Bayerische Julius-Maximilians-Universität Würzburg
Fakultät für Mathematik und Informatik
Lehrstuhl für Mathematik IV (Komplexe Analysis)

An Elementary Derivation and Implementation of Schoof's Algorithm for Counting Points on Elliptic Curves

Diplomarbeit im Fach Mathematik
vorgelegt von

Peter Dinges
<me@elwedgo.de>

am 4. Mai 2010

Angefertigt am
Lehrstuhl für Mathematik IV (Komplexe Analysis)
Fakultät für Mathematik und Informatik
Bayerische Julius-Maximilians-Universität Würzburg

Betreut von
Prof. Dr. Jörn Steuding

Outline

This text explains René Schoof's algorithm for counting the points on an elliptic curve over a finite field [27]. A naive implementation of the algorithm accompanies the text.

Both, text and implementation focus on simplicity and motivation of the underlying ideas. I have tried to arrange the exposition in order of thought, first stating the problem, then telling how one might find a solution, and finally showing that the approach works. The perspective taken is that of someone with basic knowledge in mathematics who is working towards the goal of counting the points on an elliptic curve. Of course, the text omits failed ideas and backtracking; it chooses the next step with incredible accuracy.

Most of the definitions, theorems, and proofs come from the elementary introduction to elliptic curves by Charlap and Robbins [2]. In that sense, the present text can be seen as a rearranged and commented version of their introduction. Further sources are the books of Silverman [29] and Washington [31].

Structure

The derivation of Schoof's algorithm begins with the definition of elliptic curves in chapter 1. Fast point counting requires insight into the structure of elliptic curves, so chapter 2 examines groups of points with the same order. These possess a module structure if the curve is smoothed; chapter 3 explains how to compute on the module without an explicit representation of its elements. In chapter 4, characterizing the points of the non-smoothed curve hints at how to count them with information from local structure; chapter 5 supplies the required link. Finally, the algorithm is assembled in chapter 6, which also describes an implementation in the Python programming language [22].

Notation

Sometimes the notation breaks conventions to group related items more consistently. For example, the ramification index is written as $\mathrm{ram}_P(F)$ instead of the customary $e_F(P)$. However, the most prominent items in the literature treating Schoof's algorithm keep their symbols to avoid confusion: the parameters of an elliptic are A and B; ψ_ℓ still denotes the ℓ-th division polynomial.

All text elements—definitions, theorems, equations, and floats—use the same counter within a chapter, so their numbers are linearly ordered: for instance, Equation (4.2) precedes Figure (4.3) and follows Lemma (4.1). Thus, references can be followed using binary search.

Contents

Chapter 1

Elliptic Curves

Generalizations of the ElGamal [7], Diffie–Hellman [6], and Massey–Omura [14] cryptographic algorithms work on arbitrary abelian groups. Naturally, the group properties influence how well the algorithms perform; especially the group order is central for estimating the provided security [11, p. 183].

Elliptic curves over finite fields have been found to be a good choice as underlying groups for these algorithms; Koblitz [10] and Miller [17] proposed them for this setting. The present chapter defines elliptic curves, explains the assumptions, and motivates the further approach to the theory of determining the group order.

Definition 1.1. Let $A, B \in \mathbb{F}$ be elements of a field of characteristic neither 2 nor 3. The *elliptic curve* E over $\mathbb{F}$ with parameters A and B is the set of all points $(\alpha, \beta) \in \mathbb{F} \times \mathbb{F}$ that satisfy the equation

$$\beta^2 = \alpha^3 + A \cdot \alpha + B, \tag{1.2}$$

together with a special point $\mathcal{O} \notin \mathbb{F} \times \mathbb{F}$:

$$E = \big\{(\alpha, \beta) \in \mathbb{F} \times \mathbb{F} \mid \beta^2 = \alpha^3 + A \cdot \alpha + B\big\} \cup \{\mathcal{O}\}.$$

We call the points in $\mathbb{F} \times \mathbb{F}$ the *finite* points of E, and $\mathcal{O}$ the *point at infinity*. To Equation 1.2 we refer as the *fundamental relation* of the curve, and to the equation's right-hand side as the *defining polynomial* (in α).

Excluding fields of characteristic 2 or 3 simplifies our discussion and allows a clearer exposition of the underlying ideas. However, the constraint is voluntary: Menezes, Vanstone, and Zuccherato [16] derive similar results for fields of characteristic 2; Lercier and Morain build upon work by Couveignes [3, 4] to extend the algorithm to fields of small characteristic, including 2 and 3 [13, 12].

A further limitation prevents unfortunate structure in the group operation, which we will define in a moment.

Definition 1.3. We say an elliptic curve over $\mathbb{F}$ with parameters A and B is *non-singular* if its defining polynomial

$$z^3 + A \cdot z + B \quad \in \mathbb{F}[z]$$

has three distinct roots.

Elliptic curves whose defining polynomials have multiple roots form groups that are closely related to the underlying field, or simple extensions thereof [31, sec. 2.10]. The respective isomorphisms are explicitly known and easy to compute. Structure from the field thus carries over to the group, possibly introducing speedups in computation—a feature unasked for in a cryptographic setting.

Note 1.4. In the following discussion, we assume all elliptic curves to be non-singular. Furthermore, the symbol E always denotes an elliptic curve over a field $\mathbb{F}$; the symbols A and B denote the respective parameters.

Remark 1.5. The notion of non-singularity arises from the curve being smooth over a continuous field. If the characteristic is not 2, our definition is equivalent to the usual definition of the curve being free of singularities, that is, of points at which both partial derivatives of the fundamental relation vanish; non-singular curves thus contain no cusps. For a proof, see Lemma A.1 in the appendix.

Fields of characteristic also not 3 allow a simple test for non-singularity. In Lemma A.2 in the appendix, we show that an elliptic curve is non-singular if, and only if, its discriminant is non-zero:

$$4 \cdot A^3 + 27 \cdot B^2 \neq 0.$$

Next we define the group operation.

Definition 1.6. Let E be a (non-singular) elliptic curve, and $P_1, P_2 \in E \setminus \{\mathcal{O}\}$ be finite points on the curve. Writing $P_1 = (\alpha_1, \beta_1)$ and $P_2 = (\alpha_2, \beta_2)$, we define *point addition* $+ : E \times E \to E$ as follows:

(i) The *generic addition formula* applies in case $\alpha_1 \neq \alpha_2$; we put $P_1 + P_2 = (\alpha_3, \beta_3)$, where

$$\begin{aligned} \alpha_3 &= -\alpha_1 - \alpha_2 + \gamma^2, \\ \beta_3 &= -\beta_1 + \gamma \cdot (\alpha_1 - \alpha_3), \end{aligned}$$

and

$$\gamma = \frac{\beta_2 - \beta_1}{\alpha_2 - \alpha_1}.$$

(ii) *Point doubling* occurs if $P_1 = P_2$ and $\beta_1 \neq 0$. We put $P_1 + P_2 = (\alpha_4, \beta_4)$ with

$$\begin{aligned} \alpha_4 &= -2\alpha_1 + \delta^2, \\ \beta_4 &= -\beta_1 + \delta \cdot (\alpha_1 - \alpha_4), \end{aligned}$$

and

$$\delta = \frac{3\alpha_1^2 + A}{2\beta_1}.$$

(iii) In the remaining finite cases, we put

$$P_1 + P_2 = \mathcal{O};$$

these cases are $\alpha_1 = \alpha_2$, with either $\beta_1 \neq \beta_2$ or $\beta_1 = \beta_2 = 0$.

(iv) Finally, we define addition with the point at infinity by setting

$$P + \mathcal{O} = \mathcal{O} + P = P$$

for any point $P \in E$.

Theorem 1.7. *An elliptic curve with point addition forms an abelian group.*

Proof. The definition of point addition establishes $\mathcal{O}$ as neutral element. Furthermore, adding $-P = (\alpha, -\beta)$ to $P = (\alpha, \beta) \in E$ results in $\mathcal{O}$; the fundamental relation holds for this $-P$, so the inverses exist.

Commutativity follows by symmetry of the formulas. Observe that, for instance,

$$\gamma = \frac{\beta_2 - \beta_1}{\alpha_2 - \alpha_1} = \frac{\beta_1 - \beta_2}{\alpha_1 - \alpha_2};$$

likewise, the formula for the second component in generic addition yields for $P_1 + P_2$ and $P_2 + P_1$:

$$-\beta_1 + \gamma(\alpha_1 - \alpha_3) = -\beta_2 + \gamma(\alpha_2 - \alpha_3),$$

which reduces to

$$\beta_2 - \beta_1 = \gamma(\alpha_2 - \alpha_1),$$

precisely the definition of γ.

All difficulty lies in showing associativity, and there exist several ways to do this. For example, Washington [31, sec. 2.4] uses the (projective) geometric interpretation of elliptic curves. Another possibility is direct computation from the addition formulas; however, I could not find any text following this tedious route. Finally, Charlap and Robbins [2, ch. 6], as well as Silverman [29, sec. III.2], prove that elliptic curves are isomorphic to a known commutative group: the degree zero part of the divisor class group, which is a subgroup of the quotient group over the free abelian group on the curve points.

Though it might sound intimidating and overly abstract at first, this method elegantly connects points on the curve to maps between them. We use some aspects of divisors in chapters 2 and 3. □

Group Order

We have seen how an elliptic curve forms an abelian group; asking for the group order is a natural question. Besides being of theoretical interest, the group order also has practical influence on the security of cryptographic operations on the group. Having in mind cryptographic applications on computers, we are particularly interested in the group order of elliptic curves over finite fields.

The ElGamal, Diffie–Hellman, and Massey–Omura algorithms rely on the difficulty of solving the discrete logarithm problem:

> For points $P, Q \in E$ find $k \in \mathbb{Z}$ such that adding P k-times to itself yields Q (if such k exists).

In groups whose order consists of only small prime factors, the Pohlig–Hellman algorithm determines the discrete logarithm in viable time [21]. Cryptographic environments therefore insist on the order having a large prime factor—a property hard to be sure of without computing the group order. It is even sensible to require prime order because the mentioned algorithms work on cyclic subgroups generated by a chosen group element. Prime order ascertains that all points generate the whole group; it is impossible to accidentally pick an element of small order, which would open the door for a brute-force attack. Koblitz discusses the choice of generators in more depth [11, p. 184].

As group orders grow larger, the complexity of the counting algorithm gains importance. For example, suppose we planned to naively test all elements $\alpha \in \mathbb{F}_q$ of the finite field $\mathbb{F}_q$ on whether the defining polynomial

$$\alpha^3 + A\alpha + B$$

yields a square. This requires q tests to cover the whole field, if we assume a prepared table of all squares in $\mathbb{F}_q$. Consider a realistic $q \approx 10^{57}$ (see NIST recommendations [20, appendix D]), which is the field size for roughly the cryptographic strength [8, p. 19] of 128-bit AES (Advanced Encryption Standard) [19]. With a testing frequency of a million tests per second, employing all atoms of earth as computers, it would still take a hundred times the (non-creationist) age of the universe to complete [26, sec. 1.7].

In order to speed up the counting process, we thus have to exploit the internal structure of elliptic curves. As groups, they lend themselves to the common algebraic approach of learning the structure of an object through its parts.

Chapter 2

Torsion Points

To discern parts of elliptic curves, we have to pick a trait that groups the elements into subsets. We avoid far-fetched ideas and turn to the order of points for this grouping. Our goal in the present chapter is to explore the structure of the subsets, which we will later use to gather information about the curve as a whole.

Definition 2.1. Let E be an elliptic curve. *Multiplication by an integer* ℓ on E is the map $[\ell] : E \to E$ that adds a point ℓ-times to itself. For a point $P \in E$, and $\ell \in \mathbb{Z}$, we set

$$\begin{aligned} &[0](P) = \mathcal{O}; \\ &[\ell](P) = P + [\ell - 1](P) && \text{if } \ell > 0; \\ &[\ell](P) = -\big([-\ell](P)\big) && \text{if } \ell < 0. \end{aligned}$$

We write $\ell \cdot P$ as shorthand notation for $[\ell](P)$.

Multiplication by integers is the additive equivalent of exponentiation in multiplicative groups. For a fixed point, asking for the minimal ℓ such that $\ell \cdot P = \mathcal{O}$ means asking for the point's order. Conversely, we may regard the effects of multiplication by a constant ℓ and describe the points of order ℓ as the ones that $[\ell]$ maps to $\mathcal{O}$. This characterization is heavily influenced by the grid that the finite field imposes on the points: the finer the grid is, the more points exist, and the more can map to $\mathcal{O}$. We want to have all possible solutions available and therefore smooth the domain of $[\ell]$.

Definition 2.2. Let E be an elliptic curve over $\mathbb{F}$ with parameters A and B. If $\mathbb{G}$ is a field and $A, B \in \mathbb{G}$, then $E(\mathbb{G})$ denotes the curve with parameters A and B over $\mathbb{G}$:

$$E(\mathbb{G}) = \big\{(\alpha, \beta) \in \mathbb{G} \times \mathbb{G} \mid \beta^2 = \alpha^3 + A \cdot \alpha + B\big\} \cup \{\mathcal{O}\}.$$

We call $E(\mathbb{G})$ the $\mathbb{G}$-*rational points* on E.

The name stems from the common usage of above definition. Frequently, $\mathbb{G}$ is a subfield of $\mathbb{F}$; pretending that $\mathcal{O}$ lies in $\mathbb{G} \times \mathbb{G}$ for a moment, $E(\mathbb{G})$ is the subset of all points with coordinates in $\mathbb{G} \subseteq \mathbb{F}$.

However, we want to smooth the curve. We will therefore go in the opposite direction and make $\mathbb{G}$ a superfield of $\mathbb{F}$, namely its algebraic closure $\overline{\mathbb{F}}$.

Definition 2.3. The *ℓ-torsion points* of an elliptic curve E are the points $P \in E(\overline{\mathbb{F}})$ of order ℓ; we denote the set of ℓ-torsion points by

$$E[\ell] = \{P \in E(\overline{\mathbb{F}}) \mid [\ell](P) = \mathcal{O}\}$$

and call ℓ their *torsion*.

Example 2.4. Recall that the generic formulas for point doubling in Definition 1.6, case (ii), require $\beta \neq 0$ for a point (α, β) on the curve. If $\beta = 0$, then case (iii) applies and $(\alpha, 0) + (\alpha, 0) = 2 \cdot (\alpha, 0) = \mathcal{O}$. Therefore, finite points with a zero second component have order 2; the definition of point doubling furthermore makes clear that only these have order 2.

We use the fundamental relation to derive their first coordinate. Insert $(\alpha, 0)$ to get

$$0 = \alpha^3 + A\alpha + B = (\alpha - \omega_1)(\alpha - \omega_2)(\alpha - \omega_3).$$

Consequently, the first coordinates must be roots ω_i, $i = 1, 2, 3$, of the defining polynomial. We always assume a non-singular curve, so three different finite points of order 2 exist. The point at infinity, of course, also fulfills $2 \cdot \mathcal{O} = \mathcal{O}$; the set of 2-torsion points therefore is

$$E[2] = \{\mathcal{O}, (\omega_1, 0), (\omega_2, 0), (\omega_3, 0)\}.$$

Observe that ℓ-torsion points are in general $\overline{\mathbb{F}}$-rational, not $\mathbb{F}$-rational. As points of identical order, they form a subgroup of the abelian group $E(\overline{\mathbb{F}})$.

Lemma 2.5. *The set of ℓ-torsion points $E[\ell]$ of an elliptic curve E is a subgroup of $E(\overline{\mathbb{F}})$: the* ℓ-torsion subgroup.

Proof. For any torsion $\ell \in \mathbb{Z}$, $E[\ell]$ contains $\mathcal{O}$ because $\ell \cdot \mathcal{O} = \mathcal{O}$; hence $E[\ell]$ is not empty. Furthermore, $E[\ell]$ is closed under point addition: commutativity implies distributivity with multiplication by integers. Thus we have for $P, Q \in E[\ell]$

$$\ell \cdot (P + Q) = \ell \cdot P + \ell \cdot Q = \mathcal{O},$$

and $P + Q \in E[\ell]$. Finally, closure under inversion follows from

$$\ell \cdot (-P) = -(\ell \cdot P) = -\mathcal{O} = \mathcal{O}.$$

In conclusion, $E[\ell]$ is a subgroup of $E(\overline{\mathbb{F}})$ and, thus, a group. □

Next we demonstrate the benefits of working with the smoother algebraic closure.

Example 2.6. Consider the points of order 3, the 3-torsion points $E[3] = \{P \in E(\overline{\mathbb{F}}) \mid [3](P) = \mathcal{O}\}$. From $3 \cdot P = \mathcal{O}$, we derive

$$2 \cdot P = -P; \tag{2.7}$$

both sides of the equation have explicit formulas: negation on the right-hand side, point doubling on the left-hand side. Let $P = (\alpha, \beta)$, so that $-P = (\alpha, -\beta)$ as in Theorem 1.7. The formula for point doubling in Definition 1.6 yields

$$2 \cdot (\alpha, \beta) = \left(-2\alpha + \gamma^2, -\beta - \gamma \cdot (-3\alpha + \gamma^2)\right) \tag{2.8}$$

because $\beta \neq 0$, for otherwise we would have $P = -P$ and therefore order 2, not 3. Inserting Equation 2.8 into Equation 2.7 yields

$$\left(-2\alpha + \gamma^2, -\beta - \gamma \cdot (-3\alpha + \gamma^2)\right) = (\alpha, -\beta);$$

therefore, we have

$$\begin{aligned}
-2\alpha + \gamma^2 = \alpha \quad &\Leftrightarrow \quad 3\alpha - \gamma^2 = 0 \\
&\Leftrightarrow \quad 3\alpha - \left(\frac{3\alpha^2 + A}{2\beta}\right)^2 = 0 \\
&\Leftrightarrow \quad 3\alpha - \frac{(3\alpha^2 + A)^2}{4(\alpha^3 + A\alpha + B)} = 0 \\
&\Leftrightarrow \quad 3\alpha^4 + 6\alpha^2 + 12B\alpha - A^2 = 0 \qquad (2.9)
\end{aligned}$$

The roots of above polynomial consequently characterize the finite 3-torsion points; the algebraic closure makes all roots available. Thus the degree of the polynomial tells us the number of roots, and from the number of roots follows the number of 3-torsion points: the four roots correspond to eight finite points whose first coordinates are the roots, and whose second coordinates are the respective positive and negative non-zero solutions of the fundamental relation. Hence, together with the point at infinity, there are nine 3-torsion points. The thereby deduced order of $E[3]$ then tells us the structure of the abelian group $E[3]$.

In the present chapter we generalize above idea: we characterize the ℓ-torsion group $E[\ell]$ as the set of poles of multiplication by ℓ, and then analyze $[\ell]$ to count the poles. Unlike the example, we do this without explicit expressions for $[\ell]$; these will follow in chapter 3.

Before we start examining $[\ell]$ in the next section, however, we demonstrate that using the algebraic closure indeed prevents nuisances, and thus, making the ℓ-torsion points $\overline{\mathbb{F}}$-rational is sensible.

Example 2.10. Consider the elliptic curve E with parameters $A = 4$ and $B = 7$ over $\mathbb{F}_{23}$, the field with 23 elements. Equation 2.9 must hold for the first coordinate of its finite 3-torsion points; substituting the parameters yields the polynomial equation

$$3\alpha^4 + \alpha^2 - 8\alpha = (\alpha - 4)(\alpha + 6)(3\alpha^2 + 17\alpha + 16) = 0 \mod 23.$$

However, the quadratic polynomial that is the last factor has no roots in $\mathbb{F}_{23}$: using the standard formula, we obtain the zeros $1 \pm 4\sqrt{5}$ for $(3\alpha^2 + 17\alpha + 16)$, which both lie outside $\mathbb{F}_{23}$ because 5 is not a square. Thus, $P = \left(1 + 4\sqrt{5}, \sqrt{20 + 18\sqrt{5}}\right)$ is a 3-torsion point of E that is not $\mathbb{F}_{23}$-rational: $P \notin E$.

2.1 Multiplication by Integers

In Example 2.6, we identified the finite 3-torsion points with the roots of a polynomial. We derived the polynomial from the rational coordinate functions of point doubling—which we may regard as a special case of multiplication by an integer.

Our goal in this section is to show that the general case of multiplication with an arbitrary integer $\ell \in \mathbb{Z}$ is, too, described by rational coordinate functions. The next section then uses this result to count the poles of $[\ell]$, or equally the ℓ-torsion points. The order of $E[\ell]$ in turn grants us insight into its structure.

Let us start by defining the central terms. We seek to describe the ℓ-torsion points; these are $\overline{\mathbb{F}}$-rational and thus we choose extended domains for our functions.

Definition 2.11. Let E be an elliptic curve over $\mathbb{F}$. The functions $x : E(\overline{\mathbb{F}}) \to \overline{\mathbb{F}}$ and $y : E(\overline{\mathbb{F}}) \to \overline{\mathbb{F}}$ project a point $P = (\alpha, \beta)$ onto its first and second coordinate:

$$x(P) = \alpha \qquad \text{and} \qquad y(P) = \beta.$$

Definition 2.12. A *polynomial* on E is an element of $\mathbb{F}[x, y]$, the ring of polynomials in the functions x and y. We write $\mathbb{F}[E]$ to emphasize the connection with E.

Note 2.13. A polynomial on E accepts points from $E(\overline{\mathbb{F}})$ because the projections x and y accept points $(\alpha, \beta) \in E(\overline{\mathbb{F}})$. Thus, the polynomial coefficients lie in $\mathbb{F}$, but the values of x and y and the result lie in $\overline{\mathbb{F}}$.

Furthermore observe that with points on the curve as input, the fundamental relation extends to x and y:

$$y^2 = x^3 + A \cdot x + B.$$

We may thus reduce all even powers of y to a polynomial in $\mathbb{F}[x]$, so we may assume the highest appearing power of y to be one. A polynomial $s \in \mathbb{F}[E]$ consequently has a *canonical form*

$$s(x, y) = a(x) + y \cdot b(x)$$

where $a, b \in \mathbb{F}[x]$ are customary univariate polynomials.

The canonical form eliminates ambiguity when comparing polynomials: the problem of deciding whether two polynomials are equivalent within the fundamental relation reduces to a comparison of coefficients; for polynomials $s, t \in \mathbb{F}[E]$, we simply compare the coefficients of $a, b, c, d \in \mathbb{F}[x]$ where

$$\begin{aligned} s &= a(x) + y \cdot b(x) \\ t &= c(x) + y \cdot d(x). \end{aligned}$$

This is easy to implement on a computer. The reduction to canonical form also simplifies all other algorithms because univariate polynomial arithmetic suffices to handle the components a and b. More complex multivariate algorithms are unnecessary.

2.1.1 Rational Functions

With polynomials defined, we proceed to explain rational functions on an elliptic curve E.

Definition 2.14. A *rational function* on E is an equivalence class of formal quotients s/t with $s, t \in \mathbb{F}[E]$ polynomials on E and t not identically zero. We identify s/t with u/v if $s \cdot v = u \cdot t$ and denote the field of rational functions as $\mathbb{F}(E)$.

Example 2.15. The coordinate formulas of point doubling in Definition 1.6 are rational functions on E. They are the first and second component of the multiplication-by-2 map [2]. Writing them with the projections x and y as variables, we have for finite points not of order 2:

$$\begin{aligned}\big(x \circ [2]\big)(x,y) &= -2x + \Big(\frac{3x^2+A}{2y}\Big)^2 \\ &= \frac{-8x \cdot y^2 + (9x^4 + 6Ax^2 + A^2)}{4y^2} \\ &= \frac{-8x(x^3+Ax+B) + 9x^4 + 6Ax^2 + A^2}{4(x^3+Ax+B)} \\ &= \frac{x^4 - 2Ax^2 - 8Bx + A^2}{4(x^3+Ax+B)}\end{aligned}$$

and

$$\begin{aligned}\big(y \circ [2]\big)(x,y) &= -y + \Big(\frac{3x^2+A}{2y}\Big)\Big(3x - \Big(\frac{3x^2+A}{2y}\Big)^2\Big) \\ &= y \cdot \Big(-1 + \frac{3x^2+A}{2y^2} \cdot \frac{12x(x^3+Ax+B) - 9x^4 - 6Ax^2 - A^2}{4y^2}\Big) \\ &= y \cdot \frac{-8(x^3+Ax+B)^2 + (3x^2+A)(3x^4+6Ax^2+12Bx-A^2)}{8(x^3+Ax+B)^2} \\ &= y \cdot \frac{x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3}{8(x^3+Ax+B)^2}.\end{aligned}$$

We began our investigation of rational functions with the intention to characterize ℓ-torsion points, which lie on the curve $E(\overline{\mathbb{F}})$. Specifically, we wrote the finite 3-torsion points as those points on $E(\overline{\mathbb{F}})$ satisfying Equation 2.9. Accordingly, these points must evaluate to zero. Our discussion therefore calls for a definition of how to evaluate rational functions at the points of $E(\overline{\mathbb{F}})$, including $\mathcal{O}$. We begin with the finite points.

Definition 2.16. Let $s/t \in \mathbb{F}(E)$ be a rational function and $P \in E(\overline{\mathbb{F}}) \setminus \{\mathcal{O}\}$ a finite point. If there exists $u/v \in \mathbb{F}(E)$ with $u/v = s/t$ and $v(P) \neq 0$, then the value of s/t at P is

$$\frac{s}{t}(P) = \frac{u(P)}{v(P)}.$$

Otherwise $(s/t)(P)$ is infinite.

Next is the point at infinity. Following intuition, we want the value of s/t to depend on the relation of degree between s and t. Since s and t are polynomials

on the curve, we must account for the fundamental relation in our definition. In particular we need the equality

$$\deg(y^2) = \deg(x^3 + Ax + B),$$

which suggests

$$2 \cdot \deg(y) = 3 \cdot \deg(x).$$

Definition 2.17. The *degree* of a polynomial $s(x, y) = a(x) + y \cdot b(x) \in \mathbb{F}[E]$ is

$$\deg(f) = \max\big\{2 \cdot \deg_1(a), 3 + 2 \cdot \deg_1(b)\big\},$$

where $\deg_1$ denotes the common degree of polynomials in one indeterminate.

Observe that in the case $b = 0$, we have $\deg_1(b) = -\infty$. This cancels the 3 added by y.

The usual rules for degrees of products of polynomials hold for our definition.

Lemma 2.18. *For polynomials $s, t \in \mathbb{F}[E]$, the degree of their product is the sum of their degrees:*

$$\deg(s \cdot t) = \deg(s) + \deg(t).$$

Proof. Consider the product of the canonical forms $s(x, y) = a(x) + y \cdot b(x)$ and $t(x, y) = c(x) + y \cdot d(x)$:

$$\begin{aligned}(s \cdot t)(x, y) &= ac(x) + y^2 \cdot bd(x) + y \cdot \big(bc(x) + ad(x)\big) \\ &= ac(x) + (x^3 + Ax + B) \cdot bd(x) + y \cdot \big(bc(x) + ad(x)\big).\end{aligned}$$

Hence we have

$$\begin{aligned}\deg(s \cdot t) &= \max\big\{\deg(ac), 6 + \deg(bd), \deg\big(y \cdot (bc + ad)\big)\big\} \\ &= \max\big\{2\deg_1(ac), 6 + 2\deg_1(bd), 3 + \deg(bc + ad)\big\}. \qquad (2.19)\end{aligned}$$

Furthermore, the definition of deg implies

$$\deg(bc + ad) \leq \max\big\{2\deg(bc), 2\deg(ad)\big\}; \qquad (2.20)$$

the inequality stems from possible cancellation of the highest coefficient. Inserting Equation 2.20 into Equation 2.19 yields

$$\deg(st) \;=\; \max\big\{2\deg_1(ac), 6 + 2\deg_1(bd), 3 + 2\deg_1(bc), 3 + 2\deg_1(ad)\big\} \qquad (2.21)$$

and an examination of cases shows the proposition. For example let $\deg(s) = 2\deg_1(a)$ and $\deg(t) = 3 + 2\deg_1(d)$, which, by the definition of deg, means

$$2\deg_1(a) \geq 3 + 2\deg_1(b) \qquad \text{and} \qquad 2\deg_1(c) \leq 3 + 2\deg_1(d). \qquad (2.22)$$

Thus we have

$$\begin{aligned} 2\deg_1(ac) &= 2\deg_1(a) + 2\deg_1(c) \\ &\leq 2\deg_1(a) + 3 + 2\deg_1(d) \\ &= 3 + 2\deg_1(ad), \\ 6 + 2\deg_1(bd) &= 6 + 2\deg_1(b) + 2\deg_1(d) \\ &\leq 6 + 2\deg_1(a) - 3 + 2\deg_1(d) \\ &= 3 + 2\deg_1(ad), \end{aligned}$$

and

$$\begin{aligned} 3 + 2\deg_1(bc) &= 3 + 2\deg_1(b) + 2\deg_1(c) \\ &\leq 3 + 2\deg_1(b) - 3 + 3 + 2\deg_1(d) \\ &= 3 + 2\deg_1(ad). \end{aligned}$$

In conclusion it is

$$\deg(s \cdot t) = 2\deg_1(a) + 3 + 2\deg_1(d) = \deg(s) + \deg(t).$$

The remaining cases follow after similar discussion. □

Now we possess the tools to compare the growth of the polynomials in the numerator and denominator of rational functions. This allows us to define their value at the point at infinity.

