalence classes $\{[(x,y,z)] : (x,y,z) \in K^3 \setminus \{\mathbf{0}\}\}$, where $[(x,y,z)]$ denotes the set $\{(\lambda x, \lambda y, \lambda z) : \lambda \in K \setminus 0\}$. We abbreviate $[(x,y,z)]$ to $[x:y:z]$ and define $\mathbb{P}K^2$ similarly. The projective plane can be thought of as a completion of the "affine plane" $\overline{K}^2$. Indeed, there is an inclusion $\iota_z : \overline{K}^2 \to \mathbb{P}\overline{K}^2$ sending $(x,y) \in \overline{K}^2$ to $[x:y:1]$. The elements of $\mathbb{P}\overline{K}^2 \setminus \iota_z(K^2) = \{[x:y:0] : (x,y) \neq (0,0)\}$ are known as the *points at infinity* [8].

There are two other canonical inclusions $\iota_y, \iota_x : \overline{K}^2 \to \mathbb{P}\overline{K}^2$ given by

$$\iota_y : (x,z) \mapsto [x:1:z] \quad \text{and} \quad \iota_x : (y,z) \mapsto [1:y:z].$$

We define $\mathbb{A}_z, \mathbb{A}_y, \mathbb{A}_x$ to be the images of $\iota_z, \iota_y, \iota_x$, respectively. Then $\mathbb{P}\overline{K}^2 = \mathbb{A}_z \cup \mathbb{A}_y \cup \mathbb{A}_x$.

Note if $[x:y:z] \in \mathbb{A}_z$, we can recover $\iota_z^{-1}([x:y:z]) = (\frac{x}{z}, \frac{y}{z}) \in \overline{K}^2$, where $\iota_z^{-1} : \mathbb{A}_z \to \overline{K}^2$ is the inverse of ι_z. Hence, suppose

$$ax + by + c = 0$$

is the equation of a line in $\overline{K}^2$. Replace x with $\frac{X}{Z}$ and y with $\frac{Y}{Z}$. Then after expanding, we can identify this line with the equation

$$aX + bY + cZ = 0$$

defined over $\mathbb{P}\overline{K}^2$. This equation is well-defined over $\mathbb{P}\overline{K}^2$ as (x,y,z) solves the equation if and only if $(\lambda x, \lambda y, \lambda z)$ does for some non-zero $\lambda \in \overline{K}$. In general, given $a, b, c \in \overline{K}$ not all zero, define the *projective line* as the set of solutions to $aX + bY + cZ = 0$ over $\mathbb{P}\overline{K}^2$.

We now discuss some theory regarding cubic curves, and, in particular, elliptic curves. Let K be a field, as before, and $\overline{K}$ its algebraic closure. A *cubic curve* C over K is the locus of zeros $[x:y:z] \in \mathbb{P}\overline{K}^2$ of a polynomial P of the form

$$P = e_1X^3 + e_2Y^3 + e_3Z^3 + e_4X^2Y + e_5X^2Z + e_6XY^2 + e_7Y^2Z + e_8XZ^2 + e_9YZ^2 + e_{10}XYZ$$

for $e_1, \ldots, e_{10} \in K$. Furthermore, we define $C \cap \mathbb{P}K^2$ to be the *K-rational points of C*.

Now, suppose $\mathbf{p} \in C$, and let $\frac{\partial P}{\partial X}, \frac{\partial P}{\partial Y}, \frac{\partial P}{\partial Z}$ be the formal partial derivatives of P with respect to $X, Y,$ and Z, respectively. If at least one of those partial derivatives is non-vanishing at $\mathbf{p}$, we define the *tangent line* at $\mathbf{p}$ as the projective line

$$\frac{\partial P}{\partial X}\mathbf{p} + \frac{\partial P}{\partial Y}\mathbf{p} + \frac{\partial P}{\partial Z}\mathbf{p} = 0.$$

The cubic C is *non-singular* if every point has a well-defined tangent line. Equivalently, C is non-singular if $\frac{\partial P}{\partial X}, \frac{\partial P}{\partial Y}$, and $\frac{\partial P}{\partial Z}$ never simultaneously vanish over C.

We now define elliptic curves. An *elliptic curve* E over K is a non-singular cubic curve with a distinguished K-rational point. Upon an appropriate change of variable, the equation of every elliptic curve over K can be put into projective *Weierstraß form*

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3, \tag{1}$$

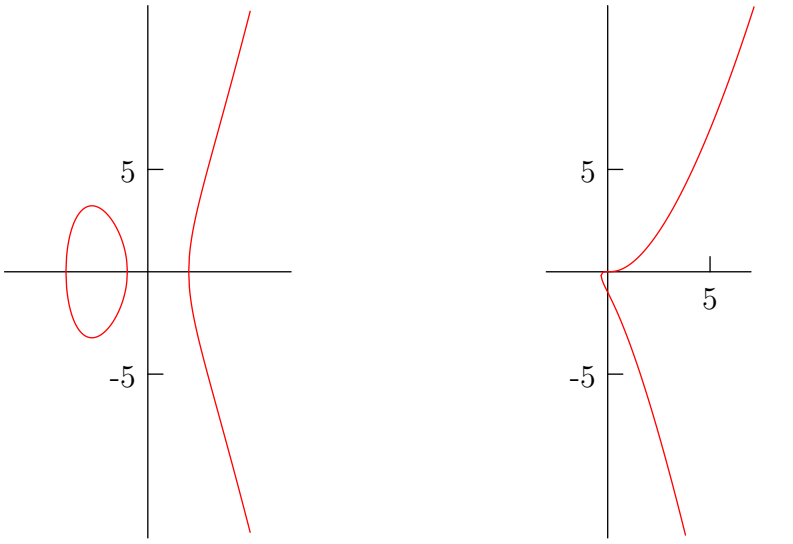
where $a_1, a_2, a_3, a_4, a_6 \in K$ [26, Proposition III.3.1]. Hence, by default, elliptic curves in this essay are assumed to be written in Weierstraß form (1).

Suppose that E is an elliptic curve in projective Weierstraß form. Then, E has just one point at infinity. Indeed, setting $Z = 0$ implies $X^3 = 0$, so the only point at infinity lying on E is $[0 : 1 : 0]$. We call this point $\mathbf{o}$ and observe $\mathbf{o}$ lies on every "vertical" line $X = cZ$, $c \in K$. Moreover, we take $\mathbf{o}$ to be the distinguished K-rational point on E.

Notice that $E \cap \mathbb{A}_z$ can be identified with the solutions $(x, y) \in \overline{K}^2$ to the affine Weierstraß equation:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{2}$$

As $\mathbf{o}$ is the only point at infinity on E, we can think of E as the solutions to (2) together with $\mathbf{o}$; hence, we mostly work with (2) for notational convenience. Similarly, when specifying an elliptic curve, we simply write down its affine form (2) and refer to it as the "elliptic curve E". By this, we really mean the solutions of (2) viewed in projective space together with $\mathbf{o}$. In Figure 1, we show two examples of elliptic curves over $\mathbb{R}$.



(a) $y^2 = (x + 4)(x + 1)(x - 2)$ (b) $y^2 + 2xy + y = x^3$

Figure 1: Two elliptic curves over $\mathbb{R}$

When analysing the behaviour of E around $\mathbf{o}$, we work over $\mathbb{A}_y$. As $\iota_y^{-1} : \mathbb{A}_y \to \overline{K}^2$ is given by $[X : Y : Z] \mapsto (\frac{X}{Y}, \frac{Z}{Y})$, the points $E \cap \mathbb{A}_y$ can be identified with solutions to

$$z + a_1xz + a_3z^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3 \tag{3}$$

over $\overline{K}^2$. In particular, $\mathbf{o}$ is identified with the solution $(0, 0)$ to (3).

We now turn to highlighting a few properties of elliptic curves. We begin by noting that every (projective) line intersects E in three points, counting multiplicities. Indeed, suppose $aX + bY + cZ = 0$ is a projective line in $\mathbb{P}\overline{K}^2$. We have three cases.

- If the line is $Z = 0$ (i.e., $a = b = 0$), substituting this into the equation of E yields $X^3 = 0$. Thus, the line $Z = 0$ intersects E at $\mathbf{o}$ with multiplicity 3;
- If the line is $aX + cZ = 0$, and $a \neq 0$, then we can assume $a = -1$ by scaling. Hence, this corresponds to the vertical line $x = c$ over $\overline{K}^2$. Substituting into equation (2) gives a quadratic in y, so we will get two solutions, counting multiplicities, over $\overline{K}$. Noting $\mathbf{o}$ is also on the line, we thus have three intersections;

- Finally, if $b \neq 0$, we can assume $b = -1$ by scaling. The equation of the line is thus $Y = aX + cZ$. This corresponds to the line $y = ax + c$ over $\overline{K}^2$, so that substituting into (2) gives a cubic equation in x. Hence, we have three solutions over $\overline{K}^2$, counting multiplicities. Finally, $\mathbf{o}$ is not on the line, so that we have exactly three points of intersection over $\mathbb{P}\overline{K}^2$.

Above, and in the rest of this essay, we take an intuitive approach to intersection multiplicity. This can be made rigorous by the discussion in [9, Chapter 3].

Now suppose $\mathbf{p}$ and $\mathbf{q}$ are two K-rational points on the intersection of $aX+bY+cZ = 0$ with E, and let $\mathbf{r}$ be the other intersection point. We can assume[1] $a, b, c \in K$. We claim that $\mathbf{r}$ is also K-rational. This is clear in the case when the line is $Z = 0$. In the second case, if $x = c$ is the vertical line, with $c \in K$, then the resulting quadratic in y has all coefficients in K. Hence, if the quadratic has one solution in K, the other solution will also be in K. The third case is similar, noting that if a cubic equation with coefficients in K has two roots in K, the other root will also be in K.

We now describe an operation $+ : E \times E \to E$. Suppose $\mathbf{p}, \mathbf{q} \in E$. Draw the line ℓ going through both points (if $\mathbf{p} = \mathbf{q}$, then take ℓ to be the tangent line at $\mathbf{p}$). This intersects E at another point, $\mathbf{r}'$. The line through $\mathbf{o}$ and $\mathbf{r}'$ intersects E at a new point $\mathbf{r}$. Define $\mathbf{p}+\mathbf{q} = \mathbf{r}$. Then $+$ is commutative, and $\mathbf{o}+\mathbf{p} = \mathbf{p}+\mathbf{o} = \mathbf{p}$. It is an astonishing

Theorem 1.1. *$(E, +)$ forms an Abelian group with identity element $\mathbf{o}$.*

In particular, $+$ is associative. See [12, Chapter 7] for a proof of Theorem 1.1 and [21] for the historical development of said Theorem. We illustrate the group law in Figure 2.

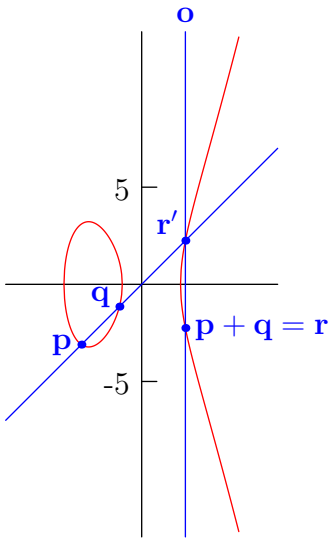


Figure 2: The group law

Given $\mathbf{r} = (x_0, y_0) \in E \setminus \{\mathbf{o}\}$, notice that $-\mathbf{r}$ is the other point of intersection between the vertical line $x = x_0$ and E. Thus, we could alternatively phrase the group law as three points sum to $\mathbf{o}$ if and only if they are collinear. It will be the case that every elliptic curve considered in this essay can be endowed with this same group law, even if they are not in Weierstraß form by [12, Chapter 7].

Let $E(K)$ denote the K-rational points of E, i.e.,

[1] By Proposition 7 of Part A Projective Geometry [8].

Definition 1.2. Let $E(K)$ be the set $\{[x : y : z] : x, y, z \in K, \text{ and } [x : y : z] \in E\}$.

As a line through two K-rational points intersects E at a third K-rational point, we see that the K-rational points of E form an additive subgroup of $(E, +)$.

Now, recall the following:

Theorem 1.3 (The Fundamental Theorem of finitely generated Abelian groups, [4, Corollary 11.7])**.** *Let $(G, +)$ be a finitely generated Abelian group. Then, there is a non-negative integer r, and there are integers $c_1, c_2, \ldots, c_k$ each greater than 1 so that $c_1 \mid c_2 \mid \cdots \mid c_k$, and*

$$G \cong \mathbb{Z}^r \oplus (\mathbb{Z}/c_1\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/c_k\mathbb{Z}).$$

The integer r is known as the *rank* of G.

It turns out that $E(K)$ is finitely generated in two essential contexts, which we state without proof.

Theorem 1.4 (Mordell [16])**.** *$E(\mathbb{Q})$ is finitely generated.*

Theorem 1.5 (Néron-Lang [14])**.** *If k is $\mathbb{Q}$ or a finite field, and $K = k(t)$ is the field of univariate rational functions over k, then $E(K)$ is finitely generated.*

Thus, we can discuss the *rank* of $E(K)$ is either context. In 1901, Poincaré [18, p. 173] raised the question "What values can we attribute to [...] the rank of an [elliptic curve]?" We focus on the following related question: is the rank of an elliptic curve bounded?

Over $\mathbb{Q}$ and $\mathbb{Q}(t)$, this is not known; see the surveys [19, 20, 24] and the references therein for approaches to this question. To gain intuition for what the answer might be, one could ask the same question over $\mathbb{F}_q(t)$, where $\mathbb{F}_q$ is the finite field with q elements. Here, it is known that the rank of elliptic curves can be arbitrarily large. The first examples are due to Tate and Shaferevich [11] and Shioda [22, Section 5] and were found over forty years ago. Beginning with Ulmer's article from 2002 [29], this question has enjoyed greater interest in recent years. See the articles [1, 17, 31, 23] for various examples of constructions and [32] for a general reference.

The aim of this essay is to exhibit explicit, elementary constructions of families of elliptic curves over $\mathbb{F}_q(t)$ that have unbounded rank. We do this by constructing explicit sets of points on prescribed elliptic curves and showing that they generate a subgroup of large rank. The examples discussed in this essay illustrate various tools one can employ to achieve this. We begin by giving an annotation of Ulmer's proof [30] that the family of so-called *Legendre* elliptic curves defined over $\mathbb{F}_q(t)$ for odd q

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

has arbitrarily large rank as d varies in section 2. In section 3, we give a few examples due to Conceição and discuss a method of constructing points on elliptic curves [3]. In section 4, we discuss original progress towards generalising these ideas to the case of the *Hessian* family of elliptic curves, given by $y^2 + \alpha xy + y = x^3$ for some $\alpha \in \mathbb{F}_q(t)$. We conclude the essay with some remarks on possible directions for future investigation.

Unless otherwise mentioned, all results in this essay have appeared in print, elsewhere. However, the presentation of these results is due to the author. We emphasise that the author simplified the background theory required of Conceição's arguments in section 3. We additionally highlight the parts of this essay that are original extensions of the author. Part (b) of the proof of Proposition 2.3, as well as the proof of Theorem 3.15,

were left as exercises for the reader; we fill in the details. The construction of points in Theorem 3.17 was initially only stated over $\mathbb{F}_{q^2}(t)$ in [3, Theorem 4.7], but we show that this construction holds over $\mathbb{F}_q(t)$. Also, the proof of the $\mathbb{Z}$-linear independency of the points in Theorem 3.17 does not appear to be in print elsewhere, and is an original extension of the author's. Finally, besides subsection 4.1, whose presentation is inspired by those of [10, Chapter 4.2] and [35], the remainder of section 4 is due to the author. We add that all matrix computations in this essay were verified with SymPy [15].

Throughout the body of this essay, we omit the computation that an elliptic curve with a prescribed equation is non-singular; a listing of all elliptic curves in this essay, along with proofs that they are non-singular is found in Appendix A. We also give the explicit addition formulae on an elliptic curve in Appendix A. Importantly, if "+" is the addition law on an elliptic curve and $(x, y) + (x', y') = (w, z)$, then w, z can be expressed as rational functions of x, x', y, y'. As Ulmer's proof only holds over fields $\mathbb{F}_q(t)$ where q is odd, the author also attempted to generalise Ulmer's proof for even q by considering different normal forms for elliptic curves in characteristic 2 presented in [13]; see appendix B. Finally, appendix C contains a program written in Magma [2] that was used in our investigation of the Hessian curve.

1.1 Galois Theory

We record some facts about Galois theory from [7].

Let L/K be a finite extension of fields, i.e., L, K are two fields such that $L \supseteq K$ and L is a finite-dimensional K-vector space. Let $[L : K]$ be the dimension of L, viewed as a K-vector space. Denote by $\mathrm{Aut}(L/K)$ the group of K-fixing automorphisms of L, with group multiplication being composition.

Definition 1.6. A finite extension of fields L/K is *Galois* if $[L : K] = |\mathrm{Aut}(L/K)|$. In this case, we say L is a *Galois extension* of K, and we write $\mathrm{Gal}(L/K)$ to mean $\mathrm{Aut}(L/K)$.

Definition 1.7. Given a polynomial $f \in K[x]$, the field L is the *splitting field* of f if f factors completely into linear factors over L, and f does not factor completely over any proper subfield of L containing K.

We will use the following:

Proposition 1.8. *Let L/K be a finite extension of fields.*

(a) L/K is Galois if and only if L is the splitting field of some polynomial in $K[x]$.

(b) K is the fixed field of $\mathrm{Gal}(L/K)$. In other words,

$$K = \{a \in L : \sigma a = a \quad \forall \sigma \in \mathrm{Gal}(L/K)\}.$$

Proof. See [7, Chapter 14, Theorem 13] for (a), and [7, Chapter 14, Corollary 10] for (b). □

1.2 Functions on Curves

Given a mathematical object, one often wishes to study the maps ("morphisms") between similar objects. In this section, we develop some basic theory regarding functions on elliptic curves. This section is based on [26, Chapters 1-3].

Let $E \subset \mathbb{P}\overline{K}^2$ be the elliptic curve (1), and let $E_z \subset \overline{K}^2$ be the set of points satisfying the affine Weierstraß equation (2). Further define $P_z = y^2+a_1xy+a_3y-x^3-a_2x^2-a_4x-a_6$ so that $P_z = 0$ is the equation of E_z.

We begin by noting that any polynomial $f \in K[x, y]$ defines a function $\overline{K}^2 \to \overline{K}$ and thus restricts to a function $E_z \to \overline{K}$. By definition, all polynomials in $(P_z) \subseteq K[x, y]$, the ideal generated by the equation of E_z, evaluate to zero on E_z. Hence, if $f_1, f_2 \in K[x, y]$ differ by a multiple of P_z, then f_1 and f_2 agree everywhere on E_z. Hence, we see that a function on E_z can be defined modulo multiples of P_z. This motivates the following:

Definition 1.9. The coordinate ring of E_z, denoted $K[E_z]$, is defined to be $\frac{K[x,y]}{(P_z)}$.

Definition 1.10. The function field of E, denoted $K(E)$, is the field of fractions of $K[E_z]$.

Remark 1.11. (1) Any element of $K(E)$ can be extended to function on E by the map ι_z. (2) Recall that E_z can be identified with $E \cap \mathbb{A}_z$. If we use the corresponding identifications to define E_x, E_y, then it is the case that the resulting function fields are all canonically isomorphic, so that we get the same definitions. To analyse the behaviour of a function at $\mathbf{o}$, we will need to work in $\mathbb{A}_y$.

We write $K[E]_{\mathbf{p}}$ to be the ring of functions regular at $\mathbf{p} \in E$, i.e.,

Definition 1.12. Define $K[E]_{\mathbf{p}}$ to be the set $\{f/g : f, g \in K(E), g(\mathbf{p}) \neq 0\}$.

Making the analogous definitions by replacing K with $\overline{K}$, consider the ideal $M_{\mathbf{p}} \trianglelefteq \overline{K}[E]_{\mathbf{p}}$ of functions that vanish at $\mathbf{p}$. As $M_{\mathbf{p}}$ is the kernel of the map $\overline{K}[E]_{\mathbf{p}} \to \overline{K}$ given by evaluating at $\mathbf{p}$, we see $\overline{K}[E]_{\mathbf{p}}/M_{\mathbf{p}} \cong \overline{K}$. Thus, $M_{\mathbf{p}}$ is a maximal ideal of $\overline{K}[E]_{\mathbf{p}}$. Note,

$$\overline{K}[E]_{\mathbf{p}} := M_{\mathbf{p}}^0 \supseteq M_{\mathbf{p}} \supseteq M_{\mathbf{p}}^2 \supseteq M_{\mathbf{p}}^3 \supseteq \cdots$$

is a decreasing set of ideals.

Definition 1.13. Let $f \in \overline{K}[E]_{\mathbf{p}}$. We define its multiplicity of vanishing, denoted, $\mathrm{ord}_{\mathbf{p}}(f)$, as $\sup\{n : f \in M_{\mathbf{p}}^n\}$. More generally, given $f/g \in \overline{K}(E)$, with $f, g \in \overline{K}[E]$, we can set $\mathrm{ord}_{\mathbf{p}}(f/g) = \mathrm{ord}_{\mathbf{p}}(f) - \mathrm{ord}_{\mathbf{p}}(g)$.

Definition 1.14. Suppose $f \in \overline{K}(E)$. We say f has a zero at $\mathbf{p}$ if $\mathrm{ord}_{\mathbf{p}}(f) > 0$, and we say f has a pole at $\mathbf{p}$ if $\mathrm{ord}_{\mathbf{p}}(f) < 0$.

