Elliptic Curves in Cryptography

David Jao

February 26, 2007

Contents

Chapter 1

Introduction

The aim of this volume is to present, in as self contained a manner as possible, the mathematical foundations of elliptic curve cryptography and pairing based cryptography, with an eye towards recent developments and active areas of current research. In my experiences with students and researchers, I have found that many cryptographers and computer scientists feel inadequate to the task of learning and mastering elliptic curve cryptography because of a lack of mathematical background in elliptic curves. Existing books on the subject tend to either lack mathematical depth, or focus so heavily on the mathematics audience that there is no serious discussion of crypto. Those books which do succeed in encompassing both aspects usually refer heavily to other texts, which breaks continuity and makes it harder for a student to learn the subject. In this work, we aim to satisfactorily treat both the theoretical and practical aspects of elliptic curve cryptography, while keeping the discussion self-contained to the greatest extent possible. When a thorough treatment is not possible, we will adopt the approach of explaining why a result holds, and presenting special cases in detail, rather than giving a technically correct proof which is too abstract to impart understanding.

We begin with a discussion of the theory of elliptic curves over the complex numbers. Even though elliptic curve cryptography deals primarily with elliptic curves over finite fields, there are many reasons for beginning our treatment with complex numbers. One reason is that some of the algorithms used in cryptography, for example the complex multiplication method for generating curves with a known number of points (part of the IEEE P1363 standard), are based directly on elliptic curves over complex numbers. However, a more compelling reason is that the complex theory (besides being historically first) provides us not only with direct proofs but also with a good intuition for many of the elliptic curve phenomena that arise over finite fields. For example, we will see that the structure of n-torsion points and divisors on an elliptic curve is best explained by appealing to complex geometry.

Chapter 2

Geometry of Elliptic Curves

2.1 Lattices

Definition 2.1.1. A *lattice* in $\mathbb{C}$ is the set of integer linear combinations of two $\mathbb{R}$-linearly independent points $w_1, w_2 \in \mathbb{C}$, which are called the *periods* of the lattice. We denote such a lattice by $\Lambda(w_1, w_2)$, so that

$$\Lambda(w_1, w_2) := \{aw_1 + bw_2 \mid a, b \in \mathbb{Z}\}.$$

For the remainder of this section, we fix a lattice Λ, with the periods w_1, w_2 being understood from context.

Definition 2.1.2. The *Weierstrass* $\mathfrak{p}$*-function* is the function

$$\mathfrak{p}(z) := \frac{1}{z^2} + \sum_{\substack{w \in \Lambda \\ w \neq 0}} \left(\frac{1}{(z-w)^2} - \frac{1}{w^2} \right),$$

defined for all values $z \in \mathbb{C} \setminus \Lambda$.

Theorem 2.1.3. *The series for* $\mathfrak{p}(z)$ *converges absolutely and uniformly for all complex numbers* $z \notin \Lambda$.

Proof. We have

$$\frac{1}{(z-w)^2} - \frac{1}{w^2} = \frac{w^2 - (z-w)^2}{(z-w)^2 w^2} = \frac{2wz - z^2}{(z-w)^2 w^2} = O\left(\frac{1}{w^3}\right),$$

and the sum of any $O\left(\frac{1}{w^3}\right)$ function over a two-dimensional real lattice is absolutely and uniformly convergent. □

Theorem 2.1.4. $\mathfrak{p}(z + \ell) = \mathfrak{p}(z)$ *for any* $\ell \in \Lambda$.

Proof. First observe that $\mathfrak{p}(z)$ is an even function. Next, we calculate

$$\mathfrak{p}'(z) = \frac{-2}{z^3} - \sum_{\substack{w \in \Lambda \\ w \neq 0}} \frac{2}{(z-w)^3} = -2 \sum_{w \in \Lambda} \frac{1}{(z-w)^3}.$$

The series for $\mathfrak{p}'(z)$ is absolutely and uniformly convergent, and $\mathfrak{p}'(z+\ell) = \mathfrak{p}'(z)$ for all $\ell \in \Lambda$. Fix an element $\ell \in \Lambda$, and let $f(z)$ be the function $\mathfrak{p}(z+\ell) - \mathfrak{p}(z)$. We have shown that $f'(z) = 0$, so $f(z)$ must be a constant function. However, $f(\frac{\ell}{2}) = 0$ since $\mathfrak{p}(z)$ is an even function, so $f(z)$ is identically 0. □

Theorem 2.1.4 shows that $\mathfrak{p}(z)$ is periodic with two independent periods w_1 and w_2; that is, $\mathfrak{p}(z + w_1) = \mathfrak{p}(z + w_2) = \mathfrak{p}(z)$. The periodicity of $\mathfrak{p}(z)$ is the reason why w_1 and w_2 are called periods.

Definition 2.1.5. For each positive integer $k \geq 3$, let G_k be the complex number given by the (convergent) series

$$G_k := \sum_{\substack{w \in \Lambda \\ w \neq 0}} \frac{1}{w^k}.$$

Note that $G_k = 0$ for odd values of k.