Definition 2.23. Let $s/t \in \mathbb{F}(E)$ be a rational function.

(i) If $\deg(s) < \deg(t)$, we set $(s/t)(\mathcal{O}) = 0$.

(ii) In case $\deg(s) > \deg(t)$, $(s/t)(\mathcal{O})$ is infinite.

(iii) If $\deg(s) = \deg(t)$, we may write the the leading terms of s and t, with $\alpha, \beta \in \mathbb{F}$ and $k \in \mathbb{N}_0$, as

$$\begin{aligned} \alpha \cdot x^k \text{ and } \beta \cdot x^k &\quad \text{if the degree is even, or} \\ \alpha \cdot yx^k \text{ and } \beta \cdot yx^k &\quad \text{if it is odd.} \end{aligned}$$

In either case we set $(s/t)(\mathcal{O}) = \alpha/\beta$.

Points that a function evaluates to zero or infinity are of special interest because they characterize the behavior of the function.

Definition 2.24. Let f be a rational function on E. We say that f has a *zero* at $P \in E(\overline{\mathbb{F}})$ if $f(P) = 0$, and that f has a *pole* at P if $f(P)$ is infinite.

Note that poles at finite points originate from zeros in the denominator polynomial.

2.1.2 Rational Maps

Rational functions evaluate to a field element or infinity. If we make the convention that

$$x(\mathcal{O}) \text{ is infinity} \qquad \text{and} \qquad y(\mathcal{O}) \text{ is infinity},$$

we may interpret the output of a rational function as a single coordinate of another point in $\overline{\mathbb{F}} \times \overline{\mathbb{F}}$. Pairs of functions then map points onto points—which is precisely what multiplication by ℓ, that is $[\ell]$, does for a constant ℓ. It is easy to make sure that the resulting point lies on the curve: for $f, g \in \mathbb{F}(E)$ with f describing the first coordinate, we require the fundamental relation to hold for f and g.

Definition 2.25. A *rational map* F on an elliptic curve E is a pair (f, g) of rational functions $f, g \in \mathbb{F}(E)$ with

$$g^2 = f^3 + A \cdot f + B.$$

We call the functions f and g the *component functions* of F. If f and g are infinite at some point P, we set $F(P) = \mathcal{O}$.

With this convention, F defines a map of $E(\overline{\mathbb{F}})$ onto itself:

$$F : E(\overline{\mathbb{F}}) \to E(\overline{\mathbb{F}}), \qquad F(P) = \big(f(P), g(P)\big).$$

The definition is valid because the fundamental relation links the component functions of a rational map: f is infinite at P if, and only if, g is infinite at P.

Example 2.26. In Example 2.15, we rewrote the point doubling formulas on elliptic curves as rational functions in x and y. That way, we derived expressions for both components of the multiplication-by-2 map $[2]$. The functions had a restricted domain because Definition 1.6 demands finite points not of order 2. However, if we examine the functions closer, we see that they behave correctly on the whole curve: recall that

$$\begin{aligned}
\big(x \circ [2]\big)(x, y) &= -2x + \Big(\frac{3x^2 + A}{2y}\Big)^2 \\
&= \frac{x^4 - 2Ax^2 - 8Bx + A^2}{4(x^3 + Ax + B)}; && (2.27) \\
\big(y \circ [2]\big)(x, y) &= -y + \Big(\frac{3x^2 + A}{2y}\Big)\Big(3x - \Big(\frac{3x^2 + A}{2y}\Big)^2\Big) \\
&= y \cdot \frac{x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3}{8(x^3 + Ax + B)^2}. && (2.28)
\end{aligned}$$

The first expression tells us that at finite points $(\omega, 0)$ of order 2 (compare Example 2.4), the denominator of both functions vanishes. The numerator is non-zero since the curve is non-singular, which means the defining polynomial has three distinct roots, so $(x^3 + Ax + B)' = 3x^2 + A$ cannot have a zero at ω. Therefore both functions have poles at $(\omega, 0)$. With the convention of Definition 2.25, we thus have $[2](\omega, 0) = \mathcal{O}$. This matches the definition: doubling points of order 2 yields the point at infinity.

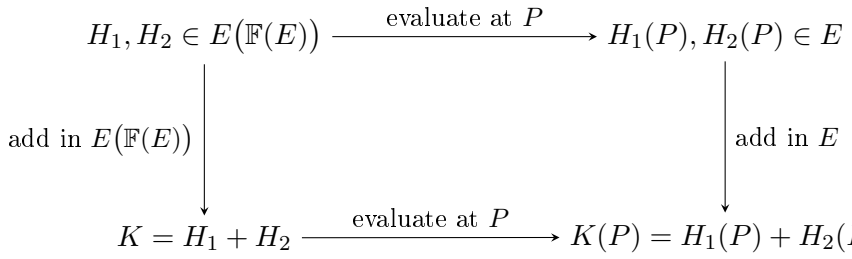

Figure 2.30: Adding rational maps in $E\big(\mathbb{F}(E)\big)$ and then evaluating at a point P yields the same result as first evaluating the maps and then adding the results in E. See Theorem 2.29.

The second expression makes determining the numerator and denominator degrees easy and hence tells us the behavior at $\mathcal{O}$: clearly

$$\deg(x^4 - 2Ax^2 - 8Bx + A^2) = 8 > 6 = \deg(x^3 + Ax + B).$$

Consequently, $\big(x \circ [2]\big)$ has a pole at $\mathcal{O}$. Similar computation reveals that $\big(y \circ [2]\big)$ has a pole at $\mathcal{O}$, too. Therefore the behavior of $[2]$ at $\mathcal{O}$ again matches Definition 1.6:

$$\mathcal{O} + \mathcal{O} = 2 \cdot \mathcal{O} = [2](\mathcal{O}) = \mathcal{O},$$

and the expressions (2.27) and (2.28) describe multiplication by 2 on the whole curve.

Observe that the fundamental relation induces an elliptic curve with identical parameters over the field of rational functions

$$E\big(\mathbb{F}(E)\big) = \big\{(f, g) \in \mathbb{F}(E) \times \mathbb{F}(E) \mid g^2 = f^3 + A \cdot f + B\big\} \cup \big\{\overline{\mathcal{O}} : P \mapsto \mathcal{O}\big\}.$$

The constant-$\mathcal{O}$ map $\overline{\mathcal{O}}$ is the neutral element of this curve and is treated as a rational map, too. Strictly speaking, the rational maps are the finite points of the curve.

The interpretation as points on an elliptic curve yields a natural addition for rational maps: that on $E\big(\mathbb{F}(E)\big)$. This is useful because it allows us to construct higher multiplication maps by means of addition of simpler maps. The sum of two rational maps behaves as expected; see Figure 2.30 for a diagram of the following theorem:

Theorem 2.29. *Let $H_1, H_2 \in E\big(\mathbb{F}(E)\big)$ be rational maps on the elliptic curve E. If $K = H_1 + H_2$, then $K(P) = H_1(P) + H_2(P)$ for any point P on $E(\overline{\mathbb{F}})$.*

We will prove the theorem by discussing the various cases. This will require a lot of reasoning about whether or not a rational function has a pole at a certain point. To ease the discussion, we therefore first introduce a device for splitting rational functions into a harmless, finite and non-zero portion, and a dominant rest.

Lemma 2.31. *For each point $P \in E(\overline{\mathbb{F}})$, there exists a rational function e, zero at P, with the following property: if f is a rational function not identically zero, then*

$$f = e^k \cdot g$$

for some integer $k \in \mathbb{Z}$ and some rational function $g \in \mathbb{F}(E)$ that is finite and non-zero at P. Furthermore, the number k is independent of the choice of the function e.

Note 2.32. The rational function e depends solely on P, and k only on P and f.

Proof. First of all, observe that it suffices to show the proposition for $f = s/t$ having a zero at P: if f has a pole at P, then $1/f$ has a zero; the desired representation then is $f = e^{-k} \cdot (1/g)$ if we derived $1/f = e^k \cdot g$. Furthermore, for f finite and non-zero at P, we put $g = f$ and $k = 0$, which makes immaterial what e is.

The choice of the rational function e only depends on the point P. We will show the existence of respective e in a constructive way by giving valid choices at all points on E. To this end, we distinguish three cases: the point at infinity, points of order 2, and all other points.

(i) Suppose that $P = (\alpha, \beta)$ is finite and not of order 2. By our introductory remark, we may assume $f(\alpha, \beta) = s(\alpha, \beta)/t(\alpha, \beta) = 0$, which implies $s(\alpha, \beta) = 0$ and $t(\alpha, \beta) \neq 0$. Hence, it is enough to find a valid decomposition for the polynomial s because the rational case follows from division by t.

We show $e(x, y) = (x - \alpha)$ to be a valid choice by examining the structure of the canonical form of s, $s(x, y) = a(x) + y \cdot b(x)$. A case discussion of additional side-conditions on the interaction between a and b provides us with more information.

If we assume $a(\alpha) - \beta b(\alpha) = 0$, we obtain linear equations in the variables $a(\alpha)$ and $b(\alpha)$:

$$\begin{aligned} a(\alpha) - \beta b(\alpha) &= 0, \\ a(\alpha) + \beta b(\alpha) &= 0, \end{aligned}$$

where the second equation is s evaluated at P. The field characteristic not being 2 means $\gamma \neq -\gamma$ for every non-zero field element γ, so the equations resolve to $a(\alpha) = b(\alpha) = 0$. Therefore we can split off a factor $(x - \alpha)$ from the polynomials a, b in x alone and decompose s into

$$s(x, y) = (x - \alpha) \cdot \hat{g}(x, y)$$

for some polynomial $\hat{g} \in \mathbb{F}[E]$ that must be finite at P.

Otherwise, if $a(\alpha) - \beta b(\alpha) \neq 0$, then $a(x) - y \cdot b(x)$ is not the zero function. We use this fact by interpreting the polynomial s as rational function and

removing y from the numerator with help of the fundamental relation. We write

$$\begin{aligned} s(x,y) &= a(x) + y \cdot b(x) \\ &= \frac{a(x)^2 - y^2 \cdot b(x)^2}{a(x) - y \cdot b(x)} \\ &= \frac{a(x)^2 - (x^3 + Ax + B) \cdot b(x)^2}{a(x) - y \cdot b(x)}. \end{aligned}$$

Our assumption is $s(\alpha, \beta) = 0$ and thus the numerator must vanish at P, which means

$$a(x)^2 - (x^3 + Ax + B) \cdot b(x)^2 = 0 \qquad \text{at } x = \alpha.$$

Again we can therefore split off the factor $(x - \alpha)$ and express s as

$$s(x,y) = (x - \alpha) \cdot \hat{g}(x,y)$$

where this time $\hat{g} \in \mathbb{F}(E)$ is a rational function that is finite at P.

In either case, if $\hat{g}(P) = 0$, we can apply the same reasoning to $\hat{g}$. The process eventually ends because $\hat{g}$ is finite at P, and therefore $(x - \alpha)$ can only appear as a factor of the denominator of $\hat{g}$ if it also is a factor of the numerator. Each iteration extracts one power of $(x - \alpha)$ from the numerator, so for

$$f(x,y) = (x - \alpha)^k \cdot \hat{g}(x,y),$$

the exponent k is limited by the (finite) degree of the numerator of $\hat{g}$.

(ii) Next we consider the case where $P = (\omega_1, 0)$ is a point of order 2; we will show $e(x,y) = y$ to be a valid choice.

Recall that we assume $f(P) = (s/t)(P) = 0$, which implies that $s(x,y) = a(x) + y \cdot b(x)$ has a zero at P. Hence

$$s(\omega_1, 0) = a(\omega_1) + 0 \cdot b(\omega_1) = 0$$

and a must be zero at ω_1. This allows us to rewrite the polynomial a in x as $a(x) = (x - \omega_1) \cdot \hat{a}(x)$ for some $\hat{a} \in \mathbb{F}[x]$. We then apply the fundamental relation to convert the zero of $(x - \omega_1)$ into an expression in y. Since the roots ω_1, ω_2, and ω_3 of the defining polynomial $x^3 + Ax + B$ are distinct, $(x - \omega_2)$ and $(x - \omega_3)$ are non-zero at P and we have

$$\begin{aligned} s(x,y) &= (x - \omega_1) \cdot \hat{a}(x) + y \cdot b(x) \\ &= \frac{(x - \omega_1)(x - \omega_2)(x - \omega_3) \cdot \hat{a}(x) + y \cdot \hat{b}(x)}{(x - \omega_2)(x - \omega_3)} \\ &= \frac{y^2 \cdot \hat{a}(x) + y \cdot \hat{b}(x)}{(x - \omega_2)(x - \omega_3)} \\ &= y \cdot \left(\frac{y \cdot \hat{a}(x) + \hat{b}(x)}{(x - \omega_2)(x - \omega_3)} \right), \end{aligned}$$

where $\hat{b} = (x - \omega_2)(x - \omega_3) \cdot b(x)$.

We repeat the process in case $y \cdot \hat{a}(x) + \hat{b}(x)$ has a zero at P. However, a has a finite degree and each iteration extracts a linear factor $(x - \omega_1)$; the process therefore terminates and $e(x, y) = y$ is a valid choice at points of order 2.

(iii) Finally, we regard $P = \mathcal{O}$; we will show that in this case, choosing $e(x, y) = x/y$ works.

Our assumption $f(\mathcal{O}) = 0$ implies, by Definition 2.23, that $\deg(s) < \deg(t)$. Therefore we have

$$k = \deg(s) - \deg(t) < 0.$$

We restore a finite value for s/t at the point at infinity by balancing the degrees: it is $\deg(y) - \deg(x) = 1$, and thus $\deg(y^k \cdot s) = \deg(x^k \cdot t)$. Hence, $(y/x)^k \cdot f$ is finite and non-zero at $\mathcal{O}$. Factorizing f as

$$f(x, y) = (x/y)^k \cdot \big((y/x)^k \cdot f(x, y)\big)$$

then yields the desired representation at the point at infinity.

It remains to show that the exponent k is unique, that is, independent of the choice of e. Suppose e and $\hat{e}$ were rational functions both satisfying the proposition at some point P. Then we have $e = \hat{e}^{\hat{k}} \cdot \hat{g}$ and $\hat{e} = e^k \cdot g$, and hence $e = e^{k\hat{k}} \cdot g^k \hat{g}$. If $k\hat{k} \neq 1$, then dividing by e and evaluating at P yields $1 = 0$. Therefore, we must have $k, \hat{k} = 1$ and

$$f = e^k \cdot g = \hat{e}^k \cdot \hat{g}$$

for any rational function f not identically zero. □

Definition 2.33. A rational function that satisfies Lemma 2.31 is called a *uniformizing variable* or a *uniformizer* at P.

Now we prove Theorem 2.29, which states that addition of rational maps on $E\big(\mathbb{F}(E)\big)$ harmonizes with function evaluation.

Proof. Let H_1 and H_2 be rational maps on the elliptic curve E. Then H_1 and H_2 are elements of the elliptic curve $E\big(\mathbb{F}(E)\big)$ and we want to show that

$$\text{if} \qquad H_1 + H_2 = K \qquad \text{then} \qquad H_1(P) + H_2(P) = K(P),$$

where P is any point on the curve E. The problem is that even with H_1 none of H_2, $-H_2$, or $\overline{\mathcal{O}}$, the point $H_1(P)$ may nevertheless equal $H_2(P)$, $-H_2(P)$, or $\mathcal{O}$. To verify the proposition, we compare the cases of Definition 1.6 for both additions on elliptic curves: $H_1 + H_2$ on $E\big(\mathbb{F}(E)\big)$, and $H_1(P) + H_2(P)$ on $E(\overline{\mathbb{F}})$.

The infinite cases on $E\big(\mathbb{F}(E)\big)$ are trivial. If H_1 or H_2 is the constant-$\mathcal{O}$ map $\overline{\mathcal{O}}$, then $H_1(P)$ or $H_2(P)$ is $\mathcal{O}$ and the equations turn into, for instance, $H_1 = K$ and $H_1(P) = K(P)$, which obviously holds. Likewise if $K = \overline{\mathcal{O}}$, then $H_1 = -H_2$ and thus $H_1(P) + H_2(P) = \mathcal{O}$; again the proposition is true. Therefore cases (iii) and (iv) of Definition 1.6 are already covered; we only have to distinguish the following combinations of $H_1 = (f_1, g_1)$ and $H_2 = (f_2, g_2)$:

(i) Generic addition: $f_1 \neq f_2$;

(ii) Point doubling: $f_1 = f_2$ and $g_1 = g_2 \neq 0$.

Unfortunately, more cases arise in the discussion of occurring values of H_1 and H_2 at a point P:

(a) Generic addition: $f_1(P) \neq f_2(P)$, and both are finite;

(b) Point doubling: $f_1(P) = f_2(P)$ and $g_1(P) = g_2(P) \neq 0$ where all values are finite;

(c) Adding inverses: $f_1(P) = f_2(P)$ and either $g_1(P) \neq g_2(P)$ or $g_1(P) = g_2(P) = 0$, again with finite values only;

(d) Adding one point at infinity: either $f_1(P)$ or $f_2(P)$ is infinite;

(e) Adding two points at infinity: both $f_1(P)$ and $f_2(P)$ are infinite.

Let us assume we are in case (i) and discuss all cases (a) to (e) of addition on E. Suppose thus that $f_1 \neq f_2$ and $H_1 + H_2 = K = (f_3, g_3)$, where

$$\begin{aligned} f_3 &= -f_1 - f_2 + \gamma^2, \\ g_3 &= -g_1 + \gamma(f_1 - f_3), \\ \gamma &= \frac{g_2 - g_1}{f_2 - f_1}. \end{aligned}$$

(a) If $f_1(P)$ and $f_2(P)$ are finite and unequal, then the addition on E—$H_1(P) + H_2(P) = K(P)$—uses the same formulas. Thus the results are identical and the proposition is true.

(b) Suppose we have finite values for $f_1(P)$, $f_2(P)$, and $g_1(P)$ with $f_1(P) = f_2(P)$ and $g_1(P) = g_2(P) \neq 0$. Then $H_1(P) + H_2(P)$ uses similar formulas to the ones above; only δ replaces γ. From $g_1(P) = g_2(P) \neq 0$, we see that $g_1 \neq -g_2$ and use this to expand γ as follows:

$$\begin{aligned} \gamma &= \frac{g_2 - g_1}{f_2 - f_1} \cdot \frac{g_2 + g_1}{g_2 + g_1} \\ &= \frac{(f_2^3 + Af_2 + B) - (f_1^3 + Af_1 + B)}{(f_2 - f_1)(g_2 + g_1)} \\ &= \frac{(f_2^3 - f_1^3) - A(f_2 - f_1)}{(f_2 - f_1)(g_2 + g_1)} \\ &= \frac{f_1^2 + f_1 f_2 + f_2^2 + A}{(g_2 + g_1)}. \end{aligned}$$

We assume $f_1(P) = f_2(P)$ and $g_1(P) = g_2(P) \neq 0$, so the rational function γ evaluates at P to the δ used in the addition on E:

$$\gamma(P) = \frac{3f_1(P)^3 + A}{2g_1(P)}.$$

(c) There are two variants of adding inverses: either $g_1(P) \neq g_2(P)$, or $g_1(P) = g_2(P) = 0$. Both times we have $f_1(P) = f_2(P)$.

First, consider what happens if $g_1(P) \neq g_2(P)$, which means $g_1(P) = -g_2(P)$. The original definition of γ clearly has a pole at P in this case, so $K(P) = \mathcal{O}$. Thus K behaves as desired since we assume $H_1(P)$ and $H_2(P)$ to be inverses.

Second, suppose $g_1(P) = g_2(P) = 0$. We see that the expansion of case (b) exposes the desired pole at P. However, we must make sure that $g_1 \neq -g_2$ in order to use it. The current outer case says $f_1 \neq f_2$, so the fundamental relation on $E\big(\mathbb{F}(E)\big)$ rules out $g_1 = -g_2 \neq 0$. Furthermore, if g_1 and g_2 were identically zero, then the relation would dictate that

$$f_1^3 + Af_1 + B = 0 = f_2^3 + Af_2 + B.$$

A rational function that is zero at the infinitely many points on $E(\overline{\mathbb{F}})$ must be the zero function. Therefore f_1 and f_2 would be constant and equal, a contradiction to $f_1 \neq f_2$. Hence we have $g_1 \neq -g_2$, may use the expansion of γ, and obtain $K(P) = \mathcal{O}$.

(d) Assume that $H_1 = \mathcal{O}$, so $f_1(P)$ and $g_1(P)$ have poles at P. To separate the pole causing factor in the denominators from the finite rest of f_1 and g_1, we use a uniformizing variable e at P:

$$f_1 = \frac{\hat{f}_1}{e^i} \qquad \text{and} \qquad g_1 = \frac{\hat{g}_1}{e^j}$$

where i, j are positive integers and $\hat{f}, \hat{g}$ are rational functions that are finite and non-zero at P. The fundamental relation links f_1 and g_1, so $g_1^2 = f_1^3 + Af_1 + B$ implies $3i = 2j$. Then

$$\frac{\hat{g}_1^2}{e^{2j}} = \frac{\hat{f}_1^3}{e^{3i}} + \frac{A\hat{f}_1}{e^i} + B,$$

or equivalently

$$\frac{\hat{g}_1^2}{\hat{f}_1^3} = 1 + \frac{A\hat{f}_1 e^{2i} + Be^{3i}}{\hat{f}_1^3}.$$

Therefore $\hat{f}_1^3(P) = \hat{g}_1^2(P)$ because e is a uniformizer and zero at P. Let us insert these results into the expression for f_3 and show that it equals

f_2 at P. We write

$$\begin{aligned} f_3 &= -(f_2+f_1) + \frac{(g_2-g_1)^2}{(f_2-f_1)^2} \\ &= \frac{-(f_2^3 - f_1^2 f_2 - f_1 f_2^2 + f_1^3) + (g_2^2 - 2g_1g_2 + g_1^2)}{(f_2-f_1)^2} \\ &= \frac{-f_2^3 + f_1^2 f_2 + f_1 f_2^2 - f_1^3 + f_1^3 + Af_1 + B - 2g_1g_2 + g_2^2}{(f_2-f_1)^2} \\ &= \frac{f_1^2 f_2 + (f_2^2 + A)f_1 + (g_2^2 - f_2^3 + B - 2g_1g_2)}{f_2^2 - 2f_1f_2 + f_1^2} \\ &= \frac{\hat{f}_1^2 e^{-2i} f_2 + (f_2^2 + A)\hat{f}_1 e^{-i} + (g_2^2 - f_2^3 + B - 2\hat{g}_1 e^{-j} g_2)}{f_2^2 - 2\hat{f}_1 e^{-i} f_2 + \hat{f}_1^2 e^{-2i}} \cdot \frac{e^{2i}}{e^{2i}} \\ &= \frac{\hat{f}_1^2 f_2 + h_1 e^i - 2\hat{g}_1 e^{2i-j} g_2}{\hat{f}_1^2 + h_2 e^i} \end{aligned}$$

where

$$h_1 = (f_2^2 + A)\hat{f}_1 + e^i(g_2^2 - f_2^3 + B),$$

and

$$h_2 = e^i f_2^2 - 2\hat{f}_1 f_2.$$

Observe that both h_1 and h_2 are finite at P, and that $3i = 2j$ implies $2i - j > 0$. The uniformizing variable e vanishes at P, so we obtain $f_3(P) = f_2(P)$—which is what we wanted because $H_1(P) + H_2(P) = H_2(P)$ when $H_1(P) = \mathcal{O}$.

Instead of using a similar construction to show $g_3(P) = g_2(P)$, we use associativity on $E\big(\mathbb{F}(E)\big)$: rewrite $H_1 + H_2 = K$ as $H_1 = K - H_2$ and evaluate at P. Above computation shows that $x\big(K(P)\big)$ is finite, so $K(P) \neq \mathcal{O}$. Thus $K(P)$ and $H_2(P)$ both are finite, and by one of the previous cases we know that $(K - H_2)(P) = K(P) - H_2(P) = H_1(P) = \mathcal{O}$. Therefore $H_2(P) = K(P)$ as desired. Symmetry makes a discussion of $H_2(P) = \mathcal{O}$ unnecessary.

(e) Suppose that both $f_1(P)$ and $f_2(P)$ are infinite, so $H_1(P) = \mathcal{O}$ and $H_2(P) = \mathcal{O}$. As in the second part of the previous case, we use associativity on the elliptic curve of rational maps $E\big(\mathbb{F}(E)\big)$ to show that $K(P) = \mathcal{O}$. We write $H_1 + H_2 = K$ as $(H_1 + H_2) - K = \overline{\mathcal{O}}$, which equals $H_1 + (H_2 - K) = \overline{\mathcal{O}}$ by associativity. At the point P we have $H_2(P) = \mathcal{O}$, so $H_2(P) - K(P) = -K(P)$ by the previous case. Similarly we get $H_1(P) + \big(H_2(P) - K(P)\big) = -K(P)$ and $K(P) = \mathcal{O}$ follows.

We completed the generic addition case (i); next is case (ii): point doubling on $E\big(\mathbb{F}(E)\big)$. Thus we assume $H_1 = (f_1, g_1) = (f_2, g_2) = H_2$ where $g_1 = g_2$ is

not identically zero. Put $H_1 + H_2 = (f_4, g_4)$ with

$$\begin{aligned} f_4 &= -2f_1 + \delta^2, \\ g_4 &= -g_1 + \delta(g_1 - g_4), \\ \delta &= \frac{3f_1^2 + A}{2g_1}. \end{aligned}$$

Little effort suffices to discuss the combinations of finite values for $H_1(P)$ and $H_2(P)$: case (a) cannot occur since $f_1 = f_2$; case (b) uses identical formulas so the proposition holds. In case (c), the first part $g_1(P) \neq g_2(P)$ is impossible, for $g_1 = g_2$. If $g_1(P) = g_2(P) = 0$, then $H_1(P) + H_2(P) = \mathcal{O}$. This matches our result of $H_1 + H_2$ because δ has a pole at P if $g_1(P) = 0$.

As for the infinite cases of $H_1(P)$ and $H_2(P)$, only case (e) remains because we assume $f_1 = f_2$, so either each or neither one has a pole. If we expand δ in the expression for f_4, we get

$$f_4 = -2f_1 + \Big(\frac{3f_1^2 + A}{2g_1}\Big)^2.$$

Suppose $H_1(P) = H_2(P) = \mathcal{O}$, so f_1 and g_1 have poles at P. Regardless of the growth of f_1 and g_1, f_4 also always has a pole at P: if g_1 dominates f_1^2 at P, or if they grow equally fast, then $\delta(P)$ is finite, so $-2f_1$ drives f_4 to infinity. If f_1^2 dominates g_1, then the term $3f_1^2$ from δ grows faster than $-f_1$; again we have a pole at P. This is the correct behavior because $H_1(P)+H_2(P) = \mathcal{O}+\mathcal{O} = \mathcal{O}$. □

Finally, we can show that multiplication with arbitrary integers is a rational map on E.

Theorem 2.34. *The component functions of $[\ell]$ are rational; for $\ell \in \mathbb{Z} \setminus \{0\}$ and $[\ell] = (f_\ell, g_\ell)$, we have $f_\ell, g_\ell \in \mathbb{F}(E)$. Furthermore, the poles of f_ℓ and g_ℓ are precisely the ℓ-torsion points $E[\ell]$, and $E[\ell]$ is finite for all ℓ.*

Proof. The idea is to write multiplication by an integer ℓ as sum of rational maps

$$[\ell] = [\ell - 1] + [1].$$

We then apply the previous Theorem 2.29 in an induction on positive ℓ; negative ℓ follow by $[\ell] = -[-\ell]$. The case $\ell = 0$ is excluded because $[0]$ is the constant-$\mathcal{O}$ map $\overline{\mathcal{O}}$, which is rational by definition only. Its component functions have infinitely many poles on $E(\overline{\mathbb{F}})$ and, thus, cannot be rational functions. For the same reason, we have to verify that $[\ell] \neq \overline{\mathcal{O}}$ in the inductive step.

We start the induction at $\ell = 1$. Then $[1] = (x, y)$ with rational functions x and y. Furthermore $E[1] = \{\mathcal{O}\}$ clearly is finite.

For the inductive step, we assume that $[m]$ is a rational map for $m < \ell$ and that $E[m]$ is finite. We have to exclude the case $[\ell] = \overline{\mathcal{O}}$; this case would mean $E[\ell] = E(\overline{\mathbb{F}})$, so if we can establish the finiteness of $E[\ell]$, then we know $[\ell] \neq \overline{\mathcal{O}}$.

Suppose $E[\ell] = E(\overline{\mathbb{F}})$ and $m > 1$ divides ℓ with $\ell/m = n$. Then $E[m]$ is a subgroup of $E[\ell] = E(\overline{\mathbb{F}})$ and for every point $P \in E[\ell]$ we have $n \cdot P \in E[m]$. The subgroup $E[m]$ is, however, finite by the inductive hypothesis, and for all

its points $Q \in E[m]$, only finitely many P exist with $n \cdot P = [n](P) = Q$. Otherwise, the rational map $[n] - Q$ would have an infinite number of poles, and thus $[n] - Q = \overline{\mathcal{O}}$. This is a contradiction to the inductive hypothesis, which tells us that $[n]$ is not the constant map Q. So if ℓ has non-trivial divisors, then $E[\ell]$ is finite.