It is the case that if $f, g \in \overline{K}(E)$, then $\mathrm{ord}_p(fg) = \mathrm{ord}_{\mathbf{p}}(f) + \mathrm{ord}_{\mathbf{p}}(g)$ by [26, Chapter II.2]. We will also need the following:

Proposition 1.15. *Let E be an elliptic curve.*

(a) Every rational function has finitely many zeros and poles on E.

(b) Every rational function has the same number of zeros as poles (counting multiplicities) on E.

(c) (Abel's Theorem) Suppose f is a rational function on E, with zeros and poles $\mathbf{p}_1, \mathbf{p}_2, \ldots \mathbf{p}_n$ with multiplicities $m_1, m_2, \ldots, m_n$ (respectively). Then $\sum_{i=1}^{n} m_i\mathbf{p}_i = \mathbf{o}$.

Proof. See [26, Proposition II.1.2] for (a). See [26, Corollary III.3.5] for (b) and (c). □

2 Legendre curves of large rank over $\mathbb{F}_p(t)$

Let E be the elliptic curve

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

expressed in projective coordinates over some field K. A point $\mathbf{p} = [x_0 : y_0 : z_0] \in E$ has order 2 if and only if $\mathbf{p} \neq \mathbf{o}$ and $2\mathbf{p} = \mathbf{o}$, i.e., the tangent line to $\mathbf{p}$ contains $\mathbf{o}$. Note this happens if and only if

$$\frac{\partial P}{\partial y}(\mathbf{p}) = 2y_0z_0 + a_1x_0z_0 + a_3z_0^2$$

vanishes. As $z_0 \neq 0$, we deduce that the order 2 points on E are precisely the points lying on the intersection of E with the line $a_1X + 2Y + a_3Z = 0$; in particular, they sum to $\mathbf{o}$ in the group law. If $\operatorname{char} K \neq 2$, then $\mathbf{o}$ is not on this line. Hence, this line is not tangent to any of the order 2 points of E, implying that E has three distinct order 2 points over $\overline{K}$. It follows that $E(K)$ has zero, one, or three order 2 points.

Now, let K be a field with characteristic different than 2. The *Legendre family* of elliptic curves are described by an equation of the form

$$E_\lambda : y^2 = x(x-1)(x-\lambda)$$

for some $\lambda \in K \setminus \{0, 1\}$. The Legendre family is distinguished by the fact that the points $(0,0), (1,0)$, and $(\lambda, 0)$ all have order 2 in $E_\lambda(K)$. Indeed, we can easily check that the lines $x = 0, x = 1$, and $x = \lambda$ are all tangent to E_λ at $(0,0), (1,0)$, and $(\lambda, 0)$, respectively.

2.1 Ulmer's construction

Consider, now, a minor variant of the Legendre curve

$$E_d : y^2 = x(x+1)(x+t^d)$$

over the field $\mathbb{F}_p(t)$, for some odd prime p. We immediately see that the points

$$\mathbf{q}_0 = (0,0), \quad \mathbf{q}_1 = (-1,0), \quad \mathbf{q}_t = (-t^d, 0)$$

have order 2. For specific values of d, we can easily find additional points on E_d. Indeed, if we let $x = t$, we get $y^2 = t^2(t+1)(t^{d-1}+1)$. Recalling the Frobenius homomorphism of $\mathbb{F}_p(t)$ [7, Proposition 13.35], we see that if $d-1$ is a power of p, then $t^{d-1}+1 = (t+1)^{d-1}$. This implies $y^2 = t^2(t+1)^d$. Thus, $(t, t(t+1)^{d/2})$ is a point on E_d, given $d = p^f + 1$ for some $f \in \mathbb{N}$.

If we set $u = t^d$, then we can think of t as a d^{th} root of u. But note that if ζ_d is a fixed primitive d^{th} root of unity, then $\zeta_d^i t$ is also a d^{th} root of u for all integers i. Hence, if μ_d is the set of d^{th} roots of unity and $K_d = \mathbb{F}_p(\mu_d, t)$, we see that $E_d(K_d)$ contains all the points

$$\mathbf{p}_i = (\zeta_d^i t, \zeta_d^i t(\zeta_d^i t + 1)^{d/2}), \qquad i \in \mathbb{Z}/d\mathbb{Z}. \tag{4}$$

Alternatively, note K_d is the splitting field of the polynomial $x^d - t^d \in \mathbb{F}_p(t^d)[x]$, so $K_d/\mathbb{F}_p(t^d)$ is Galois by Proposition 1.8. Then, letting the elements of $\operatorname{Gal}(K_d/\mathbb{F}_p(t^d))$ act on $(t, t(t+1)^{d/2})$ coordinate-wise, the points $\mathbf{p}_i$ constitute the resulting orbit [30]. We stress that, apart from $\mathbf{p}_0$, all $\mathbf{p}_i$ lie in $K_d \setminus \mathbb{F}_p(t)$.

By Theorem 1.5, $E_d(\mathbb{F}_p(t))$ is finitely generated. The aim of this section is to give an annotation of Ulmer's proof that $E_d(\mathbb{F}_p(t))$ can have arbitrarily large rank as $d = p^f + 1$ varies. The general idea is as follows.

- We first work over $K_d \supset \mathbb{F}_p(t)$ as we have constructed many points (the $\mathbf{p}_i$s) on $E_d(K_d)$. We will see that the $\mathbf{p}_i$s are "sufficiently" independent: if we set $2E_d(K_d) = \{2\mathbf{p} : \mathbf{p} \in E_d(K_d)\}$ and consider $E_d(K_d)/2E_d(K_d)$ as a $\mathbb{Z}/2\mathbb{Z}$ vector space, the cosets of the $\mathbf{p}_i$s will be $\mathbb{Z}/2\mathbb{Z}$-linearly independent.
- After computing some relations among the $\mathbf{p}_i$s, an infinite-descent-type argument reveals that the subgroup of $E_d(K_d)$ generated by the $\mathbf{p}_i$s has rank $d-2$.
- We finally use a simple idea from Galois theory to find points in the subgroup generated by the $\mathbf{p}_i$s that lie in $E_d(\mathbb{F}_p(t))$ and show that these points generate a group of large rank.

2.1.1 A homomorphism from $E(K_d)$ onto $(\mathbb{Z}/2\mathbb{Z})^d$

We begin by considering an elliptic curve E' with Weierstraß form $y^2 = x^3 + a_2x^2 + a_4x$ over an arbitrary field k. Let $k^\times$ be the multiplicative group of k, and let $k^{\times 2} \subset k^\times$ be the subgroup of perfect squares. Consider an affine line $y = \lambda x + \mu$, and suppose it intersects E' at $\mathbf{r}_1, \mathbf{r}_2$, and $\mathbf{r}_3$. We note none these points are $\mathbf{o}$. The x-coordinates x_1, x_2, x_3 of $\mathbf{r}_1, \mathbf{r}_2, \mathbf{r}_3$ thus solve

$$x^3 + (a_2 - \lambda^2)x^2 + (a_4 - 2\lambda\mu)x - \mu^2 = 0.$$

If $\mu \neq 0$, then by Viète's formulas, $x_1x_2x_3 = \mu^2$ is a perfect square in $k^\times$. If $\mu = 0$ and we assume $\mathbf{r}_1 = (0,0)$, without loss of generality, then $x_2x_3 = a_4$. Finally, if we have a vertical line $x = \lambda$ intersecting E' at $\mathbf{o}, \mathbf{r}_1, \mathbf{r}_2$, then the product of the x-coordinates of $\mathbf{r}_1$ and $\mathbf{r}_2$ is again a perfect square in $k^\times$. Recalling that three points sum to $\mathbf{o}$ if and only if they are collinear, and checking the case of the 'line at infinity' $Z = 0$, it follows that $\tilde{\varphi} : E'(k) \to k^\times/k^{\times 2}$ given by

$$\tilde{\varphi} : \mathbf{p} \mapsto \begin{cases} x, & \text{if } \mathbf{p} = (x,y), \mathbf{p} \neq (0,0) \\ a_4, & \text{if } \mathbf{p} = (0,0) \\ 1, & \text{if } \mathbf{p} = \mathbf{o} \end{cases}$$

is a group homomorphism. As $2E'(k) = \{2\mathbf{p} : \mathbf{p} \in E'(k)\} \subseteq \ker\tilde{\varphi}$, it follows that $\tilde{\varphi}$ induces a homomorphism $\varphi : E'(k)/2E'(k) \to k^\times/k^{\times 2}$.

Now, for every $z \in \overline{k}$, there is a homomorphism $k(t)^\times \to \mathbb{Z}$ given by mapping $f(t) \in k(t)^\times$ to $\mathrm{ord}_{t=z} f(t)$, the order of the zero or pole of f at $t = z$. We conclude that, given $z_0, z_2, \ldots, z_{d-1} \in \overline{k}$, there is a map $\psi : k(t)^\times/k(t)^{\times 2} \to (\mathbb{Z}/2\mathbb{Z})^d$ given by sending

$$f \mapsto (\mathrm{ord}_{t=z_j} f(t) \pmod 2)_{j=0,1,\ldots,d-1}.$$

Now let the ground field be $k(t)$, and take E' an elliptic curve over $k(t)$. Then we have a homomorphism $\psi \circ \phi : E'(k(t))/2E'(k(t)) \to (\mathbb{Z}/2\mathbb{Z})^d$. Under the coordinate change $X = x + 1, Y = y$, we see that E_d has the Weierstraß form of E' with $a_2 = t^d - 2$ and $a_4 = 1 - t^d$. Thus, we have proved the following:

Proposition 2.1 ([30, Proposition 4.1])**.** *The map $E_d(K_d) \to (\mathbb{Z}/2\mathbb{Z})^d$ given by*

$$\mathbf{p} \mapsto \begin{cases} (\mathrm{ord}_{t=\zeta_d^j}(x+1) \pmod 2)_{j=0,\ldots,d-1}, & \text{if } \mathbf{p} = (x,y), \mathbf{p} \neq (-1,0) \\ (1,1,\ldots,1), & \text{if } \mathbf{p} = (-1,0) \\ (0,0,\ldots 0), & \text{if } \mathbf{p} = \mathbf{o} \end{cases}$$

induces a homomorphism $\nu : E_d(K_d)/2E_d(K_d) \to (\mathbb{Z}/2\mathbb{Z})^d$.

As a result, we have

Corollary 2.2. *The homomorphism ν maps the subgroup of $E_d(K_d)/2E_d(K_d)$ generated by $\mathbf{p}_i + 2E_d(K_d)$, $i \in \mathbb{Z}/d\mathbb{Z}$, onto $(\mathbb{Z}/2\mathbb{Z})^d$. Moreover, the cosets $\mathbf{p}_i + 2E(K_d)$ are $\mathbb{Z}/2\mathbb{Z}$-linearly independent.*

Proof. Recall that $\mathbf{p}_i = (\zeta_d^i t, \zeta_d^i t(\zeta_d^i t+1)^{d/2})$ from equation (4), and notice that $\zeta_d^i t+1 = 0$ if and only if $t = -\zeta_d^{-i} = \zeta_d^{d/2-i}$. Thus, ν maps the coset of $\mathbf{p}_i + 2E(K_d)$ to the vector with a 1 in the $d/2 - i$ position and 0s elsewhere. The claim follows. □

2.1.2 Computing relations among the $\mathbf{p}_i$s

From the previous subsection we see that, intuitively, the $\mathbf{p}_i$s have potential to generate a group of large rank. To make this precise, we now study the relations satisfied by the $\mathbf{p}_i$s. Recalling Abel's theorem (Proposition 1.15(c)), one way to do this is to consider functions that vanish at the $\mathbf{p}_i$s. For example, we see that the x- and y-coordinates of the $\mathbf{p}_i$s solve $y = x(x+1)^{d/2}$, whence $f = y - x(x+1)^{d/2}$ is a clear choice. We also have that the x- and y-coordinates of the $\mathbf{p}_i$s solve $yx^{d/2-1} = (-1)^i t^{d/2}(x+1)^{d/2}$. By considering the vertical line $x = \zeta_d^i t$, it is easily seen that $-\mathbf{p}_i$ is the reflection of $\mathbf{p}_i$ across the x-axis. Hence, the function $g = yx^{d/2-1} - t^{d/2}(x+1)^{d/2}$ vanishes at $(\zeta_d^i t, (-1)^i \zeta_d^i t(\zeta_d^i t+1)^{d/2}) = (-1)^i \mathbf{p}_i$.

Proposition 2.3. *The following equalities hold over $E_d(K_d)$:*

$$\textit{(a)} \quad \sum_{i=0}^{d-1} \mathbf{p}_i = \mathbf{q}_t \quad \textit{and} \quad \textit{(b)} \quad \sum_{i=0}^{d-1} (-1)^i \mathbf{p}_i = \mathbf{q}_1.$$

Proof. Consider the rational function $f = y - x(x+1)^{d/2} \in K_d(E_d)$. As f is a polynomial in x and y, it is regular at every point on E_d except possibly $\mathbf{o}$. The zeros of f on E_d have x-coordinates that solve $x^2(x+1)^d = x(x+1)(x+t^d)$. Noting $x = 0$ and $x = -1$ solve this polynomial, we can verify that $\mathbf{q}_0$ and $\mathbf{q}_1$ solve $f = 0$. As previously discussed, every $\mathbf{p}_i$, $i \in \mathbb{Z}/d\mathbb{Z}$, also solves $f = 0$. Thus, f has at least $d+2$ zeros over $E_d \cap \mathbb{A}_z$.

We now switch coordinates to $\mathbb{A}_y$, to analyse the behaviour of f at $\mathbf{o}$. By replacing x with $\frac{X}{Z}$ and y with $\frac{Y}{Z}$, we see that f has equation

$$\frac{YZ^{d/2} - X(X+Z)^{d/2}}{Z^{1+d/2}}$$

in projective coordinates. Setting $Y = 1$, we see that

$$f = \frac{z^{d/2} - x(x+z)^{d/2}}{z^{1+d/2}}$$

over $\mathbb{A}_y$. The equation of E_d over $\mathbb{A}_y$ is similarly $z = x(x+z)(x+t^d z)$, whence we see $x \mid z$ in $M_{\mathbf{o}}$. Recalling that $M_{\mathbf{o}} = (x,z) = (x)$ is a maximal ideal of $K_d[E_d]_{\mathbf{o}}$, we see x is irreducible in $K_d[E_d]_{\mathbf{o}}$. Thus, we have $x \in M_{\mathbf{o}} \setminus M_{\mathbf{o}}^2$, proving $\mathrm{ord}_{\mathbf{o}}(x) = 1$. It follows that $\mathrm{ord}_{\mathbf{o}}(z) = \mathrm{ord}_{\mathbf{o}}(x) + \mathrm{ord}_{\mathbf{o}}(x+z) + \mathrm{ord}_{\mathbf{o}}(x+t^d z) = 3$. Consequently, we have $\mathrm{ord}_{\mathbf{o}}(f) = -(d+2)$. Recalling that f has the same number of zeros as poles by Proposition 1.15(b), it follows that $\mathbf{q}_0$, $\mathbf{q}_1$, and the $\mathbf{p}_i$s are all the zeros of f. Moreover, each must be an order 1 zero of f. By Abel's theorem, we get

$$\sum_{i=0}^{d-1} \mathbf{p}_i = \mathbf{q}_0 + \mathbf{q}_1 = \mathbf{q}_t.$$

This proves (a).

For (b), consider the rational function $g = yx^{d/2-1} - t^{d/2}(x+1)^{d/2}$, which is again regular on E_d except possibly at $\mathbf{o}$. The x-coordinates of its zeros on $E_d \cap \mathbb{A}_z$ solve $x^{d-1}(x+1)(x+t^d) = t^d(x+1)^d$. Noting $x = -1$ is a root of this polynomial, we can verify that $\mathbf{q}_1$ is a zero of g. As previously discussed, all $(-1)^i\mathbf{p}_i$, $0 \leq i \leq d-1$, are also zeros of g. Now note

$$g = \frac{x^{d/2-1} - t^{d/2}(x+z)^{d/2}}{z^{d/2}}$$

over $\mathbb{A}_y$. We read off that $\mathrm{ord}_{\mathbf{o}}(g) = -(d+1)$ so that the previously mentioned zeros are, in fact, all the zeros of g. More precisely, they are order 1 zeros of g. Abel's theorem now yields the required result. □

Adding and subtracting the two relations yield

$$2\sum_{i=0}^{(d-2)/2} \mathbf{p}_{2i} = 2\sum_{i=0}^{(d-2)/2} \mathbf{p}_{2i+1} = \mathbf{q}_0. \tag{5}$$

Hence, the subgroup generated by the $\mathbf{p}_i$s contains every order 2 point of E_d.

There is a homomorphism $\mathbb{Z}^d \to E_d(K_d)$ sending $a = (a_0, \ldots, a_{d-1}) \in \mathbb{Z}^d$ to $\sum_{i=0}^{d-1} a_i\mathbf{p}_i$. By Proposition 2.3, $\langle (2,2,2,2,\ldots,2), (2,-2,2,-2,\ldots,-2)\rangle$ is in the kernel of this map. Thus, if

$$G = \mathbb{Z}^d/\langle (2,2,2,\ldots,2), (2,-2,2,-2,\ldots,-2)\rangle,$$

then we have an induced homomorphism $G \to E_d(K_d)$. As the $d \times 2$ $\mathbb{Z}$-matrix

$$\begin{bmatrix} 2 & 2 & 2 & 2 & \cdots & 2 \\ 2 & -2 & 2 & -2 & \cdots & -2 \end{bmatrix}$$

has Smith Normal Form[2]

$$\begin{bmatrix} 2 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 4 & 0 & 0 & \cdots & 0 \end{bmatrix},$$

we see[3]

$$G \cong \mathbb{Z}^{d-2} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}. \tag{6}$$

We remark that, by Proposition 2.3 and equation (5), every order 2 element of E_d is the image of an order 2 element of G. We to use this to establish the following:

Proposition 2.4. *The homomorphism $G \to E_d(K_d)$ given by mapping the coset of $(a_0, \ldots, a_{d-1})$ in G to $\sum_{i=0}^{d-1} a_i\mathbf{p}_i \in E_d(K_d)$ is injective. In particular, the subgroup of $E_d(K_d)$ generated by $\mathbf{p}_0, \mathbf{p}_1, \ldots, \mathbf{p}_{d-1}$ is isomorphic to G.*

Proof. Recall from Corollary 2.2 that the map $\nu : E_d(K_d)/2E_d(K_d) \to (\mathbb{Z}/2\mathbb{Z})^d$ restricted to the subgroup generated by $\mathbf{p}_0 + 2E_d(K_d), \ldots, \mathbf{p}_{d-1} + 2E_d(K_d)$ is a surjection. The homomorphism $G \to E_d(K_d)$ induces a homomorphism $G/2G \to E_d(K_d)/2E_d(K_d)$. As the image of $G \to E_d(K_d)$ is the subgroup of $E_d(K_d)$ generated by $\mathbf{p}_0, \ldots, \mathbf{p}_{d-1}$, we deduce that the composed map

$$G/2G \to E_d(K_d)/2E_d(K_d) \xrightarrow{\nu} (\mathbb{Z}/2\mathbb{Z})^d \tag{7}$$

[2]as defined in Part A Rings and Modules [4, Theorem 10.3].

[3]by the proof of [4, Theorem 11.4] from Part A Rings and Modules.

is surjective. As $|G/2G| = |(\mathbb{Z}/2\mathbb{Z})^d|$, we deduce that (7) is an isomorphism, so that $G/2G \to E_d(K_d)/2E_d(K_d)$ is injective.

Suppose $\sum_{i=0}^{d-1} a_i \mathbf{p}_i = \mathbf{o}$ for some $a = (a_0, \ldots, a_{d-1}) \in \mathbb{Z}^d$. Denote the coset of a in G by $\overline{a}$. Then, $\overline{a} \in 2G$, so that each a_i is even. Hence, we can write $a = 2a'$ in $\mathbb{Z}^d$. It follows that $\sum_{i=0}^{d-1} a_i' \mathbf{p}_i$ has order 2, so there is $b^{(1)} \in \mathbb{Z}^d$ whose coset in G has order 2 and $\sum_{i=0}^{d-1} a_i' \mathbf{p}_i = \sum_{i=0}^{d-1} b_i^{(1)} \mathbf{p}_i$. Then, the coset of $a' - b^{(1)}$ is in $2G$, so that $\frac{1}{2}(a' - b^{(1)}) \in \mathbb{Z}^d$ and $\sum_{i=0}^{d-1} \frac{a_i' - b_i^{(1)}}{2} \mathbf{p}_i$ has order 2. Repeating this argument, there are $b^{(\ell)}$, $\ell \in \mathbb{N}$, whose coset in G has order 2, such that $\frac{1}{2^k}(a' - \sum_{\ell=1}^{k} 2^{\ell-1} b^{(\ell)}) \in \mathbb{Z}^d$ for every $k \in \mathbb{N}$.

As $\overline{a} = 2\overline{a'} - \sum_{\ell=1}^{k} 2^\ell \overline{b^{(\ell)}}$, we see that $\overline{a}$ is divisible by arbitrarily large powers of 2 in G. As there are no non-trivial elements of $\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}$, and $\mathbb{Z}/4\mathbb{Z}$ divisible by arbitrarily large powers of 2, equation (6) forces $\overline{a} = 0_G$. Hence, $G \to E_d(K_d)$ is injective. □

Thus, we see that the subgroup of $E_d(K_d)$ generated by the $\mathbf{p}_i$s has rank $d-2$.