Theorem 2.1.6. *We have the formula*

$$\mathfrak{p}(z) := \frac{1}{z^2} + \sum_{k=2}^{\infty} (2k-1) G_{2k} z^{2k-2}.$$

Proof. To start with,

$$\begin{aligned}(z-w)^{-2} - w^{-2} &= w^{-2}\left(\left(1 - \frac{z}{w}\right)^{-2} - 1\right) = w^{-2}\left(\sum_{n=0}^{\infty} (n+1)\left(\frac{z}{w}\right)^n - 1\right) \\ &= w^{-2} \sum_{n=1}^{\infty} (n+1)\left(\frac{z}{w}\right)^n = \sum_{n=1}^{\infty} (n+1)\frac{z^n}{w^{n+2}}.\end{aligned}$$

Hence,

$$\begin{aligned}\mathfrak{p}(z) &= \frac{1}{z^2} + \sum_{\substack{w \in \Lambda \\ w \neq 0}} (z-w)^{-2} - w^{-2} = \frac{1}{z^2} + \sum_{\substack{w \in \Lambda \\ w \neq 0}} \sum_{n=1}^{\infty} (n+1)\frac{z^n}{w^{n+2}} \\ &= \frac{1}{z^2} + \sum_{n=1}^{\infty} \sum_{\substack{w \in \Lambda \\ w \neq 0}} (n+1)\frac{z^n}{w^{n+2}} = \frac{1}{z^2} + \sum_{n=1}^{\infty} (n+1) z^n \sum_{\substack{w \in \Lambda \\ w \neq 0}} \frac{1}{w^{n+2}}\end{aligned}$$

Note that the inner summation in the last expression can be restricted to even integers n. The theorem now follows from the substitution $n = 2k - 2$. □

Theorem 2.1.7. *The function $\mathfrak{p}(z)$ satisfies the differential equation*

$$\left(\frac{\mathfrak{p}'(z)}{2}\right)^2 = \mathfrak{p}(z)^3 - (15G_4)\mathfrak{p}(z) - (35G_6).$$

Proof. By Theorem 2.1.6, we have

$$\begin{array}{lccccccc}
\mathfrak{p}(z) = & 0 & + \frac{1}{z^2} & + 0 & + 3G_4 z^2 & + 5G_6 z^4 & + \cdots \\
\frac{\mathfrak{p}'(z)^2}{4} = & \frac{1}{z^6} & - \frac{6}{z^2} & - 20G_6 & + (9G_4 - 42G_8) z^2 & + (60G_4G_6 - 72G_8) z^4 & + \cdots \\
\mathfrak{p}(z)^3 = & \frac{1}{z^6} & + \frac{9G_4}{z^2} & + 15G_6 & + (27G_4^2 + 21G_8) z^2 & + (90G_4G_6 + 27G_{10}) z^4 & + \cdots
\end{array}$$

Let $f(z)$ be the function $(\mathfrak{p}'(z)/2)^2 - (\mathfrak{p}(z)^3 - (15G_4)\mathfrak{p}(z) - (35G_6))$. Note first that $f(z)$ is periodic with periods w_1 and w_2. From the calculations above, we see that $f(z)$ has a power series representation about 0 consisting only of z^2 and higher order terms. It follows that the power series representation of $f(z)$ converges absolutely and uniformly on the entire complex plane. By standard real (or complex) analysis, a power series is always continuous and differentiable wherever it is defined.

Moreover, $f(z)$ is bounded, because any fundamental parallelogram of the period lattice Λ is a compact set, and a continuous function is always bounded on a compact set.

Liouville's theorem from complex analysis states that any bounded differentiable function on the entire complex plane is equal to a constant. We conclude that $f(z)$ is equal to a constant, and this constant must be 0, since $f(0) = 0$ by the power series representation of f. □

Theorem 2.1.4 shows that $\mathfrak{p}(z)$ represents a well defined function from the quotient group $\mathbb{C}/\Lambda$ to $\mathbb{C}$. This function is surjective (by Picard's theorem of complex analysis), but it is not injective, since $\mathfrak{p}(z)$ is an even function, so of course $\mathfrak{p}(z)$ and $\mathfrak{p}(-z)$ must map to the same point. However, observe that $\mathfrak{p}'(z)$ and $\mathfrak{p}'(-z)$ have opposite signs (again, because $\mathfrak{p}(z)$ is an even function), so that the pair of values $(\mathfrak{p}(z), \mathfrak{p}'(z)/2)$ does suffice (at least usually) to distinguish between z and $-z$. Theorem 2.1.7 states that the pair $(x, y) = (\mathfrak{p}(z), \mathfrak{p}'(z)/2)$ satisfies the equation $y^2 = x^3 + ax + b$, where $a = -15G_4$ and $b = -35G_6$. It turns out (Theorem 2.3.7) that the map $\phi\colon \mathbb{C}/\Lambda \to \mathbb{C} \times \mathbb{C}$ given by $\phi(z) = (\mathfrak{p}(z), \mathfrak{p}'(z)/2)$ is in fact a *bijection* and an *isomorphism of complex manifolds* between $\mathbb{C}/\Lambda$ and the set

$$\{(x, y) \in \mathbb{C}^2 \mid y^2 = x^3 + ax + b\}. \tag{2.1}$$

Those of you who have seen elliptic curves before will recognize the set (2.1) to be the set of points on an elliptic curve. It is in this sense that the quotient group $\mathbb{C}/\Lambda$ is equal to an elliptic curve: namely, there exists a bijection between points on $\mathbb{C}/\Lambda$ and points on the elliptic curve, given by the mapping $\phi(z)$.