Assume, thus, that ℓ is a prime. If we have $E[\ell] = E(\overline{\mathbb{F}})$, then $E[2]$ is a subgroup of $E[\ell]$. Therefore ℓ must be even; otherwise we would have $\ell \cdot P = (2m+1) \cdot P = P$ for all $P \in E[2] \subseteq E[\ell]$. Hence ℓ must be the single even prime 2—but we already know that $E[2]$ is finite from Example 2.4. In conclusion, $E[\ell] \neq E(\overline{\mathbb{F}})$, $[\ell] \neq \overline{\mathcal{O}}$, $[\ell]$ has rational components, and these possess only a finite number of poles. Therefore $E[\ell]$ is finite, which completes the inductive step and thereby the proof. □

2.2 Group Order

The previous section showed the finiteness of the ℓ-torsion group $E[\ell]$. As subgroup of an (abelian) elliptic curve $E(\overline{\mathbb{F}})$, it is also abelian. Hence, if we determine its order, then the fundamental theorem of finite abelian groups reveals its structure.

The ℓ-torsion points are precisely the poles of $[\ell]$, the multiplication by ℓ. In the present section we therefore count the poles of $[\ell]$ by exploiting its decomposition $[\ell] = [\ell - m] + [m]$. Observe that points in both $E[\ell - m]$ and $E[m]$ also lie in $E[\ell]$; points in just one of $E[\ell - m]$ or $E[m]$, however, lie outside $E[\ell]$. Thus, there is a connection between the poles of $[\ell - m]$, $[m]$ and $[\ell]$. If we gather enough information on the relation, we obtain a recurrence for the number of poles of $[\ell]$. The known cases [1] and [2] (compare Example 2.26) seed the recurrence.

Note that using a general decomposition of $[\ell]$ is essential. Fixed decompositions, for instance $[\ell] = [\ell - 1] + [1]$, will cause problems if the components are not prime to the field characteristic p: for example, if p divides $\ell - 1$, then

$$\ell \cdot P = (\ell - 1) \cdot P + P = 0 \cdot P + P = P,$$

and the dependency of poles becomes obscure.

2.2.1 Multiplicities of Zeros and Poles

Our plan involves counting the poles of $[\ell]$. If we ignore possible multiplicities in the process, our result would behave strangely; the polynomials x^3 and x, for instance, would be indistinguishable, both having a pole at $\mathcal{O}$. Clearly this is not what we want. Hence we begin by devising a way to count multiplicities of zeros and poles.

Recall that uniformizing variables encapsulate the interesting behavior of rational functions: by Lemma 2.31, we can split a rational function f into a product

$$f = e^k \cdot g,$$

where g is a rational function, finite and non-zero at P. Therefore the uniformizing variable e must drive f to zero or infinity at P. The exponent k is independent of the particular e; it describes *how* zero or infinite f is at P.

Definition 2.35. Let $e \in \mathbb{F}(E)$ be a uniformizing variable at the point $P \in E(\overline{\mathbb{F}})$. For a rational function f and $f = e^k \cdot g$, we define the order of f at P as

$$\mathrm{ord}_P(f) = k.$$

If f has a zero at P, the zero's multiplicity is the order k of f at P; if f has a pole at P, the pole's multiplicity is the negative $-k$ of the order of f at P.

Zeros of multiplicity one, two or three we call simple, double, or triple respectively.

Example 2.36. The polynomial $(x-\alpha)$ is a uniformizer at (α, β) and $(\alpha, -\beta)$. Thus, we have $(x-\alpha) = (x-\alpha)^1 \cdot 1$ and its order is 1 at both points. The points are obviously zeros, so $(x-\alpha)$ has single zeros at (α, β) and $(\alpha, -\beta)$. As a polynomial, $(x-\alpha)$ has a pole at $\mathcal{O}$; since $\deg(x-\alpha) = 2$, uniformizing at $\mathcal{O}$ yields

$$(x-\alpha) = \Big(\frac{x}{y}\Big)^{-2} \cdot \Big(\frac{x^2(x-\alpha)}{y^2}\Big),$$

so $\mathrm{ord}_{\mathcal{O}}(x-\alpha) = -2$ and the pole has multiplicity 2. At all other points, $(x-\alpha)$ already is finite and non-zero, so its order there is 0.

Using similar reasoning, we see that the defining polynomial of the curve,

$$x^3 + Ax + B = (x-\omega_1)(x-\omega_2)(x-\omega_3),$$

possesses three distinct double zeros at the points of order 2 because the curve is non-singular. It also has a pole of order 6 at $\mathcal{O}$.

A pattern hides in above example: zeros and poles of polynomials are balanced, counting multiplicities. The reason becomes evident if we look back at how we defined the value of rational functions at the point at infinity in Definition 2.23. A uniformizer at $\mathcal{O}$ must extract the highest power from a polynomial to split off a finite, non-zero part. Its exponent hence equals the degree of the polynomial, which is the number of roots over the algebraically closed field $\overline{\mathbb{F}}$; the number of roots, in turn, determines the number of points on the curve at which the polynomial vanishes. Consequently the degree tells us the total number of zeros.

Lemma 2.37. *For any polynomial s on E, the sum of the multiplicities of the zeros of s equals the degree of s:*

$$\sum_{\substack{P \in E, \\ s(P)=0}} \mathrm{ord}_P(s) = \deg(s).$$

Proof. We connect deg back to $\deg_1$, and then use our knowledge about univariate polynomials to relate the degree and the number of roots. Let $\deg(s) = k$ and

$s(x,y) = a(x) + y \cdot b(x)$ be the canonical form of s. For $\bar{s}(x,y) = a(x) - y \cdot b(x)$, observe that

$$\begin{aligned} s(x,y) \cdot \bar{s}(x,y) &= a(x)^2 - y^2 \cdot b(x)^2 \\ &= a(x)^2 - (x^3 + Ax + B) \cdot b(x)^2 \end{aligned}$$

and therefore

$$\begin{aligned} \deg(s) &= \max\bigl\{2\deg_1(a), 3 + 2\deg_1(b)\bigr\} \\ &= \deg_1(s \cdot \bar{s}); \end{aligned}$$

cancellation of the highest powers is impossible because the degrees are even and odd respectively.

Hence we have $\deg_1(s \cdot \bar{s}) = k$ and thus k roots for $s\bar{s} \in \mathbb{F}[x]$ in the algebraically closed field $\overline{\mathbb{F}}$. On the curve $E(\overline{\mathbb{F}})$, the number of zeros of $s\bar{s}$ is $2k$ because for $\alpha \in \overline{\mathbb{F}}$ a root and $(\alpha, \beta) \in E(\overline{\mathbb{F}})$ a zero of s or $\bar{s}$, $(\alpha, -\beta)$ is another zero if $\beta \neq 0$; and if $\beta = 0$, then $(\alpha, 0)$ is a zero of both s and $\bar{s}$. Therefore the number of zeros of $s\bar{s}$ on $E(\overline{\mathbb{F}})$ is $2k$.

To complete the proof, we show that s and $\bar{s}$ have the same number of zeros. For this, note that $s(\alpha, \beta) = 0$ implies one of two cases: either $a(\alpha) = 0$ and $b(\alpha) = 0$ or $\beta = 0$, and thus (α, β) is a zero of $\bar{s}$, too; or $a(\alpha) \neq 0$, thus $b(\alpha) \neq 0$ and $\beta \neq 0$, and therefore $\bar{s}(\alpha, -\beta) = 0$. Equality of the number of zeros follows from the symmetry of the argument because for every zero of $\bar{s}$, we find one for $\bar{\bar{s}} = s$.

Therefore, s must have k zeros on $E(\overline{\mathbb{F}})$, counting multiplicities. □

Corollary 2.38. *A rational function f on an elliptic curve E possesses an equal number of zeros and poles;*

$$\sum_{P \in E} \operatorname{ord}_P(f) = 0.$$

Proof. The result for rational functions follows immediately if we can show it for polynomials because s/t has a pole at a finite point P, if $t(P) = 0$. Furthermore a pole at the point at infinity is, by Definition 2.23, a direct consequence of a polynomial's pole there.

Above lemma states that for a polynomial s we have

$$\sum_{\substack{P \in E, \\ s(P) = 0}} \operatorname{ord}_P(s) = \deg(s).$$

As a polynomial, s can only have zeros at finite points, no poles. Furthermore the degree of s determines the behavior at the point at infinity, creating a pole of this order. In conclusion, we have

$$\sum_{P \in E \setminus \{\mathcal{O}\}} \operatorname{ord}_P(s) = \sum_{\substack{P \in E, \\ s(P) = 0}} \operatorname{ord}_P(s) = \deg(s) = -\operatorname{ord}_{\mathcal{O}}(s).$$

and hence, as proposed, the sum of orders at all points vanishes. □

2.2.2 Poles of Multiplication by Integers

One point is element of every ℓ-torsion group: the point at infinity $\mathcal{O}$. Hence it must be a pole of both component functions of multiplication $[\ell] = (f_\ell, g_\ell)$. As our first step to count the poles, we derive its multiplicity by uniformizing the functions there: we carefully increase the denominator degree in f_ℓ and g_ℓ until both yield finite, non-zero values at $\mathcal{O}$. The increase of degree equals the order of the function, which tells us the multiplicity of the pole.

Lemma 2.39. *Let $[\ell] = (f_\ell, g_\ell)$ and $\ell \in \mathbb{N}$ be prime to the field characteristic. Then*

$$\frac{f_\ell(x,y)}{x}(\mathcal{O}) = \frac{1}{\ell^2} \qquad \text{and} \qquad \frac{g_\ell(x,y)}{y}(\mathcal{O}) = \frac{1}{\ell^3}.$$

Proof. We show the proposition by an induction on ℓ; the cases $\ell = 1$ and $\ell = 2$ form our induction basis. Note that we need both cases because $[2] = [1] + [1]$ uses the doubling formula on the curve of rational maps. Therefore it does not follow from the inductive step, which uses the generic addition formula.

For $\ell = 1$, we have $f_1(x,y) = x$ and $g_1 = y$, so $f_1(x,y)/x$ and $g_1(x,y)/y$ are the constant-1 function; thus $\big(f_1(x,y)/x\big)(\mathcal{O}) = 1$ and $\big(g_1(x,y)/y\big)(\mathcal{O}) = 1$ as desired. For $\ell = 2$ recall the explicit expressions for f_2 and g_2 in Example 2.26. Dividing Equation 2.27 by x and Equation 2.28 by y yields

$$\begin{aligned}
\frac{f_2(x,y)}{x} &= \frac{x^4 - 2Ax^2 - 8Bx + A^2}{4x(x^3 + Ax + B)}, \\
\frac{g_2(x,y)}{y} &= y \cdot \frac{x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3}{8y \cdot (x^3 + Ax + B)^2}.
\end{aligned}$$

Both times the degrees of numerator and denominator agree. Hence we get $\big(f_2(x,y)/x\big)(\mathcal{O}) = 1/4$ and $\big(g_2(x,y)/y\big)(\mathcal{O}) = 1/8$ as desired.

Now suppose $(f_m(x,y)/x)(\mathcal{O}) = 1/m^2$ and $(g_m(x,y)/y)(\mathcal{O}) = 1/m^3$ for all $m \le \ell$, m prime to the field characteristic. Similarly to Theorem 2.34, we write

$$[\ell + 1] = [\ell] + [1]$$

if ℓ and $\ell + 1$ are prime to the field characteristic. By the generic addition formula on the curve of rational maps, we thus have

$$\begin{aligned}
\frac{f_{\ell+1}(x,y)}{x} &= -\frac{f_\ell(x,y)}{x} - 1 + \frac{1}{x} \cdot \Big(\frac{y - g_\ell(x,y)}{x - f_\ell(x,y)}\Big)^2 \\
&= -\frac{f_\ell(x,y)}{x} - 1 + \frac{1}{x} \cdot \Big(\frac{1 - g_\ell(x,y)/y}{1 - f_\ell(x,y)/x} \cdot \frac{y}{x}\Big)^2 \\
&= -\frac{f_\ell(x,y)}{x} - 1 + \frac{y^2}{x^3} \cdot \Big(\frac{1 - g_\ell(x,y)/y}{1 - f_\ell(x,y)/y}\Big)^2.
\end{aligned}$$

At the point at infinity, we have $(y^2/x^3)(\mathcal{O}) = 1$ by Definition 2.23. Together

with the inductive hypothesis, this yields

$$\begin{aligned}
\frac{f_{\ell+1}(x,y)}{x}(\mathcal{O}) &= -\ell^{-2} - 1 + \Big(\frac{1-\ell^{-3}}{1-\ell^{-2}}\Big)^2 \\
&= -(\ell^{-2}+1) + \Big(\frac{\ell^3-1}{\ell^3-\ell}\Big)^2 \\
&= -(\ell^{-2}+1) + \Big(\frac{(\ell-1)(\ell^2+\ell+1)}{\ell(\ell+1)(\ell-1)}\Big)^2 \\
&= \frac{-(\ell^{-2}+1)\ell^2(\ell+1)^2 + (\ell^2+\ell+1)^2}{\ell^2(\ell+1)^2} \\
&= \frac{-(1+\ell^2)(\ell+1)^2 + (1+\ell^2)(\ell+1)^2 + \ell^2}{\ell^2(\ell+1)^2} \\
&= \frac{1}{(\ell+1)^2}.
\end{aligned}$$

If $\ell+1$ is not prime to the field characteristic p, then p divides $\ell+1$ because p is a prime, so $\ell+1$ is zero in the field. Above computation fails in this case, for $\ell+1$ appears in the denominator. As a workaround, we skip the multiples of p in the induction by jumping to $\ell+2$ via $[\ell+2] = [\ell] + [2]$. Note that if p divides $\ell+1$, then both ℓ and $\ell+2$ are prime to p. The respective computations are

$$\begin{aligned}
\frac{f_{\ell+2}(x,y)}{x} &= -\frac{f_\ell(x,y)}{x} - \frac{f_2(x,y)}{x} + \frac{1}{x}\cdot\Big(\frac{g_2(x,y)-g_\ell(x,y)}{f_2(x,y)-f_\ell(x,y)}\Big)^2 \\
&= -\frac{f_\ell(x,y)}{x} - \frac{f_2(x,y)}{x} + \frac{y^2}{x^3}\cdot\Big(\frac{g_2(x,y)/y-g_\ell(x,y)/y}{f_2(x,y)/x-f_\ell(x,y)/x}\Big)^2;
\end{aligned}$$

furthermore

$$\begin{aligned}
\frac{f_{\ell+2}(x,y)}{x}(\mathcal{O}) &= -\frac{1}{\ell^2} - \frac{1}{4} + \Big(\frac{8^{-1}-\ell^{-3}}{4^{-1}-\ell^{-2}}\Big)^2 \\
&= -(\ell^{-2}+4^{-1}) + \Big(\frac{\ell^3-8}{2\ell^3-8\ell}\Big)^2 \\
&= -(\ell^{-2}+4^{-1}) + \Big(\frac{(\ell-2)(\ell^2+2\ell+4)}{2\ell(\ell-2)(\ell+2)}\Big)^2 \\
&= \frac{-(\ell^{-2}+4^{-1})4\ell^2(\ell+2)^2 + (\ell^2+2\ell+4)^2}{4\ell^2(\ell+2)^2} \\
&= \frac{-(4+\ell^2)(\ell+2)^2 + (4+\ell^2)(\ell+2)^2 + 4\ell^2}{4\ell^2(\ell+2)^2} \\
&= \frac{1}{(\ell+2)^2}.
\end{aligned}$$

The result for g_ℓ follows by analogous computations. □

As stated above, the lemma tells us the order of f_ℓ and g_ℓ: introducing x and y in the denominator balances the degrees inside f_ℓ and g_ℓ respectively. The uniformizer at $\mathcal{O}$ from the proof of Lemma 2.31 (iii) shifts the degree just by one; the absolute value of its exponent must therefore equal the degree of x

for f_ℓ and y for g_ℓ. To increase the denominator degree, the exponent must be negative. Thus we have the following corollary:

Corollary 2.40. *Let $[\ell] = (f_\ell, g_\ell)$ and $\ell \in \mathbb{N}$ be prime to the field characteristic. Then*

$$\operatorname{ord}_{\mathcal{O}}(f_\ell) = -2 \qquad \textit{and} \qquad \operatorname{ord}_{\mathcal{O}}(g_\ell) = -3.$$

Next we generalize this result and determine the multiplicities of all poles of $[\ell]$. The idea is to shift, or translate, other ℓ-torsion points onto $\mathcal{O}$.

Definition 2.41. *Translation* of a rational function f by a point P is the map $T_P : \mathbb{F}(E) \to \mathbb{F}(E)$,

$$\big(T_P(f)\big)(\cdot) = f(P + \cdot).$$

The ℓ-torsion points vanish under multiplication by ℓ. This implies that the components of $[\ell]$ are invariant under translations by $P \in E[\ell]$:

$$T_P(f_\ell)(Q) = f_\ell(P + Q) = f_\ell(Q)$$

for any point Q because $\ell \cdot (P + Q) = \ell \cdot Q$. Therefore we can shift the ℓ-torsion points onto $\mathcal{O}$. The translation influences uniformizing variables, and thus the function order, in an obvious way.

Lemma 2.42. *If e is a uniformizing variable at point P, then $T_Q(e)$ is a uniformizing variable at $P - Q$.*

Proof. Recall that, as a uniformizer, e has a zero at P. Then $T_Q(e)$ has a zero at $P - Q$, and its order k must be greater than zero: $\operatorname{ord}_{P-Q}\big(T_Q(e)\big) = k > 0$.

Now suppose that $T_Q(e)$ is not a uniformizer at $P - Q$ and thus has a decomposition $T_Q(e) = \hat{e}^k \cdot \hat{g}$ where $\hat{e}$ is a uniformizer at $P - Q$. Translation by Q then maps a rational function f of order j at P onto a function of order $j \cdot k$ at $P - Q$:

$$\begin{aligned} T_Q(f) &= T_Q(e)^j \cdot T_Q(g) \\ &= \big(\hat{e}^k \cdot \hat{g}\big)^j \cdot T_Q(g) \\ &= \hat{e}^{k \cdot j} \cdot \big(\hat{g}^j \cdot T_Q(g)\big). \end{aligned}$$

Conversely, T_{-Q} maps a function of order j at $P + Q$ onto a function of order j/k, which is absurd. Therefore, $T_Q(e)$ is a uniformizing variable at $P - Q$. □

In the proof we relied on the well-behavior and reversibility of translation. Therefore it remains to show that T_Q is an automorphism on $\mathbb{F}(E)$.

Lemma 2.43. *Translation by a point P, $T_P : \mathbb{F}(E) \to \mathbb{F}(E)$, is an automorphism of rational functions.*

Proof. First, note that T_P is well-defined: if $s/t = u/v$ are two representations of a rational function, then by Definition 2.14 $sv = ut$ and thus $T_P(sv) = T_P(ut)$. Multiplication of polynomial functions works point-wise, so

$$\begin{aligned} T_P(sv)(Q) &= (sv)(P+Q) \\ &= s(P+Q) \cdot v(P+Q) \\ &= \big(T_P(s) \cdot T_P(v)\big)(Q) \end{aligned}$$

for any point Q. Applied to $T_P(sv) = T_P(ut)$, we therefore have $T_P(s)T_P(v) = T_P(u)T_P(t)$ as required.

Like multiplication of functions, all field operations on $\mathbb{F}(E)$ are defined point-wise, which makes immediate why T_P is an endomorphism:

$$\begin{aligned} T_P(f+g)(Q) &= f(P+Q) + g(P+Q) = \big(T_P(f) + T_P(g)\big)(Q); \\ T_P(f \cdot g)(Q) &= f(P+Q) \cdot g(P+Q) = \big(T_P(f) \cdot T_P(g)\big)(Q). \end{aligned}$$

Finally, T_P is surjective because for any $f \in \mathbb{F}(E)$, the function $T_{-P}(f)$ is mapped to f. It is injective because

$$\begin{aligned} T_P(f) = T_P(g) \quad &\Leftrightarrow \quad f(P+Q) = g(P+Q) \quad \text{for all } Q \in E(\overline{\mathbb{F}}) \\ &\Leftrightarrow \quad f = g. \end{aligned}$$

□

In conclusion, all poles of $[\ell]$ have identical multiplicities in the component functions.

Corollary 2.44. *Let $[\ell] = (f_\ell, g_\ell)$ and $P \in E[\ell]$. Then*

$$\operatorname{ord}_P(f_\ell) = -2 \qquad \textit{and} \qquad \operatorname{ord}_P(g_\ell) = -3.$$

Proof. By Lemma 2.42 and Corollary 2.40 we have

$$\operatorname{ord}_P(f_\ell) = \operatorname{ord}_P\big(T_{-P}(f_\ell)\big) = \operatorname{ord}_{\mathcal{O}}(f_\ell) = -2,$$

and similarly

$$\operatorname{ord}_P(g_\ell) = \operatorname{ord}_{\mathcal{O}}(g_\ell) = -3.$$

□

2.2.3 Divisors

We know the multiplicities of the poles of component functions of multiplication; thus we know how often to count each pole. However, the number of different poles is yet to be found. Lacking explicit expressions for the components of $[\ell]$, we cannot approach the problem directly.

For a more indirect approach we concentrate on what we are interested in for now: not the specific component functions, but only their zeros and poles. Consequently we abstract away unnecessary details and introduce a device to track the zeros and poles of a rational function: at each point of an elliptic curve E, we record the function's order and thereby obtain a map $E \to \mathbb{Z}$ that characterizes the function.

Definition 2.45. For an elliptic curve E let $\mathrm{Div}(E)$ denote the set of maps $E \to \mathbb{Z}$ that assign a non-zero value to only finitely many points. Together with point-wise addition, $\mathrm{Div}(E)$ is the *group of divisors* of E.

We write $\langle P \rangle$ for the divisor that assigns 1 to a point P, and 0 to all other points.

With this notation, every divisor Δ has a representation as a linear combination

$$\sum_{P \in E} \Delta(P) \cdot \langle P \rangle.$$

Note that the sum means addition on $\mathrm{Div}(E)$, not on E. The nature of Δ ascertains that the sum is finite. Using linear combinations, the sum of divisors Δ_1, Δ_2 becomes

$$\sum_{P \in E} \Delta_1(P) \cdot \langle P \rangle + \sum_{P \in E} \Delta_2(P) \cdot \langle P \rangle = \sum_{P \in E} \big(\Delta_1(P) + \Delta_2(P)\big) \cdot \langle P \rangle.$$

Remark 2.46. Writing divisors as linear combinations brings them closer to their usual definition as elements of the free abelian group generated by the points on E. We use a different definition to emphasize the difference between P and $\langle P \rangle$, and their respective addition.

Next we associate divisors with rational functions to track the zeros and poles.

Definition 2.47. Let f be a rational function on E. The *divisor* of f is

$$\mathrm{div}(f) = \sum_{P \in E} \mathrm{ord}_P(f) \cdot \langle P \rangle.$$

Example 2.48. We know the zeros and poles of the defining polynomial from Example 2.36 on page 22. Its divisor therefore is

$$\mathrm{div}(x^3 + Ax + B) = 2\langle(\omega_1, 0)\rangle + 2\langle(\omega_2, 0)\rangle + 2\langle(\omega_3, 0)\rangle - 6\langle\mathcal{O}\rangle.$$

The result of Corollary 2.44 tells us something about the divisor of f_ℓ, where $[\ell] = (f_\ell, g_\ell)$:

$$\mathrm{div}(f_\ell) = \sum_{\substack{P \in E, \\ f_\ell(P) = 0}} \mathrm{ord}_P(f_\ell) \cdot \langle P \rangle - 2\langle E[\ell] \rangle.$$

We plan to count the different poles of multiplication by ℓ by relating the poles of $[\ell]$ to those of $[m]$ and $[\ell - m]$, $m < \ell$, thereby obtaining a recurrence. Translated to divisors, we are looking for a connection between $\mathrm{div}(f_\ell), \mathrm{div}(f_m)$, and $\mathrm{div}(f_{\ell-m})$. Discussing only the first component function suffices: by the fundamental relation for coordinates of rational maps, g_ℓ has a pole at a point if, and only if, f_ℓ has a pole there.

2.2.4 Derivation on Elliptic Curves

The second part of Example 2.48 hinted that in order to obtain a meaningful relation between the divisors of multiplication by different integers, we have to also know the multiplicities of the zeros. To count these, we transfer a well-established tool from regular polynomials to those over elliptic curves: the algebraic derivative. We can then deduce the multiplicity of a zero by checking whether the derivatives, too, have a zero.

As with the degree, we have to respect the fundamental relation: the derivative of the polynomial $y^2 - x^3 - Ax - B$ must be zero. Differentiating the fundamental relation yields

$$2y\mathrm{D}y = (3x^2 + A)\mathrm{D}x,$$

which motivates the following definition.

Definition 2.49. Let E be an elliptic curve over $\mathbb{F}$ with parameters A and B. We define a derivation D on the field of rational functions $\mathbb{F}(E) = \mathbb{F}(x, y)$ by setting

$$\mathrm{D}x = 2y \qquad \text{and} \qquad \mathrm{D}y = 3x^2 + A;$$

we extend D to arbitrary functions via

$$\begin{aligned} \mathrm{D}\alpha &= 0, & \mathrm{D}(\alpha f + \beta g) &= \alpha \mathrm{D}f + \beta \mathrm{D}g, \\ \mathrm{D}(fg) &= g\mathrm{D}f + f\mathrm{D}g, & \mathrm{D}(f \circ g) &= \big((\mathrm{D}f) \circ g\big) \cdot \mathrm{D}g, \\ \mathrm{D}(f/g) &= (g\mathrm{D}f - f\mathrm{D}g)/g^2. \end{aligned}$$

Lemma 2.50. *The derivation* D *is well-defined.*

Proof. The derivative of the fundamental relation vanishes by construction:

$$\begin{aligned} \mathrm{D}(y^2 - x^3 - Ax - B) &= \mathrm{D}y^2 - \mathrm{D}(x^3 - Ax - B) \\ &= 2y \cdot \mathrm{D}y - 3x^2 \cdot \mathrm{D}x - A \cdot \mathrm{D}x \\ &= 2y \cdot (3x^2 + A) - 3x^2 \cdot 2y - A \cdot 2y \\ &= 0. \end{aligned}$$

Hence equivalent polynomials on the curve have the same derivative.

Let s/t and u/v be two representations of a rational function $f \in \mathbb{F}(E)$, so s, t, u, and v are polynomials. By Definition 2.14, we know that $sv = ut$. Therefore $\mathrm{D}(sv) = \mathrm{D}(ut)$; furthermore the derivation rules tell us $\mathrm{D}(sv) = v\mathrm{D}s + s\mathrm{D}v$ and $\mathrm{D}(ut) = t\mathrm{D}u + u\mathrm{D}t$.

Using these identities, we write

$$\begin{aligned}
\mathrm{D}(s/t) &= \frac{t\mathrm{D}s - s\mathrm{D}t}{t^2} \\
&= \frac{tv\mathrm{D}s - sv\mathrm{D}t}{vt^2} \\
&= \frac{v\mathrm{D}s - u\mathrm{D}t}{vt} \\
&= \frac{\mathrm{D}(sv) - s\mathrm{D}v - \mathrm{D}(ut) + t\mathrm{D}u}{vt} \\
&= \frac{vt\mathrm{D}u - sv\mathrm{D}v}{vt} \\
&= \frac{v\mathrm{D}u - u\mathrm{D}v}{v^2} \\
&= \mathrm{D}(u/v).
\end{aligned}$$

Thus, the derivation of rational functions is independent of the representative. □

We want to use derivation to count multiplicities of zeros. Hence we are interested in the effect on the order of a rational function. The following lemma establishes that differentiating a function reduces its order as expected.

Lemma 2.51. *Let f be a rational function. If, for a point P, $\mathrm{ord}_P(f) = k \neq 0$ is prime to the field characteristic, then $\mathrm{ord}_P(\mathrm{D}f) = k - 1$.*

Proof. Decompose the rational function into $f = e^k \cdot g$ where e is a uniformizing variable at P and $g(P)$ is finite and non-zero. Differentiating f then yields

$$\mathrm{D}f = \mathrm{D}(e^k \cdot g) = g \cdot ke^{k-1}\mathrm{D}e + e^k\mathrm{D}g.$$

We have to show that both derivatives, $\mathrm{D}e$ and $\mathrm{D}g$, are finite and that $\mathrm{D}e$ is also non-zero at P. This yields the desired decomposition $\mathrm{D}f = e^{k-1} \cdot \hat{g}$ with $\hat{g} = kg\mathrm{D}e$ finite and non-zero; $e^k\mathrm{D}g$ vanishes because the uniformizer e has a zero at P.

First, we examine $\mathrm{D}g$. By choice, g is finite at P, which has two interpretations depending on P. If P is a finite point, then $g = s/t$ has no pole at P. Thus $t(P) \neq 0$ and $\mathrm{D}g = (t\mathrm{D}s - s\mathrm{D}t)/t^2$, too, is finite at P.