2.1.3 From K_d to $\mathbb{F}_p(t)$

We now establish $E_d(\mathbb{F}_p(t))$ also has large rank. Note $K_d/\mathbb{F}_p(t)$ is Galois as K_d is the splitting field of $x^d - 1 \in \mathbb{F}_p(t)[x]$. As every automorphism in $\mathrm{Gal}(K_d/\mathbb{F}_p(t))$ fixes t, $\mathrm{Gal}(K_d/\mathbb{F}_p(t)) \cong \mathrm{Gal}(\mathbb{F}_p(\mu_d)/\mathbb{F}_p)$. It is well-known that the latter is cyclic and generated by the Frobenius automorphism [7, Chapter 14.3]. Now, as $d = p^f + 1 \mid p^{2f} - 1$, we conclude $x^d - 1 \mid x^{p^{2f}} - x$. Conversely, if $x^d - 1 \mid x^{p^a} - x$ for some integer a, then $d | p^a - 1$. Hence, $d \mid p^a + p^f = p^f(p^{a-f} + 1)$, so that $d \mid p^{a-f} + 1$. Thus, $p^{a-f} \geq p^f$, implying $a \geq 2f$. Therefore, the smallest value of a for which $x^d - 1 \mid x^{p^a} - x$ is $2f$, so that $\mathbb{F}_p(\mu_d) = \mathbb{F}_{p^{2f}}$. Consequently, $\mathrm{Gal}(K_d/\mathbb{F}_p(t)) = \langle \mathrm{Fr} \rangle$ where $\mathrm{Fr} : K_d \to K_d$ is the automorphism acting on $\mathbb{F}_p(\mu_d)$ by the usual map $x \mapsto x^p$ for $x \in \mathbb{F}_p(\mu_d)$ and identity on t. Note Fr has order $2f$.

For $\mathbf{p} \in E_d(K_d)$, let Fr act coordinate-wise on $\mathbf{p}$, noting that as the equation of E_d is defined over $\mathbb{F}_p(t)$, $\mathrm{Fr}(\mathbf{p}) \in E_d(K_d)$. Let o denote the orbit of $\mathbf{p}$. If $\mathbf{q}_1, \mathbf{q}_2, \ldots, \mathbf{q}_r$ are the distinct elements of o, then Fr simply permutes them. Moreover, if $\mathbf{p}, \mathbf{q} \in E_d(K_d)$, recall that $\mathbf{p} + \mathbf{q}$ can be expressed by rational functions of the coordinates of $\mathbf{p}$ and $\mathbf{q}$. Thus, $\mathrm{Fr}(\mathbf{p} + \mathbf{q}) = \mathrm{Fr}(\mathbf{p}) + \mathrm{Fr}(\mathbf{q})$. Hence, $\sum_{\mathbf{q} \in o} \mathbf{q} \in E_d(\mathbb{F}_p(t))$ by Proposition 1.8(b).[4]

Proposition 2.5. *Let ϕ be Euler's totient function, and $\mathrm{ord}_e(p)$ the order of p in $(\mathbb{Z}/e\mathbb{Z})^\times$. Then,*

$$\mathrm{Rank}\, E_d(\mathbb{F}_p(t)) \geq \sum_{e | d, e > 2} \frac{\phi(e)}{\mathrm{ord}_e(p)}.$$

In particular, $\mathrm{Rank}\, E_d(\mathbb{F}_p(t)) \geq \frac{p^f - 1}{2f}$.

Proof. Recall $\mathbf{p}_i = (\zeta_d^i t, \zeta_d^i t(\zeta_d^i t + 1)^{d/2})$. Thus, $\mathrm{Fr}^j \mathbf{p}_i = (\zeta_d^{ip^j} t, \zeta_d^{ip^j} t(\zeta_d^{ip^j} t + 1)^{d/2}) = \mathbf{p}_{ip^j}$. Thus, the orbit of $\mathbf{p}_i$ is $\{\mathbf{p}_k : k \equiv ip^j \pmod d, 0 \leq j \leq 2f - 1\}$. If o is such an orbit write

$$\mathbf{p}_o = \sum_{\mathbf{p}_i \in o} \mathbf{p}_i \in E_d(\mathbb{F}_p(t)).$$

Let H be the subgroup of G corresponding to the subgroup generated by the $\mathbf{p}_o$, where o ranges over all possible orbits. We have $H \cong \mathbb{Z}^r \oplus H^{\mathrm{tor}}$, where H^{tor} is a subgroup of $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ by equation (6). Hence, $H/2H \cong (\mathbb{Z}/2\mathbb{Z})^{r+s}$ where $s = 0, 1$, or 2 depending on whether H contains $0, 1$, or all 3 order 2 elements of G.

[4] This is akin to the "trace" operator of algebraic number theory.

By Corollary 2.2, the points $\mathbf{p}_o$ are $\mathbb{Z}/2\mathbb{Z}$-linearly independent. Thus, $r+s$ is the number of orbits, which we now compute. Notice that $k \equiv ip^j \pmod{d}$ if and only if $\frac{k}{\gcd(i,d)} \equiv \frac{i}{\gcd(i,d)} p^j \pmod{\frac{d}{\gcd(i,d)}}$. Letting $e = \frac{d}{\gcd(i,d)}$, we conclude that the orbit of $\mathbf{p}_i$ consists of $\mathrm{ord}_e(p)$ elements when $e > 1$, and contains 1 element when $e = 1$. As the orbit of $\mathbf{p}_i$ is a subset of the $\phi(e)$ elements $\mathbf{p}_j$, where $\gcd(j,d) = \gcd(i,d)$, and each such $\mathbf{p}_j$ has a same-size orbit, this gives

$$\text{number of orbits} = 1 + \sum_{e|d, e\geq 2} \frac{\phi(e)}{\mathrm{ord}_e(p)}.$$

Finally, note that $\mathbf{q}_t = \sum \mathbf{p}_o$, where the sum ranges over the possible orbits. Also, as d is even, if $\mathbf{p}_i$ and $\mathbf{p}_j$ share the same orbit, then $i \equiv j \pmod{2}$. Thus, both $\sum_{i \text{ even}} \mathbf{p}_i$ and $\sum_{i \text{ odd}} \mathbf{p}_i$ are in the subgroup generated by the $\mathbf{p}_o$, so that $\mathbf{q}_0$ and $\mathbf{q}_1$ are both in the said subgroup. Thus, $s = 2$ and, noting $\phi(2)/\mathrm{ord}_2(p) = 1$,

$$\text{Rank } E_d(\mathbb{F}_p(t)) \geq r = \sum_{e|d, e>2} \frac{\phi(e)}{\mathrm{ord}_e(p)} \tag{8}$$

as claimed.

For the final remark, note that $d \mid p^{2f}-1$, implies $p^{2f} \equiv 1 \pmod{e}$ for every e dividing d. Thus, for all such e, $\mathrm{ord}_e(p) \leq 2f$. Combining equation (8) with $\sum_{e|d} \phi(e) = d$, we see that $\text{Rank } E_d(\mathbb{F}_p(t)) \geq \frac{p^f-1}{2f}$. □

As $f \to \infty$, it is clear that $\text{Rank } E_d(\mathbb{F}_p(t)) \to \infty$. Hence, we have proved the following:

Theorem 2.6. *Let p be an odd prime. The family of Legendre elliptic curves*

$$E_d : y^2 = x(x+1)(x+t^d)$$

defined over $\mathbb{F}_p(t)$ has unbounded rank as d varies.

3 Conceição's Construction

In this section, we present Conceição's construction [3] of a family of elliptic curves with arbitrarily large rank. The curves under consideration are so-called "quadratic twists" of the Legendre curve

$$\tilde{E}_d : (t^{q^d} - t)y^2 = x^3 - x,$$

defined over $\mathbb{F}_q(t)$, where $q \equiv 3 \pmod{4}$ and q is a power of a prime. The underlying philosophy of Conceição's construction is that elliptic curves with many integral points (points defined over $\mathbb{F}_q[t]$) tend to have large rank. Hence, Conceição demonstrates that $\tilde{E}_d(\mathbb{F}_q(t))$ has rank at least d by constructing many integral points on this curve.

The methodology of proof is similar to Ulmer's strategy showing that the family of Legendre curves had large rank over $\mathbb{F}_p(t)$. Recall that in section 2, we first proved that the $\mathbf{p}_i$s were $\mathbb{Z}/2\mathbb{Z}$-linearly independent, then computed relations among the $\mathbf{p}_i$s to prove that they generate a group of rank $d-2$. We follow a similar course of action: after constructing the integral points in section 3.1, and introducing some geometric ideas in section 3.2, we prove that the constructed points are $\mathbb{F}_p$-linearly independent in section 3.3. This allows us to conclude that the constructed points are $\mathbb{Z}$-linearly independent in section 3.4. We then apply similar methods to two other examples in section 3.5, and conclude by discussing a procedure for finding points on elliptic curves in section 3.6.

3.1 Construction of Points

We now describe Conceição's construction of many integral points on the curves $\tilde{E}_d$. We take a brief detour into the world of $\mathbb{F}_q$-additive polynomials.

3.1.1 Properties of $\mathbb{F}_q$-additive polynomials

Definition 3.1. Let q be a power of a prime p. An $\mathbb{F}_q$-additive polynomial is an element of $\mathbb{F}_q[t]$ of the form $A(t) = \sum_{i=0}^{N} a_i t^{q^i}$, for some integer $N \geq 0$ and $a_i \in \mathbb{F}_q$, for $0 \leq i \leq N$.

Note if $\mathbf{F} : t \mapsto t^q$ is the usual q-power Frobenius map, then we can regard every $\mathbb{F}_q$-additive polynomial as a polynomial in $\mathbf{F}$. For example, we can regard $A(t) = \sum_{i=0}^{N} a_i t^{q^i}$ as the polynomial $\sum_{i=0}^{N} a_i \mathbf{F}^i$, where $\mathbf{F}^0 = t$ and $\mathbf{F}^i = \mathbf{F} \circ \mathbf{F}^{i-1}$ for $i \geq 1$. We hence denote the set of $\mathbb{F}_q$-additive polynomials as $\mathbb{F}_q[\mathbf{F}]$.

Proposition 3.2. *The set of $\mathbb{F}_q$-additive polynomials, $\mathbb{F}_q[\mathbf{F}]$, is a commutative ring with multiplication given by composition. Moreover, $\mathbb{F}_q[\mathbf{F}]$ is isomorphic to $\mathbb{F}_q[t]$.*

Proof. It is clear that $(\mathbb{F}_q[\mathbf{F}], +)$ forms an additive subgroup of $(\mathbb{F}_q[t], +)$. Now suppose $A(t) = \sum_{i=0}^{N} a_i t^{q^i}$ and $B(t) = \sum_{i=0}^{M} b_i t^{q^i}$. Then

$$A(B(t)) = \sum_{i=0}^{N} a_i \left(\sum_{j=0}^{M} b_j t^{q^j} \right)^{q^i} = \sum_{i=0}^{N} \sum_{j=0}^{M} a_i b_j t^{q^{i+j}} = \sum_{k=0}^{M+N} \left(\sum_{\substack{i+j=k, \\ i,j \geq 0}} a_i b_j \right) t^{q^k}.$$

Hence, $\mathbb{F}_q[\mathbf{F}]$ is closed under multiplication. By symmetry, $A(B(t)) = B(A(t))$, so $\mathbb{F}_q[\mathbf{F}]$ is a commutative ring. The computation of $A \circ B$ makes it clear that the map $\mathbb{F}_q[t] \to \mathbb{F}_q[\mathbf{F}]$ given by

$$\sum_{i=0}^{N} a_i t^i \mapsto \sum_{i=0}^{N} a_i t^{q^i}$$

is an isomorphism of rings. □

Hence, given an $\mathbb{F}_q$-additive polynomial $A(t) = \sum_{i=0}^{N} a_i \mathbf{F}^i \in \mathbb{F}_q[\mathbf{F}]$, we can associate a polynomial $A_0(t) = \sum_{i=0}^{N} a_i t^i \in \mathbb{F}_q[t]$. Then, $A(t) = A_0(\mathbf{F})$.

3.1.2 Many points on E_A

We now work with a slightly more general elliptic curve

$$E_A : A(t)y^2 = x^3 - x,$$

where $A(t) = A_0(\mathbf{F})$ is a squarefree $\mathbb{F}_q$-additive polynomial. Note the curves $\tilde{E}_d$ are the curves E_A where $A(t) = t^{q^d} - t \in \mathbb{F}_q[\mathbf{F}]$. We shall show that, under certain assumptions on $A(t)$ that are readily satisfied by $t^{q^d} - t$, the curve E_A contains many integral points.

We begin by observing that if $d \equiv 3 \pmod 4$, the cubic curve $(t^d - t)y^2 = x^3 - x$ contains the point $(t^{\frac{d-1}{2}}, t^{\frac{d-3}{4}})$.

Lemma 3.3. *Let E_A be as above. Suppose $t^{m_i} - 1 \mid A_0(t)$, where the m_i are odd positive integers, with $1 \leq i \leq \ell$, and $q \equiv 3 \pmod 4$. Then E_A has at least ℓ integral points.*

Proof. For each i, write $A_0(t) = (t^{m_i} - 1)B_i(t)$. By the isomorphism between $\mathbb{F}_q[t]$ and $\mathbb{F}_q[\mathbf{F}]$ described in Proposition 3.2, this means that $A(t) = B_i(\mathbf{F})^{q^{m_i}} - B_i(\mathbf{F})$. Then, $q^{m_i} \equiv 3 \pmod 4$, so, by our earlier observation, E_A contains the points

$$\mathbf{b}_i = (B_i(\mathbf{F})^{(q^{m_i}-1)/2}, B_i(\mathbf{F})^{(q^{m_i}-3)/4}). \tag{9}$$

It remains to see that the $\mathbf{b}_i$s are distinct. Suppose that $A(t)$ has degree q^n, so that $B_i(\mathbf{F})$ has degree q^{n-m_i}. Then, $B_i(\mathbf{F})^{(q^{m_i}-1)/2}$ has degree $\frac{1}{2}(q^n - q^{n-m_i})$, so that the x-coordinates of the $\mathbf{b}_i$s all have different degrees. Hence, the $\mathbf{b}_i$s are a set of ℓ distinct, integral points. □

We now record some information about the $\mathbf{b}_i$s that will be useful when proving that the $\mathbf{b}_i$s are $\mathbb{F}_p$-linearly independent. For convenience, we set $F_i = B_i(\mathbf{F})^{(q^{m_i}-1)/2}$ and $G_i = B_i(\mathbf{F})^{(q^{m_i}-3)/4}$, so that $\mathbf{b}_i = (F_i, G_i)$.

Proposition 3.4. *Let $A(t)$ be as in the setting Lemma 3.3, and let $\mathbf{b}_i = (F_i, G_i)$, for $1 \le i \le \ell$, be the set of ℓ distinct integral points on E_A. Then for every i, there is a $\beta_i \in \mathbb{F}_q^\times$ such that $F_i' = \beta_i G_i^2$.*

Proof. Suppose $A(t) = \sum_{i=0}^{N} a_i t^{q^i}$ is square-free. Then $a_0 \neq 0$, so that $t \nmid B_i(t)$. Hence, the coefficient of t in the expansion of $B_i(\mathbf{F})$ is non-zero, implying $B_i(\mathbf{F})' \in \mathbb{F}_q^\times$. Thus, $F_i' = \left(\frac{q^{m_i}-1}{2} B_i(\mathbf{F})'\right) G_i^2$, so we can take $\beta_i = -2^{-1} B_i(\mathbf{F})' \neq 0$. □

Thus, we have constructed ℓ integral points on E_A, and have made a simple, but crucial, observation that will help show that these points are $\mathbb{F}_p$-linearly independent.

3.2 Some geometric machinery

One of the key ideas in modern geometry is that the properties of a geometric space can be characterised "well by ... the functions on this space" [33, Chapter 3.1]. The purpose of this section is to show that the points $\mathbf{b}_i$ can be viewed as maps between curves, enabling us to translate the problem of $\mathbb{Z}$-linear independence of the $\mathbf{b}_i$ to $\mathbb{Z}$-linear independence of maps between curves. As we shall later see, the latter can be more readily analysed.

3.2.1 Curves and rational maps

Let K be a field. A *(planar) curve* is defined as the locus of zeros of a polynomial $P \in K[x, y]$ viewed in projective space $\mathbb{P}\overline{K}^2$ [9, Chapter 5.1]. Notice that elliptic curves are a special type of curve. We similarly define the coordinate-ring $K[C]$, function field $K(C)$, and K-rational points $C(K)$ for a curve C as we did for elliptic curves.

Definition 3.5 ([26, Chapter I.3])**.** Let C_1 and C_2 be curves over a field K. A K-rational map from C_1 to C_2 is a map of the form

$$\phi : C_1 \to C_2, \qquad \phi : \mathbf{p} \mapsto [f_1(\mathbf{p}) : f_2(\mathbf{p}) : f_3(\mathbf{p})]$$

where $f_1, f_2, f_3 \in K(C_1)$ are functions, not all zero, so that for every point $\mathbf{p} \in C_1$, $[f_1(\mathbf{p}) : f_2(\mathbf{p}) : f_3(\mathbf{p})] \in C_2$ whenever the latter is well-defined. We denote the set of K-rational maps from C_1 to C_2 by $\mathrm{Rat}_K(C_1, C_2)$.

If the ground field K is clear from the context, or unimportant, we often drop the prefix K.

Remark 3.6. A rational map $\phi = [f_1 : f_2 : f_3]$ can be thought as the statement that there are p_1, p_2, and p_3 representatives of f_1, f_2, and f_3, respectively, such that if $P(X, Y, Z) = 0$ is the projective equation of C_2, then the formal equality

$$P(p_1(X, Y, Z), p_2(X, Y, Z), p_3(X, Y, Z)) = 0$$

holds. This is the perspective taken in this essay. The qualification "whenever ... well-defined" arises because there may be points $\mathbf{p} \in C_1$ where every f_i vanishes or some f_i has a pole. Hence, we exclude those points. See [9, Chapter 6] or [33, Chapter 7.5] for a more rigorous treatment.

3.2.2 A change of view

We now return to the particular case of elliptic curves. Suppose $\phi, \psi : C \to E$ are two rational maps from a curve C to an elliptic curve E. Then, we can define $(\phi+\psi) : C \to E$ sending $\mathbf{p} \in C$ to $\phi(\mathbf{p}) + \psi(\mathbf{p})$, the latter being addition using the group law on E. As addition on E is given by rational functions, it follows that $\phi + \psi$ is also a rational map. It follows that $\mathrm{Rat}(C, E)$ is an Abelian group.

Now let E be the elliptic curve $y^2 = x^3 - x$ over $\mathbb{F}_q$, C the curve $s^2 = A(t)$ over $\mathbb{F}_q$, and E_A as before. Let L be the function field of C. We show that the points of $E_A(L)$ can be identified with $\mathrm{Rat}_{\mathbb{F}_q}(C, E)$.

First, suppose $\mathbf{p} = [F(s,t) : G(s,t) : H(s,t)] \in E_A(L)$. Then, we have

$$A(t)G^2H = (sG)^2H = F^3 - FH^2.$$

Hence, given $(s, t) \in C(\mathbb{F}_q)$, we simply evaluate $[F : sG : H]$ at $(s, t) \in C$ to obtain a point on $E(\mathbb{F}_q)$, provided this is well-defined. This gives an element of $\mathrm{Rat}_{\mathbb{F}_q}(C, E)$. In the other direction, suppose that $\phi = [f_1 : f_2 : f_3] \in \mathrm{Rat}_{\mathbb{F}_q}(C, E)$. Then, $[f_1 : f_2/s : f_3] \in E_A(L)$. It is clear that these maps are inverses to each other, so $E_A(L)$ and $\mathrm{Rat}_{\mathbb{F}_q}(C, E)$ are in bijection with each other. Appealing to the fact that addition on an elliptic curve can be given by rational functions, it is easy to see that the map $E_A \to \mathrm{Rat}_{\mathbb{F}_q}(C, E)$ and its inverse are isomorphisms of Abelian groups.

Observe that we can regard $\mathbb{F}_q(t) \subseteq L$, and hence $E_A(\mathbb{F}_q(t)) \subseteq E_A(L)$. To each $\mathbf{b}_i = (F_i, G_i)$ we can therefore associate the rational map $\phi_i : C \to E$ given by sending $(s, t) \mapsto (F_i, sG_i)$. As $E_A(L) \cong \mathrm{Rat}_{\mathbb{F}_q}(C, E)$, and thus $E_A(\mathbb{F}_q(t))$ injects into $\mathrm{Rat}_{\mathbb{F}_q}(C, E)$, we see that the $\mathbf{b}_i$ are $\mathbb{Z}$-linearly independent if and only if the ϕ_i are.

3.3 A homomorphism

Recall that in Ulmer's proof that the family of Legendre curves have arbitrarily large rank, once the points were constructed on $E_d(K_d)$, the next task was to understand their rank. As explicit computations using the group law is unwieldy, it is natural to find a group homomorphism from the group of points on an elliptic curve to a familiar structure—in Ulmer's case $(\mathbb{Z}/2\mathbb{Z})^d$. Our aim in this section is essentially the same: we construct a homomorphism to a 1-dimensional $\overline{\mathbb{F}_q}(C)$-vector space—the space of differential forms on C (which we define below). This will reveal that the ϕ_i are $\mathbb{F}_p$-linearly independent.