The differential equation in Theorem 2.1.7 can be solved for z in terms of $\mathfrak{p}$ by separation of variables. If you do this, you will find that the inverse of $\mathfrak{p}(z)$ is an integral of the form

$$\mathfrak{p}^{-1}(w) = \int_0^w \frac{dx}{\sqrt{x^3 + ax + b}} \tag{2.2}$$

where the integral is taken over a path from 0 to w in the complex plane. This integral is, up to a (tricky and non-obvious) change of variable, the same integral that arises if one attempts to compute the arc length of an ellipse. It is this connection to ellipses that gives rise to the term "elliptic curve." Indeed, a powerful analogy can be made to the computation of the arc length of a circle, which of course is given by the integral

$$\sin^{-1}(w) = \int_0^w \frac{dx}{\sqrt{1 - x^2}}. \tag{2.3}$$

The analogy extends in many other ways which are not obvious at first sight. For example, the integral (2.3) is not well defined, because of the ambiguity caused by the square root — it is only well defined up to multiples of 2π. Consequently, the non-inverted function $\sin(z)$ is singly periodic with period 2π, just as $\mathfrak{p}(z)$ is doubly periodic with periods w_1 and w_2[1]. Moreover, if we shift perspective for a moment, and consider the singly periodic function $\exp(z)$ (essentially the same function as $\sin(z)$, by Euler's identity), then we find that $\exp(z)$ represents a bijection between the quotient group $\mathbb{C}/2\pi i\mathbb{Z}$ and the multiplicative group $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$, in much the same way that $\phi(z) = (\mathfrak{p}(z), \mathfrak{p}'(z)/2)$ induces a bijection between the quotient group $\mathbb{C}/\Lambda$ and the elliptic curve group of (2.1).

Oh, wait, did I say group? Yes, the points on an elliptic curve form a group, and in fact $\phi(z)$ is a group homomorphism, just as $\exp(z)$ is a group homomorphism. The visualization of the group structure is but one of the many ways in which the complex theory yields profitable insights into the behavior of elliptic curves.

2.2 Elliptic functions

Most of the material in this section is copied from [5, §VI].

Definition 2.2.1. An *elliptic curve* over the complex numbers is the set of solutions $(x, y) \in \mathbb{C}^2$ satisfying an equation of the form

$$y^2 = x^3 + ax + b,$$

together with a single (formal) point ∞, where $a, b \in \mathbb{C}$ are fixed constants such that the polynomial x^3+ax+b has no repeated roots. The elliptic curve with coefficients a and b is denoted $E(a, b)$, or E when the constants a, b are clear from context.

[1]The extra periodicity of $\mathfrak{p}(z)$ arises from the fact that a square root of a cubic polynomial has three zero points and hence three branch cuts to contend with, thus increasing the number of ambiguities in the integral.

The motivation for this definition should be clear. We have seen that every lattice Λ satisfies the equation $y^2 = x^3 - (15G_4)x - (35G_6)$. This equation would define an elliptic curve if it could be shown that the cubic on the right hand side has no repeated roots. In order to prove that the cubic has no repeated roots, we need to undertake a more detailed study of elliptic functions, which are the subject of the next definition. The study of elliptic functions will yield many other benefits as well. For example, it will allow us to prove the fact, mentioned in the last section, that $\phi(z) = (\mathfrak{p}(z), \mathfrak{p}'(z)/2)$ represents a bijection between $\mathbb{C}/\Lambda$ and the points (x, y) on the elliptic curve.

One thing which we will not prove is that every complex elliptic curve $y^2 = x^3 + ax + b$ arises as the differential equation of some lattice Λ. A proof of this fact can be found in [6, §1.4].

Definition 2.2.2. An elliptic function over a lattice $\Lambda \in \mathbb{C}$ is a meromorphic function on $\mathbb{C}$ satisfying the property

$$f(z + \ell) = f(z) \text{ for all } \ell \in \Lambda.$$

The field of elliptic functions over Λ is denoted $\mathbb{C}(\Lambda)$.

Relationship to algebraic goemetry: An elliptic function, by Definition 2.2.2, is a meromorphic function on the compact complex manifold $\mathbb{C}/\Lambda$. We have seen that $\mathfrak{p}(z)$ and $\mathfrak{p}'(z)$ are examples of elliptic functions. We will see later (Theorem 2.3.8) that every elliptic function is a rational function in $\mathfrak{p}(z)$ and $\mathfrak{p}'(z)$. If we write $x = \mathfrak{p}(z)$ and $y = \mathfrak{p}'(z)/2$, then we see that every meromorphic function on $\mathbb{C}/\Lambda$ is a rational function in the two variables x, y. Compare this to the case of the complex plane, where every meromorphic function on the extended complex plane is always equal to a rational function in one variable z [1, p. 130].

We now recall the definitions of *order* and *residue* from complex analysis. Given any nonzero meromorphic function f, and any point $w \in \mathbb{C}$, there exists a series expansion

$$f(z) = \sum_{i=n}^{\infty} a_i (z - w)^i,$$

with a_n nonzero, for some integer $n \in \mathbb{Z}$. The *order* of f at w, denoted $\mathrm{ord}_w(f)$, is defined to be the integer n, and the *residue* of f at w, denoted $\mathrm{Res}_w(f)$, is the coefficient a_{-1} in the above series (or 0 if $n \geq 0$). If $n > 0$ or $n < 0$, then we say respectively that f has a *zero* or *pole* of order $|n|$ at w, and a pole of order one is called a *simple pole*.