On the other hand, a finite value at $\mathcal{O}$ means $\deg(s) \leq \deg(t)$ for $g = s/t$. In the case $\deg(s) < \deg(t)$, clearly the degree of $t\mathrm{D}s - s\mathrm{D}t$ is less than or equal to the degree of t^2. But g is finite at P, so we are in the case $\deg(s) = \deg(t)$ and simply comparing degrees only yields $\deg(t\mathrm{D}s - s\mathrm{D}t) - 1 = \deg(t^2)$. However, closer examination shows that the leading terms of the polynomials $t\mathrm{D}s$ and $s\mathrm{D}t$ are equal, so subtraction cancels them. Therefore we again have identical degrees, and $\mathrm{D}g$ is finite at $\mathcal{O}$.

Next we verify that $\mathrm{D}e$ is finite and non-zero at P. Since the choice of the uniformizing variable e is ours, we may use the representation from the proof of Lemma 2.31. There are three cases.

(i) Suppose P is finite and not of order 2. Then $e(x,y) = x - x(P)$ is a valid uniformizer, so $\mathrm{D}e = 2y$, which is finite and non-zero at such P.

(ii) If P is a point of order 2, we use $e(x,y) = y$ as uniformizer. Then $\mathrm{D}e = 3x^2 + A$, which is precisely the derivative of the curve's defining polynomial $x^3 + Ax + B$. The curve being non-singular, its defining polynomial has three distinct zeros and therefore the derivative must be non-zero at any of these zeros. But one of these zeros is $x(P)$ because P is of order 2.

(iii) Finally, let $P = \mathcal{O}$ and thus $e(x,y) = x/y$. Then we have

$$\begin{aligned}\mathrm{D}e(x,y) &= \frac{2y^2 - 3x^3 - Ax}{y^2} \\ &= \frac{2y^2 - 3(x^3 + A + B) + 2Ax + 3B}{y^2} \\ &= \frac{-y^2 + 2Ax + 3B}{y^2},\end{aligned}$$

which is -1 at $\mathcal{O}$. □

We can even find explicit expressions for the derivatives of multiplication by an integer.

Lemma 2.52. *The derivatives of the components of* $[\ell] = (f_\ell, g_\ell)$ *are*

$$\mathrm{D}f_\ell = 2\ell \cdot g_\ell \qquad \textit{and} \qquad \mathrm{D}g_\ell = \ell \cdot (3f_\ell^2 + A).$$

Proof. Observe that showing $\mathrm{D}f_\ell = 2\ell \cdot g_\ell$ suffices; $\mathrm{D}g_\ell = \ell \cdot (3f_\ell^2 + A)$ follows from the fundamental relation between f_ℓ and g_ℓ: from $g_\ell^2 = f_\ell^3 + Af_\ell + B$ we get

$$2g_\ell \cdot \mathrm{D}g_\ell = \mathrm{D}f_\ell \cdot (3f_\ell^2 + A) = 2\ell \cdot g_\ell(3f_\ell^2 + A),$$

which implies that $\mathrm{D}g_\ell$ has the proposed form.

To show the proposition for $\mathrm{D}f_\ell$, we once more use induction on ℓ. Definition 2.49 of derivation on E provides the first base case $\ell = 1$: $[1] = (x,y)$, so $\mathrm{D}f_1(x,y) = \mathrm{D}x = 2y = 2g_1(x,y)$. The second base case is $\ell = 2$; we show it by differentiating the expression for f_2 from Equation 2.27

$$f_2(x,y) = \frac{x^4 - 2Ax^2 - 8Bx + A^2}{4(x^3 + Ax + B)}.$$

We have

$$\begin{aligned}&(x^3 + Ax + B)\cdot \\ \mathrm{D}(x^4 - 2Ax^2 - 8Bx + A^2) &= (x^3 + Ax + B) \cdot 2y(4x^3 - 4Ax - 8B) \\ &= 2y(4x^6 - 4Bx^3 - 4A^2x^2 - 12ABx - 8B^2), \\ &(x^4 - 2Ax^2 - 8Bx + A^2)\cdot \\ \mathrm{D}(x^3 + Ax + B) &= (x^4 - 2Ax^2 - 8Bx + A^2) \cdot 2y(3x^2 + A) \\ &= 2y(3x^6 - 5Ax^4 - 24Bx^3 - A^2x^2 - 8ABx + A^3);\end{aligned}$$

thus

$$\begin{aligned}\mathrm{D}f_2(x,y) &= 4 \cdot \frac{2y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 + 4ABx - 8B^2 - A^3)}{16(x^3 + Ax + B)^2} \\ &= 4 \cdot g_2(x,y)\end{aligned}$$

as required.

For the inductive step we decompose multiplication by ℓ into $[\ell] = [\ell-1]+[1]$. From the generic addition formula on the curve of rational maps we obtain

$$f_\ell(x,y) = -f_{\ell-1} - x + \Big(\frac{y - g_{\ell-1}}{x - f_{\ell-1}}\Big)^2, \tag{2.53}$$

$$g_\ell(x,y) = -y - \Big(\frac{y - g_{\ell-1}}{x - f_{\ell-1}}\Big)(f_\ell - x), \tag{2.54}$$

where f_m and g_m denote $f_m(x,y)$ and $g_m(x,y)$ for brevity. Furthermore we have the inductive hypothesis and the fundamental relation:

$$\mathrm{D}g_{\ell-1} = (\ell-1)(3f_{\ell-1}^2 + A), \tag{2.55}$$

$$g_{\ell-1}^2 = f_{\ell-1}^3 + Af_{\ell-1} + B. \tag{2.56}$$

Differentiating Equation 2.53 yields

$$\begin{aligned}\mathrm{D}f_\ell(x,y) = -\mathrm{D}f_{\ell-1} - 2y + 2\Big(\frac{y - g_{\ell-1}}{x - f_{\ell-1}}\Big)\cdot \\ \Big(\frac{(x - f_{\ell-1})(\mathrm{D}y - \mathrm{D}g_{\ell-1}) - (y - g_{\ell-1})(\mathrm{D}x - \mathrm{D}f_{\ell-1})}{(x - f_{\ell-1})^2}\Big)^2;\end{aligned}$$

applying the inductive hypothesis (2.55), we get an expression in powers of $f_{\ell-1}$ and $g_{\ell-1}$. The proposition then follows after reducing even powers of $g_{\ell-1}$ with the fundamental relation (2.56), multiplying and collecting terms, and finally comparing the result with 2ℓ times Equation 2.54. The computation, however, is long and offers no insights; thus we leave it for a rainy morning. □

2.2.5 Order Recurrence

Finally we can express how alternating ℓ influences the divisors of the component functions of the multiplication-by-ℓ map $[\ell]$.

Theorem 2.57. *Let $[n] = (f_n, g_n)$ denote multiplication by n. Furthermore, let $m > \ell > 0$ be integers such that m, ℓ, $m-\ell$, and $m+\ell$ are all prime to the field characteristic p. The divisor of $f_m - f_\ell$ then is*

$$\mathrm{div}(f_m - f_\ell) = \langle E[m+\ell]\rangle + \langle E[m-\ell]\rangle - 2\langle E[m]\rangle - 2\langle E[\ell]\rangle,$$

where $\langle E[n]\rangle$ denotes the divisor that assigns 1 precisely to the points in $E[n]$.

Proof. Recall that the divisor of a rational function assigns to each point P the order of the function at P. To show the theorem, we thus have to determine the order of $f_m - f_\ell$ at its zeros and poles. All relevant points lie in $E[m]$, $E[\ell]$,

$E[m+\ell]$, and $E[m-\ell]$, so discussing these cases suffices: the point at infinity is in any of these sets; finite points P must be zeros or poles to have a non-zero order. Hence they either fulfill

$$\begin{aligned} f_m(P) - f_\ell(P) = 0 \quad &\Leftrightarrow \quad f_m(P) = f_\ell(P) \\ &\Leftrightarrow \quad m \cdot P = \pm\ell \cdot P \\ &\Leftrightarrow \quad P \in E[m \pm \ell], \end{aligned} \tag{2.58}$$

or $f_m(P) - f_\ell(P)$ has to be infinite, which is possible only at m- or ℓ-torsion points.

Consider the cases of membership of points in the various torsion groups:

(i) Suppose a point lies in both, $E[m]$ and $E[\ell]$. Then it is also in $E[m+\ell]$ and $E[m-\ell]$. According to the proposition, the order of $f_m - f_\ell$ at this point must equal $1+1-2-2=-2$.

The point at infinity is such a point in both torsion groups; by Corollary 2.40, f_m and f_ℓ have poles of multiplicity two there. These poles cannot cancel out because the coefficient of the highest powers are $1/m^2$ and $1/\ell^2$, and by our hypothesis $(m+\ell)(m-\ell) \not\equiv 0$ modulo p and thus $m^2 \not\equiv \ell^2$. Consequently $f_m - f_\ell$ has a pole of multiplicity two at $\mathcal{O}$.

Using translation, we then determine the order at all other points $P \in E[m] \cap E[\ell]$. The functions f_m and f_ℓ are invariant under translation by $-P$; thus we can shift $f_m - f_\ell$ by $-P$ and, by Corollary 2.40, have

$$\operatorname{ord}_P(f_m - f_\ell) = \operatorname{ord}_{\mathcal{O}}\big(T_{-P}(f_m - f_\ell)\big) = \operatorname{ord}_{\mathcal{O}}(f_m - f_\ell) = -2.$$

(ii) Next we consider points in $E[m]$, but not in $E[\ell]$. These lie neither in $E[m+\ell]$ nor in $E[m-\ell]$, so we must show that the order of $f_m - f_\ell$ there is -2. By assumption, these points are not poles of f_ℓ. Therefore, $f_m - f_\ell$ inherits the pole of f_m, which we, analogously to the previous case, shift onto $\mathcal{O}$ to see that it has multiplicity two.

(iii) Symmetry to case (ii) implies the proposition for points in $E[\ell]$ but not in $E[m]$.

(iv) Finally we examine the points in $E[m+\ell]$ or $E[m-\ell]$, but neither in $E[m]$ nor $E[\ell]$. As before, we distinguish three sub-cases: points lying in exactly one of $E[m+\ell]$ or $E[m-\ell]$, and points from the intersection. Equation 2.58 immediately shows that $f_m - f_\ell$ is zero at these points; the problem is to determine the multiplicity.

Consider the derivative

$$\mathrm{D}(f_m - f_\ell) = 2m \cdot g_m - 2\ell \cdot g_\ell.$$

If $P \in E[m-\ell] \setminus E[m+\ell]$ we must have

$$\mathcal{O} \neq m \cdot P = \ell \cdot P \neq -\ell \cdot P$$

and therefore $g_m(P) = g_\ell(P)$, so $\mathrm{D}(f_m - f_\ell) = 2(m-\ell)f_m(P)$. This is non-zero because $m - \ell$ is prime to p, and $g_\ell(P) \neq 0$ for $\ell \cdot P \neq -\ell \cdot P$ means that P is not of order 2. By Lemma 2.51, the non-zero derivative at P implies that $f_m - f_\ell$ has a simple zero at P as required. The sub-case $P \in E[m+\ell] \setminus E[m-\ell]$ is symmetric.

Suppose for the final sub-case that $P \in E[m+\ell] \cap E[m-\ell]$. Thus we have $(m+\ell)\cdot P = \mathcal{O}$ and $(m-\ell)\cdot P = \mathcal{O}$, and hence

$$m \cdot P = \ell \cdot P \neq \mathcal{O} \qquad \text{and} \qquad m \cdot P = -\ell \cdot P \neq \mathcal{O}.$$

Equivalently we have $2 \cdot (m \cdot P) = \mathcal{O}$ and $2 \cdot (\ell \cdot P) = \mathcal{O}$; points of order 2 have a zero second component and therefore $g_m(P) = g_\ell(P) = 0$. The zero at P consequently has multiplicity at least two.

Differentiating once more yields, by Lemma 2.52,

$$\begin{aligned}\mathrm{DD}(f_m - f_\ell) &= 2m^2(3f_m^2 + A) - 2\ell^2(3f_\ell^2 + A) \\ &= 2(m^2 - \ell^2)(3f_m^2 + A)\end{aligned}$$

by the equalities assumed in this sub-case. This expression is non-zero: $m \cdot P = \big(f_m(P), g_m(P)\big) = (\omega, 0)$ is a point of order 2. Therefore $f_m(P) \neq 0$ because otherwise ω would be a double root of the curve's defining polynomial—observe that $3x^2 + A$ is precisely its first derivative. Furthermore, $m^2 \not\equiv \ell^2$ modulo p by hypothesis and P is a zero of order 2 as desired. □

Above theorem links the poles and zeros of multiplication by different integers; in particular it links their numbers. By exploiting this link, we prove the main theorem of this section.

Theorem 2.59. *If ℓ is prime to the field characteristic, then the ℓ-torsion group has order ℓ^2:*

$$|E[\ell]| = \ell^2.$$

Proof. We construct a recurrence relation for the number of ℓ-torsion points, give a solution, and show that the solution is unique.

Consider the divisor of $f_m - f_\ell$, which by Theorem 2.57 is

$$\mathrm{div}(f_m - f_\ell) = \langle E[m+\ell]\rangle + \langle E[m-\ell]\rangle - 2\langle E[m]\rangle - 2\langle E[\ell]\rangle.$$

As divisor of a rational function, summing the order over all points yields zero. Furthermore we defined the divisors $\langle E[n]\rangle$ to be 1 precisely at the points in $E[n]$. Thus we obtain the recurrence

$$0 = |E[m+\ell]| + |E[m-\ell]| - 2\,|E[m]| - 2\,|E[\ell]|\,; \tag{2.60}$$

seed values are $|E[1]| = 1$ and $|E[2]| = 4$.

Clearly $|E[n]| = n^2$ satisfies the recurrence. We show the uniqueness by establishing that the difference k_n between solutions for $|E[n]|$ is zero for all

n prime to p. Obviously k_n must, too, satisfy the recurrence; its seed values are $k_1 = 0$ and $k_2 = 0$.

Let n be prime to p and assume that $k_i = 0$ for all $i < n$ prime to p. By examining the recurrence relation (2.60) for decompositions $n = m + \ell$, we show how to solve the appearing cases. These are

$$\begin{aligned} m = n-1, \ell = 1 \quad &\Rightarrow \quad 0 = k_n + k_{n-2} - 2 \cdot k_{n-1} - 2 \cdot 0 \\ &\Leftrightarrow \quad k_n = 2k_{n-1} - k_{n-2} \\ m = n-2, \ell = 2 \quad &\Rightarrow \quad k_n = 2k_{n-2} - k_{n-4} \\ m = n-3, \ell = 3 \quad &\Rightarrow \quad k_n = 2k_{n-3} - k_{n-6} \end{aligned}$$

Hence, if $n-1$ and $n-2$ are prime to p, the hypothesis says $k_{n-1} = k_{n-2} = 0$; the first decomposition then yields $k_n = 0$. Similarly, the second and third decomposition imply $k_n = 0$ if $n-2$ and $n-4$, or $n-3$ and $n-6$ respectively are prime to p.

To complete the proof, we handle the remaining cases.

(i) Suppose $n-1$ is not prime to p. Then $n-2$ must be prime to p, and if $n-4$ were not prime to p, then we would have field characteristic $p = 3$, contrary to our assumption. Therefore we can use the second decomposition to get $k_n = 0$.

(ii) Assume that $n-2$ is not prime to p. Then $n-3$ must be prime to p; now in case we had $n-6$ not prime to p, 4 would be a multiple of p, which is impossible.

In conclusion, we can always find a decomposition to ascertain $k_n = 0$ for n prime to p. □

2.3 Module Structure

We have seen that the ℓ-torsion group is a finite abelian group of order $|E[\ell]| = \ell^2$ if ℓ is prime to the field characteristic. Thus we may apply the structure theorem of finite abelian groups to learn the inner composition of $E[\ell]$.

Theorem 2.61. *If ℓ is prime to the field characteristic, then $E[\ell]$ is isomorphic to $\mathbb{Z}_\ell \times \mathbb{Z}_\ell$. In symbols:*

$$E[\ell] \simeq \mathbb{Z}_\ell \times \mathbb{Z}_\ell.$$

Proof. The group $E[\ell]$ is abelian and has finite order ℓ^2. By the structure theorem for finite abelian groups, $E[\ell]$ thus is isomorphic to a direct product of cyclic groups $(\mathbb{Z}_{\ell_i}, +)$,

$$E[\ell] \simeq \mathbb{Z}_{\ell_1} \times \cdots \times \mathbb{Z}_{\ell_k},$$

with ℓ_i dividing ℓ_{i+1} for all $i = 1, \ldots, k-1$; see, for example, the book of Robinson [25, (9.3.1)]. The orders ℓ_i are uniquely determined by the structure of $E[\ell]$.

Let m be a prime dividing ℓ_1. Then m divides ℓ, so $\ell \cdot P = \mathcal{O}$ for all m-torsion points P, and thus $E[m]$ is a subgroup of $E[\ell]$. Furthermore the choice

of the ℓ_i implies that m divides the order ℓ_i of every $\mathbb{Z}_{\ell_i}$. Therefore each cyclic group $\mathbb{Z}_{\ell_i}$ has a subgroup of order m, and multiplication by m annihilates all subgroup elements. Consequently, the number of m-torsion points is m^k, which tells us $k = 2$ by Theorem 2.59:

$$E[l] \simeq \mathbb{Z}_{\ell_1} \times \mathbb{Z}_{\ell_2}.$$

Multiplication by ℓ annihilates all elements of $\mathbb{Z}_{\ell_1}$ and $\mathbb{Z}_{\ell_2}$, so ℓ_1 and ℓ_2 divide ℓ; from $|E[\ell]| = \ell^2 = \ell_1 \cdot \ell_2$ then follows $\ell_1, \ell_2 = \ell$, for otherwise we would have $\ell_1 \cdot \ell_2 < \ell^2$. In conclusion

$$E[\ell] \simeq \mathbb{Z}_\ell \times \mathbb{Z}_\ell$$

as proposed. □

The isomorphism deepens our understanding of $E[\ell]$ because we know $\mathbb{Z}_\ell \times \mathbb{Z}_\ell$ well. In particular, we may regard $\mathbb{Z}_\ell \times \mathbb{Z}_\ell$ as a free module of rank 2, which adds linear algebra to our tool set for examining the ℓ-torsion points.

Yet, the theorem does not provide an exact correspondence between ℓ-torsion points and vectors in $\mathbb{Z}_\ell \times \mathbb{Z}_\ell$. Rather, it tells us that there exist linearly independent points $P, Q \in E[\ell]$, such that for all $m \in \mathbb{Z}$

$$m \cdot P \neq Q.$$

From these points we may construct a basis of $\mathbb{Z}_\ell \times \mathbb{Z}_\ell$ by assigning to them the vectors $(1, 0)^T$ and $(0, 1)^T$. Thereby we obtain vector representations for all points in $E[\ell]$, and matrix representations for endomorphisms of $E[\ell]$.

In the discussion of the following chapters, however, choosing a particular basis is not necessary and we will be satisfied with the general correspondences that hold for any isomorphism: the point at infinity $\mathcal{O}$ is the zero vector $(0, 0)^T$, and multiplication of points by integers is scalar multiplication of vectors in the module.

Chapter 3

Division Polynomials

The previous chapter ended with a result about the structure of most ℓ-torsion groups $E[\ell]$ of an elliptic curve E: $E[\ell]$ is isomorphic to $\mathbb{Z}_\ell \times \mathbb{Z}_\ell$. We derived this while carefully avoiding to use actual finite points from $E[\ell]$, other than the special cases of the point at infinity and the points of order 2. However, our goal is to count the points of concrete elliptic curves. If we want to computationally verify properties implied by interpreting $E[\ell]$ as a module, then we need a way to compute with ℓ-torsion points.

Considering that the coordinates of ℓ-torsion points come from an algebraically closed field, explicit representations for them might clash with the finiteness of computers. Thus we are looking for an implicit representation like the polynomial that characterized the 3-torsion points in Example 2.6. There, we derived the polynomial from the addition and negation formulas. In the general case, however, this approach is intractable: too many cases offer little chance to unify the expressions. In the present chapter we therefore take another approach and recursively construct polynomials whose zeros encode the ℓ-torsion points.

3.1 Polynomials with Zeros at Torsion Points

Suppose ℓ is prime to the field characteristic. We know that the component functions of multiplication by ℓ are rational, each having ℓ^2 poles. Finite poles originate from zeros in the denominator polynomial. Thus we are looking for a polynomial s that has zeros at all finite ℓ-torsion points. To have minimal degree, we want single zeros; in accordance with Corollary 2.38, we must balance them with a pole of respective multiplicity at $\mathcal{O}$. Single zeros at the $\ell^2 - 1$ finite ℓ-torsion points mean, in divisor notation, the polynomial s should have the divisor

$$\operatorname{div}(s) = \langle E[\ell] \setminus \{\mathcal{O}\}\rangle - (\ell^2 - 1)\langle\mathcal{O}\rangle = \langle E[\ell]\rangle - \ell^2\langle\mathcal{O}\rangle.$$

To construct s, we employ the same technique as with polynomials in one indeterminate: we simply use a product of polynomials, each having desired zeros. The divisor then adds up.

Lemma 3.1. *The divisor of a product of rational functions is the sum of the individual divisors. Let f, g be rational functions on E, then*

$$\operatorname{div}(f \cdot g) = \operatorname{div}(f) + \operatorname{div}(g).$$

Proof. At any point P, decompose the functions with a uniformizing variable e at P: $f = e^{\mathrm{ord}_P(f)} \cdot \hat{f}$ and $g = e^{\mathrm{ord}_P(g)} \cdot \hat{g}$. Then

$$f \cdot g = e^{\mathrm{ord}_P(f)+\mathrm{ord}_P(g)} \cdot \hat{f}\hat{g}$$

and therefore $\mathrm{ord}_P(f \cdot g) = \mathrm{ord}_P(f) + \mathrm{ord}_P(g)$. Applying the Definition 2.47 of divisors of rational functions, we get

$$\begin{aligned}\mathrm{div}(f \cdot g) &= \sum_{P \in E} \mathrm{ord}_P(f \cdot g)\langle P\rangle \\ &= \sum_{P \in E} \big(\mathrm{ord}_P(f) + \mathrm{ord}_P(g)\big)\langle P\rangle \\ &= \mathrm{div}(f) + \mathrm{div}(g).\end{aligned}$$

□

However, things are not that simple. For instance, the polynomial $(x - \alpha)$, $\alpha \in \mathbb{F}$, has degree 2 and therefore two zeros, counting multiplicities; see Example 2.36. Nevertheless, things turn out nicely because we chose no arbitrary set of zeros, but one with structure: the group $E[\ell]$.

Lemma 3.2. *Let E be an elliptic curve over a field $\mathbb{F}$, and ℓ be prime to the field characteristic. Then there exists a polynomial s on E with divisor*

$$\mathrm{div}(s) = \langle E[\ell]\rangle - \ell^2\langle\mathcal{O}\rangle.$$

Proof. Let $L = E[\ell] \setminus \{\mathcal{O}\}$ denote the finite ℓ-torsion points. Consider the polynomial defined by the finite product

$$\prod_{(\alpha,\beta)\in L} (x - \alpha). \tag{3.3}$$

It consists of $\ell^2 - 1$ factors and has its zeros at all finite ℓ-torsion points; their multiplicities however are too big.

(i) If $(\alpha, \beta) \in E[\ell] \setminus \{\mathcal{O}\}$ is not of order 2, then the polynomial $(x - \alpha)$ has zeros at both (α, β) and $(\alpha, -\beta)$. Its divisor is therefore $\mathrm{div}(x - \alpha) = \langle(\alpha, \beta)\rangle + \langle(\alpha, -\beta)\rangle - 2\langle\mathcal{O}\rangle$. The ℓ-torsion points $E[\ell]$ form a group and therefore both (α, β) and $(\alpha, -\beta)$ appear in the product (3.3). The factor $(x - \alpha)$ thus appears squared.

(ii) For $(\omega, 0) \in E[\ell] \setminus \{\mathcal{O}\}$ of order 2, we have $\mathrm{div}(x - \omega) = 2\langle(\omega, 0)\rangle - 2\langle\mathcal{O}\rangle$ and the factor appears once in product (3.3).

The discussion implies that

$$\begin{aligned}\mathrm{div}\Big(\prod_{(\alpha,\beta)\in L} (x - \alpha)\Big) &= 2\langle L\rangle - 2(\ell^2 - 1)\langle\mathcal{O}\rangle \\ &= 2\langle E[\ell] \setminus \{\mathcal{O}\}\rangle - 2(\ell^2 - 1)\langle\mathcal{O}\rangle.\end{aligned}$$

We thus have constructed the square of the wanted polynomial. For points not of order 2, we eliminate one factor by using only one of (α, β) and $(\alpha, -\beta)$. For points of order 2, observe that either all of them, or none lie in $E[\ell]$, depending on whether ℓ is even or odd. If ℓ is even, then the product (3.3) contains $(x-\omega_1)(x-\omega_2)(x-\omega_3) = y^2$; a factor of y will thus contribute a single zero at every root of the defining polynomial:

$$\operatorname{div}(y) = \langle(\omega_1, 0)\rangle + \langle(\omega_2, 0)\rangle + \langle(\omega_3, 0)\rangle - 3\langle\mathcal{O}\rangle.$$

Let L' be the set of ℓ-torsion points that contains only one of a pair of (distinct) inverses, $L' = \big\{(\alpha, \beta) \in E[\ell] \setminus \{\mathcal{O}\} \mid (\alpha, -\beta) \notin L'\big\}$. Note that the points of order 2 are not in L'. A polynomial with divisor $\langle E[\ell]\rangle - \ell^2$ is

$$\prod_{(\alpha,\beta)\in L'} (x-\alpha) \quad \text{for odd } \ell, \qquad \text{and} \qquad y \cdot \prod_{(\alpha,\beta)\in L'} (x-\alpha) \quad \text{for even } \ell. \qquad \square$$

Above method yields a whole class of polynomials, differing only by a scalar factor. To make our choice unique, we simply have to pick a leading coefficient.

Lemma 3.4. *Polynomials with identical divisors and leading coefficients are equal.*

Proof. Suppose s and t are polynomials with the same divisor and the same coefficient at their highest power. Their quotient has divisor $\operatorname{div}(s/t) = \operatorname{div}(s) - \operatorname{div}(t) = 0$; thus the quotient is constant. By definition, its value at $\mathcal{O}$ is the quotient of the leading coefficients, which is 1. Therefore s and t must be identical. $\square$

Which leading coefficient should we choose? We should use this degree of freedom to integrate the polynomial with our previous theory. Recall Theorem 2.57, in which we determined the divisor of the components f_m, f_l of multiplication by m and ℓ:

$$\operatorname{div}(f_m - f_\ell) = \langle E[m+\ell]\rangle + \langle E[m-\ell]\rangle - 2\langle E[m]\rangle - 2\langle E[\ell]\rangle.$$

The divisor is non-zero only at points of diverse ℓ-torsion groups; using the polynomial from Lemma 3.2, we hence can express $f_m - f_l$ as a recurrence of polynomials. This links the polynomials to the rational function f_ℓ, not just its denominator. A good choice of leading coefficients would be one that avoids additional scalar factors in the recurrence, so we choose the leading coefficient on the right-hand side to match the fixed and known one on the left-hand side.

Definition 3.5. Let u_ℓ be the unique polynomial whose divisor is $\operatorname{div}(u_\ell) = \langle E[\ell]\rangle - \ell^2\langle\mathcal{O}\rangle$ and whose leading coefficient is ℓ.

Note 3.6. The degree of u_ℓ is $\ell^2 - 1$. This is evident from the construction; it also follows immediately from the divisor and Lemma 2.37, which says that the sum of the multiplicities of a polynomial's zeros equals the degree.