3.3.1 Differential forms, the invariant differential, and linearity of the pull-back

We begin by discussing properties of differential forms from [26, Chapter II].

Definition 3.7. Let C be a curve over a field K. The space of differential forms on C, denoted by Ω_C is the $\overline{K}(C)$-vector space generated by symbols of the form df, $f \in \overline{K}(C)$, subject to the relations

- $d(f+g) = df + dg$, for every $f, g \in \overline{K}(C)$;
- $d(fg) = fdg + gdf$, $f, g \in \overline{K}(C)$;
- $d(a) = 0$, for every $a \in \overline{K}$.

Remark. Differential forms arise naturally when the ground field is $\mathbb{C}$. See [28].

We will see that differential forms can turn addition of rational maps from a curve C to an elliptic curve E (which is really addition using the group law on E) into addition on a vector space.

Lemma 3.8. *Ω_C is a 1-dimensional $\overline{K}(C)$-vector space.*

Proof. See [26, Proposition II.2.4.2]. □

An immediate consequence of Lemma 3.8 is that if df, dg are non-zero elements of Ω_C, then there is $h \in \overline{K}(C)$ such that $df = hdg$. We denote h by $\frac{df}{dg}$.

Let C_1 and C_2 be two curves over a field K, and let Ω_{C_1} and Ω_{C_2} be their respective spaces of differentials forms. Suppose that $\phi : C_1 \to C_2$ is a rational map. Then, there is a homomorphism of function fields

$$\phi^* : \overline{K}(C_2) \to \overline{K}(C_1), \qquad f \mapsto f \circ \phi.$$

Additionally, ϕ^* induces a pullback of differential forms (which we also denote by ϕ^*) given by

$$\phi^* : \Omega_{C_2} \to \Omega_{C_1}, \qquad \sum_{i=1}^{n} f_i dg_i \mapsto \sum_{i=1}^{n} \phi^*(f_i) d\phi^*(g_i).$$

As $\phi^* : \overline{K}(C_2) \to \overline{K}(C_1)$ is a field homomorphism, one easily checks that the induced map $\Omega_{C_2} \to \Omega_{C_1}$ is well-defined.

We now record some properties of the space of differential forms on an elliptic curve E with the usual Weierstraß equation (2) from [26, Chapter III].

Definition 3.9. The invariant differential $\omega \in \Omega_E$ is defined by

$$\omega = \frac{dx}{2y + a_1 x + a_3} = \frac{dy}{3x^2 + a_2 x + a_4}$$

One easily checks that $dx/(2y + a_1x + a_3) = dy/(3x^2 + a_2x + a_4)$ by differentiating through the Weierstraß equation of E (2).

Proposition 3.10 (Linearity of the Pullback)**.** *Let C be a curve and an E an elliptic curve, both defined over K. Suppose ϕ, ψ are elements of the Abelian group $\mathrm{Rat}_K(C, E)$. Then if ω is the invariant differential of E,*

$$(\phi + \psi)^*(\omega) = \phi^*\omega + \psi^*\omega.$$

Proof. See [26, Proposition III.5.2]. Even though the statement of [26, Proposition III.5.2] only deals with the case of C being an elliptic curve, the proof holds even without that assumption. □

Thus we see that the invariant differential has the special property that the it makes the pullback of differentials linear. Consequently, we have a well-defined homomorphism of Abelian groups $\mathrm{Rat}(C, E) \to \Omega_C$.

3.3.2 The ϕ_i are $\mathbb{F}_p$-linearly independent

Let E_A, E, and C be as in section 3.2.2. Recall that we had constructed various points $\mathbf{b}_i \in E_A(\mathbb{F}_q(t))$, and to each $\mathbf{b}_i$ we associated a rational map $\phi_i \in \mathrm{Rat}_{\mathbb{F}_q}(C, E)$. Suppose $\omega_E = \frac{dx}{2y}$ is the invariant differential on E. Noting that $A'(t) \in \mathbb{F}_q^\times$ as $A(t)$ is a square-free $\mathbb{F}_q$-additive polynomial, let $\omega_C \in \Omega_C$ be the differential $\frac{dt}{2s} = \frac{ds}{A'(t)}$. As ds and dt generate the 1-dimensional $\overline{\mathbb{F}_q}(C)$-vector space Ω_C, at least one of them must be non-zero. Consequently, we have $\omega_C \neq 0$. Then, by the calculation in Proposition 3.4,

$$\phi_i^*(\omega_E) = \frac{d(\phi^*(x))}{2\phi^*(y)} = \frac{dF_i(t)}{2sG_i(t)} = \beta_i G_i(t)\omega_C. \tag{10}$$

Lemma 3.11. *Suppose that there are integers $m_1, m_2, \ldots, m_\ell \in \mathbb{Z}$ so that $\sum_{i=1}^{\ell} m_i \mathbf{b}_i = \mathbf{o}$. Then $p \mid m_i$ for every $1 \leq i \leq \ell$.*

Proof. Suppose $\sum_{i=1}^{\ell} m_i \mathbf{b}_i = \mathbf{o}$. By section 3.2.2, this implies $\sum_{i=1}^{\ell} m_i \phi_i = 0$. By linearity of the pullback,

$$0 = \left(\sum_{i=1}^{\ell} m_i \phi_i\right)^* (\omega_E) = \sum_{i=1}^{\ell} \overline{m_i} \phi_i^*(\omega_E) = \left(\sum_{i=1}^{\ell} \overline{m_i} \beta_i G_i(t)\right) \omega_C,$$

where $\overline{m_i}$ denotes the reduction of m_i modulo p. As ω_C is non-zero, it follows that $\sum_{i=1}^{\ell} \overline{m_i} \beta_i G_i(t) = 0$ in $\mathbb{F}_q(t)$. But, we have already seen that the F_is have distinct degrees in the proof of Lemma 3.3, so, by Proposition 3.4, we conclude that the polynomials $\beta_i G_i$ also have distinct degrees. Hence, the polynomials $\beta_i G_i(t)$ are $\mathbb{F}_q$-linearly independent, so we must have $\overline{m_i} = 0$ for every i. □

We conclude that the ϕ_i, and hence the $\mathbf{b}_i$, are $\mathbb{F}_p$-linearly independent.

3.4 The p-torsion group

We now leverage Lemma 3.11 to prove that the $\mathbf{b}_i$ are $\mathbb{Z}$-linearly independent.

Definition 3.12. Let E be an elliptic curve and m a positive integer. The m-torsion subgroup, denoted $E[m]$, is the subgroup $\{\mathbf{p} \in E : m\mathbf{p} = \mathbf{o}\}$.

The elliptic curve E_A from before belongs to a family of elliptic curves known as *supersingular* elliptic curves. These elliptic curves are characterised by the fact that their p-torsion group is trivial. When an elliptic curve has Weierstraß form $y^2 = f(x)$, there is a simple criterion for determining if the curve is supersingular.

Proposition 3.13. *Let q be a power of an odd prime p, let C be a curve over $\mathbb{F}_q$, and let $L = \mathbb{F}_q(C)$ be its function field. Suppose E is an elliptic curve over L with Weierstraß form $y^2 = f(x)$, for some cubic polynomial $f \in L[x]$. Then, E is supersingular if and only if the coefficient of x^{p-1} in the expansion of $f(x)^{(p-1)/2}$ is zero.*

Proof. See [32, Lecture 1, Section 3]. □

We now return to the elliptic curve $E_A : A(t)y^2 = x^3 - x$. As before, let C be the curve $s^2 = A(t)$ over $\mathbb{F}_q$, and let L be its function field. Then, under the change of variable $(\tilde{x}, \tilde{y}) = (x, sy)$, the elliptic curve E_A assumes Weierstraß form $\tilde{y}^2 = \tilde{x}^3 - \tilde{x}$ over L. As

$$(\tilde{x}^3 - \tilde{x})^{(p-1)/2} = \tilde{x}^{(p-1)/2}(\tilde{x}^2 - 1)^{(p-1)/2},$$

the coefficient of $\tilde{x}^{(p-1)/2}$ in $(\tilde{x}^2-1)^{(p-1)/2}$ is zero provided $p \equiv 3 \pmod 4$ (as $\frac{p-1}{2}$ is then odd). As $(\tilde{x},\tilde{y}) = (x, sy)$ is a linear change of variable, supersingularity is preserved under this transformation due to the geometric description of the group law. Thus, E_A is supersingular over L when $p \equiv 3 \pmod 4$. Viewing $\mathbb{F}_q(t) \subset L$, it follows that E_A is supersingular over $\mathbb{F}_q(t)$.

Suppose there are $m_1, \dots m_\ell \in \mathbb{Z}$ not all zero such that $\sum_{i=1}^{\ell} m_i \mathbf{b}_i = \mathbf{o}$. Let p^k be the largest power of p dividing $m_1, \dots, m_\ell$. Then $m_i' = m_i/p^k$ is an integer for each i, and

$$\sum_{i=1}^{\ell} m_i \mathbf{b}_i = p^k \sum_{i=1}^{\ell} m_i' \mathbf{b}_i = \mathbf{o}.$$

As the p-torsion group of E_A is trivial, it follows that $\sum_{i=1}^{\ell} m_i' \mathbf{b}_i = \mathbf{o}$. But then there exists some integer i such that $p \nmid m_i'$, contradicting Lemma 3.11. Hence, the $\mathbf{b}_i$ are $\mathbb{Z}$-linearly independent. We have thus proved the following:

Theorem 3.14 ([3, Theorem 7.1])**.** *Let q be a power of a prime such that $q \equiv 3 \pmod 4$, and let $A(t) = A_0(\mathbf{F})$ be a squarefree $\mathbb{F}_q$-additive polynomial. Suppose there are distinct odd positive integers $m_1, m_2, \dots m_\ell$ such that $t^{m_i} - 1 \mid A_0(t)$. Then the elliptic curve $E_A : A(t)y^2 = x^3 - x$ contains the $\mathbb{Z}$-linearly independent integral points $\mathbf{b}_1, \dots, \mathbf{b}_\ell$ defined in (9). In particular, E_A has rank at least ℓ.*

If we now specialise $A(t) = t^{q^d} - t$, we see that for every odd divisor m of d, the polynomial $t^m - 1$ divides $A_0(t) = t^d - 1$. Thus, we conclude that the curves $\tilde{E}_d : (t^{q^d} - t)y^2 = x^3 - x$ considered at the start of this section has rank at least the number of odd divisors of d. This is clearly unbounded as d varies.

3.5 Two more examples

We now show how Conceição's proof adapts to two other elliptic curves. In both examples, we follow Conceição's construction of explicit points on the curves [3]. Conceição remarks (without proof) that the methods of Theorem 3.14 may be adapted to the elliptic curve $A(t)x^3 = y^2 - y$. We fill in the details in the first example below. The proof of $\mathbb{Z}$-linear independency of the constructed points in the second example is also similar to the proof of Theorem 3.14, and is an original extension of the author's.

Theorem 3.15 ([3, Remark 7.3])**.** *Suppose $A(t) = A_0(\mathbf{F})$ is a squarefree $\mathbb{F}_q$-additive polynomial, where q is a prime power such that $q \equiv 2 \pmod 3$. Suppose there are distinct odd positive integers $m_1, m_2, \dots m_\ell$ such that $t^{m_i} - 1 \mid A_0(t)$. Then the elliptic curve $E_A : y^2 - y = A(t)x^3$ has rank at least ℓ.*

Remark. These curves are so-called *cubic twists* of the Hessian elliptic curve. We discuss the properties of the Hessian family in section 4.

Proof. We begin with the observation that the curve $y^2 - y = (t^d - t)x^3$ contains the integral point $(t^{(d-2)/3}, t^{d-1})$ whenever $d \equiv 2 \pmod 3$. Writing $A_0(t) = (t^{m_i} - 1)B_i(t)$ for each i, so that $A(t) = (B_i(\mathbf{F}))^{q^{m_i}} - B_i(\mathbf{F})$, we find E_A contains the integral point $\mathbf{b}_i = (B_i(\mathbf{F})^{(q^{m_i}-2)/3}, B_i(\mathbf{F})^{q^{m_i}-1})$. Write $\mathbf{b}_i = (F_i(t), G_i(t))$. Then, as the degree of $B_i(\mathbf{F})$ is q^{n-m_i}, the degree of G_i is $q^n - q^{n-m_i}$. It follows that the G_is all have different degrees.

Let C be the non-singular curve $s^3 = A(t)$ over $\mathbb{F}_q$, E the elliptic curve $y^2 - y = x^3$ over $\mathbb{F}_q$, and $L = \mathbb{F}_q(C)$. We again have that if $[F(s,t) : G(s,t) : H(s,t)] \in E_A(L)$, then

evaluating $(s,t) \mapsto [sF : G : H]$ gives a $\mathbb{F}_q$-rational map $C \to E$. Hence, this determines a map $E_A(L) \to \mathrm{Rat}_{\mathbb{F}_q}(C,E)$. As before, this map is invertible and is an isomorphism of Abelian groups. Viewing $E_A(\mathbb{F}_q(t)) \subset E_A(L)$, we can associate each $\mathbf{b}_i$ to a rational map $\phi_i \in \mathrm{Rat}_{\mathbb{F}_q}(C,E)$; moreover the $\mathbf{b}_i$ are $\mathbb{Z}$-linearly independent if and only if the ϕ_i are.

Let $\omega_E = \frac{dy}{3x^2}$ be the invariant differential on E. Then,

$$\phi_i^*(\omega_E) = \frac{dG_i(t)}{3F_i^2 s^2} = \frac{G_i' dt}{3F_i^2 s^2}.$$

Now, if $\beta_i = -(B_i(\mathbf{F}))'$, then $\beta_i \in \mathbb{F}_q^\times$ because $A(t)$ is square-free and

$$G_i' = -B_i(\mathbf{F})^{q^{m_i}-2}(B_i(\mathbf{F}))' = -F_i^3(B_i(\mathbf{F}))' = \beta_i (F_i)^3. \tag{11}$$

Hence, as the G_is all have different degrees, so do the F_is by equation (11). Thus, if $\omega_C = \frac{dt}{3s^2} \in \Omega_C$,

$$\phi_i^*(\omega_E) = \beta_i F_i \omega_C.$$

As ds, dt generate Ω_C, and $A'(t) \in \mathbb{F}_q^\times$, we again see $\omega_C = \frac{dt}{3s^2} = \frac{ds}{A'(t)}$ is non-zero. By essentially the same argument as Lemma 3.11, we see that the ϕ_is, and hence the $\mathbf{b}_i$s, are $\mathbb{F}_p$-linearly independent.

It remains to show that the curve E_A is supersingular. Observe that the change of variable $(\tilde{x}, \tilde{y}) = (sx, y)$ puts E_A in the form of E over L; thus, E_A is supersingular over L, and hence over $\mathbb{F}_q(t)$, provided E is supersingular over L. For q a power of 2, we give an elementary proof of this in Appendix B. If q is odd, then we can write the equation of E as $(y - 2^{-1})^2 = x^3 + 4^{-1}$. So, if we change coordinates $X = x$, $Y = y - 2^{-1}$, E will then have Weierstraß form $Y^2 = X^3 + 4^{-1}$. Then, the coefficient of X^{p-1} in the expansion of $(X^3 + 4^{-1})^{(p-1)/2}$ is zero if $3 \nmid p-1$. Hence, by Proposition 3.13, we see that E is supersingular if $p \equiv 2 \pmod 3$ (which must be the case as $q \equiv 2 \pmod 3$).

Thus, suppose there are integers $m_1, \dots m_\ell$ not all zero such that $\sum_{i=1}^{\ell} m_i \mathbf{b}_i = \mathbf{o}$. As E_A is supersingular, we can assume the m_i are not all divisible by p. But then, this contradicts the $\mathbb{F}_p$-linear independence of the $\mathbf{b}_i$s. It follows that the $\mathbf{b}_i$s are $\mathbb{Z}$-linearly independent; consequently, $E_A(\mathbb{F}_q(t))$ has rank at least ℓ. □

Corollary 3.16. *The elliptic curve $(t^{q^d} - t)x^3 = y^2 - y$ has rank at least the number of odd divisors of d over $\mathbb{F}_q(t)$, where $q \equiv 2 \pmod 3$. In particular, this curve has unbounded rank as d varies.*

Proof. As we have noted before, if $A(t) = t^{q^d} - t$ then for every odd divisor m of d, $t^m - 1 \mid A_0(t)$. Thus by Theorem 3.15, the claim follows. □

We now present a second family of elliptic curves with arbitrarily large rank.

Theorem 3.17. *Let n be an odd, positive integer. Suppose $p \geq 7$ is a prime, and $q \equiv 3 \pmod 4$ is a power of p. Then the family of elliptic curves $E_n^{(2)} : y^2 = x^3 - (t^{q^n+1} + 1)x$ has unbounded rank over $\mathbb{F}_q(t)$ as n varies.*

We begin with the following lemma:

Lemma 3.18. *Suppose $A = (a_{ij})_{i,j=1,2}$ is a 2×2 orthogonal matrix over $\mathbb{F}_q$. Then, for any non-negative integer m, the identity*

$$(a_{11}X + a_{12}Y)^{q^m+1} + (a_{21}X + a_{22}Y)^{q^m+1} = X^{q^m+1} + Y^{q^m+1}$$

holds over $\mathbb{F}_q[X,Y]$.

Proof. This follows from the following computation:

$$\begin{aligned} X^{q^m+1} + Y^{q^m+1} &= \begin{bmatrix} X^{q^m} & Y^{q^m} \end{bmatrix} \begin{bmatrix} X \\ Y \end{bmatrix} \\ &= \begin{bmatrix} X^{q^m} & Y^{q^m} \end{bmatrix} A^T A \begin{bmatrix} X \\ Y \end{bmatrix} \\ &= \left(A \begin{bmatrix} X^{q^m} \\ Y^{q^m} \end{bmatrix} \right)^T \left(A \begin{bmatrix} X \\ Y \end{bmatrix} \right) \\ &= \begin{bmatrix} (a_{11}X + a_{12}Y)^{q^m} \\ (a_{21}X + a_{22}Y)^{q^m} \end{bmatrix}^T \begin{bmatrix} a_{11}X + a_{12}Y \\ a_{21}X + a_{22}Y \end{bmatrix} \\ &= (a_{11}X + a_{12}Y)^{q^m+1} + (a_{21}X + a_{22}Y)^{q^m+1}. \end{aligned}$$

□

Proof (of Theorem 3.17). Let m be a (odd) positive divisor of n, so that $q^m + 1 \mid q^n + 1$. Set $r = \frac{q^n+1}{q^m+1}$. Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ be a 2×2 orthogonal $\mathbb{F}_q$ matrix with $abcd \neq 0$. We may further assume $a = d$ and $b = -c$. Certainly, such a matrix exists over $\mathbb{F}_q$ as we could take $A = \begin{bmatrix} 3 \cdot 5^{-1} & 4 \cdot 5^{-1} \\ -4 \cdot 5^{-1} & 3 \cdot 5^{-1} \end{bmatrix}$. Conceição notes that the curve $E_n^{(2)}$ has the integral point

$$\mathbf{b}_r = (-(ct^r + d)^{(q^m+1)/2}, (at^r + b)^{(q^m+1)/2}(ct^r + d)^{(q^m+1)/4}).$$

We explain the existence of this point in the next section. For now, we can verify that $\mathbf{b}_r$ lies on $E_n^{(2)}$ as by Lemma 3.18:

$$t^{q^n+1} + 1 = (t^r)^{q^m+1} + 1 = (at^r + b)^{q^m+1} + (ct^r + d)^{q^m+1}.$$

Then,

$$(at^r + b)^{q^m+1}(ct^r + d)^{(q^m+1)/2} = -(ct^r + d)^{3(q^m+1)/2} + (ct^r + d)^{(q^m+1)/2}(t^{q^n+1} + 1)$$

from which it is clear that $\mathbf{b}_r \in E_n^{(2)}$. Note the conditions of the theorem ensure that $q^m + 1 \equiv 0 \pmod 4$, so that $\mathbf{b}_r$ is a well-defined integral point of $E_n^{(2)}(\mathbb{F}_q(t))$.

Let C be the curve $s^4 = t^{q^n+1} + 1$ over $\mathbb{F}_q$, $L = \mathbb{F}_q(C)$ its function field, and E be the elliptic curve $y^2 = x^3 - x$ over $\mathbb{F}_q$. Note if $y^2 = x^3 - s^4x$, then $(y/s^3)^2 = (x/s^2)^3 - x/s^2$. Hence, under a linear coordinate change in L, the elliptic curve $E_n^{(2)}$ assumes the equation of E; consequently, by the computation in section 3.4, $E_n^{(2)}$ is supersingular over L. Also, every point $(F, G) \in E_n^{(2)}(L)$ corresponds to a rational map $(s, t) \mapsto (F/s^2, G/s^3)$ from $C \to E$. As usual, this correspondence is invertible so $E_n^{(2)}(L) \cong \mathrm{Rat}_{\mathbb{F}_q}(C, E)$. Viewing $E_n^{(2)}(\mathbb{F}_q(t)) \subset E_n^{(2)}(L)$, let ϕ_r be the $\mathbb{F}_q$-rational map corresponding to each $\mathbf{b}_r$.