Proposition 2.2.3. *An elliptic function with no poles is constant.*

Proof. An elliptic function f with no poles is continuous on a fundamental parallelogram of Λ, which is a compact set. Hence f is bounded and differentiable, so by Liouville's theorem [1, §4.2.3], it is constant. □

Corollary 2.2.4. *An elliptic function with no zeros is constant.*

Proof. If f has no zeros, then $1/f$ has no poles, so $1/f$ is constant. □

Theorem 2.2.5. *Let $f \in \mathbb{C}(\Lambda)$ be a nonzero elliptic function.*

(a) $\displaystyle\sum_{w \in \mathbb{C}/\Lambda} \mathrm{Res}_w(f) = 0.$

(b) $\displaystyle\sum_{w \in \mathbb{C}/\Lambda} \mathrm{ord}_w(f) = 0.$

(c) $\displaystyle\sum_{w \in \mathbb{C}/\Lambda} w \cdot \mathrm{ord}_w(f) \equiv 0 \pmod{\Lambda}.$

Proof. We first remark that all three sums are finite, because the poles and zeros of a meromorphic function are isolated, and $\operatorname{Res}_w(f)$ (resp., $\operatorname{ord}_w(f)$) can only be nonzero at a pole (resp., a pole or zero) of f.

Let D be a fundamental parallelogram for Λ, translated if necessary so that its boundary avoids all poles and zeros of f.

(a) By the Cauchy residue theorem,

$$\sum_{w \in \mathbb{C}/\Lambda} \operatorname{Res}_w(f) = \frac{1}{2\pi i} \int_{\partial D} f(z)\, dz.$$

Since f is periodic, the line integral cancels itself out along the boundary of D, so the value of the integral is 0.

(b) The function $f'(z)/f(z)$ is an elliptic function, so

$$\sum_{w \in \mathbb{C}/\Lambda} \operatorname{ord}_w(f) = \sum_{w \in \mathbb{C}/\Lambda} \operatorname{Res}_w\left(\frac{f'}{f}\right) = \frac{1}{2\pi i} \int_{\partial D} \frac{f'(z)}{f(z)}\, dz = 0.$$

(c) We have

$$\sum_{w \in \mathbb{C}/\Lambda} w \cdot \operatorname{ord}_w(f) \equiv \sum_{w \in D} w \cdot \operatorname{Res}_w\left(\frac{f'}{f}\right) \pmod{\Lambda},$$

and moreover

$$\sum_{w \in D} w \cdot \operatorname{Res}_w\left(\frac{f'}{f}\right) = \sum_{w \in D} \operatorname{Res}_w\left(\frac{((z-w)+w)f'}{f}\right)$$

since $\operatorname{Res}_w((z-w)f'/f) = 0$ for any meromorphic f. We conclude that

$$\sum_{w \in \mathbb{C}/\Lambda} w \cdot \operatorname{ord}_w(f) \equiv \sum_{w \in D} \operatorname{Res}_w\left(\frac{zf'(z)}{f(z)}\right) \pmod{\Lambda}.$$

Now apply the Cauchy residue theorem to $zf'(z)/f(z)$. Even though this function is not an elliptic function, the residue theorem nevertheless holds. We have

$$\sum_{w \in D} w \cdot \operatorname{ord}_w(f) = \frac{1}{2\pi i} \int_{\partial D} \frac{zf'(z)}{f(z)}\, dz = \frac{1}{2\pi i} \left(\int_a^{a+w_1} + \int_{a+w_1}^{a+w_1+w_2} + \int_{a+w_1+w_2}^{a+w_2} + \int_{a+w_2}^{a} \right) \frac{zf'(z)}{f(z)}\, dz.$$

By making the substitutions $z \to z - w_1$ and $z \to z - w_2$ in the second and third integrals, we find

$$\sum_{w \in \mathbb{C}/\Lambda} w \cdot \operatorname{ord}_w(f) = -\frac{w_2}{2\pi i} \int_a^{a+w_1} \frac{f'(z)}{f(z)}\, dz + \frac{w_1}{2\pi i} \int_a^{a+w_2} \frac{f'(z)}{f(z)}\, dz.$$

The result now follows from Lemma 2.2.6 below. □

Lemma 2.2.6. *Let $g(z)$ be any meromorphic function satisfying $g(a) = g(b)$. Then*

$$\int_a^b \frac{g'(z)}{g(z)}\, dz = 2\pi i k$$

for some integer $k \in \mathbb{Z}$.

Proof. Define a function $F(s)$ by

$$F(s) := \int_a^s \frac{g'(z)}{g(z)}\, dz,$$

valid for all $s \in \mathbb{C}$ lying on the path of the line integral from a to b, where the integral is taken over the initial segment from a to s. Then $F'(s) = \frac{g'(s)}{g(s)}$, and by the product rule,

$$\frac{d}{ds} g(s)e^{-F(s)} = 0.$$

Thus $g(s)e^{-F(s)}$ is a constant. Setting $s = a$, we find that

$$e^{F(s)} = \frac{g(s)}{g(a)},$$

and setting $s = 1$, we find that $e^{F(b)} = 1$ since $g(b) = g(a)$. It follows that $F(b) = 2\pi ik$ for some integer $k \in \mathbb{Z}$. □

2.3 Divisors

We will spend some time studying the mathematics and the geometry of divisors on an elliptic curve, because modern advances in the theory of elliptic curve cryptography use the concept of divisors in a rather essential way. This is especially true in the case of cryptographic pairings, for which divisors are necessary not only to define the pairings but also to compute them in an algorithmic fashion.