Theorem 3.7. *Let $m > \ell$ and m, ℓ, $m-\ell$ and $m+\ell$ be prime to the field characteristic. Then*

$$f_m - f_\ell = -\frac{u_{m+\ell} \cdot u_{m-\ell}}{u_m^2 \cdot u_\ell^2}. \tag{3.8}$$

Proof. By Lemma 3.2, the left-hand side of the equation has divisor

$$\operatorname{div}(f_m - f_\ell) = \langle E[m+\ell] \rangle + \langle E[m-\ell] \rangle - 2\langle E[m] \rangle - 2\langle E[\ell] \rangle;$$

the right-hand side of the equation has divisor

$$\begin{aligned}
\operatorname{div}\Big(\frac{u_{m+\ell} \cdot u_{m-\ell}}{u_m^2 \cdot u_\ell^2}\Big) &= \operatorname{div}(u_{m+\ell}) + \operatorname{div}(u_{m-\ell}) - 2\operatorname{div}(u_m) - 2\operatorname{div}(u_\ell) \\
&= \langle E[m+\ell] \rangle + \langle E[m-\ell] \rangle 2\langle E[m] \rangle - 2\langle E[\ell] \rangle \\
&\quad - \big((m+\ell)^2 + (m-\ell)^2 - 2m^2 - 2\ell^2\big)\langle \mathcal{O} \rangle \\
&= \langle E[m+\ell] \rangle + \langle E[m-\ell] \rangle - 2\langle E[m] \rangle - 2\langle E[\ell] \rangle.
\end{aligned}$$

As in the proof of Lemma 3.4, the quotient of both sides thus has a zero divisor and therefore is constant. Equality follows because the sides agree at the point at infinity: Lemma 2.39 tells us that f_m/x is $1/m^2$ at $\mathcal{O}$; thus $\big(f_m/x - f_\ell/x\big)(\mathcal{O}) = (\ell^2 - m^2)/(m^2\ell^2)$. Furthermore, Definition 3.5 chooses the leading coefficient of the polynomial u_m as m, so $u_{m+\ell} \cdot u_{m-\ell}$ has leading coefficient $\ell^2 - m^2$, and $u_m^2 \cdot u_\ell^2$ has leading coefficient $m^2\ell^2$. Both polynomials have equal degree, and thus $\big(u_{m+\ell} \cdot u_{m-\ell}/u_m \cdot u_\ell\big)(\mathcal{O}) = (\ell^2 - m^2)/(m^2\ell^2)$. □

On the consequences of Theorem 3.7: analogously to Theorem 2.57, Equation 3.8 implies a recurrence relation between the polynomials u_ℓ. Write $f_m - f_\ell = (f_m - f_1) - (f_\ell - f_1)$ to obtain with $u_1 = 1$

$$-\frac{u_{m+\ell}u_{m-\ell}}{u_m^2 u_\ell^2} = -\frac{u_{m+1}u_{m-1}}{u_m^2} + \frac{u_{\ell+1}u_{\ell-1}}{u_\ell^2},$$

which is equivalent to the polynomial identity

$$u_{m+\ell}u_{m-\ell} = u_{m+1}u_{m-1}u_\ell^2 - u_m^2 u_{\ell+1}u_{\ell-1}. \tag{3.9}$$

Thus we can calculate u_ℓ recursively until we reach a known polynomial u_n. These u_n are easy to compute in the beginning, so we can seed the recurrence. The theorem hence implies a method to compute the u_ℓ without explicit knowledge of the ℓ-torsion points.

Corollary 3.10. *Let $0 \le n-2$, $n-1$, n, $n+1$, and $n+2$ be prime to the field characteristic. Denoting $u_\ell(x, y)$ as u_ℓ, we have*

$$u_{2n}(x, y) = \frac{u_n}{2y}(u_{n+2}u_{n-1}^2 - u_{n+1}^2 u_{n-2}), \tag{3.11}$$

$$u_{2n+1}(x, y) = u_{n+2}u_n^3 - u_{n+1}^3 u_{n-1}. \tag{3.12}$$

Furthermore, the first six polynomials are:

(-i) $u_{-1}(x, y) = -1$

(o) $u_0(x, y) = 0$

(i) $u_1(x, y) = 1$

(ii) $u_2(x, y) = 2y$

(iii) $u_3(x, y) = 3x^4 + 6Ax^2 + 12Bx - A^2$

(iv) $u_4(x, y) = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3)$

Proof. Take $m = n + 1$ and $\ell = n - 1$ in Equation 3.9 to obtain the first recurrence; for the second, take $m = n + 1$ and $\ell = n$.

Next we discuss the seed values. Every point is 0-torsion, so $E[0] = E(\overline{\mathbb{F}})$ and u_0 must be the zero function, which proves case (o). Only $\mathcal{O}$ is 1-torsion, so $E[1]$, $E[-1] = \{\mathcal{O}\}$; thus u_1 and u_{-1} must be constant to have divisors $\operatorname{div}(u_1)$, $\operatorname{div}(u_1) = 0$. The leading coefficients 1 and -1 clearly match the index as required by Definition 3.5, so cases (i) and (-i) are complete.

To see case (ii), recall that the 2-torsion group is

$$E[2] = \big\{\mathcal{O}, (\omega_1, 0), (\omega_2, 0), (\omega_3, 0)\big\}$$

where ω_1, ω_2, and ω_3 are the roots of the curve's defining polynomial; compare Example 2.4. The polynomial y has the matching divisor $\langle(\omega_1, 0)\rangle + \langle(\omega_2, 0)\rangle + \langle(\omega_3, 0)\rangle - 3\langle\mathcal{O}\rangle$, as we saw in the proof of Lemma 3.2. Thus $u_2 = 2y$ has the correct divisor and leading coefficient.

Case (iii) motivated our search for an implicit representation of ℓ-torsion points; in Example 2.6, we saw that u_3 vanishes at the finite 3-torsion points. The zeros must be single since $\deg(u_3) = 8$, so u_3 has the desired divisor $\operatorname{div}(u_3) = \langle E[3]\rangle - 9\langle\mathcal{O}\rangle$.

For case (iv), observe that a 4-torsion point P is of order either 2 or 4. If P is of order 2, then $y(P) = 0$. If P is of order 4, then $y(2 \cdot P) = 0$. The expansion of point doubling in Example 2.26 yielded

$$\big(y \circ [2]\big)(x, y) = y \cdot \frac{x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3}{8(x^3 + Ax + B)^2};$$

thus u_4 has its zeros at the finite 4-torsion points. From $\deg(u_4) = 15$ we see that these are single zeros, so u_4 has divisor $\operatorname{div}(u_4) = \langle E[4]\rangle - 16\langle\mathcal{O}\rangle$ and leading coefficient 4 as required. □

Note 3.13. The rest of this chapter builds upon above recurrence. In mixed expressions of functions and projections x and y such as Equation 3.11, complete notation requires the specification of the function variables: the product of a rational function $f \in \mathbb{F}(E)$ with the projection x, for example, is $f(x, y) \cdot x$. This becomes tedious in large products and, worst of all, buries the structure of an expression in useless formalism. Therefore this chapter uses the convention that functions—unless specified otherwise—are functions in x and y; the symbol f denotes $f(x, y)$, so above product shrinks to $f \cdot x$.

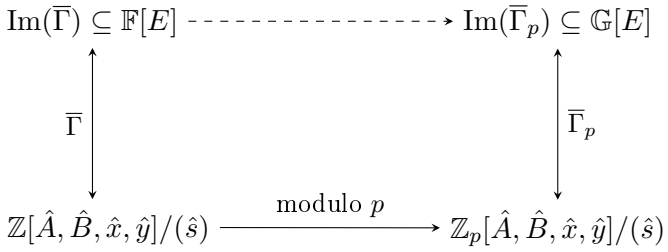

Figure 3.14: Polynomials in $\mathbb{F}[E]$ whose coefficients are products of integers and the field elements A and B may be interpreted as polynomials in $\mathbb{Z}[\hat{A}, \hat{B}, \hat{x}, \hat{y}]/(\hat{s})$, where $\hat{s} = \hat{y} - \hat{x}^3 - \hat{A}\hat{x} - \hat{B}$. Identities remain unaffected by reduction modulo p and imply identities in $\mathbb{Z}_p[\hat{A}, \hat{B}, \hat{x}, \hat{y}]/(\hat{s})$. These, in turn, translate back to $\mathbb{G}[E]$, where $\mathbb{G}$ is a field of characteristic p. As a consequence, polynomial identities in characteristic 0 hold in positive characteristics. See Lemma 3.15.

3.2 Definition in Arbitrary Characteristic

The recurrence of Corollary 3.10 is complete in characteristic 0; in positive characteristic, it has gaps because the indices must be prime to the characteristic. To solve this problem, we reverse the direction of our argumentation: instead of completing the recurrence, we use it as definition in positive characteristic and show that this yields precisely the polynomials u_ℓ of Definition 3.5.

The idea behind this step is as follows: examine Corollary 3.10 and suppose the field characteristic is 0. If we take A and B to be symbols of variables, then the polynomials in item (-i) to (iv) have integer coefficients. Equation 3.12 preserves this property and if we temporarily assume the same for Equation 3.11, then we may interpret all u_ℓ as polynomials with integer coefficients in the indeterminates A, B, x, and y. For clarity we distinguish the new symbols from their original meaning by adding a hat. Thus we discuss polynomials in $\mathbb{Z}[\hat{A}, \hat{B}, \hat{x}, \hat{y}]$.

From this perspective, Corollary 3.10 describes a relation between the elements of $\mathbb{Z}[\hat{A}, \hat{B}, \hat{x}, \hat{y}]$, and this relation carries over to the polynomials in $\mathbb{F}[E]$. The respective map Γ between the rings of polynomials assigns the variables $\hat{x}$ and $\hat{y}$ to their counterparts x and y; $\hat{A}$ and $\hat{B}$ become the field elements A and B; and integer coefficients i are interpreted as i-times repeated addition in $\mathbb{F}[E]$. Extended to all polynomials, we have

$$\begin{aligned} \Gamma : \mathbb{Z}[\hat{A}, \hat{B}, \hat{x}, \hat{y}] &\to \mathbb{F}[E] \\ \sum_{k,l,m,n} i_{(k,l,m,n)} \hat{A}^k \hat{B}^l \hat{x}^m \hat{y}^n &\mapsto \sum_{k,l,m,n} (i_{(k,l,m,n)} \cdot 1) A^k B^l x^m y^n. \end{aligned}$$

The fundamental relation holds for the codomain of Γ, so the kernel $\mathrm{Ker}(\Gamma)$ consists of the polynomial

$$\hat{s}(\hat{x}, \hat{y}) = \hat{y}^2 - \hat{x}^3 - \hat{A}\hat{x} - \hat{B}.$$

It is therefore sufficient to use the map induced on the quotient ring

$$\overline{\Gamma} : \mathbb{Z}[\hat{A}, \hat{B}, \hat{x}, \hat{y}]/(\hat{s}) \to \mathbb{F}[E].$$

The map $\overline{\Gamma}$ is a ring homomorphism; with its image as codomain, it is an isomorphism [25, (6.2.4)]. The image $\mathrm{Im}(\overline{\Gamma})$ contains the u_ℓ and furthermore all polynomials with integer coefficients in $\mathbb{F}[E] = \mathbb{F}[x, y]$. Thus, identities expressed in such polynomials of $\mathbb{F}[E]$ must be valid in $\mathbb{Z}[\hat{A}, \hat{B}, \hat{x}, \hat{y}]/(\hat{s})$; the inverse of $\overline{\Gamma}$ translates them.

Reducing identities in $\mathbb{Z}[\hat{A}, \hat{B}, \hat{x}, \hat{y}]/(\hat{s})$ modulo a prime p yields identities in $\mathbb{Z}_p[\hat{A}, \hat{B}, \hat{x}, \hat{y}]/(\hat{s})$. The respective map is the canonical epimorphism; the map is well-defined, so images of equivalent elements are equivalent.

Similarly to the construction of $\overline{\Gamma}$, we identify elements of $\mathbb{Z}_p[\hat{A}, \hat{B}, \hat{x}, \hat{y}]/(\hat{s})$ with polynomials in $\mathbb{G}[E]$, where $\mathbb{G}$ is a field of characteristic $p > 3$ and $A, B \in \mathbb{G}$. Let $\overline{\Gamma}_p$ denote this map. As with $\overline{\Gamma}$, the image of $\overline{\Gamma}_p$ contains all polynomials in x and y whose coefficients are products of integers and the field elements $A, B \in \mathbb{G}$.

Therefore we may lift identities between the polynomials u_ℓ in characteristic 0 to $\mathbb{Z}[\hat{A}, \hat{B}, \hat{x}, \hat{y}]/(\hat{s})$ and translate them to identities in characteristics p as depicted in Figure 3.14. The preceding discussion shows the following:

Lemma 3.15. *Identities in the image of $\overline{\Gamma}$ imply identities in the image of $\overline{\Gamma}_p$.*

In our considerations above, we assumed integer coefficients for the polynomials u_ℓ. Let us now supply this foundation.

Lemma 3.16. *The polynomials u_ℓ appearing in Corollary 3.10 interpreted as having variables A, B, x, and y possess integer coefficients only.*

Proof. The single problematic case is Equation 3.11 because it contains a division by $2y$:

$$u_{2n}(x, y) = \frac{u_n}{2y}(u_{n+2}u_{n-1}^2 - u_{n+2}^2 u_{n-2}).$$

Note, however, that u_{2n} always has integer coefficients and contains a factor of $2y$ if $n > 0$: for u_2 and u_4 this is true. Now assume this is the case for all u_{2m}, $m < n$.

If n is even, so are $n+2$ and $n-2$. By the inductive hypothesis, we can thus divide u_n by $2y$ without losing integer coefficients; the additional factor of $2y$ comes from u_{n+2} and u_{n-2}. If n is odd, then $n+1$ and $n-1$ are even and we can safely extract $4y^2$ from u_{n+1}^2 and u_{n-1}^2. Again, no integer coefficients are harmed and an additional factor of $2y$ exists, which completes the induction. □

With above intuition, we start the construction of polynomials with divisor $\langle E[\ell] \rangle - \ell^2 \langle \mathcal{O} \rangle$. The recurrence of Corollary 3.10 serves as definition.

Definition 3.17. Let $\mathbb{F}$ be a field of any characteristic neither 2 nor 3. The *division polynomials* $\psi_\ell \in \mathbb{F}[E]$ are the unique polynomials generated by the following recurrence:

(-i) $\psi_{-1}(x, y) = -1$

(o) $\psi_0(x, y) = 0$

(i) $\psi_1(x, y) = 1$

(ii) $\psi_2(x,y) = 2y$

(iii) $\psi_3(x,y) = 3x^4 + 6Ax^2 + 12Bx - A^2$

(iv) $\psi_4(x,y) = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3)$

(v) For $n > 2$ put

$$\psi_{2n}(x,y) = \frac{\psi_n}{2y}(\psi_{n+2}\psi_{n-1}^2 - \psi_{n+1}^2\psi_{n-2});$$

for $n \geq 2$ put

$$\psi_{2n+1}(x,y) = \psi_{n+2}\psi_n^3 - \psi_{n+1}^3\psi_{n-1}.$$

Note 3.18. In characteristic 0, this definition agrees with our former Definition 3.5; compare Corollary 3.10.

The ψ_ℓ are indeed the desired polynomials; we show this as follows: in characteristic 0, we express the rational component functions $f_\ell, g_\ell \in \mathbb{F}(E)$ of multiplication by ℓ through u_ℓ, convert this expression to an identity of polynomials in $\mathbb{F}[E]$, and lift the identity to $\mathbb{Z}[\hat{A}, \hat{B}, \hat{x}, \hat{y}]/(\hat{s})$. Reduction modulo a prime p does not bother the lifted identity; it thus holds in $\mathbb{G}[E]$ for $\mathbb{G}$ of any characteristic. Finally we reconstruct the expression of f_ℓ, g_ℓ through ψ_ℓ—only this time in arbitrary characteristic. The set of zeros of ψ_ℓ then is immediate from this expression.

Lemma 3.19. *For multiplication $[\ell] = (f_\ell, g_\ell)$, $\ell > 0$, on an elliptic curve over a field of characteristic 0, we have*

$$f_\ell(x,y) = x - \frac{u_{\ell+1}u_{\ell-1}}{u_\ell^2}; \tag{3.20}$$

and

$$g_\ell(x,y) = \frac{u_{\ell+2}u_{\ell-1}^2 - u_{\ell+1}^2u_{\ell-2}}{4y \cdot u_\ell^3}. \tag{3.21}$$

Proof. The first equation is a corollary of Theorem 3.7: take $\ell - 1$ with $f_1(x,y) = x$ and $u_1(x,y) = 1$ in Equation 3.8.

The second equation follows by induction. We start by inserting the polynomials for $\ell = 1$, which yields

$$g_1(x,y) = \frac{u_3u_0^2 - u_2^2u_{-1}}{4y \cdot u_1^3} = \frac{4y^2}{4y} = y.$$

For $\ell = 2$ we have

$$\begin{aligned} g_2(x,y) &= \frac{u_4u_1^2 - u_3^2u_0}{4y \cdot u_2^3} \\ &= \frac{4y \cdot x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3}{4 \cdot 8(x^3 + Ax + B)^2}; \end{aligned}$$

a glance at Equation 2.28 shows that this is correct. In fact, this was how we found u_4 in Corollary 3.10.

Assume Equation 3.21 to hold for $k < \ell$. Writing g_ℓ with the generic point addition formula and using Equations 3.20 and 3.21, we get

$$\begin{aligned} g_\ell(x,y) &= -y + \Big(\frac{g_{\ell-1}-y}{f_{\ell-1}-x}\Big)\cdot(x-f_\ell) \\ &= -y + \frac{\big((u_{\ell+1}u_{\ell-2}^2 - u_\ell^2 u_{\ell-3})/(4y\cdot u_{\ell-1}^3)\big) - y}{u_\ell u_{\ell-2}/u_{\ell-1}^2}\cdot\Big(-\frac{u_{\ell+1}u_{\ell-1}}{u_\ell^2}\Big) \\ &= \frac{-4y^2\cdot u_\ell^3 u_{\ell-2} - u_{\ell+1}^2 u_{\ell-2}^2 + u_{\ell+1}u_\ell^2 u_{\ell-3} + 4y^2\cdot u_{\ell+1}u_{\ell-1}^3}{4y\cdot u_\ell^3 u_{\ell-2}}. \end{aligned}$$

Next we subtract the right-hand side of Equation 3.21 and compare to zero. Multiplying away the denominator and substituting u_2 for $2y$ results in

$$u_{\ell+1}u_\ell^2 u_{\ell-3} - u_{\ell+2}u_{\ell-1}^2 u_{\ell-2} - u_\ell^3 u_{\ell-2}u_2^2 + u_{\ell+1}u_{\ell-1}^3 u_2^2 = 0.$$

We derive our result by applying Equation 3.9 with $m = \ell - 1$ and $\ell = 2$, and $m = \ell$ and $\ell = 2$ to the last two terms respectively. □

Now we use these new expressions for f_ℓ and g_ℓ to find polynomial identities that can be lifted.

Corollary 3.22. *In the situation of the previous lemma, the relations*

$$-x - f_{\ell-1} + \Big(\frac{g_{\ell-1}-y}{f_{\ell-1}-x}\Big) = x - \frac{u_{\ell+1}u_{\ell-1}}{u_\ell^2} \tag{3.23}$$

and

$$-y - \Big(\frac{g_{\ell-1}-y}{f_{\ell-1}-x}\Big)\cdot(x-f_\ell) = \frac{u_{\ell+2}u_{\ell-1}^2 - u_{\ell+1}^2 u_{\ell-2}}{4y u_\ell^3} \tag{3.24}$$

are polynomial identities in $\mathbb{F}[E]$ with integer coefficients.

Proof. Both equations express the components of multiplication by ℓ; the left-hand side is the definition of point addition, the right-hand side uses above Lemma 3.19. To obtain polynomial identities, insert the expressions for f_ℓ, $f_{\ell-1}$, and $g_{\ell-1}$ from Lemma 3.19; then multiply with the respective denominators. □

The exact look of the identities is irrelevant. What is relevant is that by lifting Equations 3.23 and 3.24 to $\mathbb{Z}[\hat{A}, \hat{B}, \hat{x}, \hat{y}]/(\hat{s})$, we can re-derive the expressions of Lemma 3.19 in fields of arbitrary characteristic.

Theorem 3.25. *The division polynomials ψ_ℓ are not identically zero for all $\ell > 0$. Furthermore, with $[\ell] = (f_\ell, g_\ell)$ and denoting $\psi_\ell(x,y)$ as ψ_ℓ, we have*

$$f_\ell(x,y) = x - \frac{\psi_{\ell+1}\psi_{\ell-1}}{\psi_\ell^2}; \tag{3.26}$$

and

$$g_\ell(x,y) = \frac{\psi_{\ell+2}\psi_{\ell-1}^2 - \psi_{\ell+1}^2\psi_{\ell-2}}{4y\cdot\psi_\ell^3}. \tag{3.27}$$

Proof. We start an induction on ℓ by noting that clearly ψ_ℓ is not identically zero for $0 < \ell \leq 4$; Equation 3.26 and 3.27 likewise hold for $\ell = 1$. Assume now that ψ_m is not identically zero for $m < \ell + 1$ and that both equations hold for $m < \ell$.

We know that Equations 3.20 and 3.21 are polynomial identities in $\mathbb{F}[E]$ if $\mathbb{F}$ has characteristic 0. Only integer coefficients appear, so they are elements of $\mathrm{Im}(\overline{\Gamma})$ and we may interpret them in $\mathbb{Z}[\hat{A}, \hat{B}, \hat{x}, \hat{y}]/(\hat{y}^2 - \hat{x}^3 - \hat{A}\hat{x} - \hat{B})$; see the discussion on page 42. Lemma 3.15 tells us that reduction modulo a prime preserves the identities, so they are valid in $\mathbb{G}[E]$ with $\mathbb{G}$ a field of any characteristic $p > 3$. Therefore, all we have to do in the inductive step is to reconstruct Equations 3.26 and 3.27. This requires dividing by $\psi_{\ell-2}$, $\psi_{\ell-1}$ and ψ_ℓ, all of which are not identically zero by the inductive hypothesis.

It remains to show that $\psi_{\ell+1}$ is not identically zero. From Equation 3.26 we get

$$f_\ell(x, y) - x = -\frac{\psi_{\ell+1}\psi_{\ell-1}}{\psi_\ell^2};$$

if it were identically zero, we would have $\ell \cdot P = \pm P$ for all points P. Equivalently we had $(\ell \pm 1) \cdot P = \mathcal{O}$ and $E[\ell \pm 1] \subseteq E(\overline{\mathbb{F}})$ or $E(\overline{\mathbb{G}})$ would be infinite, a contradiction to Theorem 2.59. □

Finally we can prove that our recursive construction yields the right polynomials:

Theorem 3.28. *Let E be an elliptic curve over a field of characteristic neither 2 nor 3. The polynomials ψ_ℓ of Definition 3.17 fulfill the original characterization in Definition 3.5; if ℓ is prime to the field characteristic, then their divisor is*

$$\mathrm{div}(\psi_\ell) = \langle E[\ell] \rangle - \ell^2 \langle \mathcal{O} \rangle.$$

Proof. Again, write Equation 3.26 as

$$f_\ell(x, y) - x = -\frac{\psi_{\ell+1}(x, y)\psi_{\ell-1}(x, y)}{\psi_\ell^2(x, y)}.$$

Finite poles of $f_\ell(x, y) - x$ can originate only in the rational function f_ℓ, so by Corollary 2.44, $f_\ell(x, y) - x$ has double poles on $E[\ell] \setminus \{\mathcal{O}\}$, a total of $2(\ell^2 - 1)$. Therefore ψ_ℓ has its zeros on $E[\ell]$; they are simple and the only zeros because ψ_ℓ^2 has degree $2(\ell^2-1)$: we have $\deg(u_\ell) = \ell^2-1$ in characteristic 0 by Definition 3.5, and the leading coefficient ℓ does not vanish because it is prime to the field characteristic. Hence the finite ℓ-torsion points $E[\ell] \setminus \{\mathcal{O}\}$ are the zeros of ψ_ℓ, which yields the proposed divisor. □

3.3 Computation on Torsion Points

We started thinking about division polynomials at the beginning of this chapter out of desire for an implicit representation for ℓ-torsion points. With this representation, we want to computationally verify properties derived by interpreting

$E[\ell]$ as module $\mathbb{Z}_\ell \times \mathbb{Z}_\ell$. Our tool set for examining modules is linear algebra; it provides us information about how linear maps act on $E[\ell]$.

To analyze the behavior of maps on $E[\ell]$, we need a way to compare them to maps we know. Thus we are looking for a way to verify identities between rational maps F and G on $E[\ell]$. A test telling whether a rational map is constant-$\mathcal{O}$ on $E[\ell]$ suffices: $F = G$ on $E[\ell]$ if, and only if, $F - G = \overline{\mathcal{O}}$ on $E[\ell]$.

Suppose $F \neq \overline{\mathcal{O}}$ is not the globally constant-$\mathcal{O}$ map and consider the component functions of $F = (f, g)$. If $F = \overline{\mathcal{O}}$ on $E[\ell]$, then f and g have poles at all finite ℓ-torsion points. This is equivalent to their denominator polynomials t and v having zeros there. Hence, every zero of the division polynomial ψ_ℓ is a zero of t and v. By Theorem 3.28, all zeros of ψ_ℓ are single; therefore their multiplicities are less than or equal to the multiplicities of the zeros of t and v. This implies that ψ_ℓ divides t and v; in consequence, t and v are identically zero modulo ψ_ℓ. Conversely, we see that every polynomial that is identically zero modulo ψ_ℓ, and thus a multiple of it, has zeros at all finite ℓ-torsion points.

Translated back to the rational component functions of F, both f and g must therefore be infinite if their numerator and denominator polynomials are reduced modulo ψ_ℓ. On the curve of rational maps with reduced components, F thus equals $\overline{\mathcal{O}}$. Writing $\mathbb{F}(E)/\psi_\ell$ for the field of rational functions with polynomials from $\mathbb{F}[E]/\psi_\ell$, the curve of such reduced rational maps is $E\big(\mathbb{F}(E)/\psi_\ell\big)$. Therefore

$$F(P) = \mathcal{O} \text{ for every } P \in E[\ell] \qquad \Leftrightarrow \qquad F = \overline{\mathcal{O}} \text{ on } E\big(\mathbb{F}(E)/\psi_\ell\big).$$

Given a rational map $F \in E\big(\mathbb{F}(E)\big)$, reduction of its components modulo ψ_ℓ works by applying F to the point $(x, y) \in E\big(\mathbb{F}(E)/\psi_\ell\big)$: the field $\mathbb{F}(E)/\psi_\ell$ is closed under all operations that rational functions from $\mathbb{F}(E)$ perform. Therefore, feeding the function $(x \bmod \psi_\ell)$ to $f \in \mathbb{F}(E)$ yields $(f \bmod \psi_\ell)$; similarly for $(y \bmod \psi_\ell)$, so $F(x, y) \in E\big(\mathbb{F}(E)/\psi_\ell\big)$.

In conclusion, we have shown the following lemma; it allows us to verify identities of rational maps on $E[\ell]$:

Lemma 3.29. *Let E be an elliptic curve over $\mathbb{F}$ and ℓ be prime to the field characteristic. A rational map $F \in E\big(\mathbb{F}(E)\big)$ maps every ℓ-torsion point $P \in E[\ell]$ to the point at infinity if, and only if, it maps $(x, y) \in E\big(\mathbb{F}(E)/\psi_\ell\big)$ to $\overline{\mathcal{O}}$. In symbols:*

$$F = \overline{\mathcal{O}} \text{ on } E[\ell] \qquad \Leftrightarrow \qquad F(x, y) = \overline{\mathcal{O}} \text{ for } (x, y) \in E\big(\mathbb{F}(E)/\psi_\ell\big). \tag{3.30}$$

Chapter 4

Frobenius Endomorphism

We have seen that ℓ-torsion groups are isomorphic to $\mathbb{Z}_\ell \times \mathbb{Z}_\ell$ if ℓ and the field characteristic are relatively prime. Hence we may regard the ℓ-torsion group as a free module; if ℓ is prime, then $\mathbb{Z}_\ell$ is a field and $\mathbb{Z}_\ell \times \mathbb{Z}_\ell$ a vector space. To obtain this regular structure, we allowed ℓ-torsion points to have coordinates in the algebraic closure of $\mathbb{F}$, the field over which the curve E was defined. Therefore we now understand parts of the curve $E(\overline{\mathbb{F}})$, and we may interpret our original task as counting the $\mathbb{F}$-rational points on $E(\overline{\mathbb{F}})$. What we are looking for is, thus, a method to exclude non-$\mathbb{F}$-rational points and derive the global information of the number of $\mathbb{F}$-rational points by exploiting the local structure of the ℓ-torsion subgroups of $E(\overline{\mathbb{F}})$. Developing such a characterization is our task for the present chapter.

Note 4.1. In this chapter we assume that elliptic curves are defined over the finite field with q elements $\mathbb{F}_q$, $q = p^k$ where p is prime. The finiteness is used in many places; unlike the previous chapters, it is fundamental to our discussion.

4.1 Characterization of Rational Points

To discern finite $\mathbb{F}_q$-rational points from the other points of $E(\overline{\mathbb{F}}_q)$, we have to recognize points with both coordinates in $\mathbb{F}_q$. Thus we need a property that sets apart the elements in $\mathbb{F}_q \subsetneq \overline{\mathbb{F}}_q$ from those in $\overline{\mathbb{F}}_q \setminus \mathbb{F}_q$. The most salient feature of $\mathbb{F}_q$ is that it is finite, so we exploit the finite order of its elements in the (multiplicative) unit group $\mathbb{F}_q^\star$.

Lemma 4.2. *In the field with q elements, taking elements to the q-th power is the identity; for $\alpha \in \mathbb{F}_q$*

$$\alpha^q = \alpha.$$

Proof. The equation clearly holds for $0 \in \mathbb{F}_q$. Suppose $\alpha \neq 0$, so α is a unit. Dividing the equation by α results in

$$\alpha^{q-1} = 1.$$

Because $\mathbb{F}_q$ is a field, its unit group $\mathbb{F}_q^\star$ has order $q-1$. Thus, by Lagrange's theorem, all units have an order dividing $q-1$, which implies that taking them to the $(q-1)$-th power yields $1 \in \mathbb{F}_q$. Above equation thus holds for all units in $\mathbb{F}_q$. Therefore it is valid for all elements of $\mathbb{F}_q$ and the proof is complete. □

This behavior even characterizes the elements of $\mathbb{F}_q \subsetneq \overline{\mathbb{F}}_q$.