Let $\omega_E = \frac{dx}{2y}$ be the invariant differential of E. Then if $\mathbf{b}_r = (F_r(t), G_r(t))$

$$\phi_r^*(\omega_E) = \frac{d(F_r(t)/s^2)}{2G_r(t)/s^3} = \frac{sF_r'(t)dt}{2G_r(t)} - \frac{F_r(t)ds}{G_r(t)}.$$

Now, $s^4 = t^{q^n+1} + 1$ implies $4s^3t^{-q^n}ds = dt$. Consequently, as ds and dt generate Ω_C, the

differential $t^{-q^n}ds$ is non-zero. Thus, noting $r \equiv 1 \pmod{p}$,

$$\begin{aligned}
\phi_r^*(\omega_E) &= \left(\frac{2s^4F_r'(t)}{G_r(t)} - \frac{t^{q^n}F_r(t)}{G_r(t)}\right)\frac{ds}{t^{q^n}} \\
&= \left(\frac{-c(t^{q^n+1}+1)(ct^r+d)^{(q^m-1)/2}t^{r-1} + t^{q^n}(ct^r+d)^{(q^m+1)/2}}{(at^r+b)^{(q^m+1)/2}(ct^r+d)^{(q^m+1)/4}}\right)\frac{ds}{t^{q^n}} \\
&= \left(\frac{-c(t^{q^n+1}+1)(ct^r+d)^{(q^m-3)/4}t^{r-1} + t^{q^n}(ct^r+d)^{(q^m+1)/4}}{(at^r+b)^{(q^m+1)/2}}\right)\frac{ds}{t^{q^n}} \\
&= t^{r-1}(ct^r+d)^{(q^m-3)/4}\left(\frac{-c(t^{q^n+1}+1) + t^{q^n-r+1}(ct^r+d)}{(at^r+b)^{(q^m+1)/2}}\right)\frac{ds}{t^{q^n}} \\
&= t^{r-1}(ct^r+d)^{(q^m-3)/4}\left(\frac{t^{q^n-r+1}d - c}{(at^r+b)^{(q^m+1)/2}}\right)\frac{ds}{t^{q^n}}.
\end{aligned}$$

Recalling that $q^n+1 = r(q^m+1)$, $a=d$, and $b=-c$ gives

$$\begin{aligned}
\phi_r^*(\omega_E) &= t^{r-1}(ct^r+d)^{(q^m-3)/4}\left(\frac{t^{rq^m}d - c}{(at^r+b)^{(q^m+1)/2}}\right)\frac{ds}{t^{q^n}} \\
&= t^{r-1}(ct^r+d)^{(q^m-3)/4}\left(\frac{(at^r+b)^{q^m}}{(at^r+b)^{(q^m+1)/2}}\right)\frac{ds}{t^{q^n}} \\
&= (t^{r-1}(at^r+b)^{(q^m-1)/2}(ct^r+d)^{(q^m-3)/4})\frac{ds}{t^{q^n}}.
\end{aligned}$$

The degree of the first non-zero term in the polynomial $t^{r-1}(at^r+b)^{(q^m-1)/2)}(ct^r+d)^{(q^m-3)/4}$ is $r-1$. Therefore, these polynomials are $\mathbb{F}_q$-linearly independent. Consequently, the ϕ_r, and hence the $\mathbf{b}_r$, are $\mathbb{F}_p$-linearly independent. The fact that $E_n^{(2)}(\mathbb{F}_q(t))$ is supersingular allows us to conclude that the $\mathbf{b}_r$ are $\mathbb{Z}$-linearly independent.

We conclude that the $E_n^{(2)}(\mathbb{F}_q(t))$ has rank at least the number of divisors of n. This is clearly unbounded as n varies. □

We have thus seen two additional examples of families of elliptic curves that have unbounded rank over appropriate function fields $\mathbb{F}_q(t)$. In these classes of examples, we have seen that proving a set of integral points are $\mathbb{Z}$-linearly independent followed by essentially the same technique: after viewing the integral points as rational maps between a curve and a supersingular elliptic curve, we consider the action of the rational maps on the invariant differential. By linearity of the pullback, this allowed us to see that our constructed points were $\mathbb{F}_p$-linearly independent. We concluded our argument by appealing to supersingularity. It remains to consider the task of constructing integral points on elliptic curves.

3.6 The Conceição-Shioda Procedure for constructing points

In both Ulmer's construction and the first two of Conceição's constructions (Theorems 3.14 and 3.15), the key step to proving that their elliptic curves have unbounded rank rested on finding a *single* integral point. For example, Ulmer first found $(t, t(t+1)^{(p^f+1)/2})$ on the Legendre curve $y^2 = x(x+1)(x+t^{p^f+1})$ before considering its $\mathrm{Gal}(K_d/\mathbb{F}_p(t^d))$-orbit to find the d points $\mathbf{p}_i$ in equation (4). Similarly, in Theorems 3.14 and 3.15, Conceição first finds an integral point on each of the curves $(t^d-t)y^2 = x^3-x$ and $y^2-y = (t^d-t)x^3$ before employing the theory of $\mathbb{F}_q$-additive polynomials to find many integral points on

$A(t)y^2 = x^3 - x$ and $y^2 - y = A(t)x^3$, respectively. In this section, we exhibit a procedure of Shioda [22, Sections 2-3] that was adapted by Conceição [3, Section 3] to construct (integral) points on elliptic curves. We hence refer to this procedure as the "Conceição-Shioda procedure". We will show how this procedure explains the points $\mathbf{b}_r$ in the proof of Theorem 3.17. As usual, we begin with the definitions.

Definition 3.19. Let n be a positive integer, and let $A = (a_{ij})_{1\leq i,j\leq n}$ be a $n \times n$ matrix with non-negative integer entries and non-zero determinant. Let $e = (e_1, e_2, \ldots, e_n) \in \mathbb{F}_q^n$. The *Delsarte hypersurface* associated to A and e, $\mathcal{X}_A(e)$, is defined to be the set of solutions $(X_1, X_2, \ldots, X_n) \in \mathbb{F}_q^n$ to the equation

$$\sum_{i=1}^{n} e_i X_1^{a_{i1}} X_2^{a_{i2}} \cdots X_n^{a_{in}} = 0.$$

Remark 3.20. These are so-named due to Delsarte's investigation of the number of solutions to similar equations over $\mathbb{F}_q$. See [6, Section 3].

Proposition 3.21. *Let $e = (e_i)_{1\leq i\leq n} \in \mathbb{F}_q^n$. Suppose A and C are two $n \times n$ matrices with non-negative integer entries and non-vanishing determinant. Then, there is a positive integer d such that $B = dA^{-1}C$ has integer entries, and we have a map $\mathcal{X}_{dC}(e) \to \mathcal{X}_A(e)$ given by*

$$(X_1, X_2, \ldots, X_n) \mapsto \left(\prod_{j=1}^{n} X_j^{b_{1j}}, \prod_{j=1}^{n} X_j^{b_{2j}}, \ldots, \prod_{j=1}^{n} X_j^{b_{nj}} \right)$$

whenever the latter is well-defined.

Remark 3.22. Just as with rational maps, this map need not make sense when, for example, there are i, j such that $X_i = 0$ and $b_{ji} < 0$. This is the only exception, though.

Proof (of Proposition 3.21). The existence of such an integer d is clear. The following computation affirms the existence of the proposed map:

$$\sum_{i=1}^{n} e_i \prod_{j=1}^{n} \left(\prod_{k=1}^{n} X_k^{b_{jk}} \right)^{a_{ij}} = \sum_{i=1}^{n} e_i \prod_{j=1}^{n} \prod_{k=1}^{n} X_k^{a_{ij}b_{jk}} = \sum_{i=1}^{n} e_i \prod_{k=1}^{n} X_k^{\sum_{j=1}^{n} a_{ij}b_{jk}} = \sum_{i=1}^{n} e_i \prod_{k=1}^{n} X_k^{dc_{ik}}.$$

□

Definition 3.23. Let E be the elliptic curve

$$y^2 + a_1(t)xy + a_3(t)y = x^3 + a_2(t)x^2 + a_4(t)x + a_6(t)$$

over $\mathbb{F}_q(t)$. The *(affine) elliptic surface*[5] $\mathcal{E}$ associated to E is defined to be the set of solutions $([X : Y : Z], T) \in \mathbb{P}\overline{\mathbb{F}_q}^2 \times \overline{\mathbb{F}_q}$ to

$$Y^2Z + a_1(T)XYZ + a_3(T)YZ^2 = X^3 + a_2(T)X^2Z + a_4(T)XZ^2 + a_6(T)Z^3.$$

Remark 3.24. The elliptic surface $\mathcal{E}$ can be thought of as the graph of E as t varies. In this analogy, a point $[X(t) : Y(t) : Z(t)]$ on the elliptic curve E corresponds to a parametrised curve $([X(T) : Y(T) : Z(T)], T)$ on $\mathcal{E}$.

[5] Our definition of an elliptic surface slightly departs from the usual definition in the literature, but this definition suffices for our purposes. See [32, Lecture 3] for the full construction.

Conceição's idea is to view appropriate elliptic surfaces $\mathcal{E}$ as Delsarte hypersurfaces. By Proposition 3.21, this results in a map $\mathcal{X}_{dC}(e) \to \mathcal{E}$ for suitable d, C, and e, where $\mathcal{X}_{dC}(e)$ is a Delsarte hypersurface. Then, the images of parametrised curves ℓ on $\mathcal{X}_A(c)$ are parametrised curves on $\mathcal{E}$, and thus correspond to a point on the elliptic curve E by Remark 3.24.

For example, take the elliptic curve $E_n^{(2)}$ from Theorem 3.17. The associated elliptic surface $\mathcal{E}$ is

$$Y^2Z + (-X)^3 - T^d(-X)Z^2 - (-X)Z^2 = 0, \tag{12}$$

where $d = q^n + 1$, n is odd, and $q \equiv 3 \pmod 4$ is a power of a prime $p \geq 7$. If we think of this as a Delsarte hypersurface, then its associated matrix is

$$A = \begin{bmatrix} 0 & 2 & 1 & 0 \\ 3 & 0 & 0 & 0 \\ 1 & 0 & 2 & d \\ 1 & 0 & 2 & 0 \end{bmatrix}.$$

Then if $s = q^m + 1$ for some $m \mid n$,

$$A^{-1} = \begin{bmatrix} 0 & 1/3 & 0 & 0 \\ 1/2 & 1/12 & 0 & -1/4 \\ 0 & -1/6 & 0 & 1/2 \\ 0 & 0 & 1/d & -1/d \end{bmatrix} \quad \text{and} \quad A^{-1}\begin{bmatrix} s & 0 & 0 & 0 \\ 0 & s & 0 & 0 \\ 0 & 0 & d & 0 \\ 0 & 0 & 0 & d \end{bmatrix} = \begin{bmatrix} 0 & s/3 & 0 & 0 \\ s/2 & s/12 & 0 & -d/4 \\ 0 & -s/6 & 0 & d/2 \\ 0 & 0 & 1 & -1 \end{bmatrix}.$$

Suppose that $12 \mid s$. By Proposition 3.21, there is a map from the Delsarte hypersurface $\mathcal{X}$ given by

$$X_1^s + X_2^s - X_3^d - X_4^d = 0 \tag{13}$$

to the elliptic surface $\mathcal{E}$ given by

$$(X_1, X_2, X_3, X_4) \mapsto \left([-X_2^{s/3} : X_1^{s/2}X_2^{s/12}X_4^{-d/4} : X_2^{-s/6}X_4^{d/2}], X_3/X_4\right).$$

Note the extra minus sign in front of $X_2^{s/3}$ comes from the way we have written the equation of the elliptic surface $\mathcal{E}$ in equation (12). We rearrange the map $\mathcal{X} \to \mathcal{E}$ to read

$$(X_1, X_2, X_3, X_4) \mapsto \left([-X_2^{s/2}X_4^{d/4} : X_1^{s/2}X_2^{s/4} : X_4^{3d/4}], X_3/X_4\right).$$

One can now verify that this map $\mathcal{X} \to \mathcal{E}$ holds when just $4 \mid s$.

Now note there are several parametrised curves on $\mathcal{X}$. For example, Conceição takes $(1, T^r, T, 1)$, where $r = d/s$. This maps to the parametrised curve $([-T^{d/2} : T^{d/4} : 1], T)$ on $\mathcal{E}$, and (by our earlier remarks) we see that this corresponds to the integral point $(-t^{d/2} : t^{d/4})$ on $E_n^{(2)}$. More generally, Lemma 3.18 shows that the group of 2×2 orthogonal $\mathbb{F}_q$ matrices, $O_2(\mathbb{F}_q)$, acts on $\mathcal{X}$. Indeed, if $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in O_2(\mathbb{F}_q)$ and $(X_1, X_2, X_3, X_4) \in \mathcal{X}$, then $(aX_2 + bX_1, cX_2 + dX_1, X_3, X_4) \in \mathcal{X}$. We readily obtain new parametrised curves $(aT^r + b, cT^r + d, T, 1)$ on $\mathcal{X}$ which map to the curves

$$([-(cT^r + d)^{s/2} : (aT^r + b)^{s/2}(cT^r + d)^{s/4} : 1], T)$$

on $\mathcal{E}$. These curves correspond to the points $\mathbf{b}_r$ the proof of Theorem 3.17.

We conclude this section by mentioning that in [3, Section 3], Conceição employs this procedure to find integral points on the elliptic curves $(t^d - t)y^2 = x^3 - x$ and $y^2 - y = (t^d - t)x^3$, and also explains the integral point on Ulmer's contstruction this way.

4 The Hessian Family

The aim of this section is to give an account of the author's attempt to generalise the approaches of Ulmer and Conceição to the *Hessian* family of elliptic curves. This is a family of elliptic curves that come with a order 3 rational point. In section 4.1, we introduce some theory regarding order 3 points on elliptic curves and describe the Hessian family. In section 4.2, we search for suitable Hessian curves that would allow for a construction similar to Ulmer's construction of large-rank Legendre curves. Our strategy is of a number-theoretic flavour. In section 4.3, we describe the results of applying Conceição-Shioda. In section 4.4, we give a geometric reinterpretation of our earlier number-theoretic approach and apply Conceição-Shioda in this new framework. We conclude with some directions for future investigation in section 4.5.

4.1 Order 3 points on Elliptic curves

Recall the Weierstraß equation of an elliptic curve:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

The Legendre family of elliptic curves has the special property that they contain all three order 2 points. In this section, we seek to describe a family of elliptic curves with order 3 points, the *Hessian* family, and a slight generalisation. Our approach is modelled off [35] and [10], with minor simplifications.

Proposition 4.1. *Let K be a field, and E an elliptic curve over K. Then, E has at most eight order 3 points.*

Proof. Suppose E has Weierstraß equation as above, and let $\mathbf{p} \in E(\overline{K})$ have order 3; i.e., $\mathbf{p} + \mathbf{p} + \mathbf{p} = \mathbf{o}$ and $\mathbf{p} \neq \mathbf{o}$. Thus, we can write $\mathbf{p} = (x_0, y_0)$, and there is a line L such that L intersects E at $\mathbf{p}$ with multiplicity 3. In particular, L does not contain $\mathbf{o}$, so it is not a vertical line. Hence, L has an equation $y = ux + v$, and it follows that x_0 is the only solution to

$$\begin{aligned} x^3 + a_2x^2 + a_4x + a_6 - (ux+v)^2 - a_1x(ux+v) - a_3(ux+v) \\ &= x^3 + x^2(a_2 - u^2 - a_1u) + x(a_4 - 2uv - a_1v - ua_3) + (a_6 - v^2 - a_3v) \\ &= 0. \end{aligned}$$

Thus, we must have

$$x^3 + x^2(a_2 - u^2 - a_1u) + x(a_4 - 2uv - a_1v - ua_3) + (a_6 - v^2 - a_3v) = (x - x_0)^3.$$

Comparing coefficients of x, we get

$$\begin{cases} x_0^3 = v^2 + a_3v - a_6 \\ 3x_0^2 = a_4 - 2uv - a_1v - a_3u \\ 3x_0 = u^2 + a_1u - a_2 \end{cases}.$$

Hence, if $\operatorname{char} K \neq 2$, we see

$$\begin{aligned} \left(v + \frac{a_3}{2}\right)^2 &= x_0^3 + a_6 + \frac{a_3^2}{4}, \\ \left(u + \frac{a_1}{2}\right)\left(v + \frac{a_3}{2}\right) &= \frac{1}{4}(2a_4 + a_1a_3 - 6x_0^2), \quad \text{and} \\ \left(u + \frac{a_1}{2}\right)^2 &= 3x_0 + a_2 + \frac{a_1^2}{4}. \end{aligned}$$

We deduce

$$\left(\frac{1}{4}(2a_4 + a_1a_3 - 6x_0^2)\right)^2 = \left(x_0^3 + a_6 + \frac{a_3^2}{4}\right)\left(3x_0 + a_2 + \frac{a_1^2}{4}\right).$$

Similarly, if $\operatorname{char} K = 2$, one can verify

$$(x_0^2 + a_4)^2 + a_1a_3(x_0^2 + a_4) = a_1^2(x_0^3 + a_6) + a_3^2(x_0 + a_2).$$

Either way, we get a quartic (or a cubic if $\operatorname{char} K = 3$) in x_0, so there are at most four distinct solutions over $\overline{K}$. As each x_0 corresponds to at most two points on E, we thus have at most eight order 3 points. □

Corollary 4.2. *Let E be an elliptic curve in Weierstraß form (2), and let $\mathbf{p}_1$ and $\mathbf{p}_2$ be two order 3 points on E with distinct x-coordinates. Then the subgroup they generate is isomorphic to $(\mathbb{Z}/3\mathbb{Z})^2$ so that there are eight order 3 points on E.*

Proof. Recall that for every $\mathbf{p} \in E$, $\mathbf{p}$ and $-\mathbf{p}$ share the same x-coordinate. Hence, $\mathbf{p}_2 \notin \langle \mathbf{p}_1 \rangle$. Let $\mathbb{Z}^2 \to \langle \mathbf{p}_1, \mathbf{p}_2 \rangle$ be the homomorphism given by $(a, b) \mapsto a\mathbf{p}_1 + b\mathbf{p}_2$. Noting that $(3\mathbb{Z})^2$ is in the kernel of this map, and that none of $a\mathbf{p}_1 + b\mathbf{p}_2$ can be $\mathbf{o}$ for $a, b \in \{-1, 1\}$, we have $\langle \mathbf{p}_1, \mathbf{p}_2 \rangle \cong (\mathbb{Z}/3\mathbb{Z})^2$. Hence, we have all eight order 3 points. □

Let K be a field with $\operatorname{char} K \neq 3$. The *Hessian* family is a family of elliptic curves with Weierstraß equation

$$E_\alpha : y^2 + \alpha xy + y = x^3$$

for α in the ground field K. E_α is non-singular provided $\alpha^3 \neq 27$, which we show in Appendix A. This family is constructed so that $(0, 0)$ is a point of order 3, which can be seen as the line $y = 0$ intersects E_α at $(0, 0)$ with multiplicity 3. More generally, the curves

$$E_{a_1,a_3} : y^2 + a_1xy + a_3y = x^3$$

also have this property. The curves E_{a_1,a_3} are non-singular provided $a_3^3(a_1^3 - 27a_3) \neq 0$, which we also show in Appendix A.

We can arrange to find another order 3 point distinct from $(0, 0)$ and $-(0, 0)$ on E_{a_1,a_3} as follows. Suppose the line $y = ux + v$ intersects E_{a_1,a_3} at (x_0, y_0), $x_0 \neq 0$, with multiplicity 3. Then, as in the proof of Proposition 4.1, we see

$$\begin{cases} x_0^3 = v^2 + a_3v & \text{(14a)} \\ 3x_0^2 = -(2uv + a_1v + a_3u) & \text{(14b)} \\ 3x_0 = u^2 + a_1u & \text{(14c)} \end{cases}$$

Note, if u or v is zero then $x_0 = 0$, contradiction. Hence, we assume $u, v \neq 0$. Then, by equations (14c) and (14a),

$$a_1 = \frac{3x_0 - u^2}{u} \quad \text{and} \quad a_3 = \frac{x_0^3 - v^2}{v}.$$

Substituting this into (14b) and expanding yields

$$x_0^3u^2 + 3x_0^2uv + 3x_0v^2 = 0.$$

We conclude

$$(ux_0 + v)^3 = (ux_0)^3 + 3(ux_0)^2 v + 3(ux_0)v^2 + v^3 = v^3.$$

Thus, as $ux_0 \neq 0$, we must have $\frac{u}{v}x_0 = \rho - 1$, ρ being a primitive third root of unity. Using $\rho^2 + \rho + 1 = 0$, and rearranging, gives

$$v = -\frac{1}{3}(\rho + 2)ux_0.$$

Thus,

$$a_3 = (\rho - 1)\frac{x_0^2}{u} + \frac{1}{3}(\rho + 2)ux_0.$$

Noting $y_0 = ux_0 + v$, we put this together in the following

Proposition 4.3. *Suppose $u \neq 0$ and $a_1 = a_1(x_0, u)$ and $a_3 = a_3(x_0, u)$ are given by*

$$a_1 = \frac{3}{u}x_0 - u \quad \textit{and} \quad a_3 = \frac{\rho - 1}{u}x_0^2 + \frac{1}{3}(\rho + 2)ux_0.$$

The elliptic curve E_{a_1,a_3} then contains the order 3 point $(x_0, ux_0(1 - \rho)/3)$.

Remark 4.4. (1) The proposition above is a generalisation of the approach in [10, 35] as those texts only consider the intersection of a line $y = x + v$ with the elliptic curve E_{a_1,a_3}. (2) Given an elliptic curve of the form E_{a_1,a_3}, one can use the formulae in the proposition above to solve for u and x_0, and thus obtain an order 3 point on E_{a_1,a_3}.