Recall the fundamental theorem of arithmetic, which states that every nonzero integer (more generally, every rational number) admits a unique factorization into a product of prime numbers. For example,

$$\begin{aligned} 6 &= 2 \cdot 3 \\ 50 &= 2 \cdot 5^2 \\ \frac{4}{105} &= 2^2 \cdot 3^{-1} \cdot 5^{-1} \cdot 7^{-1} \\ 1 &= \emptyset \end{aligned}$$

or, in additive notation,

$$\begin{aligned} \log(6) &= \log(2) + \log(3) \\ \log(50) &= \log(2) + 2\log(5) \\ \log\left(\frac{4}{105}\right) &= 2\log(2) + (-1)\log(3) + (-1)\log(5) + (-1)\log(7) \\ \log(1) &= 0 \end{aligned}$$

Observe that prime factorizations satisfy the following properties:

1. The sum is finite,
2. The coefficient of each prime is an integer,
3. The sum is unique: no two sums are equal unless all the coefficients are equal.

These properties motivate the definition of divisor on an algebraic curve:

Definition 2.3.1. A divisor on an algebraic curve C is a formal sum $\sum_{p \in C} a_p(p)$ of points p on the curve such that:

1. The sum is finite,

2. The coefficient a_p of each point p is an integer,

3. The sum is unique: no two sums are equal unless all the coefficients are equal.

The *degree* of a divisor $D = \sum_{p \in C} a_p(p)$, denoted $\deg(D)$, is the integer given by the finite sum $\sum_{p \in C} a_p$. The empty divisor is denoted $\emptyset$, and its degree by definition is 0.

The idea here is that a divisor is the geometric analogue of a product of primes in the algebraic setting. This analogy is more than merely an artificial construct; it is in many cases a literal correspondence. For example, if $f(x, y) \in \mathbb{C}[x, y]$ is the equation of an algebraic curve, then the maximal ideals in the quotient ring $\mathbb{C}[x, y]/(f(x, y))$ are exactly the ideals $(x - a, y - b)$ where $(a, b) \in \mathbb{C}^2$ is a point on the curve, i.e. $f(a, b) = 0$. Thus in this case, the divisors on the curve correspond exactly to products of primes.

The analogue of a principal ideal in the geometric setting is the notion of principal divisor, which is defined as follows.

Definition 2.3.2. Let f be a nonzero meromorphic function on an algebraic curve C. The divisor generated by f, denoted $\operatorname{div}(f)$, is the divisor

$$\operatorname{div}(f) := \sum_{w \in \mathbb{C}} \operatorname{ord}_w(f) \cdot (w),$$

taken as a finite sum over all the points $w \in C$ at which f has a zero or a pole. A divisor D on C is called a *principal divisor* if $D = \operatorname{div}(f)$ for some meromorphic function f on C.

Note that $\operatorname{div}(fg) = \operatorname{div}(f) + \operatorname{div}(g)$, and $\operatorname{div}(1) = \emptyset$. Hence div is a homomorphism from the multiplicative group of nonzero meromorphic functions of C to the additive group of divisors of C. Accordingly, the image of div is a subgroup of the group of divisors.

Remark: In the notation of divisors, Theorem 2.2.5(b) states that $\deg \operatorname{div}(f) = 0$ for any elliptic function f, and Theorem 2.2.5(c) states that $\sum_{p \in \mathbb{C}/\Lambda} a_p \cdot p = 0$ in the additive group $\mathbb{C}/\Lambda$, for any principal divisor $\sum_{p \in \mathbb{C}/\Lambda} a_p \cdot (p)$. We will show later that the converse of this theorem also holds: namely, a divisor $D = \sum a_p \cdot (p)$ is a principal divisor if and only if $\deg(D) = 0$ and $\sum a_p \cdot p = 0$.

Example 2.3.3. Let f be a rational function on the complex plane, i.e.,

$$f(z) = c\frac{(z - r_1) \cdots (z - r_m)}{(z - s_1) \cdots (z - s_n)}$$

for some $c, r_1, \ldots, r_m, s_1, \ldots, s_n \in \mathbb{C}$, and $m, n \in \mathbb{N}$. Then

$$\operatorname{div}(f) = (r_1) + (r_2) + \cdots + (r_m) - (s_1) - (s_2) - \cdots - (s_n) + (n - m)(\infty), \tag{2.4}$$

where the $(n - m)(\infty)$ term represents the order of vanishing or order of divergence of the rational function f in the limit as $z \to \infty$. Note that the degree of $\operatorname{div}(f)$ is 0, thanks to the inclusion of the (∞) term.

Example 2.3.4. The elliptic function $\mathfrak{p}(z)$ has a double pole at $z = 0$, and no other poles on $\mathbb{C}/\Lambda$ since the series converges everywhere except 0. By Theorem 2.2.5(b), it must have two (and exactly two) other zeros somewhere, and since $\mathfrak{p}(z)$ is an even function, we conclude that these two zeros are symmetric about the origin, so

$$\operatorname{div}(\mathfrak{p}) = -2(0) + (r) + (-r)$$

for some $r \in \mathbb{C}/\Lambda$.