Lemma 4.3. *An element $\alpha \in \overline{\mathbb{F}}_q$ is in $\mathbb{F}_q$ if, and only if, $\alpha^q = \alpha$.*

Proof. Lemma 4.2 states the first implication: if $\alpha \in \mathbb{F}_q$ then $\alpha^q = \alpha$. Conversely if $\alpha^q = \alpha$ for an element $\alpha \in \overline{\mathbb{F}}_q$, then α is a root of the polynomial $b(z) = z^q - z$ in $\overline{\mathbb{F}}_q[z]$. As a univariate polynomial, b has degree $\deg_1(b) = q$, and therefore q roots in $\overline{\mathbb{F}}_q$. But we already know q roots of b, namely the elements of $\mathbb{F}_q$. Therefore the elements of $\mathbb{F}_q$ are all roots of b; only for them we have $\alpha^q = \alpha$. □

Taking the q-th power of field elements defines the Frobenius map on $\overline{\mathbb{F}}_q$. We skip the formal definition and immediately extend it to elliptic curves.

Definition 4.4. Let E be an elliptic curve over $\mathbb{F}_q$. The *Frobenius map* is the rational map $\varphi : E(\overline{\mathbb{F}}_q) \to E(\overline{\mathbb{F}}_q)$,

$$\varphi(\alpha, \beta) = (\alpha^q, \beta^q) \quad \text{if } (\alpha, \beta) \text{ is finite,} \qquad \text{and} \qquad \varphi(\mathcal{O}) = \mathcal{O}.$$

Observe that the images of φ lie on the curve. For finite points $(\alpha, \beta) \in E(\overline{\mathbb{F}}_q)$, we see that the fundamental relation holds for the images:

$$\begin{aligned}(\beta^q)^2 &= (\beta^2)^q \\ &= (\alpha^3 + A\alpha + B)^q \\ &= (\alpha^3)^q + (A\alpha)^q + \beta^q \\ &= (\alpha^q)^3 + A(\alpha^q) + B.\end{aligned}$$

To obtain the fourth equality, we have used Lemma 4.2 and that A and B are elements of $\mathbb{F}_q$; the third equality follows from a fundamental result on arithmetic in $\overline{\mathbb{F}}_q$.

Lemma 4.5. *For $n \in \mathbb{N}$ and $\alpha_i \in \overline{\mathbb{F}}_q$*

$$\left(\sum_{i=1}^{n} \alpha_i\right)^q = \sum_{i=1}^{n} \alpha_i^q.$$

Proof. Verifying the equation for $n = 2$ suffices: the other (finite) cases then follow by using associativity and writing

$$\left(\sum_{i=1}^{n} \alpha_i\right)^q = \left(\alpha_1 + \left(\sum_{i=2}^{n} \alpha_i\right)\right)^q.$$

The general binomial formula states

$$(\alpha_1 + \alpha_2)^q = \sum_{k=0}^{q} \binom{q}{k} \alpha_1^k \alpha_2^{q-k}.$$

We observe that the field characteristic p divides every binomial coefficient except $\binom{q}{0} = \binom{q}{q} = 1$. Hence, we have

$$(\alpha_1 + \alpha_2)^q = \alpha_1^q + \alpha_2^q + \sum_{k=1}^{q-1} 0 \cdot \alpha_1^k \alpha_2^{q-k} = \alpha_1^q + \alpha_2^q. \qquad \square$$

If taking the q-th power characterizes the elements of $\mathbb{F}_q$, then the Frobenius map characterizes the $\mathbb{F}_q$-rational points.

Theorem 4.6. *The Frobenius map fixes the $\mathbb{F}_q$-rational points in $E(\overline{\mathbb{F}}_q)$: $P \in E(\mathbb{F}_q) = E$ if, and only if, $\varphi(P) = P$.*

Proof. The Frobenius map fixes a point if, and only if, it fixes both coordinates. By Lemma 4.3, this is equivalent to both coordinates being elements of $\mathbb{F}_q$. Thus, the fixed points of φ are the $\mathbb{F}_q$-rational points. □

Invariance under the Frobenius map makes for a compact description of the $\mathbb{F}_q$-rational points in $E(\overline{\mathbb{F}}_q)$: the fixed points of φ are the elements in $\operatorname{Ker}(\mathrm{id} - \varphi)$, so

$$\begin{aligned} E &= \operatorname{Ker}(\mathrm{id} - \varphi) \subseteq E(\overline{\mathbb{F}}_q), \\ |E| &= |\operatorname{Ker}(\mathrm{id} - \varphi)|\,. \end{aligned}$$

4.2 Combination with Torsion Point Structure

Besides characterizing E in $E(\overline{\mathbb{F}}_q)$, φ also harmonizes with the group structure.

Definition 4.7. An *endomorphism* of an elliptic curve E over a field $\mathbb{F}$ is a rational map $\eta : E(\overline{\mathbb{F}}) \to E(\overline{\mathbb{F}})$ that respects the group structure: for all points $P, Q \in E(\overline{\mathbb{F}})$

$$\eta(P + Q) = \eta(P) + \eta(Q).$$

Theorem 4.8. *The Frobenius map is a group endomorphism of the elliptic curve $E(\overline{\mathbb{F}}_q)$.*

Proof. On page 49 we saw that φ is a rational map. Hence we only have to show that φ respects the group structure, that is,

$$\varphi(P_1 + P_2) = \varphi(P_1) + \varphi(P_2)$$

for all points $P_1 = (\alpha_1, \beta_1)$ and $P_2 = (\alpha_2, \beta_2)$ on $E(\overline{\mathbb{F}}_q)$. Clearly $\varphi(\mathcal{O}) = \mathcal{O}$, for the component functions of φ are polynomials and so have poles at $\mathcal{O}$. Furthermore $\varphi(-P_1) = \big(\alpha_1^q, (-\beta_1)^q\big) = \big(\alpha_1^q, -(\beta_1^q)\big) = -\varphi(P_1)$.

Thus only the generic addition and point doubling cases of Definition 1.6 remain. Applying the binomial theorem on $\overline{\mathbb{F}}_q$ (Lemma 4.5) we pull the exponent q inside the rational addition formulas. For example, suppose $\alpha_1 \neq \alpha_2$. Then

$$\begin{aligned} x\big(\varphi(P_1 + P_2)\big) &= \Big(-\alpha_1 - \alpha_2 + \Big(\frac{\beta_2 - \beta_1}{\alpha_2 - \alpha_1}\Big)^2\Big)^q \\ &= -\alpha_1^q - \alpha_2^q + \Big(\frac{\beta_2^q - \beta_1^q}{\alpha_2^q - \alpha_1^q}\Big)^2 \\ &= x\big(\varphi(P_1) + \varphi(P_2)\big); \end{aligned}$$

the other formulas follow by similar computation. □

Note 4.9. As a consequence of above theorem, we call the Frobenius map φ the *Frobenius endomorphism.*

Filtering $\mathbb{F}_q$-rational points with the Frobenius endomorphism not only works on the whole curve. Endomorphisms preserve the order of group elements, thus φ maps ℓ-torsion points onto ℓ-torsion points: for $P \in E[\ell]$,

$$\mathcal{O} = \varphi(\mathcal{O}) = \varphi(\ell \cdot P) = \ell \cdot \varphi(P).$$

Therefore, φ is an endomorphism of $E[\ell]$.

We hence may localize the Frobenius endomorphism to the subgroup $E[\ell] \subseteq E(\overline{\mathbb{F}}_q)$. Combining this with the structure result $E[\ell] \simeq \mathbb{Z}_\ell \times \mathbb{Z}_\ell$ of section 2.3, we obtain an interpretation of φ on $E[\ell]$ as a linear map on the free module $\mathbb{Z}_\ell \times \mathbb{Z}_\ell$.

Lemma 4.10. *Let ℓ be prime to the field characteristic. Then the Frobenius endomorphism φ is a linear map on the ℓ-torsion subgroup interpreted as free module.*

Proof. The Frobenius endomorphism φ maps ℓ-torsion points onto ℓ-torsion points; thus $\varphi : E[\ell] \to E[\ell]$. For $P, Q \in E[\ell] \simeq \mathbb{Z}_\ell \times \mathbb{Z}_\ell$, we use that φ is an endomorphism to get

$$\begin{aligned}\varphi(m \cdot P + n \cdot Q) &= \varphi(m \cdot P) + \varphi(n \cdot Q) \\ &= m \cdot \varphi(P) + n \cdot \varphi(Q).\end{aligned}$$

Therefore φ is a linear map on $E[\ell] \simeq \mathbb{Z}_\ell \times \mathbb{Z}_\ell$. □

Characteristic Equation

When examining φ in its linear map interpretation, we must be careful: our results should be independent of the basis of $E[\ell]$ because we have not defined the exact correspondence between ℓ-torsion points and vectors in $\mathbb{Z}_\ell \times \mathbb{Z}_\ell$. A tool that circumvents the peculiarities of basis choice and provides insight into the behavior of φ on $E[\ell]$ is the characteristic polynomial.

Definition 4.11. The *characteristic polynomial* of a linear map λ is

$$\chi_\lambda(z) = \det(\mathrm{id} \cdot z - \lambda),$$

where id denotes the identity map and det denotes the determinant.

The module $\mathbb{Z}_\ell \times \mathbb{Z}_\ell$ has rank 2, so we can expand the characteristic polynomial and derive a more explicit expression: for a fixed basis of $\mathbb{Z}_\ell \times \mathbb{Z}_\ell$, write the linear map λ as its 2×2 matrix to get

$$\begin{aligned}\chi_\lambda(z) &= \det \begin{pmatrix} z-a & -b \\ -c & z-d \end{pmatrix} \\ &= (z-a)(z-d) - cb \\ &= z^2 - (a+d)z + ad - cb \\ &= z^2 - \mathrm{tr}(\lambda)z + \det(\lambda).\end{aligned}$$

Note that $\det(\lambda)$ is independent of the matrix of λ; however, at a first glance, the trace $\mathrm{tr}(\lambda)$ is not. Hence, we once more use that the module has rank 2: for any 2×2 matrix λ we have

$$\mathrm{tr}(\lambda) = 1 + \det(\lambda) - \det(\mathrm{id} - \lambda),$$

an equality that is easily verified by direct computation.

For ℓ prime to the field characteristic, we thus have the characteristic polynomial of φ on $E[\ell] \simeq \mathbb{Z}_\ell \times \mathbb{Z}_\ell$

$$\begin{aligned}\chi_\varphi(z) &= z^2 - \mathrm{tr}(\varphi) \cdot z + \det(\varphi) \\ &= z^2 - \big(1 + \det(\varphi) - \det(\mathrm{id} - \varphi)\big) \cdot z + \det(\varphi).\end{aligned}$$

Now consider the following intuitions: (i) the determinants probably depend on the global behavior of the maps with only minor local adjustments; (ii) we know the behavior of φ; (iii) the map $(\mathrm{id} - \varphi)$ characterizes the $\mathbb{F}_q$-rational points; (iv) the characteristic polynomial χ_φ annihilates φ by the Theorem of Cayley-Hamilton.

We want to get information on $(\mathrm{id} - \varphi)$. Let us suppose that we know $\det(\varphi)$. Then we can guess the value $k = \det(\mathrm{id} - \varphi)$ and check whether the characteristic equation holds:

$$\varphi \circ \varphi - [1 + \det(\varphi) - k] \circ \varphi + [\det(\varphi)] = \overline{\mathcal{O}} \quad \text{on } E[\ell] \tag{4.12}$$

if ℓ is prime to the field characteristic.

Using Lemma 3.29, above equation is a computable test that gives us information on the local behavior of $(\mathrm{id} - \varphi)$—which we hope to be strongly related to the global behavior of $(\mathrm{id} - \varphi)$. If we discover a bidirectional link between the behavior of rational maps on the curve and their determinants on $E[\ell]$, then we therefore have a method to derive information on $(\mathrm{id} - \varphi)$, which is our characterization of $E \subseteq E(\overline{\mathbb{F}}_q)$ with $|\mathrm{Ker}(\mathrm{id} - \varphi)| = |E|$.

Chapter 5

Weil Pairing

In this chapter we motivate and discuss a link between the local mapping behavior of endomorphisms on ℓ-torsion groups, and their global mapping behavior on the curve $E(\overline{\mathbb{F}})$. The link completes the theoretical foundation for making the characteristic equation of the Frobenius endomorphism into a point counting algorithm for elliptic curves over finite fields $\mathbb{F}_q$.

Note 5.1. The main result of this chapter requires deeper and more abstract theory than fits the scope of this thesis. Nevertheless we will give a concrete motivation for all steps. These might not catch every relevant aspect, but provide some intuition when studying the deeper theory.

5.1 Mapping Behavior of Endomorphisms

The characteristic polynomial of the Frobenius endomorphism χ_φ applied to φ yields a map that is identically $\mathcal{O}$ on the ℓ-torsion group $E[\ell]$; the polynomial coefficients involve the determinants of endomorphisms on the free module $\mathbb{Z}_\ell \times \mathbb{Z}_\ell \simeq E[\ell]$. Suppose ℓ is a prime and not the field characteristic. Then the module is a vector space and a zero determinant implies that the image of the endomorphism has reduced dimension. Therefore the image contains only some ℓ-torsion points, all of which are multiples of a single point. Conversely, when we observe such a collapsing of ℓ-torsion points onto each other, we know that the determinant must be zero on $E[\ell]$.

If ℓ is not prime, then $\mathbb{Z}_\ell$ is a ring with zero divisors. This complicates the relation between the determinant and the collapsing of ℓ-torsion points: a unit determinant guarantees a bijective map just like above, for

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad - bc} \cdot \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

However, if the determinant is a zero divisor, then only some points collapse.

Example 5.2. Let $P, Q \in E[4]$ be linearly independent 4-torsion points on an elliptic curve E. Suppose η is an endomorphism of E, and $\eta(P) = 2 \cdot P + 2 \cdot Q$, $\eta(Q) = Q$. Then η acts on $E[4]$ as depicted in Figure 5.3. Observe that $\eta\big(E[\ell]\big)$ contains only eight points, and that the order of $\eta(P)$ is 2.

In any case, the way an endomorphism collapses ℓ-torsion points tells us something about its determinant on $E[\ell]$. This collapsing has to follow certain

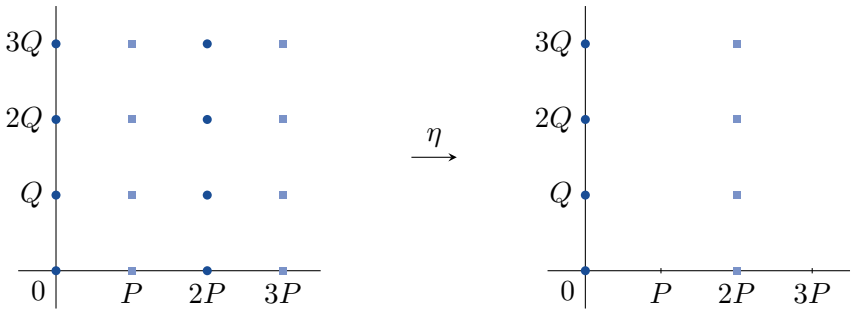

Figure 5.3: The curve endomorphism η is a linear map on the 4-torsion group $E[4]$. The images of the basis elements P and Q completely determine its mapping behavior; here $\eta(P) = 2 \cdot P + 2 \cdot Q$, and $\eta(Q) = Q$.

The order of $\eta(P)$ is 2, so the multiples of P with order 4 vanish: the columns of P and $3P$ collapse onto the $2P$ column in the image. The $2P$ column merges with the 0 column. See Example 5.2.

rules because endomorphisms preserve the structure among all points on the curve, not just the ℓ-torsion points. By intuition, the global mapping behavior of endomorphisms therefore determines the local collapsing of ℓ-torsion points, and thus the determinant on $E[\ell]$. Consequently we examine how endomorphisms act globally, on the whole curve.

First, recall that endomorphisms are rational maps; these hit every point on the curve if they are non-constant.

Lemma 5.4. *A non-constant rational map $F : E(\overline{\mathbb{F}}) \to E(\overline{\mathbb{F}})$ is surjective.*

Proof. A rational map F is a pair (f, g) of rational functions, so we first examine the mapping behavior of these.

Suppose $h = s/t$ is a non-constant rational function. Then its numerator s or its denominator t (or both) involve an x or a y that does not cancel out. Therefore, h has at least one zero or pole: if $\deg(s) \neq 0$, then s has a pole at $\mathcal{O}$ and, by Corollary 2.38, a finite zero. Similarly, if $\deg(t) \neq 0$, then t has a pole at $\mathcal{O}$ and a finite zero. At least one zero and one pole cause a zero and a pole in h, for otherwise h would be constant.

In consequence, any non-constant rational function h has at least one zero and one pole. In particular, $h - \alpha$ has a zero for any $\alpha \in \overline{\mathbb{F}}$, so h outputs all values in $\overline{\mathbb{F}}$; the pole adds infinity.

Now we apply this result to the components of $F = (f, g)$. Assume that g were constant. By the fundamental relation between f and g, f could then have only finitely many values and hence would be constant. Likewise, g must be constant if f is. In both cases F would be constant, which contradicts our initial assumption about F. Therefore both components of f output all values, including infinity, so F is surjective on $E(\overline{\mathbb{F}})$. □

The endomorphism η therefore outputs every point $P \in E(\overline{\mathbb{F}})$. However, η does not have to be injective, so the preimage of P may be ambiguous: the fiber $\eta^{-1}(P)$ of a point P might contain several elements.

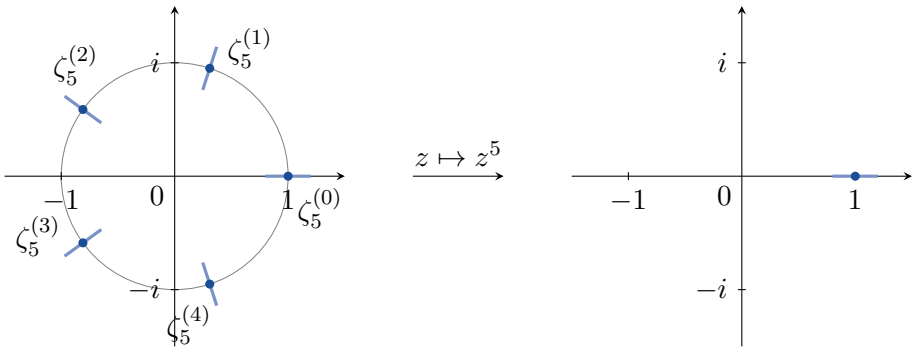

Figure 5.6: Under the complex function $z \mapsto z^5$, 1 has five preimages $\zeta_5^{(k)}$. If we move on a path through 1 in the codomain, we observe that the fibers of traversed points form five preimage paths. These preimage paths intersect in 0, for it is the only preimage of the zero 0; however, the zero's multiplicity is 5, and in an environment of 0, the fibers of all points (except 0) contain five elements. Therefore we can count the fiber elements by determining the zero's multiplicity. See Example 5.5.

Example 5.5. Let us forget elliptic curves for a moment and regard the complex function $\mathbb{C} \to \mathbb{C}$, $z \mapsto z^5$. The field $\mathbb{C}$ is algebraically closed, so 1 has five preimages $\zeta_5^{(k)}$, $k = 0, \ldots, 4$: the fifth roots of unity, which Figure 5.6 depicts. As we move through 1 along the real axis in the codomain, we observe that the fibers of the traversed points form five paths in the preimage. Their direction and curvature depends on the movement in the codomain; other image paths yield five different preimage paths. At 0, all preimage paths intersect, thus 0 has only one preimage. However, if we continue to consider the preimage paths as separate entities, then each path contributes to the zero of $z \mapsto z^5$ at 0. In this way we obtain an interpretation for the zero's multiplicity 5 as the number of preimage paths running through it.

We may also take the opposite perspective: if we have a polynomial b with a zero at α of multiplicity k, then we may write

$$b(z) = (z - \alpha)^k \cdot \hat{b}(z)$$

with $\hat{b}(\alpha) \neq 0$ because $\mathbb{C}$ is algebraically closed. The factor $(z - \alpha)^k$ behaves like the initial example $z \mapsto z^5$, shifted by α; the fibers of elements in an environment of 0 thus contain k preimages. The other factor $\hat{b}(z)$ does not interfere because polynomials are continuous, which implies that $\hat{b}(z)$ is non-zero in an environment of α. The values of $\hat{b}(z)$ hence scale and rotate, but cannot cancel preimages around α.

Collecting our observations, we may count the preimage paths of a polynomial that intersect at α by determining the multiplicity k of the zero at α; by continuity, the same works for rational functions. Since the paths seem to spread out from α, we call α a *ramification point*. In a sufficiently small environment of α, the fibers of all points except α will contain exactly k elements.

Back to elliptic curves. We want to examine how an endomorphism η collapses points and find a link to its behavior on ℓ-torsion groups. The component

functions of η are rational; their domain is an algebraically closed field. Thus the situation resembles the example and the number of elements in a fiber provides us insight into the collapsing.

To count the elements in the fiber of a point P, we convert η into a rational function f that is zero at P. The number of fiber elements then equals the multiplicity of the zero of f at P. Therefore we set $f = e \circ \eta$, where e is a uniformizer at $\eta(P)$. It is irrelevant that η is an endomorphism, so we generalize our idea to rational maps.

Definition 5.7. Let F be a rational map that is not identically zero. Furthermore let P be a point on the curve, and e be a uniformizing variable at $F(P)$. Then the *ramification index* of F at P is

$$\mathrm{ram}_P(F) = \mathrm{ord}_P(e \circ F).$$

Note that the definition is independent of the specific choice of e. Furthermore note that the rational function $e \circ F$ has a zero at P, so $\mathrm{ram}_P(F) \geq 1$; also, $e \circ F$ is the same function for all preimages of $F(P)$.

Next we break down the problem of determining the ramification index of rational maps into smaller parts: instead of looking at the map as a whole, we study the contributions of its components. If we understand the effects of function composition on the ramification index, we can determine the index for the parts and combine these results. Furthermore, we may use transformations to simplify rational maps of interest.

Composition of rational maps reduces to composition of a rational function with a rational map:

$$(f, g) \circ H = (f \circ H, g \circ H).$$

Hence we start with this case.

Lemma 5.8. *Let F be a non-constant rational map, and g be a rational function that is not identically zero. For any point P on the curve*

$$\mathrm{ord}_P(g \circ F) = \mathrm{ord}_{F(P)}(g) \cdot \mathrm{ram}_P(F).$$

Proof. Recall that the order of the rational function $g \circ F$ at P is the exponent k of the uniformizer e at P in $g \circ F = e^k \cdot h$, where h is finite and non-zero at P. To show the proposition, we uniformize the components of $g \circ F$ accordingly.

Write $g = d^i \cdot \hat{g}$ with d a uniformizer at $F(P)$ and $\hat{g}$ finite and non-zero at $F(P)$. Then

$$g \circ F = (d^i \cdot \hat{g}) \circ F = (d \circ F)^i \cdot (\hat{g} \circ F).$$

Using the uniformizer e at P, we next decompose the rational function $d \circ F$ into $e^j \cdot \hat{f}$ with $\hat{f}$ finite and non-zero at P. Above equation yields

$$g \circ F = (d \circ F)^i \cdot (\hat{g} \circ F) = (e^j \hat{f})^i \cdot (\hat{g} \circ F) = e^{ij} \cdot \hat{f}^i \cdot (\hat{g} \circ F).$$

Clearly, $\hat{g} \circ F$ is finite and non-zero at P. Setting $h = \hat{f}^i \cdot (\hat{g} \circ F)$, we therefore obtain our desired expression $g \circ F = e^k \cdot h$. Thus

$$\mathrm{ord}_P(g \circ F) = k = i \cdot j = \mathrm{ord}_{F(P)}(g) \cdot \mathrm{ram}_P(F),$$

since $i = \mathrm{ord}_{F(P)}(g)$ and $j = \mathrm{ord}_P(d \circ F) = \mathrm{ram}_P(F)$ by construction. □

The lemma easily extends to rational maps.

Lemma 5.9. *Let F and G be non-constant rational maps. Then the rational map $F \circ G$ is non-constant and its ramification index at any point P is*

$$\operatorname{ram}_P(F \circ G) = \operatorname{ram}_{G(P)}(F) \cdot \operatorname{ram}_P(G).$$

Proof. The rational maps F and G are non-constant and therefore surjective, see Lemma 5.4. Their composition then is surjective, too, and thus non-constant.

For e a uniformizing variable at $F\big(G(P)\big)$, the multiplicative identity follows from

$$\begin{aligned}\operatorname{ram}_P(F \circ G) &= \operatorname{ord}_P(e \circ F \circ G) \\ &= \operatorname{ord}_{G(P)}(e \circ F) \cdot \operatorname{ram}_P(G) \\ &= \operatorname{ram}_{G(P)}(F) \cdot \operatorname{ram}_P(G),\end{aligned}$$

where we obtained the second equality by applying the previous lemma to the rational function $e \circ F$. □

To determine the ramification index of endomorphisms, we exploit that they preserve the group structure: similarly to subsection 2.2.2, we shift the input of η. We then know how the composition behaves, and the previous lemma tells us how the ramification index changes. From a comparison of effects, we derive the following theorem:

Theorem 5.10. *The ramification index $\operatorname{ram}_P(\eta)$ of a non-zero endomorphism $\eta : E(\overline{\mathbb{F}}) \to E(\overline{\mathbb{F}})$ is independent of the point P.*

Proof. Let T'_Q denote translation by Q, $P \mapsto P + Q$; observe that unlike $T_P : \mathbb{F}(E) \to \mathbb{F}(E)$ from Definition 2.41, it is a rational map. Then

$$(\eta \circ T'_Q)(P) = \eta(P) + \eta(Q) = (T'_{\eta(Q)} \circ \eta)(P)$$

for any point P because η is an endomorphism. Applying the previous lemma to the ramification index of both sides at the point at infinity yields

$$\operatorname{ram}_{T'_Q(\mathcal{O})}(\eta) \cdot \operatorname{ram}_{\mathcal{O}}(T'_Q) = \operatorname{ram}_{\eta(Q)}(T'_{\eta(Q)}) \cdot \operatorname{ram}_{\mathcal{O}}(\eta).$$

Observe that translation T'_Q by Q has ramification index 1. Expanding the definition yields

$$\operatorname{ram}_P(T'_Q) = \operatorname{ord}_P(e \circ T'_Q) = \operatorname{ord}_P\big(T_Q(e)\big),$$

where e is a uniformizer at $T'_Q(P) = P + Q$. By Lemma 2.42, $T_Q(e)$ then is a uniformizer at $P + Q - Q = P$, and thus has a single zero at P. Furthermore we know that $T'_Q(\mathcal{O}) = Q$, so the equation becomes

$$\operatorname{ram}_Q(\eta) = \operatorname{ram}_{\mathcal{O}}(\eta);$$

this proves the proposition because the point Q is arbitrary. □

Let us transfer this result to our original question of how an endomorphism η collapses points. Equivalently we may ask how many elements the fiber of a point contains.

On the one hand, we have the same ramification index for every point, and therefore the same number of elements in its fiber. On the other hand, η is interchangeable with addition; for any preimage P of Q we have

$$P = \eta(Q) = \eta(Q) + \mathcal{O} = \eta(Q + R),$$

where R is in the kernel of η. Thus kernel elements produce additional preimages that do not add to the multiplicity of the zero of $e \circ \eta$ at P, and hence do not influence the ramification index. Rather, they introduce additional zeros at $P+R$. Putting both sources of preimages together, we see that an endomorphism maps $\mathrm{ram}_P(\eta) \cdot |\mathrm{Ker}(\eta)|$ points onto P.

Definition 5.11. The *degree* of a non-zero endomorphism η of an elliptic curve is

$$\deg(\eta) = \mathrm{ram}_P(\eta) \cdot |\mathrm{Ker}(\eta)| .$$

Up to this point, we followed intuition in our reasoning about the relation between the mapping behavior of endomorphisms and their determinant on ℓ-torsion groups. The next theorem links degree and determinant more rigorously.

Theorem 5.12. *Let E be an elliptic curve over any field $\mathbb{F}$ and let P, P_1, P_2, Q, Q_1, $Q_2 \in E[\ell]$ be ℓ-torsion points. Then there exists a map $w : E[\ell] \times E[\ell] \to \overline{\mathbb{F}}$ with the following properties:*

(i) The value $w(P, Q)$ is an ℓ-th root of unity in $\overline{\mathbb{F}}$.

(ii) The map w is bilinear, so

$$w(P_1 + P_2, Q) = w(P_1, Q) + w(P_2, Q)$$

and

$$w(P, Q_1 + Q_2) = w(P, Q_1) + w(P, Q_2).$$

(iii) It is alternating: $w(P, Q) = w(Q, P)^{-1}$.

(iv) It is non-degenerate, that is, if $w(P, Q) = 1$ for all $P \in E[\ell]$, then $Q = \mathcal{O}$.

(v) For any endomorphism η,

$$w\big(\eta(P), \eta(Q)\big) = w(P, Q)^{\deg(\eta)}.$$

Proof. Unfortunately the proof requires a deeper theory of divisors and how endomorphisms affect them—a topic that is beyond the scope of this thesis. Therefore we refer to the expository report of Charlap and Robbins for a complete elementary proof [2, thm. 13.6]. The books of Silverman [29, sec. III.8] and Washington [31, sec. 11.2] include other proofs that use more abstract language. □

Definition 5.13. We call the map w of Theorem 5.12 the *Weil pairing.*

The last of above properties of the Weil pairing links the local and global mapping behavior of endomorphisms. In the next theorem, we translate this connection to our initial problem of finding the determinant of an endomorphism on ℓ-torsion groups.