4.2 Progress towards generalising Ulmer's proof to the Hessian family

In this section, we describe original progress towards generalising Ulmer's proof to the Hessian family from subsection 4.1. More specifically, we describe progress towards finding Hessian curves with many points. We deal with the curves E_α, the hope being that a construction of many points on E_α would generalise to the setting of suitable E_{a_1,a_3} curves. Throughout our discussion, we let q be a power of a prime $p \neq 3$.

We begin by recalling that in Ulmer's proof that the family Legendre curves E_d has arbitrarily large rank, the proof started by finding a suitable rational point $\mathbf{p} \in E_d(\mathbb{F}_p(t))$, and then obtaining many other points by letting the Galois group $\mathrm{Gal}(\mathbb{F}_p(t, \mu_d)/\mathbb{F}_p(t^d))$ act on $\mathbf{p}$. Similarly, we want to arrange a point $\mathbf{p} \in E_\alpha(\mathbb{F}_q(t))$ with α being a rational function of t^d so that $\mathbf{p}$ has large $\mathrm{Gal}(\mathbb{F}_q(t, \mu_d)/\mathbb{F}_q(t^d))$-orbit. Now, let $\mathbf{p} = (x, y)$. It is clear that if $x = 0$ or $y = 0$, then $\mathbf{p}$ has trivial $\mathrm{Gal}(\mathbb{F}_q(t, \mu_d)/\mathbb{F}_q(t^d))$-orbit, so assume $x, y \neq 0$. For simplicity, we assume that α is a polynomial of t^d.

We begin by rearranging the equation of E_α as follows:

$$\alpha = \frac{x^2}{y} - \frac{1}{x} - \frac{y}{x} = \frac{x}{X} - \frac{1}{x} - X,$$

where $X = y/x$. We can write $x = a/b$ and $X = c/d$, where $a, b, c, d \in \mathbb{F}_q[t] \setminus \{0\}$ such that $\gcd(a, b) = \gcd(c, d) = 1$ as $\mathbb{F}_q[t]$ is a unique factorisation domain [4, Section 4]. Thus,

$$\alpha = \frac{a^2d^2 - b^2cd - abc^2}{abcd}. \tag{15}$$

Now, set

$$\zeta = \gcd(a, c), \quad \mu = \gcd(a, d), \quad \xi = \gcd(b, c), \quad \lambda = \gcd(b, d).$$

By $\zeta = \gcd(a, c)$, we mean $\zeta \in \mathbb{F}_q[t]$ is a representative of $\gcd(a, c)$; similarly for the others. Then, we can write

$$\begin{aligned} a &= \zeta\mu a', \\ b &= \xi\lambda b', \\ c &= \zeta\xi c', \quad \text{and} \\ d &= \mu\lambda d', \end{aligned}$$

where

$$a' = \frac{a}{\zeta\mu}, \quad b' = \frac{b}{\xi\lambda}, \quad c' = \frac{c}{\zeta\xi}, \quad d' = \frac{d}{\mu\lambda}.$$

Notice that ζ, μ, ξ, and λ are all pairwise coprime, so that a', b', c', d' are all polynomials. Moreover, a', b', c', d' are also pairwise coprime. Note in the above factorisation, that we can arrange a', ξ, d' to have leading coefficient 1.

From equation (15), we see $a \mid b^2cd$, implying $a \mid cd$ as a is coprime with b. Thus, $a' \mid \xi\lambda c'd'$. Noting a' is coprime with b, and hence with $\xi\lambda$, we conclude that a' is a unit. By the remark at the end of the preceding paragraph, $a' = 1$.

Similarly, $b \mid a^2d^2$ implies ξ is a unit, and hence 1. Also $d \mid abc^2$ implies $d' = 1$. In summary,

$$a = \zeta\mu, \quad b = \lambda b', \quad c = \zeta c', \quad d = \mu\lambda,$$

and

$$\alpha = \frac{\zeta\lambda\mu^3 - \lambda^2(b')^2c' - \zeta^2b'(c')^2}{\zeta\lambda\mu b'c'}.$$

We have:

- $b' \mid \zeta\lambda\mu^3$ implies $b' \mid \lambda$,
- $c' \mid \zeta\lambda\mu^3$ implies $c' \mid \zeta$,
- $\lambda \mid \zeta^2b'(c')^2$ implies $\lambda \mid b'$, and
- $\zeta \mid \lambda^2(b')^2c'$ implies $\zeta \mid c'$.

Thus, $b' = \ell_1\lambda$ and $c' = \ell_2\zeta$ for some $\ell_1, \ell_2 \in \mathbb{F}_q^\times$. Hence,

$$\alpha = \frac{\mu^3 - \ell_1^2\ell_2\lambda^3 - \ell_1\ell_2^2\zeta^3}{\ell_1\ell_2\zeta\lambda\mu}. \tag{16}$$

We also have that $x = \frac{\zeta\mu}{\ell_1\lambda^2}$, $X = \frac{\ell_2\zeta^2}{\mu\lambda}$, and $y = \frac{\ell_2\zeta^3}{\ell_1\lambda^3}$.

We recall that the goal is to find μ, λ, ζ polynomials so that α is a polynomial of t^d. Note that an easy way of doing this is finding one solution $\mu, \lambda, \zeta, \ell_1, \ell_2$ so that the right-hand side of equation (16) is also a polynomial, and hence noting that

$$\frac{\mu(t^d)^3 - \ell_1^2\ell_2\lambda(t^d)^3 - \ell_1\ell_2^2\zeta(t^d)^3}{\ell_1\ell_2\zeta(t^d)\lambda(t^d)\mu(t^d)}$$

is a polynomial in t^d. This does not work for our purposes, though, since x and y would then be polynomials of t^d so that $\mathrm{Gal}(\mathbb{F}_p(t, \mu_d)/\mathbb{F}_p(t^d))$ acts trivially on (x, y). This motivates the following

Definition 4.5. Let μ, λ, ζ be pairwise coprime $\mathbb{F}_q[t]$-polynomials and let $\ell_1, \ell_2 \in \mathbb{F}_q^\times$. We say that $(\mu, \lambda, \zeta, \ell_1, \ell_2)$ is a *solution* if the equation (16) is an element of $\mathbb{F}_q[t]$. The *degree* of a solution is the largest d such that corresponding value of α is a polynomial in t^d. A solution is *primitive* if there is no integer $s > 1$ and no solution $(\tilde{\mu}, \tilde{\lambda}, \tilde{\zeta}, \tilde{\ell_1}, \tilde{\ell_2})$ with $\mu = \tilde{\mu}(t^s), \lambda = \tilde{\lambda}(t^s), \zeta = \tilde{\zeta}(t^s)$.

Now, suppose $\ell_1 = c_1^3\ell_3$ and $\ell_2 = c_2^3\ell_4$ for some $c_1, c_2, \ell_3, \ell_4 \in \mathbb{F}_q^\times$. We see that if $(\mu, \lambda, \zeta, \ell_1, \ell_2)$ is a solution, then so is $(\mu, c_1^2c_2\lambda, c_1c_2^2\zeta, \ell_3, \ell_4)$. Moreover, both solutions correspond to the same value of α. Also, we note

$$\frac{\zeta\mu}{\ell_1\lambda^2} = \frac{(c_1c_2^2\zeta)\mu}{\ell_3(c_1^2c_2\lambda)^2} \quad \text{and} \quad \frac{\ell_2\zeta^2}{\mu\lambda} = \frac{\ell_4(c_1c_2^2\zeta)^2}{\mu(c_1^2c_2\lambda)},$$

so both solutions give the same values of x, X, and hence also y. Thus, we can define two solutions $(\mu, \lambda, \zeta, \ell_1, \ell_2), (\mu', \lambda', \zeta', \ell_1', \ell_2')$, to be *equivalent* if there are $c_1, c_2 \in \mathbb{F}_q^\times$ such that $(\mu', \lambda', \zeta', \ell_1', \ell_2') = (\mu, c_1^2c_2\lambda, c_1c_2^2\zeta, \ell_1c_1^{-3}, \ell_2c_2^{-3})$. This is an equivalence relation. If $3 \nmid |\mathbb{F}_q^\times|$, then every element of $\mathbb{F}_q^\times$ is a perfect cube, so every equivalence class of solutions has a member with $\ell_1 = \ell_2 = 1$. Similarly, if $3 \mid |\mathbb{F}_q^\times|$, then let $\mathbb{F}_q^{\times 3} \subset \mathbb{F}_q^\times$ be the subgroup of perfect cubes. As $x \mapsto x^3$ is a 3-to-1 map, $|\mathbb{F}_q^\times/\mathbb{F}_q^{\times 3}| = 3$. Thus, in this case, there are essentially only nine pairs (ℓ_1, ℓ_2) to consider.

Thus, we start the search for primitive solutions by looking for those with $\ell_1 = \ell_2 = 1$. We also make the simplifying assumption that $\lambda = 1$. In this case,

$$\alpha = \frac{\mu^3 - 1 - \zeta^3}{\mu\zeta}.$$

We see $\alpha \in \mathbb{F}_q[t]$ if and only if $\mu \mid 1 + \zeta^3$ and $\zeta \mid \mu^3 - 1$, as $\gcd(\mu, \zeta) = 1$. We see that we always have the solutions

$$\mu = 1, 1 + \zeta, 1 - \zeta + \zeta^2, 1 + \zeta^3.$$

We call these the *trivial* solutions. In these cases, we get

$$\alpha = -\zeta^2, 3, \zeta^3 - 2\zeta^2 + 3\zeta - 3, \zeta^5 + 2\zeta^2,$$

respectively. Whenever these solutions are primitive, their degree is 1, except for the $\mu = 1$ case where it is 2.

The author ran the following brute-force search for primitive, non-trivial solutions of degree at least 2 over $\mathbb{F}_5[t]$:

Algorithm 1 Brute-force search for non-trivial solutions of degree at least 2

Input: S $\{S =$ search list$\}$
  for $\zeta \in S$ **do**
    for μ a divisor of $\zeta^3 + 1$ **do**
      if $\zeta \mid \mu^3 - 1$ **and** (μ, ζ) is not trivial **then**
        $\alpha \leftarrow \frac{\mu^3 - 1 - \zeta^3}{\mu\zeta}$
        $d \leftarrow \max\{s : \alpha \text{ is a polynomial in } t^s\}$
        if $d > 1$ **then**
          print (μ, ζ, α, d)
        end if
      end if
    end for
  end for

This program was implemented in MAGMA [2]. In the algorithm above, the author used S as the set of polynomials in $\mathbb{F}_5[t]$ of degree at most 8. The author then excluded non-primitive solutions. This resulted in the author finding sixty primitive degree 2 solutions, four primitive degree 3 solutions, and, dissapointingly, none of any higher degree. The exceptional degree 3 solutions were found quite early in the search. One example is

$$\mu = 3t + 1, \quad \zeta = t^2 + t + 2, \quad \alpha = 3t^3 + 1,$$

and the others are obtained by replacing t with $2t, 3t$, and $4t$, respectively. It seems plausible that we might have more success with other values of λ or changing the base field. However, the search above was already computationally intensive, requiring over two hours to complete, so we did not pursue this any further. Instead, we now try to complement our number-theoretic approach with a geometric analysis, using Conceição-Shioda.

4.3 A few applications of Conceição-Shioda

In this section, we record a few applications of Conceição-Shioda to our problem, and discuss the obstructions preventing these attempts from succeeding. Based on Ulmer's and Conceição's examples, we first describe three scenarios of interest. If α is a polynomial in t^d, then we seek a point with large $\mathrm{Gal}(\mathbb{F}_q(t, \mu_d)/\mathbb{F}_q(t^d))$-orbit. This was the chief aim of the previous subsection. We are also interested in the case when α is an $\mathbb{F}_q$-additive polynomial. In this case, if we are able to find a point on elliptic curves $y^2 - \alpha^{(k)}xy + y = x^3$, for suitable $\mathbb{F}_q$-additive polynomials $\alpha^{(1)}, \ldots, \alpha^{(\ell)}$, and we also have $A(t)$ is an $\mathbb{F}_q$-additive polynomial satisfying $\alpha_0^{(k)}(t) \mid A_0(t)$ for each k, then we get ℓ points on the Hessian curve $y^2 - Axy + y = x^3$ by a similar argument as Lemma 3.3. Based on Conceição's construction of points on the curve $y^2 = x^3 - (t^{q^n+1} + 1)x$ from the end of section 3.6, we are also interested in elliptic curves to which we can find a Delsarte hypersurface $\mathcal{X}_{dC}$ with many symmetries that interact well with the resulting Conceição-Shioda map $\mathcal{X}_{dC} \to \mathcal{E}$. To illustrate this last point, recall from the end of section 3.6 that we had associated a matrix A to $y^2 = x^3 - (t^d + 1)x$, where $d = q^n + 1$. Its inverse was

$$A^{-1} = \begin{bmatrix} 0 & 1/3 & 0 & 0 \\ 1/2 & 1/12 & 0 & -1/4 \\ 0 & -1/6 & 0 & 1/2 \\ 0 & 0 & 1/d & -1/d \end{bmatrix}.$$

Note the first two columns of A^{-1} have no dependence on d. This gives Conceição the flexibility to post-multiply A^{-1} by $C = \mathrm{diag}(s, s, d, d)$, where $4 \mid s$. Also recall that the map $\mathcal{X}_C \to \mathcal{E}$ was given by

$$(X_1, X_2, X_3, X_4) \mapsto \left([-X_2^{s/2} X_4^{d/4} : X_1^{s/2} X_2^{s/4} : X_4^{3d/4}], X_3/X_4 \right).$$

Note that the $O_2(\mathbb{F}_q)$ action on $\mathcal{X}_C$ involved just X_1 and X_2, while the T-coordinate of the resulting map only involves X_3 and X_4. Thus the $O_2(\mathbb{F}_q)$-action on $\mathcal{X}_C$ "interacts well" with the map $\mathcal{X}_C \to \mathcal{E}$ as it doesn't affect the T-coordinate of the resulting map. More generally, if a symmetry of a Delsarte hypersurface $\mathcal{X}_{dC}$ gives rise to a parametrised curve $([f_1(T), f_2(T), f_3(T)], f_4(T))$ on $\mathcal{E}$, and we are able to easily reparametrise the curve in terms of $W = f_4(T)$, then we would still say that the symmetry "interacts well" with the map $\mathcal{X}_{dC} \to \mathcal{E}$.

We first consider the Hessian curve E_1 given by $X^3 - Y^2Z + t^dXYZ - YZ^2 = 0$. Let $\mathcal{E}_1$ be the associated elliptic surface. We associate to this the matrix

$$A = \begin{bmatrix} 3 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 \\ 1 & 1 & 1 & d \\ 0 & 1 & 2 & 0 \end{bmatrix}$$

with inverse

$$A^{-1} = \begin{bmatrix} 1/3 & 0 & 0 & 0 \\ 0 & 2/3 & 0 & -1/3 \\ 0 & -1/3 & 0 & 2/3 \\ -(3d)^{-1} & -(3d)^{-1} & d^{-1} & -(3d)^{-1} \end{bmatrix}.$$

Note each column of A^{-1} has a factor of d^{-1}. Thus, letting I_4 be the 4×4 identity matrix, we have a map $\mathcal{X}_{dI_4}(1,-1,1,-1) \to \mathcal{E}_1$ given by sending (X_1, X_2, X_3, X_4) to

$$\begin{aligned} &([X_1^{d/3} : X_2^{2d/3}X_4^{-d/3} : X_2^{-d/3}X_4^{2d/3}], X_3X_1^{-1/3}X_2^{-1/3}X_4^{-1/3}) \\ =&([X_1^{d/3}X_2^{d/3}X_4^{d/3} : X_2^d : X_4^d], X_3X_1^{-1/3}X_2^{-1/3}X_4^{-1/3}) \end{aligned} \tag{17}$$

by Conceição-Shioda. Even though there are fractional exponents in the map, we will see that this still gives a point on E_1.

Take the curve $(1,1,t,t)$ on $\mathcal{X}_{dI_4}(1,-1,1,-1)$. By the map above, this corresponds to the parametrised curve $([t^{d/3} : 1 : t^d], t^{2/3})$, which we reparametrise to $([t^{d/2} : 1 : t^{3d/2}], t)$. Provided d is even, this corresponds to the point $(t^{-d}, t^{-3d/2})$ on E_1. Similarly, the point $(t^{d/2}, t^{3d/2})$ on E_1 can be found by considering the parametrised curve $(1,t,t,1)$. One can also observe that the parametrised curves $(t,t,1,1), (t,1,1,t)$ give the same points.

It is clear that these points have $\mathrm{Gal}(\mathbb{F}_q(t,\mu_d)/\mathbb{F}_q(t^d))$-orbits of size 2, so Ulmer's strategy does not work here. Also note that the T-coordinate of the map (17) involves all four variables, so it does not interact well with symmetries of $\mathcal{X}_{dI_4}(1,-1,1,-1)$. For example, if $d = q^n + 1$, note that $O_2(\mathbb{F}_q)$ acts on $\mathcal{X}_{dI_4}(1,-1,1,-1)$ just as before: a matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in O_2(\mathbb{F}_q)$ corresponds to the action

$$(X_1, X_2, X_3, X_4) \mapsto (aX_1 + bX_3, X_2, cX_1 + dX_3, X_4).$$

The curve $(1,1,t,t)$ is then sent to $(a+bt, 1, c+dt, t)$ under this action. On $\mathcal{E}_1$, this corresponds to the parametrised curve

$$\left([(a+bt)^{d/3}t^{d/3} : 1 : t^d], \frac{c+dt}{(a+bt)^{1/3}t^{1/3}} \right).$$

Even if we assume $a = c, b = -d$, it does not seem that this curve may be reparametrised to a suitable form.

We thus try to create a map to a different Delsarte surface, one that ideally has many symmetries that interact well with the resulting Conceição-Shioda map. One attempt is as follows. Notice that

$$A^{-1} \begin{bmatrix} s & 0 & 0 & 0 \\ 0 & s & 0 & 0 \\ s/3 & s/3 & 3d & 0 \\ 0 & 0 & 0 & 3d \end{bmatrix} = \begin{bmatrix} s/3 & 0 & 0 & 0 \\ 0 & 2s/3 & 0 & -d \\ 0 & -s/3 & 0 & 2d \\ 0 & 0 & 3 & -1 \end{bmatrix},$$

for some positive integer s that is divisible by 3. Conceição-Shioda gives map from the Delsarte hypersurface

$$X_1^s - X_2^s + X_1^{s/3} X_2^{s/3} X_3^{3d} - X_4^{3d} = 0$$

to $\mathcal{E}_1$ by sending (X_1, X_2, X_3, X_4) to

$$\left([X_1^{s/3} : X_2^{2s/3} X_4^{-d} : X_2^{-s/3} X_4^{2d}], X_3^3/X_4\right) = \left([X_1^{s/3} X_2^{s/3} X_4^d : X_2^s : X_4^{3d}], X_3^3/X_4\right).$$

Now, the map is nicer, but it is not clear what symmetries the resulting Delsarte hypersurface admits, nor if this surface admits curves that correspond to points with large Galois orbit.

We now record another possible approach to this problem. Recall from our earlier number-theoretic approach, we were interested in finding solutions to

$$\alpha = \frac{\mu^3 - \ell_1^2 \ell_2 \lambda^3 - \ell_1 \ell_2^2 \zeta^3}{\ell_1 \ell_2 \mu \lambda \zeta}.$$

Expanding we get

$$\mu^3 - \ell_1^2 \ell_2 \lambda^3 - \ell_1 \ell_2 \zeta^3 - \ell_1 \ell_2 \alpha \mu \lambda \zeta = 0. \tag{18}$$

If we regard α as fixed, then this defines a cubic curve in μ, λ, ζ. We denote the cubic curve (18) by E'_α. Note that our prior formulae, $x = \frac{\zeta \mu}{\ell_1 \lambda^2}$ and $y = \frac{\ell_2 \zeta^3}{\ell_1 \lambda^3}$, can be interpreted as (rational) maps from the cubic E'_α to the original Hessian curve E_α. Hence, we can run Conceição-Shioda on the cubic curve E'_α instead. If $\alpha = -t^d$, we run into similar obstructions as before, so, motivated by the $\mathbb{F}_q$-additive polynomial construction, we instead describe an attempt of running Conceição-Shioda in the case where $\alpha = at^d + bt$ for suitable $a, b \in \mathbb{F}_q^\times$.