Example 2.3.5. The elliptic function $\mathfrak{p}'(z)$ has a triple pole at $z = 0$, and no other poles on $\mathbb{C}/\Lambda$ since the series converges everywhere except 0. Thus the function must have exactly three zeros. We claim that these three zeros are at $z = w_1/2$, $z = w_2/2$, and $z = (w_1 + w_2)/2$. We will prove that $z = w_1/2$ is a zero; the proof for the other two points is similar. At $z = w_1/2$, we have

$$\mathfrak{p}'(w_1/2) = -\mathfrak{p}'(-w_1/2) = -\mathfrak{p}'(w_1/2)$$

since $\mathfrak{p}'$ is both an odd function and an elliptic function. Accordingly, $\mathfrak{p}'(w_1/2) = 0$. We obtain

$$\operatorname{div}(\mathfrak{p}') = -3(0) + \left(\frac{w_1}{2}\right) + \left(\frac{w_2}{2}\right) + \left(\frac{w_1 + w_2}{2}\right)$$

Example 2.3.6. This example is about arithmetic, not geometry, but we include it anyway because of its instructional value. Consider the "function" $4/105 \in \mathbb{Q}$ mapping primes $p \in \mathbb{Z}$ to the value of $4/105 \bmod p$. Then

$$\begin{aligned} 4/105 &\equiv 0 \pmod 2 \\ 4/105 &\equiv \infty \pmod 3 \\ 4/105 &\equiv \infty \pmod 5 \\ 4/105 &\equiv \infty \pmod 7 \end{aligned}$$

which shows that $4/105$ as a function has a zero of order two at 2 and a pole of order one at each of $3, 5, 7$. The principal divisor (or ideal) corresponding to $4/105$ is

$$\operatorname{div}(4/105) = 2\log(2) - \log(3) - \log(5) - \log(7),$$

and the astute reader will notice that the degree of this divisor does not seem to equal 0. This discrepancy is resolved by adding a new prime at ∞, namely $\mathbb{R}$, and setting the value of $4/105$ at ∞ to be the divisor $(-\log|4/105|)$ of $\mathbb{R}$. Thus, including the point at ∞, the divisor becomes

$$2\log(2) - \log(3) - \log(5) - \log(7) + (-\log|4/105|), \tag{2.5}$$

which does have *absolute value* equal to 0 (in much the same way that Equation (2.4) has degree 0 once ∞ is included), although its *degree* in the previous sense is not equal to 0. For rational functions, we speak of the "degree of a divisor" instead of the absolute value, because the degree of a rational function is the analogue of the absolute value map for the purposes of algebraic manipulations such as the Euclidean algorithm.

Notice that the vanishing of the expression (2.5) is equivalent to the statement of the product formula in algebraic number theory [3, p. 99].

We are now in a position to prove that the points on the curve $\mathbb{C}/\Lambda$ are in bijection with the points on the elliptic curve $y^2 = x^3 - (15G_4)x - (35G_6)$. In fact, the following two theorems show that the bijection preserves not only divisors but also the structure of meromorphic functions (and thus principal divisors) between the two curves.

Theorem 2.3.7. *Let $\Lambda(w_1, w_2) \subset \mathbb{C}$ be a lattice.*

1. *The cubic polynomial*
$$x^3 - (15G_4)x - (35G_6)$$
has no repeated roots and hence defines an elliptic curve E.

2. *The map $\phi\colon \mathbb{C}/\Lambda \to E$ given by*
$$\phi(z) = (\mathfrak{p}(z), \mathfrak{p}'(z)/2)$$
is a bijection.

Proof. We have already shown that $\mathfrak{p}'(z)^2 = \mathfrak{p}(z)^3 - (15G_4)\mathfrak{p}(z) - (35G_6)$ vanishes exactly at the three points $w_1/2, w_2/2, (w_1+w_2)/2$ (Example 2.3.5). It follows that the three roots of the cubic polynomial are given by $x_1 = \mathfrak{p}(w_1/2)$, $x_2 = \mathfrak{p}(w_2/2)$, $x_3 = \mathfrak{p}((w_1+w_2)/2)$. We show that these three roots are distinct.

Consider the function $h(z) = \mathfrak{p}(z + w_1/2) - \mathfrak{p}(w_1/2)$. This function is an even function, so it has a zero of order at least two at $z = 0$. Since $h(z)$ has a pole of order two at $z = w_1/2$, and no other poles, it follows that $h(z)$ has no other zeros. In particular, $\mathfrak{p}(w_2/2)$ and $\mathfrak{p}((w_1+w_2)/2)$ are not equal to $\mathfrak{p}(w_1/2)$. The same argument with $w_1/2$ replaced by $w_2/2$ proves that all three roots are distinct.

To prove the second part, we need to show that ϕ is surjective and injective. For surjectvity, let $P \in E$. If $P = \infty$ then $\phi(0) = \infty$. In all other cases, $P = (x, y)$ and the function $\mathfrak{p}(z) - x$ is a nonconstant elliptic function. By Corollary 2.2.4, this function has a zero somewhere, say $z = a$. Then $\mathfrak{p}(a) = x$ and

$$f\mathfrak{p}'(a)^2 = \mathfrak{p}(a)^3 - (15G_4)\mathfrak{p}(a) - (35G_6) = x^3 - (15G_4)x - (35G_6) = y^2,$$

so $\mathfrak{p}'(a) = \pm y$. If $\mathfrak{p}'(a) = y$ then $\phi(a) = (x, y)$, and if $\mathfrak{p}'(a) = -y$, then $\phi(-a) = (x, y)$.