Theorem 5.14. *Let η be a non-zero endomorphism and ℓ be prime to the field characteristic. Then the determinant of η on $E[\ell]$ is the degree of η modulo ℓ:*

$$\det(\eta) \equiv \deg(\eta) \mod \ell.$$

Proof. Choose any basis P, Q of $E[\ell] \simeq \mathbb{Z}_\ell \times \mathbb{Z}_\ell$. Then the images of P and Q are linear combinations

$$\eta(P) = j_1 P + j_2 Q \qquad \text{and} \qquad \eta(Q) = k_1 P + k_2 Q,$$

and the determinant of η is $\det(\eta) = j_1 k_2 - j_2 k_1$.

Inserting these expressions into item (v) of Theorem 5.12 yields

$$\begin{aligned} w(P,Q)^{\deg(\eta)} &= w\big(\eta(P), \eta(Q)\big) \\ &= w(j_1 P + j_2 Q, k_1 P + k_2 Q) \\ &= w(P,P)^{j_1 k_1} \cdot w(P,Q)^{j_1 k_2} \cdot w(Q,P)^{j_2 k_1} \cdot w(Q,Q)^{j_2 k_2} \\ &= w(P,Q)^{j_1 k_2} \cdot w(Q,P)^{j_2 k_1} \\ &= w(P,Q)^{j_1 k_2} \cdot w(P,Q)^{-j_2 k_1} \\ &= w(P,Q)^{\det(\eta)}. \end{aligned}$$

To complete the proof, we show that $w(P,Q)$ is a primitive ℓ-th root of unity; above equation then implies the proposition: suppose $w(P,Q)^m = 1$. Then $w(m \cdot P, Q) = 1$ and hence $w(m \cdot P, j_1 P + j_2 Q) = 1$ for all $j_1, j_2 \in \mathbb{Z}$. Therefore we must have $m \cdot P = \mathcal{O}$ and ℓ divides m. □

Let us revisit the characteristic polynomial χ_φ of the Frobenius endomorphism φ on $E[\ell]$. In Equation 4.12 we used the theorem of Cayley-Hamilton to construct a computable test for guesses about the determinant $\det(\mathrm{id} - \varphi)$ on $E[\ell]$. We had

$$\chi_\varphi(\varphi) = \varphi \circ \varphi - [1 + \det(\varphi) - \det(\mathrm{id} - \varphi)] \circ \varphi + [\det(\varphi)] = \overline{\mathcal{O}} \quad \text{on } E[\ell].$$

Enter the Weil pairing: combining Theorem 5.14 with the equation yields

$$\varphi \circ \varphi - [1 + \deg(\varphi) - \deg(\mathrm{id} - \varphi)] \circ \varphi + [\deg(\varphi)] = \overline{\mathcal{O}} \mod \ell, \tag{5.15}$$

where mod ℓ means that the integer factors of the multiplication maps are taken modulo ℓ.

Thus the Weil pairing transports the global information of the degrees of φ and $(\mathrm{id} - \varphi)$ to their local interpretation as linear maps on an ℓ-torsion group $E[\ell]$. Conversely, the Weil pairing globalizes local information: Equation 5.15

holds for *any* ℓ prime to the field characteristic. The congruences therefore fulfill an infinite number of equations; their solution hence is unique without modulus.

Consequently, we can define global versions of the local properties of the Frobenius endomorphism that we derived from the characteristic polynomial at the end of chapter 4.

Definition 5.16. We call Equation 5.15 the *characteristic equation* of the Frobenius endomorphism on the ℓ-torsion group $E[\ell]$, or *Frobenius equation* for short. The *trace* of the Frobenius endomorphism on $E[\ell]$ is

$$\mathrm{tr}(\varphi) = 1 + \deg(\varphi) - \deg(\mathrm{id} - \varphi) \mod \ell. \tag{5.17}$$

All we need to make the Frobenius equation into a test for guesses about $|\mathrm{Ker}(\mathrm{id} - \varphi)| = |E(\mathbb{F}_q)|$ are: the degree $\deg(\varphi)$ of the Frobenius endomorphism, and the ramification index $\mathrm{ram}_P(\mathrm{id} - \varphi)$. For the latter, recall that

$$\deg(\mathrm{id} - \varphi) = |\mathrm{Ker}(\mathrm{id} - \varphi)| \cdot \mathrm{ram}_P(\mathrm{id} - \varphi).$$

5.2 Scalars in the Frobenius Equation

We close the chapter with the computation of the degree of the Frobenius endomorphism φ and the ramification index of $(\mathrm{id} - \varphi)$.

Degree of the Frobenius Endomorphism

Let us first examine the Frobenius endomorphism on $E(\overline{\mathbb{F}}_q)$, $\varphi(\alpha, \beta) = (\alpha^q, \beta^q)$. The component functions of φ are polynomials. These have their only pole at the point at infinity $\mathcal{O}$, so the kernel of φ must be trivial: $\mathrm{Ker}(\varphi) = \{\mathcal{O}\}$. Furthermore, the ramification index of φ at $\mathcal{O}$ is q: if $e = x/y$ is a uniformizer at $\mathcal{O}$, then $e \circ \varphi = x^q/y^q = e^q$, which clearly has a zero of order q at $\mathcal{O}$. In summary, we have shown the following lemma:

Lemma 5.18. *The degree of the Frobenius endomorphism on $E(\overline{\mathbb{F}}_q)$ is q:*

$$\deg(\varphi) = q.$$

Proof. By Theorem 5.10, the ramification index of endomorphisms is independent of the point. Thus, above discussion proves

$$\deg(\varphi) = \mathrm{ram}_{\mathcal{O}}(\varphi) \cdot |\mathrm{Ker}(\varphi)| = q \cdot 1.$$

□

Ramification Index of $(\mathrm{id} - \varphi)$

Next we examine the map $(\mathrm{id} - \varphi)$ to determine its ramification index. We have shown above that φ has ramification index q by exposing a zero of multiplicity q in the composition of φ with a uniformizer at $\mathcal{O}$; from its Definition 5.7 we see that such a repeated zero is necessary for a ramification index greater 1. Furthermore we see that the repeated zeros must originate in the component

functions of the endomorphism, for uniformizers have single zeros at their point of definition. Hence, the numerator or denominator polynomials of the component functions must have a degree greater 1 to yield a ramification index greater 1.

However, the exponents of the involved polynomials cannot be arbitrary: an endomorphism $\eta = (f, g)$ preserves the group structure, so

$$(f, g)(P + Q) = (f, g)(P) + (f, g)(Q)$$

for all points P, Q, where both additions are point additions. Expanding the case $Q \neq P, -P$ with the generic addition formula of Definition 1.6 thus yields the following equation for the first component function:

$$f(P + Q) = -f(P) - f(Q) + \Big(\frac{g(Q) - g(P)}{f(P) - f(Q)}\Big). \tag{5.19}$$

If the polynomials that comprise f and g have degree greater 1, then the mixed terms of point sums must vanish similarly to the binomial theorem in $\overline{\mathbb{F}}_q$,

$$(\alpha, \beta)^q = \alpha^q + \beta^q,$$

compare Lemma 4.5. More generally, in fields of characteristic $p > 0$, this *freshman's dream* expansion is available if, and only if, p divides the exponent: we have

$$(\alpha + \beta)^n = \alpha^n + \beta^n + \sum_{k=1}^{n} \binom{n}{k} \alpha^k \beta^{n-k},$$

so the last term must vanish for arbitrary field elements α and β. Since the binomial coefficients $\binom{n}{k}$ are non-negative, the sum can evaluate to zero only if all of them are zero. If n is a multiple of p, then this is the case. Otherwise we have $n = p \cdot q + r$ with $0 < r < p$, and the binomial coefficients $\binom{n}{k}$ with $1 \leq k \leq r$ and $n - r \leq k \leq n - 1$ are non-zero modulo p.

While above discussion is far from compelling, it suggests that the field characteristic p divides the exponents of component functions of endomorphisms with ramification index greater 1. Unfortunately I could not find a constructive way to show this; instead, we use the derivation of subsection 2.2.4: derivation of powers that are multiples of p results in coefficients that are multiples of p— and these vanish. This way we obtain a criterion to distinguish endomorphisms of ramification index greater 1 from those with ramification index 1.

We develop the tool step by step: first we establish the link between the exponents and an identically zero derivative for rational functions in one indeterminate and on elliptic curves. Then we connect zero derivatives of endomorphisms to the ramification index. Finally, we combine the results and see that the exponents of the component functions must be multiples of the field characteristic if an endomorphism has ramification index greater 1.

Lemma 5.20. *Let h be a rational function of the single variable x over $\overline{\mathbb{F}}_q$ with $q = p^k$. If its (customary) derivative h' is identically zero, then $h(x) = \hat{h}(x^p)$ for some rational function $\hat{h}$.*

Proof. The proposition clearly holds for polynomials: constant terms have a zero derivative, but ignore the input, so writing x^0 or $(x^p)^0$ is irrelevant. Derivations of higher powers are identically zero only if the field characteristic p divides the exponent.

Suppose $h = a/b$ with a and b relatively prime polynomials in x. An identically zero derivative h' implies $a'b = ab'$, and because a and b are relatively prime, a divides a' and b divides b'. Differentiating removes zeros from polynomials, and thus linear factors, so a' and b' can be multiples of a and b only if they are identically zero. Therefore a and b are functions in x^p, and so is h. □

Lemma 5.21. *Let $f \in \mathbb{F}_q(E)$ be a rational function on the elliptic curve E over $\mathbb{F}_q$, $q = p^k$, with an identically zero derivative $\mathrm{D}f$. Then there exists a rational function $\hat{f} \in \mathbb{F}_q(E)$ such that*

$$f(x, y) = \hat{f}(x^p, y^p).$$

Proof. We begin by writing f in canonical form, and later use the previous lemma: let $f(x, y) = \big(a(x) + yb(x)\big)/\big(c(x) + yd(x)\big)$ with polynomials a, b, c, and d in x alone. Then $c(x)+yd(x)$ is not identically zero, and therefore neither is $c(x) - yd(x)$. Thus

$$\begin{aligned} f(x, y) &= \frac{a(x) + yb(x)}{c(x) + yd(x)} \cdot \frac{c(x) - yd(x)}{c(x) - yd(x)} \\ &= \frac{(ac)(x) + y(bc - ad)(x) - y^2(bd)(x)}{c^2(x) - y^2 d^2(x)} \\ &= g(x) + yh(x), \end{aligned}$$

where g and h are rational functions in x alone. Writing

$$y = y \cdot \Big(\frac{x^3 + Ax + B}{x^3 + Ax + B}\Big)^{(p-1)/2} = y^p \cdot \frac{1}{(x^3 + Ax + B)^{(p-1)/2}}$$

and setting $\hat{h}(x) = h(x)/(x^3 + Ax + B)^{(p-1)/2}$, we obtain a representation of f with rational functions g, $\hat{h}$ whose only variable is x:

$$f(x, y) = g(x) + y^p \hat{h}(x).$$

Combination with the identically zero derivative $\mathrm{D}f$ yields

$$\begin{aligned} \mathrm{D}f(x, y) &= 2y \cdot g'(x) + p \cdot y^{p-1}\hat{h}(x) + 2y \cdot \hat{h}'(x) \\ &= \big(g'(x) + y^p \hat{h}'(x)\big) \cdot 2y = 0; \end{aligned}$$

hence g' and $\hat{h}'$ must, too, be identically zero and by the previous lemma functions in x^p. Thus the proof is complete. □

Theorem 5.22. *An endomorphism η of an elliptic curve E over a finite field $\mathbb{F}_q$ has ramification index greater 1 if, and only if, for all rational functions $f \in \mathbb{F}_q(E)$ the derivative $\mathrm{D}(f \circ \eta)$ is identically zero. In symbols:*

$$\mathrm{ram}_P(\eta) > 1 \qquad \Leftrightarrow \qquad \mathrm{D}(f \circ \eta) = 0 \quad \textit{for all } f \in \mathbb{F}_q(E).$$

Proof. Suppose $\mathrm{D}(f \circ \eta) = 0$ for all rational functions f. A uniformizing variable e at $\eta(P)$ for some point P is a rational function, so $\mathrm{D}(e \circ \eta) = 0$. By the previous lemma, the rational function $e \circ \eta$ hence is a function in x^p and y^p, thus has order greater 1 at P, and therefore has a ramification index greater 1; compare Definition 5.7.

Conversely, assume that there exists a rational function f and a point P with $\big(\mathrm{D}(f \circ \eta)\big)(P) \neq 0$. Then we construct a rational function with a single zero at P and obtain ramification index 1 for η from the composition rule of Lemma 5.8: for $g = f - f\big(\eta(P)\big)$, we have $(g \circ \eta)(P) = 0$ and

$$\big(\mathrm{D}(g \circ \eta)\big)(P) = \big(\mathrm{D}(f \circ \eta)\big)(P) \neq 0.$$

Therefore

$$1 = \mathrm{ord}_P(g \circ \eta) = \mathrm{ord}_{\eta(P)}(g) \cdot \mathrm{ram}_P(\eta),$$

which forces $\mathrm{ram}_P(\eta) = 1$. □

Now we can confirm our intuition about the exponents of component functions of endomorphisms by combining Theorem 5.22 with Lemma 5.21.

Corollary 5.23. *An endomorphism η has ramification index greater 1 if, and only if, its component functions are functions in x^p and y^p:*

$$\mathrm{ram}_P(\eta) > 1 \qquad \Leftrightarrow \qquad \eta(x, y) = \big(\hat{f}(x^p, y^p), \hat{g}(x^p, y^p)\big).$$

Proof. By Theorem 5.22, an endomorphism $\eta = (f, g)$ has ramification index greater 1 if, and only if, $\mathrm{D}(x \circ \eta) = \mathrm{D}f = 0$ and $\mathrm{D}(y \circ \eta) = \mathrm{D}g = 0$. Lemma 5.21 then tells us that both component functions f and g are functions in x^p and y^p. Of course, if they are functions of x^p and y^p, then their derivative vanishes on $\overline{\mathbb{F}}_q$ and the proof is complete. □

Compositions of rational functions in x^p and y^p, as in the addition on the curve of rational maps, produce rational function in x^p and y^p. Therefore above corollary tells us that the set of endomorphisms with ramification index greater 1 is closed under addition.

Corollary 5.24. *Let E be an elliptic curve over $\mathbb{F}_q$ and η_1, $\eta_2 \in E\big(\mathbb{F}_q(E)\big)$ be endomorphisms on E with ramification index greater 1. Then their sum has ramification index greater 1:*

$$\mathrm{ram}_P(\eta_1 + \eta_2) > 1.$$

Finally we return to our endomorphism of interest: $\mathrm{id} - \varphi$. We already know that the ramification index of φ is $q > 1$; furthermore $\mathrm{ram}_P(\mathrm{id}) = 1$, for the uniformizer $x/y = (x/y) \circ \mathrm{id}$ at $\mathcal{O}$ has a single zero at $\mathcal{O}$. Closure under addition for endomorphisms of ramification index greater 1 then implies the following lemma, which completes our search for the scalars in the characteristic equation (5.15) of the Frobenius endomorphism:

Lemma 5.25. *The ramification index of $(\mathrm{id} - \varphi)$ is 1; $\mathrm{ram}_P(\mathrm{id} - \varphi) = 1$.*

Proof. Let $\eta = \mathrm{id} - \varphi$ and suppose $\mathrm{ram}_P(\eta) > 1$. Then Corollary 5.24 would imply

$$\mathrm{ram}_P(\mathrm{id}) = \mathrm{ram}_P(\eta + \varphi) > 1,$$

which contradicts above discussion. Hence we must have $\mathrm{ram}_P(\mathrm{id} - \varphi) = 1$. □

Chapter 6

Schoof's Algorithm

The present chapter explains a point counting algorithm for elliptic curves over finite fields that bases on the results of the previous chapters. René Schoof proposed (a slightly enhanced version of) this algorithm in his 1985 article *Elliptic Curves Over Finite Fields and the Computation of Square Roots mod p* [27].

Note 6.1. In this chapter, we assume q to be a prime number, not a prime power. Thus $q = p^1$ and $\mathbb{F}_q = \mathbb{F}_p$ is a prime field. For emphasis, we write p in place of q at all occurrences. This limitation allows a clearer and easier exposition of the underlying ideas. It should not be mistaken for a mandatory precondition; Lercier and Morain [13] extend the algorithm to fields of prime power size using deeper results by Couveignes [3, 4].

6.1 Concept

Schoof's algorithm finds the number of points on an elliptic curve over a finite field by guessing the trace of the Frobenius endomorphism modulo small primes, verifying the guesses with the Frobenius equation, and assembling them into a unique solution.

Verifying guesses

In Equation 5.15, we used the Weil pairing to replace the determinants in the characteristic equation of the Frobenius endomorphism with respective degrees of endomorphisms. This yielded

$$\varphi \circ \varphi - [1 + \deg(\varphi) - \deg(\mathrm{id} - \varphi)] \circ \varphi + [\deg(\varphi)] = \overline{\mathcal{O}} \mod \ell,$$

where ℓ is prime to the field characteristic, and mod ℓ means that the integer factors of the multiplication maps are taken modulo ℓ. In Lemma 5.18 and Lemma 5.25, we determined the appearing endomorphism degrees on an elliptic curve $E(\overline{\mathbb{F}}_p)$ as

$$\deg(\varphi) = p \qquad \text{and} \qquad \deg(\mathrm{id} - \varphi) = |\mathrm{Ker}(\mathrm{id} - \varphi)|\,.$$

The map $(\mathrm{id} - \varphi)$ characterizes the $\mathbb{F}_p$-rational points on $E(\overline{\mathbb{F}}_p)$, so we have $|\mathrm{Ker}(\mathrm{id} - \varphi)| = |E|$ for $E = E(\mathbb{F}_p)$; the characteristic equation thus becomes

$$\varphi \circ \varphi - [1 + p - |E|] \circ \varphi + [p] = \overline{\mathcal{O}} \mod \ell \tag{6.2}$$

on the ℓ-torsion group $E[\ell]$.

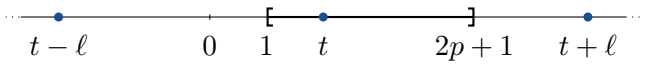

Figure 6.3: Representatives of a residue class $(t \bmod \ell) = t+\ell\cdot\mathbb{Z}$ have distance ℓ. If ℓ is strictly greater than the length of the interval $[1, 2p+1]$, then the representative in the interval is unique.

To find $|E|$, we therefore guess $t = 1 + p - |E|$ modulo ℓ and verify that the rational map

$$\varphi \circ \varphi - [t] \circ \varphi + [p] \mod \ell$$

yields $\mathcal{O}$ for all ℓ-torsion points.

Assembling the solution

If we choose ℓ large enough, then the residue class $(t \bmod \ell)$ contains a unique solution: the group order $|E|$ lies between 1 and $2p + 1$ because the point at infinity is always an element on E; furthermore each of the p possible values for the first coordinate belongs to at most two points. Hence, any torsion $\ell > (2p+1)-1 = 2p$ yields a unique solution, for the representatives of $(t \bmod \ell) = t+\ell\cdot\mathbb{Z}$ have distance ℓ; see Figure 6.3.

Choosing such a large torsion is, however, a bad decision from a practical perspective: we lack explicit knowledge of the ℓ-torsion points and instead use arithmetic in the field of rational functions on E modulo the ℓ-th division polynomial. The degree of the division polynomials grows quadratically, so the computations quickly become expensive. A better approach is to use several small torsions ℓ_i and apply the Chinese Remainder Theorem.

Theorem 6.4 (Chinese Remainder Theorem)**.** *Let $t_1, \ldots, t_k$ and $\ell_1, \ldots, \ell_k$ be integers with $\ell_i > 0$ for $i = 1, \ldots, k$. Furthermore assume that ℓ_i and ℓ_j are relatively prime if $i \neq j$. Then there exists a common solution z of the system of congruences*

$$\begin{aligned} z &\equiv t_1 \mod \ell_1 \\ z &\equiv t_2 \mod \ell_2 \\ &\vdots \\ z &\equiv t_k \mod \ell_k. \end{aligned}$$

Proof. We multiply every remainder t_i with a factor that is 1 modulo ℓ_i and that vanishes modulo ℓ_j if $i \neq j$. The sum of these products then solves every congruence in the system. Put

$$\ell = \prod_{i=1}^{k} \ell_i$$

and $\hat{\ell}_i = \ell/\ell_i$ so that $\hat{\ell}_i \equiv 0 \mod \ell_j$, if $i \neq j$. Since $\hat{\ell}_i$ and ℓ_i are relatively prime, there exists an integer m_i with $m_i \cdot \hat{\ell}_i \equiv 1 \mod \ell_i$. Setting

$$z = \sum_{i=1}^{k} t_i m_i \hat{\ell}_i,$$

we have $z \equiv t_i m_i \hat{\ell}_i \equiv t_i \mod \ell_i$ and the proof is complete. □

The Chinese Remainder Theorem yields a congruence class $z \mod \prod \ell_i$; above remark about the possible range of t then tells us that we have to choose torsions ℓ_i such that $\prod \ell_i > 2p$. The ℓ_i should be small, pair-wise prime, and also prime to the field characteristic p. Thus we simply use the first few primes $2, 3, 5, \ldots$ except p whose product exceeds $2p$.

Putting all together

We count the points on an elliptic curve E over a finite field $\mathbb{F}_p$ as $|E| = 1+p-t$, where t is the trace of the Frobenius endomorphism. The trace t, in turn, we find with Algorithm 6.5. Note that the Frobenius equation holds for exactly one candidate t_i because Equation 5.17 uniquely determines the trace for any torsion prime to the field characteristic.

For each prime ℓ_i of the first primes with $\prod \ell_i > 2p$: (Outer part)
    For each trace candidate $t_i \in \mathbb{Z}_{\ell_i}$: (Inner part)
        For each ℓ_i-torsion point $P \in E[\ell_i]$:
            If the Frobenius equation (6.2) is wrong for t_i and P:
                Try the next t_i.
        # If we reach this line, then all points passed the test.
        Remember that $t \equiv t_i \mod \ell_i$.
        Advance to the next torsion ℓ_i.
Solve $t \equiv t_i \mod \ell_i$ with the Chinese Remainder Theorem.
Return the unique representative of $(t \mod \prod \ell_i)$ in $[1, 2p+1]$.

Algorithm 6.5: Determining the trace of the Frobenius endomorphism of an elliptic curve E over a finite field $\mathbb{F}_p$.

6.2 Asymptotic Complexity

Our motivation for the preceding discussion was to speed up the point counting process. We saw the brute-force approach on page 3 fail in a cryptographic setting, for the required field sizes become too large; the asymptotic complexity of the approach is $O(p)$, which is exponential in the length of p. The present section comments on the asymptotic worst-case complexity of Algorithm 6.5.

Three loops dominate the execution time of Algorithm 6.5: the iterations over the torsions ℓ_i, the trace candidates t_i, and the ℓ_i-torsion points. We neglect the two final computations because the torsions limit the size of the Chinese Remainder Theorem argument, and finding a representative in an ordered interval is easy.

In the worst case, each step of every loop leads to one evaluation of the Frobenius equation. In the average case, early matches of candidates might advance the iteration faster; however, we cannot guarantee that this will happen and so take a pessimistic perspective.

To count the iterations, first note that an actual implementation will test the Frobenius equation for only one point $(x, y) \in E\big(\mathbb{F}_p(E)/\psi_\ell\big)$; see Lemma 3.29. Thus we only pretend to iterate over all ℓ_i-torsion points for emphasis what is meant.

Second, the number of trace candidates $t_i \in \mathbb{Z}_{\ell_i}$ clearly is at most $|\mathbb{Z}_{\ell_i}| = \ell_i$.

Third, we can estimate the number of torsions ℓ_i: a statement equivalent to the prime number theorem is

$$\lim_{k\to\infty} \frac{1}{k} \sum_{\substack{\ell \le k,\\ \ell \text{ prime}}} \log \ell = 1.$$

Hence

$$\prod_{\substack{\ell \le k,\\ \ell \text{ prime}}} \ell \approx e^k,$$

so to make the product larger than $2p$, we choose $k \approx \log 2p$. There are $O(\log p/\log\log p)$ primes less than $O(\log p)$, which is how often the outermost loop executes.

In conclusion, the number of computed instances of the Frobenius equation in Algorithm 6.5 is

$$\underbrace{O(\log p/\log\log p)}_{\text{Torsions}} \cdot \underbrace{O(\log p)}_{\text{Candidates}} = O\big((\log p)^2\big).$$

As noted above, verifying the Frobenius equation uses arithmetic on the curve $E\big(\mathbb{F}_p(E)/\psi_\ell\big)$. The asymptotic complexity therefore depends on the algorithms used for point addition and multiplication by integers on the curve. These, in turn, rely on the algorithms for operations in the field $\mathbb{F}_p(E)$, and thus in the polynomial ring $\mathbb{F}_p[E]$, which are implemented in terms of field operations in $\mathbb{F}_p$. Properly implemented, one computation of the Frobenius equation takes $O\big((\log p)^6\big)$ bit operations [29, p. 373], [1, p. 111]. With such arithmetic, the worst-case overall complexity of Algorithm 6.5 thus is

$$O\big((\log p)^2\big) \cdot O\big((\log p)^6\big) = O\big((\log p)^8\big).$$

Faster algorithms allow checking the Frobenius equation in $O\big((\log p)^3\big)$ [1, p. 111]. See the books of Blake et al. [1, ch. IV] and Hankerson et al. [8, ch. 3] for notes on fast elliptic curve arithmetic; Knuth [9, sec. 4.6] as well as Crandall and Pomerance [5, ch. 9] discuss polynomial arithmetic; the books of Menezes et al. [15, ch. 14], Blake et al. [1, ch. II], and Hankerson et al. [8, ch. 2] explain arithmetic in finite fields.

6.3 Python Implementation

This section discusses an implementation of Algorithm 6.5 in the Python programming language [22]. It focuses on the overall algorithm and assumes that the classes and auxiliary functions listed in Table 6.6 are available.

Class	Description
`Integers`	A wrapper that adds generic ring properties to Python's built-in integer type
`QuotientRing`	A quotient ring $R/(m)$; its elements are residue classes (r mod m) of ring elements $r \in R$ modulo a fixed $m \in R$
`Polynomials`	A ring of polynomials $\mathbb{F}[z]$ in one indeterminate with coefficients from a field $\mathbb{F}$
`FiniteField`	The finite field with p elements $\mathbb{F}_p$
`FractionField`	A field of formal fractions s/t, s, $t \in R$ over an integral domain R; compare Definition 2.14
`EllipticCurve`	An elliptic curve with parameters A and B; see Definition 1.1

Function	Description
`inverse_primorial()`	Returns the smallest prime p such that the product of all primes up to and including p (except one shunned prime) is greater than a given number
`primes_range()`	Returns a list of primes in a given interval
`gcd()`	Determines the greatest common divisor
`solve_congruence_equations()`	The Chinese Remainder Theorem; see Theorem 6.4
`representative_in_range()`	Returns the unique representative in a range; compare Figure 6.3

Table 6.6: The implementation of Schoof's algorithm in section 6.3 assumes that the listed classes and auxiliary functions are available.

6.3.1 Iteration Over Torsions

The function `frobenius_trace()` implements the outer part of Algorithm 6.5: it sets up the variables and iterates over the torsions ℓ_i. It expects its parameter `curve` to be an `EllipticCurve` instance.

```
def frobenius_trace(curve):
    # Initialize variables and parameters
    trace_congruences = []
    search_range = possible_frobenius_trace_range( curve.field() )
    upper_prime_bound = inverse_primorial(
                            len(search_range),
                            shunned = curve.field().characteristic()
                        )

    # Collect the congruence equations (avoid multivariate
    # polynomial arithmetic by handling 2-torsion separately)
    trace_congruences.append( frobenius_trace_mod_2( curve ) )

    torsion_group = LTorsionGroup( curve )
    for prime in primes_range( 3, upper_prime_bound+1 ):
        if prime != curve.field().characteristic():
            trace_congruences.append(
                    frobenius_trace_mod_l( torsion_group( prime ) )
                )

    # Recover the unique valid trace representative
    trace_congruence = solve_congruence_equations(
                                            trace_congruences
                                        )
    return representative_in_range( trace_congruence, search_range )
```

Initializing variables and parameters

The list `trace_congruences` collects the congruence equations $t \equiv t_i \mod \ell_i$; it is empty initially. The function `possible_frobenius_trace_range()` returns the interval $[1, 2p + 1]$ that must contain the trace of the Frobenius endomorphism. Note that the interval solely depends on the field $\mathbb{F}_p$. Since the product of the torsions ℓ_i must exceed the length of this interval, the inverse of the primorial function serves as an upper bound for the torsions: `inverse_primorial()` returns the smallest prime p such that the product of all primes up to and including p is greater than the function's argument. However, the torsions must be prime to the field characteristic. Therefore the `shunned` parameter marks the field characteristic as an exception that is not to be used as a factor.

Collecting congruence equations

Next the function collects the congruences of the trace modulo the torsions. In theory, arithmetic in the field of rational functions modulo the ℓ_i-th division polynomial ψ_{ℓ_i} allows testing rational map identities over an ℓ_i-torsion group; see section 3.3. Such computations work for any ℓ_i that is prime to the field characteristic; in particular, they work for $\ell_i = 2$.