We start with

$$\mu^3 - \ell_1^2 \ell_2 \lambda^3 - \ell_1 \ell_2 \zeta^3 - a \ell_1 \ell_2 t^d \mu \lambda \zeta - b \ell_1 \ell_2 t \mu \lambda \zeta = 0.$$

We have five terms and only four variables, so, following Conceição's analysis of the Legendre curve [3, Example 3.5], we add an extra variable. Let $\mathcal{E}_2$ be the set of solutions $([X : Y : Z], T, W) \in \mathbb{P}\overline{\mathbb{F}_q}^2 \times \overline{\mathbb{F}_q}^2$ to

$$X^3 - \ell_1^2 \ell_2 Y^3 - \ell_1 \ell_2^2 Z^3 - a \ell_1 \ell_2 T^d XYZ - b \ell_1 \ell_2 W XYZ = 0$$

with the extra constraint that $T = W$. We consider the matrix

$$M = \begin{bmatrix} 3 & 0 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 & 0 \\ 0 & 0 & 3 & 0 & 0 \\ 1 & 1 & 1 & d & 0 \\ 1 & 1 & 1 & 0 & 1 \end{bmatrix}.$$

Then,

$$M^{-1} = \begin{bmatrix} \frac{1}{3} & 0 & 0 & 0 & 0 \\ 0 & \frac{1}{3} & 0 & 0 & 0 \\ 0 & 0 & \frac{1}{3} & 0 & 0 \\ -\frac{1}{3d} & -\frac{1}{3d} & -\frac{1}{3d} & \frac{1}{d} & 0 \\ -\frac{1}{3} & -\frac{1}{3} & -\frac{1}{3} & 0 & 1 \end{bmatrix}.$$

Letting I_5 be the 5×5 identity matrix, and $c = (1, -\ell_1^2\ell_2, -\ell_1\ell_2^2, -a\ell_1\ell_2, -b\ell_1\ell_2)$, we get a map from the Delsarte hypersurface $\mathcal{X}_{3dI_5}(c)$

$$X_1^{3d} - \ell_1^2\ell_2 X_2^{3d} - \ell_1\ell_2^2 X_3^{3d} - a\ell_1\ell_2 X_4^{3d} - b\ell_1\ell_2 X_5^{3d} = 0$$

to the Delsarte hypersurface $\mathcal{X}_M(c)$ given by

$$(X_1, X_2, X_3, X_4, X_5) \mapsto \left(X_1^d, X_2^d, X_3^d, \frac{X_4^3}{X_1X_2X_3}, \frac{X_5^{3d}}{X_1^dX_2^dX_3^d}\right).$$

To get a map to $\mathcal{E}_2$, we impose the $W = T$ constraint. This amounts to enforcing the equality $X_5^{3d} = X_1^{d-1}X_2^{d-1}X_3^{d-1}X_4^3$. Hence, we get a map from the set $\mathcal{S}$ of quadruples (X_1, X_2, X_3, X_4) solving

$$X_1^{3d} - \ell_1^2\ell_2 X_2^{3d} - \ell_1\ell_2^2 X_3^{3d} - a\ell_1\ell_2 X_4^{3d} - b\ell_1\ell_2 X_1^{d-1}X_2^{d-1}X_3^{d-1}X_4^3 = 0 \tag{19}$$

to $\mathcal{E}_2$ given by

$$(X_1, X_2, X_3, X_4) \mapsto \left([X_1^d : X_2^d : X_3^d], \frac{X_4^3}{X_1X_2X_3}\right).$$

However, it seems difficult to find parametrised curves on $\mathcal{S}$. As a first step, we can note that $(X_1, X_2, X_3, X_4) \in \mathcal{S}$ if and only if $(rX_1, rX_2, rX_3, rX_4) \in \mathcal{S}$ for any non-zero $r \in \mathbb{F}_q(t)$, and that both (X_1, X_2, X_3, X_4), (rX_1, rX_2, rX_3, rX_4) have the same image under the map $\mathcal{S} \to \mathcal{E}_2$. Hence, we can assume X_1, X_2, X_3, X_4 are coprime polynomials (by scaling by an appropriate r). Moreover, as we wish to find parametrised curves on $\mathcal{E}_2$ via the map $\mathcal{S} \to \mathcal{E}_2$, we require $X_1, X_2, X_3, X_4 \neq 0$. Now, we try forcing some simplifications. For example, suppose we set

$$X_1^{3d} = a\ell_1\ell_2 X_4^{3d} \quad \text{and} \quad \ell_1^2\ell_2 X_2^{3d} + \ell_1\ell_2^2 X_3^{3d} = b\ell_1\ell_2 X_1^{d-1}X_2^{d-1}X_3^{d-1}X_4^3.$$

In this case, if X_2 and X_3 are constants, then this would force X_1 and X_4 to also be constant, and thus we don't get a parametrised curve. If we assume this to not be the case, then the second equation implies $X_2 \mid X_3^{3d}$ and $X_3 \mid X_2^{3d}$, so $\gcd(X_2, X_3)$ is non-trivial. Then, if g is a representative of $\gcd(X_2, X_3)$,

$$g^{3d} \mid X_1^{d-1}X_2^{d-1}X_3^{d-1}X_4^3,$$

implying

$$g^{d+2} \mid X_1^{d-1}(X_2/g)^{d-1}(X_3/g)^{d-1}X_4^3.$$

As g is coprime to X_2/g and X_3/g, it follows that X_2 and X_3 share a common factor with one of X_1 or X_4. But, from the equation of $\mathcal{S}$ (19), this implies X_1, X_2, X_3, and X_4 to share a non-trivial common factor, contradicting our earlier assumption that all X_1, X_2, X_3, X_4 are non-zero coprime polynomials. One also reaches a similar contradiction when trying to set $\ell_1 = -\ell_2$ and $X_2 = X_3$. So it seems that this equation requires a more careful analysis, perhaps of similar nature to our earlier number-theoretic approach together with an analysis of the degrees of X_1, X_2, X_3, X_4.

We now discuss another interesting observation that may help with our overall problem of finding points on Hessian curves.

4.4 A geometric reinterpretation

We have already seen that for $\ell_1, \ell_2 \in \mathbb{F}_q^\times$, we have a map from the cubic curve E'_α

$$\mu^3 - \ell_1^2\ell_2\lambda^3 - \ell_1\ell_2^2\zeta^3 - \alpha\ell_1\ell_2\mu\lambda\zeta = 0$$

to our original Hessian curve $E_\alpha : y^2 - \alpha xy + y = x^3$ given by $(x, y) = (\frac{\zeta\mu}{\ell_1\lambda^2}, \frac{\ell_2\zeta^3}{\ell_1\lambda^3})$. At first glance, it seems that if we were to vary ℓ_1 and ℓ_2, then we have many cubic curves "embedded" in E_α via the aforementioned map. However, as we saw section 4.2, if $\ell_3 = c_1^3\ell_1$ and $\ell_4 = c_2^3\ell_2$ for some $c_1, c_2 \in \mathbb{F}_q^\times$, then the solutions to

$$\mu^3 - \ell_1^2\ell_2\lambda^3 - \ell_1\ell_2^2\zeta^3 - \alpha\ell_1\ell_2\mu\lambda\zeta = 0$$

are in 1-to-1 correspondence with the solutions to

$$\mu^3 - \ell_3^2\ell_4\lambda^3 - \ell_3\ell_4^2\zeta^3 - \alpha\ell_3\ell_4\mu\lambda\zeta = 0$$

and corresponding solutions give the same point $(x, y) \in E_\alpha$. Thus, depending on whether 3 divides $|\mathbb{F}_q^\times|$, there are essentially only 1 or 9 such cubic curves to consider.

In this section, we investigate the effect of letting $\ell_1, \ell_2 \in \mathbb{F}_q(t)^\times$, noting that the map from the cubic curve

$$\mu^3 - \ell_1^2\ell_2\lambda^3 - \ell_1\ell_2^2\zeta^3 - \ell_1\ell_2\alpha\mu\lambda\zeta = 0$$

to E_α still holds in this context. The reason is twofold: if ℓ_1, ℓ_2 are rational functions, we might be able to find solutions more easily. Also, in the more general setting where α is a rational function of t, we might be able to use this idea that we have many cubic curves "embedded" in the Hessian curve E_α to generate many points on E_α. We focus on the former perspective, in the context where $\alpha = at^d + bt$ for some d which is a power of q.

Hence, let $\mathcal{E}_3$ be the set of solutions $([X : Y : Z], (T, \ell_1, \ell_2)) \in \mathbb{P}\overline{\mathbb{F}_q}^2 \times \overline{\mathbb{F}_q}^3$ to

$$X^3 - \ell_1^2\ell_2Y^3 - \ell_1\ell_2^2Z^3 - aT^d\ell_1\ell_2XYZ - bT\ell_1\ell_2XYZ = 0.$$

We associate to this the matrix

$$\begin{bmatrix} 3 & 0 & 0 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 & 2 & 1 \\ 0 & 0 & 3 & 0 & 1 & 2 \\ 1 & 1 & 1 & d & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

We have two problems. Firstly, the rows of this matrix are linearly dependent. One can see this by noting that the average of the first three rows is $(1, 1, 1, 0, 1, 1)$. Thus, the span of the first four rows contains $(0, 0, 0, 1, 0, 0)$, and hence also the fifth row. Secondly, we must add rows. The linear dependency in the rows can be fixed by adding a new variable W, and then requiring $W = T$ (for example). Adding rows can be accomplished by "adding zero" to the equation of $\mathcal{E}_3$, so that the rows remain linearly independent. For example, take $\mathcal{E}'_3$ as the set of solutions $([X : Y : Z], (T, W, \ell_1, \ell_2)) \in \mathbb{P}\overline{\mathbb{F}_q}^2 \times \overline{\mathbb{F}_q}^4$ to

$$X^3 - \ell_1^2\ell_2Y^3 - \ell_1\ell_2^2Z^3 - aT^d\ell_1\ell_2XYZ - bW\ell_1\ell_2XYZ + 0 \cdot Y + 0 \cdot Z = 0.$$

The resulting matrix and its inverse are

$$M = \begin{bmatrix} 3 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 & 0 & 2 & 1 \\ 0 & 0 & 3 & 0 & 0 & 1 & 2 \\ 1 & 1 & 1 & d & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix} \text{ and } M^{-1} = \begin{bmatrix} \frac{1}{3} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ -\frac{1}{3d} & -\frac{1}{3d} & -\frac{1}{3d} & \frac{1}{d} & 0 & 0 & 0 \\ -\frac{1}{3} & -\frac{1}{3} & -\frac{1}{3} & 0 & 1 & 0 & 0 \\ 0 & \frac{2}{3} & -\frac{1}{3} & 0 & 0 & -2 & 1 \\ 0 & -\frac{1}{3} & \frac{2}{3} & 0 & 0 & 1 & -2 \end{bmatrix},$$

respectively. Hence, taking $C = \text{diag}(3d, 3d, 3d, 3d, 1, 1)$, there is a map from

$$\mathcal{X}_C(1, -1, -1, -a, -b, 0, 0) : X_1^{3d} - X_2^{3d} - X_3^{3d} - aX_4^{3d} - bX_5^{3d} = 0$$

to $\mathcal{E}_3'$ given by

$$(X_1, \ldots, X_7) \mapsto \left([X_1^d : X_6 : X_7], \left(\frac{X_4^3}{X_1X_2X_3}, \frac{X_5^{3d}}{X_1^dX_2^dX_3^d}, \frac{X_2^{2d}X_7}{X_3^dX_6^2}, \frac{X_3^{2d}X_6}{X_2^dX_7^2} \right) \right).$$

Imposing the condition $W = T$ gives a map of solutions to

$$X_1^{3d} - X_2^{3d} - X_3^{3d} - aX_4^{3d} - bX_1^{d-1}X_2^{d-1}X_3^{d-1}X_4^3 = 0 \tag{20}$$

to $\mathcal{E}_3$ given by

$$(X_1, X_2, X_3, X_4, X_6, X_7) \mapsto \left([X_1^d : X_6 : X_7], \left(\frac{X_4^3}{X_1X_2X_3}, \frac{X_2^{2d}X_7}{X_3^dX_6^2}, \frac{X_3^{2d}X_6}{X_2^dX_7^2} \right) \right).$$

On one hand, it seems that the Conceição-Shioda map takes care of the values of ℓ_1, ℓ_2, so that we just need to consider equation (20). On the other hand, equation (20) puts us essentially in the same place as where we were at the end of the previous subsection, so it does not seem that this approach is of much help here.

It seems that it is, in general, quite difficult to move away from an equation of the form (20). For example, set $\mathcal{E}_4$ to be the set of solutions $([X : Y : Z], (T, W, \ell_1, \ell_2))$ to

$$X^3 - \ell_1^2\ell_2Y^3 - \ell_1\ell_2^2Z^3 - aT^{d-1}WXYZ\ell_1\ell_2 - b\ell_1\ell_2WXYZ - 0 \cdot Y - 0 \cdot Z = 0.$$

The associated matrix and inverse are

$$\begin{bmatrix} 3 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 & 0 & 2 & 1 \\ 0 & 0 & 3 & 0 & 0 & 1 & 2 \\ 1 & 1 & 1 & d-1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix} \text{ and } \begin{bmatrix} \frac{1}{3} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & \frac{1}{d-1} & -\frac{1}{d-1} & 0 & 0 \\ -\frac{1}{3} & -\frac{1}{3} & -\frac{1}{3} & 0 & 1 & 0 & 0 \\ 0 & \frac{2}{3} & -\frac{1}{3} & 0 & 0 & -2 & 1 \\ 0 & -\frac{1}{3} & \frac{2}{3} & 0 & 0 & 1 & -2 \end{bmatrix},$$

respectively. At first glance, this matrix seems much more promising as only the fourth and fifth columns depend on $d-1$. Indeed, taking $C = \text{diag}(1, 1, 1, d-1, d-1, 1, 1)$ and $e = (1, -1, -1, -a, -b, 0, 0)$, we have a map from

$$\mathcal{X}_C(e) : X_1 - X_2 - X_3 - aX_4^{d-1} - bX_5^{d-1} = 0 \tag{21}$$

to $\mathcal{E}_4$ given by

$$(X_1, \ldots, X_7) \mapsto \left([X_1^{1/3} : X_6 : X_7], \frac{X_4}{X_5}, \frac{X_5^{d-1}}{X_1^{1/3} X_2^{1/3} X_3^{1/3}}, \frac{X_2^{2/3} X_7}{X_3^{1/3} X_6^2}, \frac{X_3^{2/3} X_6}{X_2^{1/3} X_7^2} \right).$$

But now, imposing $T = W$ amounts to enforcing $X_5^d = X_1^{1/3} X_2^{1/3} X_3^{1/3} X_4$. As equation (21) has the term X_5^{d-1}, this implies that we must instead consider the Delsarte hypersurface

$$\mathcal{X}_{C'}(e) : X_1^d - X_2^d - X_3^d - a X_4^{d(d-1)} - b X_5^{d-1} = 0,$$

where $C' = \mathrm{diag}(d, d, d, d(d-1), d(d-1), 1, 1)$, with corresponding map

$$(X_1, \ldots, X_7) \mapsto \left([X_1^{d/3} : X_6 : X_7], \frac{X_4^d}{X_5}, \frac{X_5^{d-1}}{X_1^{d/3} X_2^{d/3} X_3^{d/3}}, \frac{X_2^{2d/3} X_7}{X_3^{d/3} X_6^2}, \frac{X_3^{2d/3} X_6}{X_2^{d/3} X_7^2} \right).$$

Now, the $W = T$ condition becomes $X_5^d = X_1^{d/3} X_2^{d/3} X_3^{d/3} X_4^d$. Recalling that d is a power of q, this forces $X_5 = X_1^{1/3} X_2^{1/3} X_3^{1/3} X_4$. Thus, we get a map from the solutions $(X_1, X_2, X_3, X_4, X_6, X_7)$ of

$$X_1^d - X_2^d - X_3^d - a X_4^{d(d-1)} - b X_1^{(d-1)/3} X_2^{(d-1)/3} X_3^{(d-1)/3} X_4^{d-1} = 0 \tag{22}$$

to $\mathcal{E}_4$ given by

$$(X_1, \ldots, X_7) \mapsto \left([X_1^{d/3} : X_6 : X_7], \frac{X_4^{d-1}}{X_1^{1/3} X_2^{1/3} X_3^{1/3}}, \frac{X_2^{2d/3} X_7}{X_3^{d/3} X_6^2}, \frac{X_3^{2d/3} X_6}{X_2^{d/3} X_7^2} \right).$$

In general, Conceição-Shioda appears to convert the problem of finding points on Hessian curves to finding parametrised curves on equations of the form (20) or (22). This seems difficult, in general. However, noting the various exponents appearing in the summands of equation (22), it may be possible to proceed by considering the degrees of the X_is. We leave this for future investigation.

4.5 Further thoughts and concluding remarks

Our investigation into generalising Ulmer's and Conceição's proofs to the Hessian case suggest several directions for future research. Firstly, it would be of interest to improve Algorithm 1 from section 4.2 and gather data in scenarios where $\lambda \neq 1$ or where the base field has characteristic other than 5. It would also be of interest to study the various equations that appeared by applying Conceição-Shioda to the Hessian curve in the previous two subsections, with a view towards the symmetries of such equations. As seen in [5, 34, 27], similar themes appear to be of contemporary interest. The phenomenon that there are many cubic curves "embedded" in the Hessian curve could also be a viable alternative to analysing the symmetries of the aforementioned equations.

Besides the Hessian case, one can also attempt to generalise Ulmer's and Conceição's constructions to other fields. Indeed, as Ulmer's construction misses the characteristic 2 case, and Conceição's constructions miss cases where the base field is of characteristic 1 (mod 12), it would be of interest to find similar constructions in those settings. Some discussion on the characteristic 2 case, including the author's attempt using a different normal form for elliptic curves, is given in appendix B. As a main inspiration for studying elliptic curves over $\mathbb{F}_q(t)$ is to gain an intuition about the characteristic zero case, we conclude by mentioning that it would be interesting to see if one can construct moderate- or high-rank elliptic curves over $\mathbb{Q}$ or $\mathbb{Q}(t)$ based on the elliptic curves in this essay.

A Supplementary Material

We include here some supplementary material referenced in the essay. We first include a brief list of formulas, including the addition formulae. Then, we give a list of elliptic curves covered in this essay and proofs of their non-singularity.

A.1 Formulary

With minor modifications in notation, all formulae in this subsection are reproduced from [26, Chapter III] (taking into account the errata [25]).

Let C be a cubic curve over a field K expressed in Weierstraß form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

We first record

$$\begin{aligned} b_2 &= a_1^2 + 4a_2, \\ b_4 &= 2a_4 + a_1a_3, \\ b_6 &= a_3^2 + 4a_6, \\ b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2. \end{aligned}$$

Now, define the *discriminant* $\Delta = \Delta(C)$ by

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6. \tag{23}$$

The quantity Δ will be important in the next subsection.

The following Proposition gives the explicit addition formulae on an elliptic curve E with Weierstraß form as above.

Proposition A.1. *Let E be an elliptic curve with Weierstraß form as above. Suppose $\mathbf{p} = (x, y)$ and $\mathbf{q} = (x', y')$ are two points on E. Then:*

(a) $-\mathbf{p} = (x, -y - a_1x - a_3)$.

(b) if $x = x'$ and $y + y' + a_1x + a_3 = 0$, then $\mathbf{p} + \mathbf{q} = \mathbf{o}$.

(c) if (b) does not hold, define $u, v \in K$ as follows:

	u	v
$x \neq x'$	$\dfrac{y' - y}{x' - x}$	$\dfrac{yx' - y'x}{x' - x}$
$x = x'$	$\dfrac{3x^2 + 2a_2x + a_4 - a_1y}{2y + a_1x + a_3}$	$\dfrac{-x^3 + a_4x + 2a_6 - a_3y}{2y + a_1x + a_3}$

Suppose $\mathbf{p} + \mathbf{q} = \mathbf{r}$. Then $\mathbf{r} = (x'', y'')$ where

$$\begin{aligned} x'' &= u^2 + a_1u - a_2 - x - x', \quad \text{and} \\ y'' &= -(u + a_1)x'' - v - a_3. \end{aligned}$$

Proof. See [26, Group Law Algorithm III.2.3]. □

A.2 List of Elliptic curves and proofs of their non-singularity

In this subsection, we include a list of all elliptic curves considered in this essay. It is clear that the listed curves are cubic curves containing the K-rational point $\mathbf{o} = [0 : 1 : 0]$. We will prove that they are non-singular.

In the body of the essay, we considered

(i) the Legendre curves $E_d : y^2 = x(x+1)(x+t^d)$ defined over $\mathbb{F}_p(t)$ for odd primes p in section 2;

(ii) the "quadratic twists" of the Legendre curve $E_A : A(t)y^2 = x^3 - x$ defined over $\mathbb{F}_q(t)$, where $q \equiv 3 \pmod 4$ and $A(t)$ is a square-free $\mathbb{F}_q$-additive polynomial, in Theorem 3.14. We particularly focused on the elliptic curve $\tilde{E}_d$ which are obtained by setting $A(t) = t^{q^d} - t$;

(iii) the elliptic curve $y^2 = x^3 - x$ over $\mathbb{F}_q$, $q \equiv 3 \pmod 4$, in the proof of Theorem 3.14;

(iv) the "cubic twists" of the Hessian curve $y^2 - y = A(t)x^3$ over $\mathbb{F}_q(t)$ in Theorem 3.15, where $q \equiv 2 \pmod 3$ and $A(t)$ an $\mathbb{F}_q$-additive polynomial. Our explicit example was obtained by specialising $A(t) = t^{q^d} - t$;

(v) the elliptic curve $y^2 - y = x^3$ over $\mathbb{F}_q$, $q \equiv 2 \pmod 3$, in the proof of Theorem 3.15;

(vi) the elliptic curves $E_n^{(2)} : y^2 = x^3 - (t^{q^{n+1}} + 1)x$ over $\mathbb{F}_q(t)$, where q is a power of a prime p such that $p \geq 7$ and $q \equiv 3 \pmod 4$, in Theorem 3.17;

(vii) the family of Hessian elliptic curves $y^2 + \alpha xy + y = x^3$, where $\alpha \neq 27$, over a field K with characteristic not equal to 3 in section 4. We also considered the slightly more general family $y^2 + a_1xy + a_3y = x^3$, where $a_3^3(a_1^3 - 27a_3) \neq 0$, over such fields K.