For injectivity, suppose $\phi(z_1) = \phi(z_2)$. We consider two cases. If $2z_1 \neq 0$ in $\mathbb{C}/\Lambda$, then the function $h(z) = \mathfrak{p}(z) - \mathfrak{p}(z_1)$ has two distinct zeros z_1 and $-z_1$, and no other zeros (since it has only one pole, of order two, at $z = 0$). The equation $\phi(z_1) = \phi(z_2)$ implies that $h(z_2) = 0$, so $z_2 = \pm z_1$. If $z_2 = z_1$, then we are done, since our goal is to show that $z_2 = z_1$. If $z_2 = -z_1$, then

$$\mathfrak{p}'(z_1) = \mathfrak{p}'(z_2) = \mathfrak{p}'(-z_1) = -\mathfrak{p}'(z_1),$$

where the first equality follows from the equation $\phi(z_1) = \phi(z_2)$. In this case, Example 2.3.5 implies that z_1 must have been equal to one of $w_1/2$, $w_2/2$, $(w_1+w_2)/2$, contradicting our assumption that $2z_1 \neq 0$.

On the other hand, if $2z_1 = 0$, then $h(z) = \mathfrak{p}(z) - \mathfrak{p}(z_1)$ has a zero of order two at $z = z_1$ (because $h'(z_1) = 0$), so the zero $z = z_2$ of $h(z)$ must be equal to z_1. □

Theorem 2.3.8. *Every elliptic function over Λ is equal to a rational function in $\mathfrak{p}(z)$ and $\mathfrak{p}'(z)$. That is,*

$$\mathbb{C}(\Lambda) = \mathbb{C}(\mathfrak{p}(z), \mathfrak{p}'(z)).$$

Proof. Let $f(z) \in \mathbb{C}(\Lambda)$. Then $f(z)$ is the sum of an even function and an odd function via the usual decomposition:

$$f(z) = \frac{f(z) + f(-z)}{2} + \frac{f(z) - f(-z)}{2}$$

Hence it suffices to prove the theorem for even and odd functions. In fact, it suffices to prove the theorem for even functions, since $\mathfrak{p}'$ times an odd elliptic function is an even elliptic function.

For even elliptic functions f, the identity

$$\operatorname{ord}_w f = \operatorname{ord}_{-w} f$$

holds for all $w \in \mathbb{C}$. Furthermore, if $2w \in \Lambda$, then $\operatorname{ord}_w f$ is even, because the i-th derivative satisfies

$$f^{(i)}(-w) = f^{(i)}(w) = (-1)^i f^{(i)}(-w)$$

for all odd values of i (the first equality follows because $2w \in \Lambda$, and the last equality is achieved by repeatedly differentiating $f(z) = f(-z)$). Therefore

$$\operatorname{div}(f) = \sum_{w \in H} n_w((w) + (-w))$$

for some set of integers n_w, where H is half of a fundamental parallelogram for Λ, and the sum has only finitely many nonzero terms.

Consider the function

$$g(z) = \prod_{w \in H \setminus \{0\}} (\mathfrak{p}(z) - \mathfrak{p}(w))^{n_w}.$$

We have $\operatorname{div}(\mathfrak{p}(z) - \mathfrak{p}(w)) = (w) + (-w) - 2(0)$, so $\operatorname{div}(g)$ and $\operatorname{div}(f)$ are identical except possibly at (0). By Theorem 2.2.5(b), they must be identical at (0) as well, so $f(z)/g(z)$ is an elliptic function with no poles, and thus is constant. This fact implies $f(z) \in \mathbb{C}(\mathfrak{p}(z), \mathfrak{p}'(z))$, since by definition $g(z) \in \mathbb{C}(\mathfrak{p}(z), \mathfrak{p}'(z))$. □

Corollary 2.3.9. *The field $\mathbb{C}(\Lambda)$ is isomorphic to the fraction field of the polynomial ring $\mathbb{C}[X,Y]/(Y^2 - X^3 - (15G_4)X - (35G_6))$.*

Proof. Let $x = \mathfrak{p}(z)$ and $y = \mathfrak{p}'(z)/2$. Then $\mathbb{C}(\Lambda) = \mathbb{C}(x,y)$ by Theorem 2.3.8. Moreover, we know that x and y satisfy the equation $y^2 = x^3 - (15G_4)x - (35G_6)$. To prove the corollary, it suffices to show that x is transcendental over $\mathbb{C}$, and that y is algebraic of degree 2 over $\mathbb{C}(x)$.

It is easy to see that x is transcendental over $\mathbb{C}$, since $\mathfrak{p}(z)$ has a pole of order 2 at $z = 0$. The equation $y^2 = x^3 - (15G_4)x - (35G_6)$ shows that y is algebraic over $\mathbb{C}(x)$ of degree at most 2. Finally, if y were algebraic of degree 1 over $\mathbb{C}(x)$, then $\mathfrak{p}'(z) \in \mathbb{C}(\mathfrak{p})$ would be an even function, which is a contradiction. □

2.4 The Riemann-Roch theorem

We have seen that every principal divisor has degree 0. The Riemann-Roch theorem is, at heart, motivated by the question of whether the converse holds, that is to say, the question of whether every degree 0 divisor is equal to a principal divisor.