In practice, however, we want to avoid the intricacies of multivariate polynomial division; such division is necessary for generic reduction modulo arbitrary ψ_{ℓ_i}. From their defining recurrence in Definition 3.17, we see that odd-index division polynomials ψ_{2k+1} contain only even powers of y. Their canonical form therefore is free of any powers of y; ψ_{2k+1} is a polynomial in x alone. Thus, univariate polynomial division suffices in the generic case of odd torsion. The only even prime is 2, so we remove 2 from the regular iteration over the torsions and handle it separately in the function `frobenius_trace_mod_2()`, which we explain below.

The function `frobenius_trace_mod_l()` computes the trace congruence in the generic case. It expects a torsion group as argument, for it uses the pseudo-iteration over all ℓ_i-torsion points mentioned in section 6.2. Thus the variable `torsion_group` is assigned a class of torsion groups over the input curve. An instance of this class is passed to `frobenius_trace_mod_l()` for every odd prime less than or equal to the upper torsion bound.

Remark 6.7. Although René Schoof does not say so explicitly, the same practical reason seems to motivate him to treat 2 separately from the other torsions in his article.

Recovering the trace

When the iteration over the torsions ℓ_i finishes, the list `congruence_equations` contains the Frobenius trace residue classes ($t_i \bmod \ell_i$). The trace t is then found by solving the equation system

$$t \equiv t_i \mod \ell_i$$

with the Chinese Remainder Theorem, which `solve_congruence_equations()` implements. Finally the function `representative_in_range()` determines the unique representative in the interval $[1, 2p+1]$.

6.3.2 Computation of Trace Congruences

The inner part of Algorithm 6.5 computes the residue classes of $t \bmod \ell_i$ for every torsion ℓ_i.

Odd torsion

The function `frobenius_trace_mod_l()` handles the generic case; it implements the concept of section 6.1 in a straight-forward way.

```
def frobenius_trace_mod_l(torsion_group):
    ints_mod_torsion = QuotientRing( Integers,
                                     torsion_group.torsion() )
    field_size = torsion_group.curve().field().size()

    for trace_candidate in range( 0, torsion_group.torsion() ):
        candidate_congruence = ints_mod_torsion( trace_candidate )
        for point in torsion_group.elements():
            if not frobenius_equation( candidate_congruence,
```

```
                                        field_size,
                                        point ):
                    # Exit inner loop and skip the 'else' clause.
                    break
            else:
                # Execute after the iteration completed; skip upon break.
                return candidate_congruence
```

First, the function prepares objects for later reference: it sets the variable `ints_mod_torsion` to $\mathbb{Z}_{\ell_i}$, and `field_size` to p. Then, it examines for every candidate congruence class ($t_i \bmod \ell_i$) whether the Frobenius equation holds for every ℓ_i-torsion point. Note that, as remarked above, the iteration over the ℓ_i-torsion points only serves for emphasis what the algorithm does; `torsion_group.elements()` returns a list with a single entry only: the point $(x, y) \in E\big(\mathbb{F}_p(E)/\psi_{\ell_i}\big)$.

The implementations of the Frobenius equation and the Frobenius endomorphism are naive transcriptions of Equation 6.2 and Definition 4.4 to Python. The parameter `size` is the field size p.

```
def frobenius_equation(trace, size, point):
    size_remainder = size % trace.modulus()
    result = frobenius( frobenius(point, size), size ) \
                - trace.remainder() * frobenius(point, size) \
                + size_remainder * point
    return result.is_infinite()

def frobenius(point, q):
    return point.__class__( point.x() ** q, point.y() ** q )
```

Torsion 2

Verifying the Frobenius equation on $E[2]$ uses arithmetic on $\mathbb{F}_p(E)$ modulo $\psi_2 = 2y$. This requires multivariate polynomial division, which complicates the implementation. One way to sidestep this requirement is to skip torsion 2. However, there are only two possibilities for the trace congruence modulo 2; furthermore we know from Example 2.4 what the 2-torsion points look like. This allows us to find the congruence with a different computation.

Recall that the 2-torsion points are

$$E[2] = \big\{\mathcal{O}, (\omega_1, 0), (\omega_2, 0), (\omega_3, 0)\big\};$$

the first coordinates of the finite points are the roots of the curve's defining polynomial $a(\alpha) = \alpha^3 + A\alpha + B \in \mathbb{F}_p[\alpha]$. Also, bring to mind that the polynomial $b(\alpha) = \alpha^p - \alpha \in \mathbb{F}_p[\alpha]$ characterizes the elements of $\mathbb{F}_p \subsetneq \overline{\mathbb{F}}_p$, compare Lemma 4.3. Thus, if a and b share a factor in $\mathbb{F}_p[\alpha]$, then at least one root of the defining polynomial is in $\mathbb{F}_p$, so at least one finite $\mathbb{F}_p$-rational point of order 2 exists.

If $(\omega_1, 0)$ and $(\omega_2, 0)$ are two finite $\mathbb{F}_p$-rational points of order 2, then $(\omega_3, 0) = (\omega_1, 0) + (\omega_2, 0)$ is $\mathbb{F}_p$-rational, too. Consequently the number of finite $\mathbb{F}_p$-rational points of order 2 is 0, 1, or 3. Hence, defining $\mathcal{O}$ as $\mathbb{F}_p$-rational, the set $E[2](\mathbb{F}_p)$

of $\mathbb{F}_p$-rational points of order 2 has even order if it contains at least one finite point, and odd order otherwise.

Intersections of subgroups are subgroups, so $E[2](\mathbb{F}_p) = E(\mathbb{F}_p) \cap E[2]$ is a subgroup of $E(\mathbb{F}_p) = E$. Therefore $|E[2](\mathbb{F}_p)|$ divides $|E|$. With $p+1$ always even, we thus can determine the parity of $t = p + 1 - |E|$ by testing whether a finite $\mathbb{F}_p$-rational point of order 2 exists. To summarize, t is odd if, and only if, the polynomials a and b are relatively prime:

$$t \equiv 1 \mod 2 \quad \Leftrightarrow \quad \gcd(\alpha^3 + A\alpha + B, \alpha^p - \alpha) = 1.$$

The function `frobenius_trace_mod_2()` implements this argument.

```
def frobenius_trace_mod_2(curve):
    R = Polynomials( curve.field() )

    x = R(0, 1)
    A, B = curve.parameters()

    defining_polynomial = x**3 + A*x + B
    rational_characteristic = x**curve.field().size() - x

    # gcd() has an arbitrary unit as leading coefficient;
    # relatively prime polynomials have a constant gcd.
    d = gcd( rational_characteristic, defining_polynomial )
    if d.degree() == 0:
        # The rational characteristic and the defining polynomial
        # are relatively prime: no rational point of order 2 exists
        # and the Frobenius trace must be odd.
        return QuotientRing( Integers, 2 )(1)
    else:
        return QuotientRing( Integers, 2 )(0)
```

6.3.3 Execution Profile

A rough quantitative analysis of the execution behavior completes our discussion of the implementation. The data comes from profiling the point counting of seven non-singular elliptic curves with random parameters over the finite field with $p = 4\,093$ elements. Table 6.8 lists the curve parameters, as well as the execution times and point counts.

Obviously the program is far too slow for practical use. Though the profiling introduces a major overhead, the speed up from disabling it is only linear. Consequently, using the 16-bit prime 65 521 instead of the 12-bit prime 4 093 resulted in time outs after 36 hours, even with profiling disabled.

Table 6.9 aggregates the data from the seven call profiles. It underlines the importance of fast arithmetic for elliptic curves, polynomial rings, and finite fields. The implementation thus cannot be fast, for the underlying classes of Table 6.6 use blatantly naive algorithms to be as easy to understand as possible: for example, points on elliptic curves are multiplied by an integer k by literally adding the point $(k-1)$-times. This algorithm has exponential complexity in the length of k.

A	B	$\lvert E(\mathbb{F}_{4093})\rvert$	*Time (h)*
3 005	2 016	4 120	3.1
1 881	2 267	4 028	4.8
2 955	1 331	4 158	6.7
3 499	322	4 066	10.4
1 926	3 026	4 130	14.4
7	3 697	4 059	17.7
461	112	4 058	20.4

Table 6.8: Elapsed time when counting the points on elliptic curves with randomly chosen parameters A and B over $\mathbb{F}_{4093}$ on an Intel Pentium 4 with 3.20 GHz running Linux 2.6.32.10 in multi-user mode. Profiling with the `cProfile` module was enabled; the interpreter was *CPython* 3.1.1 with byte code optimization (`-OO` flag). The execution time is the user time reported by the system; it is the time that the counting program actually executed on the processor, without I/O times and context switches.

The high variance comes from early matching candidate traces in the inner part of Algorithm 6.5: observe that $t = 4093 + 1 - 4120 = -26$ has remainders $1 \bmod 3$, $4 \bmod 5$, $2 \bmod 7$, $7 \bmod 11$, and $0 \bmod 13$. In contrast, $t = 4093 + 1 - 4058$ has remainders $0 \bmod 3$, $1 \bmod 5$, $1 \bmod 7$, $3 \bmod 11$, and $10 \bmod 13$. With the degree of the division polynomials growing quadratically, the effort for arithmetic modulo ψ_{13} dominates the execution time.

However, the table also reveals that almost half of the actual computation time is spent on constructing temporary objects for intermediate results. Python stores all objects on the heap [23], so memory allocation for the many small objects becomes a major problem. The lower arithmetic layers should thus be implemented in a language that places return values on the stack; only the high level objects, for instance $\mathbb{F}_p(E)/\psi_\ell$, should be exported to Python.

Time (%)		
Total	Self	Function name (Description)
100	2	`frobenius_trace` (Computation of $\mathrm{tr}(\varphi)$)
100	0	`naive_schoof_algorithm` (Main function)
98	1	`frobenius_equation` (Test trace candidate on $\chi_\varphi(\varphi) = \overline{\mathcal{O}}$)
98	0	`frobenius_trace_mod_l` (Computation of $\mathrm{tr}(\varphi) \mod \ell$)
98	0	`Q<E<GF<4093>>[x,y]/psi[l]>::__mul__` (Multiplication in $\mathbb{F}_{4093}(E)/\psi_\ell$)
98	0	`E<GF<4093>>[x,y]/psi[l]::__mul__` (Multiplication in $\mathbb{F}_{4093}[E]/\psi_\ell$)
97	0	`frobenius` (Frobenius endomorphism)
97	0	`Q<E<GF<4093>>[x,y]/psi[l]>::__pow__` (Exponentiation in $\mathbb{F}_{4093}(E)/\psi_\ell$)
57	0	`E<GF<4093>>[x,y]::__mod__` (Taking the remainder in $\mathbb{F}_{4093}[E]$)
57	0	`E<GF<4093>>[x,y]/psi[l]::__init__` (Object initialization)
57	0	`E<GF<4093>>[x,y]/psi[l]::<meta>__call__` (Object creation)
53	5	`GF<4093>[x]::__divmod__` (Division with remainder in $\mathbb{F}_{4093}[x]$)
44	24	`GF<4093>::<meta>__call__` (Object creation)
36	2	`GF<4093>[x]::__mul__` (Multiplication in $\mathbb{F}_{4093}[x]$)
35	0	`E<GF<4093>>[x,y]::__divmod__` (Division with remainder in $\mathbb{F}_{4093}[E]$)
33	14	`GF<4093>::__mul__` (Multiplication in $\mathbb{F}_{4093}$)
33	7	`GF<4093>::__sub__` (Subtraction in $\mathbb{F}_{4093}$)
32	14	`GF<4093>::__add__` (Addition in $\mathbb{F}_{4093}$)
26	0	`E<GF<4093>>[x,y]::__mul__` (Multiplication in $\mathbb{F}_{4093}[E]$)
20	20	`GF<4093>::__init__` (Object initialization)
11	3	`GF<4093>::__neg__` (Negation in $\mathbb{F}_{4093}$)
3	3	`GF<4093>::remainder` (Get the representative of $\alpha \in \mathbb{F}_{4093}$)

Table 6.9: Relative amount of time spent in each function from the aggregated call profiles of counting the points on the curves of Table 6.8. The *total time* is the percentage of the program's execution time spent in the function and the sub-functions called. *Self time* denotes the amount of program execution time spent directly in the function's body; it comes from performing actual computations with built-in primitives such as integer addition. Functions with less than 2 % total time were merged with their callers.

The table underlines the importance of fast modular polynomial arithmetic; it also shows the overhead created by Python's heap-only memory management: 44 % of the actual computation time are spent on result object construction.

Conclusion

Schoof's point counting algorithm for elliptic curves over finite fields [27] bases on three insights: (i) certain ℓ-torsion subgroups are structured like modules and support linear algebra (chapter 2); (ii) the Frobenius endomorphism characterizes the rational points on the curve (chapter 4); (iii) its characteristic equation on the modules is computable (chapter 3) and provides information about the number of rational points (chapter 5). Thus the characteristic equation can be used as a computable test to verify guesses about the number of points on the curve modulo small primes; the Chinese Remainder Theorem and a limited search range for the number of points then allow assembling the unique solution (chapter 6).

The algorithm presented in chapter 6 is a simplified version of Schoof's original proposition. Yet, the asymptotic complexity is the same; the original enhancements of less necessary small primes from Hasse's Theorem and smarter evaluation order result in better constants, but nothing more. Nevertheless, the speedups matter in practice, and the CD contains an implementation in the file `implementation/reduced_computation_schoof.py`.

Asymptotic complexity improvements have been made by Elkies and Atkin: the degrees of the division polynomials dominate the effort necessary to compute the Frobenius equation; Elkies showed how to instead use certain polynomials of half the degree for about half of the small primes, and Atkin explained how to derive information in the other cases. The enhancements lower the complexity class by one $\log p$ factor. However, the theory required to completely understand them is very deep; see the book of Blake, Seroussi, and Smart [1, ch. VII] for an overview, or Müller's thesis for a more complete treatment [18].

In practice, both Schoof's algorithm and the Schoof-Elkies-Atkin algorithm require too big a setup for counting the points on curves over finite fields of sizes less than about 55 bits in length [28, l. 856]. Using the quadratic residue or the Shanks-Mestre baby-step giant-step method is superior in these cases.

Appendix

A

Equivalence of Definitions

In chapter 1, we defined non-singular curves as those with a defining polynomial that has three distinct roots. We also introduced the discriminant as a criterion for recognizing non-singular curves. The present appendix provides a proof that our definition is equivalent to the usual definition of non-singularity: the curve is free of cusps; at no point vanish both partial derivatives of the fundamental relation. Furthermore we show that the discriminant is a valid criterion for non-singularity.

Lemma A.1. *Let $\mathbb{F}$ be a field of characteristic not 2, and let E be an elliptic curve over $\mathbb{F}$ with parameters A and B. Then the partial derivatives of the fundamental relation $y^2 = x^3 + Ax + B$ both vanish at some point if, and only if, the defining polynomial $x^3 + Ax + B$ has a repeated root.*

Proof. Consider the partial derivatives of the fundamental relation $s(x, y) = y^2 - x^3 - Ax - B$,

$$\frac{\partial s}{\partial x}(x, y) = -3x^2 - A \qquad \text{and} \qquad \frac{\partial s}{\partial y}(x, y) = 2y.$$

If $\partial s/\partial y$ is to vanish at a point (α, β), then we must have $\beta = 0$. Therefore α must be a root of the defining polynomial, for otherwise the point is outside the curve.

Differentiating the defining polynomial yields $-\partial s/\partial x$, so $\partial s/\partial x$ can have a zero if, and only if, the defining polynomial has one of multiplicity greater 1: only then has a polynomial a common root with its derivative. □

Note that in characteristic 2, the curve is always singular: the partial derivative in y is identically zero, so both partial derivatives vanish at $(\sqrt{A}, \sqrt{B}) \in E$.

We close the chapter with a proof that precisely the non-singular curves have a non-zero discriminant.

Lemma A.2. *Let $\mathbb{F}$ be a field of characteristic neither 2 nor 3. Furthermore let E be an elliptic curve over $\mathbb{F}$ with parameters A and B. Then E's defining polynomial $x^3 + Ax + B$ has three distinct roots if, and only if, the discriminant $4A^3 + 27B^2$ is non-zero.*

Proof. We express the parameters of E with the roots of its defining polynomial, insert the expressions into the discriminant, and derive which constellations of roots are equivalent to a zero discriminant. Thus write

$$x^3 + Ax + B = (x - \omega_1)(x - \omega_2)(x - \omega_3)$$

where ω_1, ω_2, and ω_3 come from $\overline{\mathbb{F}}$, the algebraic closure of $\mathbb{F}$. Multiplying out the right-hand side yields

$$x^3 + (-\omega_1 - \omega_2 - \omega_3)x^2 + (\omega_1\omega_2 + \omega_1\omega_3 + \omega_2\omega_3)x + (-\omega_1\omega_2\omega_3);$$

comparing coefficients with the left-hand side gives us the following equations:

$$\begin{aligned} A &= \omega_1\omega_2 + \omega_1\omega_3 + \omega_2\omega_3; \\ B &= -\omega_1\omega_2\omega_3; \\ 0 &= -\omega_1 - \omega_2 - \omega_3. \end{aligned} \tag{A.3}$$

Next insert the expressions for A and B into the discriminant and factorize the result. Then

$$4A^3 + 27B^2 = -(\omega_2 - \omega_3)^2(\omega_2 + 2\omega_3)^2(2\omega_2 + \omega_3)^2.$$

The discriminant is zero if, and only if, one of its factors is zero. With Equation A.3 we see that this is the case if, and only if, two roots are equal:

$$4A^3 + 27B^2 = -(\omega_2 - \omega_3)^2(-\omega_1 + \omega_3)^2(\omega_2 - \omega_1)^2.$$

□

Appendix

B

Implementation Manual

Part of this thesis is an elementary implementation of Schoof's point counting algorithm for elliptic curves over finite fields. Furthermore, the CD contains a slightly enhanced version of the algorithm that uses the speedups mentioned in the conclusion. The present chapter describes how to install and run the implementations.

B.1 System Requirements

The algorithm is implemented in version 3.1 of *Python*, an open licensed dynamic programming language available on all common platforms [22]. To find out whether a compatible version of Python is already installed on your system, execute `python --version` in a terminal. The command will return the version number if Python is available. Note that the version 3 interpreter could also be named `python3`. Please see the *Using Python* part of Python's documentation [24] for system installation instructions; follow the steps below to set up Python locally in your account.

Local Installation from Source Code

Installing Python from source code requires a C compiler; on Linux and Unix systems, one is almost always available. The following steps install Python on a Linux system:

Download. Download the source tar ball of version 3.1 or later from the Python website at `http://www.python.org/download/releases/`. For convenience, the `python` directory on the CD contains an archive with the source code of Python 3.1.2.

Compile. Open a terminal and create a temporary directory, say `${HOME}/tmp/`, by executing `mkdir ${HOME}/tmp/`. Change into the temporary directory and extract the source tar ball: `cd ${HOME}/tmp/` and then `tar xzvf Python-3.1.2.tgz`; adjust the path and file name accordingly. If you downloaded the bzipped source tar ball, use `tar xjvf Python-3.1.2.tar.bz2` instead.

Next, change into the directory that contains the extracted source code, for instance `${HOME}/tmp/Python-3.1.2/`. Configure the build system by executing `./configure --prefix=${HOME}/python3`. The prefix is the path that will be the root of the Python installation, so adjust it to taste. In

case required components are missing, the command will exit with an error message. In this case, please install the components and re-execute `configure`.

If everything worked, then the last line of output by `configure` will be `creating Makefile`. To start the compilation, execute `make`.

Install. Use `make install` to install Python after the compilation finished.

Set Up Environment. To enable the local Python installation, add its interpreter and modules to the respective search paths: execute `export PATH=${HOME}/python3/bin:${PATH}` to tell the shell where to find the `python3` interpreter; adjust the path to your prefix for `configure`. Likewise, execute `export PYTHONPATH=${HOME}/python3/lib/python3.1` to tell Python where to find its modules.

Note that the scope of `export` is the current shell. Thus you have to issue both commands in every freshly opened terminal you wish to use for Python 3.1 programs.

B.2 Program Execution

The implementations work without any installation; they may be executed directly from CD. However, they expect a set up Python 3.1 run-time environment as explained above.

The `implementation/` directory contains the point counting programs: the file `naive_schoof.py` is the implementation discussed in section 6.3; the file `reduced_computation_schoof.py` is the version with better constants using a smarter computation order and Hasse's theorem. Curves for counting are specified as space-separated triples $\langle p \rangle$, $\langle A \rangle$, and $\langle B \rangle$: $\langle p \rangle$ is the prime size of the field $\mathbb{F}_p$, and $\langle A \rangle$ and $\langle B \rangle$ are the curve parameters A, and B.

Example B.1. Suppose you want to count the number of points on the elliptic curve over $\mathbb{F}_{23}$ with parameters $A = 4$ and $B = 2$. If the current directory in the terminal is `implementation/` on the CD, then executing `python3 naive_schoof.py 23 4 2` yields the output

```
Counting points on y^2 = x^3 + 4x + 2 over GF<23>: 21
```

The program supports the command line options described in Table B.2, which for instance allow to read the curves from a file, or to create execution profiles for performance analysis.

Note B.3. Even if several instances of the program use the same input file, each line will be read only once: the instances synchronize via a shared file to avoid double computation. Since the synchronization mechanism bases on files, the program instances do not have to run on the same machine; the *Network File System* (NFS) supports all required operations.

Option	Description
`--version`	Show program's version number and exit.
`-h`, `--help`	Show a help message and exit.
`-i` $\langle f \rangle$, `--input-file=`$\langle f \rangle$	Read the curve parameters from file $\langle f \rangle$. Lines in $\langle f \rangle$ must contain either a comment, or a space-separated triple of curve parameters $\langle p \rangle$, $\langle A \rangle$, and $\langle B \rangle$. Comment lines start with a hash (`#`); these and empty lines are skipped.
`-o` $\langle f \rangle$, `--output-file=`$\langle f \rangle$	Write the results to file $\langle f \rangle$ instead of showing them on the terminal. Each line of input generates one corresponding line of output.
`-t` $\langle s \rangle$, `--timelimit=`$\langle s \rangle$	Terminate the program if processing an input triple takes longer than $\langle s \rangle$ seconds. The program ends if the time limit expires; no subsequent lines will be read from an input file. Thus, sort the parameters in input files ascending in length of the prime $\langle p \rangle$ to avoid triggering the time limit too early.
`-p`, `--create-profile`	Create an execution profile for each processed input triple. The profile consists of a call profile generated with the `cProfile` Python module, and a file with data about elapsed time and used memory.
`-d` $\langle d \rangle$, `--profile-directory=`$\langle d \rangle$	If profiling is enabled with the `-p` flag, then the collected data is written to the directory $\langle d \rangle$. The default value is the current directory.

Table B.2: Command line options supported by the two point counting programs `naive_schoof.py` and `reduced_computation_schoof.py`.

Remark B.4. The `tools/` directory on the CD contains several programs to post-process profiles resulting from a set `-p` flag. For example, it includes a call profile converter that outputs Callgrind files [30, Tool suite]. Use KCacheGrind to interactively inspect these [32].

B.3 Further Documentation

The implementation comes with extensive API documentation that explains the purpose and usage of all classes. The file `index.html` in the directory `implementation/doc/html` is the starting point.

Furthermore, the directory `implementation/_test` contains unit tests to verify correct arithmetic. The unit tests are designed to be easily extended to further implementations of the same objects. Thus, mistakes in new designs should be simpler to locate. To run the unit tests, execute `python3 -m _test` in the `implementation/` directory.

List of Figures

List of Tables

Bibliography

[1] Ian Blake, Gadiel Seroussi, and Nigel Smart. *Elliptic Curves in Cryptography.* Number 265 in London Mathematical Society Lecture Note Series. Cambridge University Press, Cambridge, UK, 1999.

[2] Leonard S. Charlap and David P. Robbins. An elementary introduction to elliptic curves. CRD Expository Report 31, Center for Communications Research, Princeton, NJ, USA, December 1988.

[3] Jean-Marc Couveignes. *Quelques calculs en théorie des nombres.* Thèse, Université de Bordeaux I, France, July 1994.

[4] Jean-Marc Couveignes and François Morain. Schoof's algorithm and isogeny cycles. In Leonard M. Adleman and Ming-Deh A. Huang, editors, *Algorithmic Number Theory, First International Symposium, ANTS-I, Ithaca, NY, USA, May 6–9, 1994, Proceedings*, volume 877 of *Lecture Notes in Computer Science*, pages 43–58. Springer-Verlag, 1994.

[5] Richard E. Crandall and Carl Pomerance. *Prime Numbers.* Springer-Verlag, New York, NY, USA, second edition, 2005.

[6] W. Diffie and M. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, November 1976.

[7] Taher ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. In *Proceedings of CRYPTO 84 on Advances in cryptology*, pages 10–18, New York, NY, USA, 1985. Springer-Verlag.

[8] Darrel R. Hankerson, Alfred J. Menezes, and Scott Vanstone. *Guide to elliptic curve cryptography.* Springer-Verlag, New York, NY, USA, 2004.

[9] Donald E. Knuth. *Seminumerical Algorithms*, volume 2 of *The Art of Computer Programming.* Addison Wesley, third edition, 1998.

[10] Neal Koblitz. Elliptic curve cryptosystems. *Mathematics of Computation*, 48(177):203–209, January 1987.

[11] Neal Koblitz. *A course in number theory and cryptography.* Springer-Verlag, New York, NY, USA, second edition, 1994.

[12] Reynald Lercier and François Morain. Counting the number of points on elliptic curves over finite fields: Strategies and performance. In *EUROCRYPT*, pages 79–94, 1995.

[13] Reynald Lercier and François Morain. Computing isogenies between elliptic curves over $\mathbb{F}_{p^n}$ using Couveignes's algorithm. *Mathematics of Computation*, 69(229):351–370, 2000.

[14] James L. Massey and Jimmy K. Omura. Method and apparatus for maintaining the privacy of digital messages conveyed by public transmission. U.S. Patent 4567600, Omnet Associates, January 1986.

[15] Alfred J. Menezes, Paul van Oorschot, and Scott Vanstone. *Handbook of applied cryptography*. CRC Press, 1997.

[16] Alfred J. Menezes, Scott A. Vanstone, and Robert J. Zuccherato. Counting points on elliptic curves over $\mathbb{F}_{2^m}$. *Mathematics of Computation*, 60(201):407–420, January 1993.

[17] Victor S. Miller. Use of elliptic curves in cryptography. In *CRYPTO '85: Advances in Cryptology*, pages 417–426, London, UK, 1986. Springer-Verlag.

[18] Volker Müller. *Ein Algorithmus zur Bestimmung der Punktanzahl elliptischer Kurven über endlichen Körpern der Charakteristik größer drei*. PhD thesis, Universität des Saarlandes, Saarbrücken, Germany, 1995.

[19] National Institute of Standards and Technology. Advanced encryption standard (AES). FIPS PUB 197, National Institute of Standards and Technology, Gaithersburg, MD, USA, November 2001.

[20] National Institute of Standards and Technology. Digital signature standard (DSS). FIPS PUB 186–3, National Institute of Standards and Technology, Gaithersburg, MD, USA, June 2009.

[21] S. Pohlig and M. Hellman. An improved algorithm for computing logarithms over $\mathbb{GF}(p)$ and its cryptographic significance. *IEEE Transactions on Information Theory*, 24(1):106–110, January 1978.

[22] Python Software Foundation. The Python programming language. Official Website `http://python.org/` (Retrieved on May 3, 2010).

[23] Python Software Foundation. Python/C API reference manual. Documentation available from `http://docs.python.org/3.1/c-api/index.html` (Retrieved on May 3, 2010).

[24] Python Software Foundation. Using Python. Documentation available from `http://docs.python.org/3.1/using/index.html` (Retrieved on May 3, 2010).

[25] Derek J. S. Robinson. *An Introduction to Abstract Algebra*. de Gruyter, Berlin, Germany, 2003.

[26] Bruce Schneier. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. John Wiley & Sons, second edition, 1996.

[27] René Schoof. Elliptic curves over finite fields and the computation of square roots mod p. *Mathematics of Computation*, 44(170):483–494, April 1985.

[28] Mike Scott. `schoof.cpp`, September 1999. C++ source code available from `ftp://ftp.compapp.dcu.ie/pub/crypto/schoof.cpp` (Retrieved on May 3, 2010).

[29] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Springer-Verlag, Dordrect, The Netherlands, second edition, 2009.

[30] Valgrind Developers. Valgrind instrumentation framework. Official Website `http://valgrind.org/` (Retrieved on May 3, 2010).

[31] Lawrence C. Washington. *Elliptic curves: number theory and cryptography*. CRC Press, Boca Raton, FL, USA, second edition, 2008.

[32] Josef Weidendorfer. KCacheGrind call graph viewer. Official Website `http://kcachegrind.sf.net/` (Retrieved on May 3, 2010).

Erklärung

Ich versichere, die vorliegende Arbeit selbstständig und unter ausschließlicher Verwendung der angegebenen Hilfsmittel und Quellen angefertigt zu haben.

Würzburg, den 4. Mai 2010

Peter Dinges