Now, recall the definition of Δ from equation (23).

Lemma A.2. *A cubic curve E in Weierstraß form (2) is non-singular if and only if its discriminant is non-vanishing.*

Proof. See [26, Proposition III.1.4]. □

Proposition A.3. *The cubic curves listed above are all non-singular. Consequently, they are elliptic curves.*

Proof. As cases (i), (iii), (v), (vii) are already in Weierstraß form, we compute their discriminants. We consider (iii) and (v) in a slightly more general setting.

	E	base field	$\Delta(E)$
(i)	$y^2 = x(x+1)(x+t^d)$	$\mathbb{F}_p(t)$, p odd	$16t^{2d}(t^d-1)^2$
(iii)	$y^2 = x^3 - x$	K, $\operatorname{char} K \neq 2$	64
(v)	$y^2 - y = x^3$	K, $\operatorname{char} K \neq 3$	-27
(vii)	$y^2 + a_1xy + a_3y = x^3$	K, $\operatorname{char} K \neq 3$	$a_3^3(a_1^3 - 27a_3)$

As the discriminant is non-vanishing in each case, by Lemma A.2, it follows that the aforementioned elliptic curves are non-singular.

We now turn to the remaining cases. We only prove (ii), as the remaining cases follow by essentially the same argument. Take the cubic curve $A(t)y^2 = x^3 - x$. Let C be the curve $s^2 = A(t)$ over $\mathbb{F}_q$ and let $L = \mathbb{F}_q(C)$ be its function field. Note, the linear change of variable $(\tilde{x}, \tilde{y}) = (x, sy)$ puts this elliptic curve in the form of case of (iii) in the table above. Moreover, one can see that the property of non-singularity is preserved by this change of variable, by expressing this change of variable in projective coordinates and using the chain rule for partial derivatives. Thus, by case (iii) of the table above, we conclude $A(t)y^2 = x^3 - x$ is non-singular. □

B Discussion of the Characteristic 2 Case

The aim of this appendix is to provide a few remarks on generalising Ulmer's approach to the characteristic 2 case.

We begin by discussing the nature of order 2 points on an elliptic curve E over a field K of characteristic 2. Suppose E has Weierstraß equation

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$

As we saw in the beginning of section 2, the order 2 points on E are precisely the points of intersection between the line $a_1X + 2Y + a_3Z = 0$ and E. In characteristic 2, this becomes the line $a_1X + a_3Z = 0$. We have three cases

- If $a_1 = a_3 = 0$, then $\Delta(E)$, defined in equation (23), vanishes. Consequently, by Lemma A.2, E is singular. In particular, this shows that the Legendre curves $y^2 = x(x+1)(x+t^d)$ are singular in characteristic 2.

- If $a_1 = 0$ and $a_3 \neq 0$, then the order 2 points are the points of intersection of the 'line at infinity' $Z = 0$ with E. But, this line intersects E only at $\mathbf{o}$, implying that the 2-torsion subgroup of E is trivial. In other words, E is supersingular. This proves that the elliptic curve $y^2 - y = x^3$ from the proof of Theorem 3.15 is supersingular in characteristic 2.

- If $a_1 \neq 0$, then the order 2 points form the intersection of E with the vertical line $x = -a_3/a_1$. This line intersects E at $\mathbf{o}$ and at two other points $\mathbf{p}, \mathbf{q} \in E \cap \mathbb{A}_z$. However, as this is a vertical line and $\mathbf{p}, \mathbf{q}$ have order 2, the line $x = -a_3/a_1$ must be the tangent line to E at $\mathbf{p}$ and $\mathbf{q}$. Therefore, $\mathbf{p} = \mathbf{q}$, and E has just one order 2 point.

Thus, we see that the nature of the order 2 points on an elliptic curve E changes fundamentally in characteristic 2.

By [26, Proposition A.1.1], every elliptic curve over a field of characteristic 2 can be put into one of the following two Weierstraß forms with a suitable change of coordinate:

$$y^2 + xy = x^3 + ax^2 + b, \qquad \text{or} \qquad y^2 + ay = x^3 + bx + c.$$

The former has $\Delta = b$, while the latter has $\Delta = b^3$. As the Legendre family of elliptic curves has the special property that they contain all order 2 points, noting that the second type of elliptic curves above is supersingular, it seems that the closest analogue in

characteristic 2 would be elliptic curves of the first type. We also remark that Conceição's example $y^2 - y = A(t)x^3$ from Theorem 3.15 is a family of supersingular elliptic curves with unbounded rank that holds in the characteristic 2 setting. Thus, we focus on the family of elliptic curves of the form $y^2 + xy = x^3 + ax^2 + b$.

In order to find points on such elliptic curves, the author considered formal power series expansions for $x = \sum_{i=0}^{\infty} x_i t^i$ and $y = \sum_{i=0}^{\infty} y_i t^i$ for $x_i, y_i \in \mathbb{F}_2$. In the best case, the resulting power series for x and y are finite, in which case we get an integral point on such elliptic curves. Otherwise, we are looking for power series solutions that resemble convergent power series in $\mathbb{C}$. For example, if the power series $\sum_{i=0}^{\infty} t^i$ appears in our computations, we could replace it with $(1-t)^{-1}$, and see if the latter still gives rise to a solution. This is related to the concept of the formal group of an elliptic curve from [26, Chapter IV].

The author first considered the problem abstractly, giving a and b power series expansions $a = \sum_{i=0}^{\infty} a_i t^i$ and $b = \sum_{i=0}^{\infty} b_i t^i$. As we are trying to generalise Ulmer's proof, we are particularly interested in the case where a and b are power series in t^d. In this case, we are looking for (x, y) that has a large $\mathrm{Gal}(\mathbb{F}_2(\mu_d, t)/\mathbb{F}_2(t^d))$-orbit.

Most of the difficulty was due to the x^3 term which, in characteristic 2, expands as

$$x^3 = \sum_{i=0}^{\infty} \left(\sum_{m+2n=i} x_m x_n \right) t^i.$$

In practice, this term does not lead to patterns.

This led the author to consider alternative models for elliptic curves in characteristic 2. First, we define

Definition B.1. Let K be a field. Define $\mathbb{P}K^n$ to be the set of 1-dimensional subspaces of K^{n+1}. For $(X_0, \ldots, X_n) \in K^{n+1} \setminus \{\mathbf{0}\}$ define $[X_0 : \cdots : X_n] \in \mathbb{P}K^n$ to be the one-dimensional subspace spanned by $(X_0, \ldots, X_n)$.

Note that this agrees with our earlier definition of $\mathbb{P}K^2$. Kohel [13, Section 5] defines the following normal form

Definition B.2. Let K be any field, and let c be a non-zero element of K. An elliptic curve E over K is in $\mathbb{Z}/4\mathbb{Z}$-normal form if it is given by an equation of the form

$$X_0^2 - X_1^2 + X_2^2 - X_3^2 = cX_0X_2 = cX_1X_3.$$

The $\mathbb{Z}/4\mathbb{Z}$-normal form is an elliptic curve in the sense that there is a change of variable that puts it into Weierstraß form:

Proposition B.3. *The change of variable map*

$$[X : Y : Z] = [X_1 + X_2 : X_2 : c(X_0 + X_3)]$$

converts an elliptic curve in $\mathbb{Z}/4\mathbb{Z}$-normal form to the Weierstraß form:

$$Y(Y + X)Z = X(X + c^{-1}Z)^2.$$

Proof. See [13, Lemma 9]. □

Hence, the $\mathbb{Z}/4\mathbb{Z}$-normal form inherits an induced group law. The $\mathbb{Z}/4\mathbb{Z}$ normal form is so-named because the point $\mathbf{t} = [1 : 1 : 0 : 0]$ is then an order 4 point [13, Theorem 8].

In characteristic 2, the $\mathbb{Z}/4\mathbb{Z}$-normal form takes the form

$$(X_0 + X_1 + X_2 + X_3)^2 = cX_0X_2 = cX_1X_3.$$

It intuitively appears the power series approach might see more success with this normal form as the left-hand side is a perfect square. The author attempted this by setting $c = t^d$ but did not find obvious non-trivial points. The next steps would be to continue this investigation with other values of c.

One could also attempt to modify the number-theoretic approach in section 4.2 to this setting. Namely, suppose X_0, X_1, X_2, X_3 and c are polynomials. Analysing their prime factorisations, one finds a map from the solutions $[\alpha : \beta : \gamma : \delta] \in \mathbb{PF}_2^3$ of

$$c\alpha\beta\gamma\delta = (\alpha + \beta)^2(\gamma + \delta)^2$$

to the $\mathbb{Z}/4\mathbb{Z}$-normal form given by $[X_0 : X_1 : X_2 : X_3] = [\alpha\beta : \alpha\gamma : \gamma\delta : \beta\delta]$. Kohel also notes this map in [13, Theorem 8], but explains it via different means. It would be of interest to see the results of expanding $\alpha, \beta, \gamma, \delta$ into power series. Another possible direction for future investigation would be to see how Conceição-Shioda applies here.

C Magma code used in Section 4.2

Here is the code file used in our Magma computations. The function `pfn` in line 43 is the implementation of Algorithm 1.

```
1  // presets
2  F5 := GF(5);
3  K<t> := PolynomialRing(F5);
4
5
6  // PolyDeglt returns all polynomials of degree at most n
7  function PolyDeglt(n: F:=F5, pF:=K)
8    S := [pF | elt< pF | Reverse([a : a in x]) > :
9                              x in CartesianPower(F, n)];
10   return [x : x in S | Degree(x) gt 0];
11 end function;
12
13
14 // getDivisors returns all divisors of polynomial f
15 function getDivisors(f, F, pF)
16   primefacts := Factorization(elt<pF | f>);
17   l := [];
18   d := [];
19
20   for x in primefacts do
21     Append(~l, {0..x[2]});
22   end for;
23
24   ind := CartesianProduct(l);
25   for x in ind do
26     prod := pF!1;
27     for i := 1 to #primefacts do
28       prod *:= primefacts[i][1]^x[i];
```

```
    end for;
    for x in Exclude(Set(F), F!0) do
      Append(~d, x*prod);
    end for;
  end for;

  return d;
end function;


// pfn is the Magma function implementing Algorithm 1
// S is the search list,
// F is the base field,
// pF is the polynomial ring of F.
pfn := function(S, F, pF)
  // Each list Mi will contain degree i solutions
  M2 := [];
  M3 := [];
  M4 := [];
  M5 := [];
  M6 := [];
  M7 := [];

  // Now, we implement Algorithm 1
  for zeta in S do
    for mu in getDivisors(zeta^3 + 1, F, pF) do
      if (j notin {1, zeta+1, zeta^2 -zeta + 1, zeta^3 + 1}) and
                            (((mu^3 - 1) mod zeta) eq pF!0) then
        alpha := ((j^3 - 1 - i^3) div (i*j));

        d := GCD(Support(alpha)); // GCD(Support(*)) gives the
                                  // maximal d so that * is a
                                  // polynomial in t^d

        if (d gt 1) and
           (GCD(GCD(Support(mu)), GCD(Support(zeta))) eq 1) then
          case g:
            when 2:
              Append(~M2, [zeta, mu, alpha]);
            when 3:
              Append(~M3, [zeta, mu, alpha]);
            when 4:
              Append(~M4, [zeta, mu, alpha]);
            when 5:
              Append(~M5, [zeta, mu, alpha]);
            when 6:
              Append(~M6, [zeta, mu, alpha]);
            else
              Append(~M7, [zeta, mu, alpha]);
          end case;
        end if;
      end if;
    end for;
  end for;
  return M2, M3, M4, M5, M6, M7;
end function;
```

Listing 1: Auxiliary code

Observe, that in line 64 above, we exclude non-primitive solutions. Indeed, this works because one can observe that if $a, b \in \mathbb{F}_5[t]$ are polynomials so that $a(t^d)$ divides $b(t^d)$, then $a(t)$ divides $b(t)$. This holds because if $r \in \overline{\mathbb{F}_5}$ is a root of $a(t)$, then there is $u \in \overline{\mathbb{F}_5}$ such that $u^d = r$. Then, u is a root of $a(t^d)$, so that $b(r) = b(u^d) = 0$.

The author then partitioned `PolyDeglt(8)` into smaller pieces, ordered by degree of the polynomials, and ran the function `pfn` on each of the smaller pieces.

References

[1] Lisa Berger. "Towers of surfaces dominated by products of curves and elliptic curves of large rank over function fields". In: *Journal of Number Theory* 128.12 (2008), pp. 3013–3030. ISSN: 0022-314X. DOI: https://doi.org/10.1016/j.jnt.2008.03.009. URL: https://www.sciencedirect.com/science/article/pii/S0022314X08000863.

[2] Wieb Bosma, John Cannon, and Catherine Playoust. "The Magma algebra system. I. The user language". In: *J. Symbolic Comput.* 24.3-4 (1997). Computational algebra and number theory (London, 1993), pp. 235–265. ISSN: 0747-7171. DOI: 10.1006/jsco.1996.0125. URL: http://dx.doi.org/10.1006/jsco.1996.0125.

[3] Ricardo P. Conceição. "Elliptic curves over function fields with a large set of integral points". In: *Acta Arithmetica* 161.4 (2013), pp. 351–370. URL: https://arxiv.org/pdf/0910.3417.

[4] Andrew Dancer. *Rings and Modules Lecture Notes, HT 2024*. URL: https://courses.maths.ox.ac.uk/pluginfile.php/105030/mod_resource/content/9/A3pdfLaTeX.pdf (visited on 2024).

[5] Olivier Debarre, Antonio Laface, and Xavier Roulleau. "Lines on Cubic Hypersurfaces Over Finite Fields". In: *Geometry Over Nonclosed Fields*. Ed. by Fedor Bogomolov, Brendan Hassett, and Yuri Tschinkel. Cham: Springer International Publishing, 2017, pp. 19–51. ISBN: 978-3-319-49763-1.

[6] Jean Delsarte. "Nombre de solutions des équations polynomiales sur un corps fini". In: *Séminaire Bourbaki : années 1948/49 - 1949/50 - 1950/51, exposés 1-49*. Séminaire Bourbaki 1. talk:39. Société mathématique de France, 1952, pp. 321–329. URL: https://www.numdam.org/item/SB_1948-1951__1__321_0/.

[7] David S. Dummit and Richard M. Foote. *Abstract Algebra*. 3rd. John Wiley & Sons, Inc., 2004. ISBN: 0-471-43334-9.

[8] Richard Earl. *Projective Geometry Lecture Notes, TT 2025*. URL: https://courses.maths.ox.ac.uk/pluginfile.php/111624/mod_resource/content/2/lectures25.pdf (visited on 2025).

[9] William Fulton. *Algebraic Curves: An Introduction to Algebraic Geometry*. 3rd. Jan. 2008. URL: https://dept.math.lsa.umich.edu/~wfulton/CurveBook.pdf.

[10] Dale Husemöller. *Elliptic Curves*. 2nd. Vol. 111. Graduate Texts in Mathematics. New York, NY: Springer-Verlag, 2004. ISBN: 978-0-387-95490-5. DOI: 10.1007/b97292.

[11] J. T. Tate and I. R. Shafarevich. "The rank of elliptic curves". In: *Dokl. Akad. Nauk SSSR* 175.4 (1967), pp. 770–773. URL: https://www.mathnet.ru/eng/dan33244.

[12] J. W. S. Cassels. *Lectures on Elliptic Curves*. London Mathematical Society Student Texts. Cambridge University Press, 1991. ISBN: 9781139172530. DOI: 10.1017/CBO9781139172530.

[13] David Kohel. "Efficient arithmetic on elliptic curves in characteristic 2". In: *Lecture Notes in Computer Science*. Vol. 7668. Kolkata, India, Dec. 2012, pp. 378–398. DOI: 10.1007/978-3-642-34931-7_22. URL: https://hal.science/hal-01257333.

[14] Serge Lang and André Néron. "Rational points of Abelian varieties over function fields". In: *American Journal of Mathematics* 81.1 (Jan. 1959), pp. 95–118. URL: https://www.jstor.org/stable/2372851.

[15] Aaron Meurer et al. "SymPy: symbolic computing in Python". In: *PeerJ Computer Science* 3 (Jan. 2017), e103. ISSN: 2376-5992. DOI: 10.7717/peerj-cs.103. URL: https://doi.org/10.7717/peerj-cs.103.

[16] Louis Joel Mordell. "On the rational resolutions of the indeterminate equations of the third and fourth degree". In: *Proceedings of the Cambridge Philosophical Society* XXI (1922).

[17] Thomas Occhipinti. "Mordell-Weil Groups of Large Rank in Towers". PhD thesis. University of Arizona, 2010. URL: http://hdl.handle.net/10150/194213.

[18] Henri Poincaré. "Sur les propriétés arithmétiques des courbes algébriques". In: *Journal de mathématiques pures et appliquées* 7.3 (1901), pp. 161–233. URL: https://henripoincarepapers.univ-nantes.fr/chp/hp-pdf/hp1901jm.pdf.

[19] Bjorn Poonen. "Heuristics for the Arithmetic of elliptic curves". In: *Proceedings of the International Congress of Mathematicians (ICM 2018)*. 2017, pp. 399–414. DOI: 10.1142/9789813272880_0060. URL: https://www.worldscientific.com/doi/abs/10.1142/9789813272880_0060.

[20] Karl Rubin and Alice Silverberg. "Ranks of elliptic curves". In: *Bulletin of the American Mathematical Society* 39.4 (July 2002), pp. 455–474. URL: https://www.ams.org/journals/bull/2002-39-04/S0273-0979-02-00952-7/S0273-0979-02-00952-7.pdf.

[21] Norbert Schappacher. "Développement de la loi de groupe sur une cubique". In: *Séminaire de Théorie des Nombres Paris 1988/89*. Vol. 5. MPIM Preprint Series. 1990. URL: https://archive.mpim-bonn.mpg.de/id/eprint/1782/.

[22] Tetsuji Shioda. "An Explicit Algorithm for Computing the Picard Number of Certain Algebraic Surfaces". In: *American Journal of Mathematics* 108.2 (Apr. 1986), pp. 415–432. DOI: 10.2307/2374678. URL: https://www.jstor.org/stable/2374678.

[23] Tetsuji Shioda. "Mordell-Weil Lattices and Sphere Packings". In: *American Journal of Mathematics* 113.5 (Oct. 1991), pp. 931–948. URL: https://www.jstor.org/stable/2374791.

[24] Alice Silverberg. "Ranks 'cheat sheet'". In: *WIN2: Research Directions in Number Theory*. Ed. by C. David, M. Lalin, and M. Manes. Vol. 606. Contemporary Mathematics. American Mathematical Society and Centre de Recherches Mathématiques. 2013, pp. 101–110. URL: https://www.math.uci.edu/~asilverb/bibliography/RanksCheatSheet.pdf.

[25] Joseph H. Silverman. *Errata and Corrections to The Arithmetic of Elliptic Curves*. Aug. 2013. URL: http://www.math.brown.edu/johsilve/AEC/AECErrata2013.pdf.

[26] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. 2nd. Vol. 106. Graduate Texts in Mathematics. New York, NY: Springer-Verlag, 2009. ISBN: 978-0-387-09493-9. DOI: 10.1007/978-0-387-09494-6.

[27] Jonathan Smith. "Symmetries of Del Pezzo Surfaces". PhD thesis. University of South Carolina, Apr. 2025. URL: https://scholarcommons.sc.edu/etd/8092.

[28] Terence Tao. *246C notes 1: Meromorphic functions on Riemann surfaces, and the Riemann-Roch theorem*. URL: https://terrytao.wordpress.com/2018/03/28/246c-notes-1-meromorphic-functions-on-riemann-surfaces-and-the-riemann-roch-theorem/#fg (visited on 03/28/2018).

[29] Douglas Ulmer. "Elliptic curves with large rank over function fields". In: *Annals of Mathematics* 155.2 (2002), pp. 295–315. URL: https://arxiv.org/abs/math/0109163.

[30] Douglas Ulmer. "Explicit points on the Legendre curve". In: *Journal of Number Theory* 136 (2014), pp. 165–194. URL: https://arxiv.org/pdf/1002.3313.

[31] Douglas Ulmer. "On Mordell-Weil groups of Jacobians over function fields". In: *Journal of the Institute of Mathematics of Jussieu* 12 (2013), pp. 1–29. URL: https://arxiv.org/abs/1002.3310.

[32] Douglas Ulmer. "Park City lectures on Elliptic curves over function fields". In: *Arithmetic of L-functions*. Vol. 18. IAS/Park City Mathematics Series. American Mathematical Society, 2011, pp. 211–280. URL: https://arxiv.org/pdf/1101.1939.

[33] Ravi Vakil. *The Rising Sea: Foundations of Algebraic Geometry*. Princeton, NJ: Princeton University Press, 2025. URL: http://math.stanford.edu/~vakil/216blog/FOAGoct2125public.pdf.

[34] Anastasia V. Vikulova. "The most symmetric smooth cubic surface over a finite field of characteristic 2". In: (Dec. 2023). DOI: 10.1016/j.ffa.2024.102470. eprint: 2312.17032. URL: https://arxiv.org/pdf/2312.17032.pdf.

[35] L. Wiersema. "Elliptic curves with $\mathbb{Q}$-rational points of order n". Bachelor's Thesis. University of Groningen, July 2023. URL: https://fse.studenttheses.ub.rug.nl/30431/1/bMATH_2023_WiersemaL.pdf.