The answer to this question depends on what curve C we are using. For example, on the extended complex plane, every degree 0 divisor is in fact principal. Indeed, every degree 0 divisor D on $\mathbb{C} \cup \{\infty\}$ is of the form

$$D = \sum_{i=1}^{m} (r_i) - \sum_{j=1}^{n} (s_j) + (n-m)(\infty)$$

for some sequence of zeros $r_1, r_2, \ldots, r_m$ and poles $s_1, s_2, \ldots, s_n$ (possibly repeated), and we have seen that the rational function

$$f(z) = \frac{(z-r_1)\cdots(z-r_m)}{(z-s_1)\cdots(z-s_n)}$$

has divisor equal to D. Similarly, to go back to our arithmetic example, every finite formal sum of primes in $\mathbb{Z}$ corresponds to the unique factorization of some integer $n \in \mathbb{Z}$ (this is equivalent to saying that every ideal is principal). Thus, on $\mathbb{C}$, as well as on $\mathbb{Z}$, every degree 0 divisor is principal.

The situation changes when we look at an elliptic curve $\mathbb{C}/\Lambda$. The above construction of f doesn't work here, because the function f is not doubly periodic, as required for an elliptic function. In fact, we can exhibit explicitly a degree 0 divisor on an elliptic curve which is not principal.

Proposition 2.4.1. *Let $s \in \mathbb{C}$, $s \notin \Lambda$, and let D be any divisor of the form $D = -(s) + $ positive terms. Then D is not a principal divisor on $\mathbb{C}/\Lambda$ unless $D = \emptyset$.*

Proof. If f is a non-constant function such that $\operatorname{div}(f) = -(s) + $ positive terms, then f has a single simple pole on $\mathbb{C}/\Lambda$, contradicting Lemma 2.4.2 below. □

Lemma 2.4.2. *A non-constant elliptic function f has at least 2 poles (counted with multiplicities).*

Proof. If f has a single simple pole s, then by Theorem 2.2.5(a), the residue of f at s is equal to 0, so f is holomorphic at s, which is a contradiction.

Alternatively, if f has a single simple pole s, then by Theorem 2.2.5(b), the degree of $\operatorname{div}(f)$ is 0, so $\operatorname{div}(f)$ must equal $(r) - (s)$ for some point $r \in \mathbb{C}/\Lambda$ which is a root of f. However, Theorem 2.2.5(c) implies that $r - s \equiv 0 \pmod{\Lambda}$, so $r \equiv s \pmod{\Lambda}$, which is a contradiction. □

The statement of Proposition 2.4.1 lends itself to the following definition, whose purpose is to quantify the number of meromorphic functions possessing a given configuration of zeros and poles.

Definition 2.4.3. Let D be a divisor on a curve C. The *linear space* of D, denoted $L(D)$, is the $\mathbb{C}$-vector space of meromorphic functions

$$L(D) = \{\text{meromorphic functions } f \text{ on } C \mid \operatorname{div}(f) + D = \text{positive terms}\} \cup \{0\},$$

$\deg(D)$	D	$L(D)$	$\ell(D)$
0	$\emptyset$	$\langle 1 \rangle$	1
1	(s)	$\left\langle 1, \frac{1}{z-s} \right\rangle$	2
1	$(s_1) + (s_2) - (s_3)$	$\left\langle \frac{z-s_3}{z-s_1}, \frac{z-s_3}{z-s_2} \right\rangle$	2
2	$(s_1) + (s_2)$	$\left\langle 1, \frac{1}{z-s_1}, \frac{1}{z-s_2} \right\rangle$	3
3	$(s_1) + (s_2) + (s_3)$	$\left\langle 1, \frac{1}{z-s_1}, \frac{1}{z-s_2}, \frac{1}{z-s_3} \right\rangle$	4

Figure 2.1: Linear spaces in $\mathbb{C} \cup \{\infty\}$.

where *positive terms* means that the right hand side has no negative coefficients (in particular, the empty divisor **is** allowed).

The dimension of $L(D)$ as a vector space over $\mathbb{C}$ is denoted $\ell(D)$.

Example 2.4.4. Consider the case of divisors over $\mathbb{C} \cup \{\infty\}$. If $D_0 = \emptyset$, then $L(D_0)$ consists of only the constant functions, since any non-constant rational function has a pole (including non-constant polynomials, which have a pole at ∞). Thus a basis for $L(D_0)$ is $\{1\}$, and we have $L(D_0) = \langle 1 \rangle$ and $\ell(D_0) = 1$.

Now consider the case $D_1 = (s)$ for some $s \in \mathbb{C} \cup \{\infty\}$. An element of $L(D_1)$ is a meromorphic function $f \in \mathbb{C}(z)$ satisfying the property that $\operatorname{div}(f) + (s)$ is positive[2]. Such a function f must have either no poles or one pole, and if it has one pole, that pole must be a simple pole at s. It follows that $L(D_1)$ contains at least 1 and $\frac{1}{z-s}$. We claim that these elements span $L(D_1)$. Indeed, if $f \in L(D_1)$, then $f - \operatorname{Res}_s(f) \cdot \frac{1}{z-s}$ has no poles on $\mathbb{C} \cup \{\infty\}$, so it is constant. Thus a basis for $L(D_1)$ is $\{1, \frac{1}{z-s}\}$, and we have $L(D_1) = \langle 1, \frac{1}{z-s} \rangle$ and $\ell(D_1) = 2$. Note that if $s = \infty$, then the form of the equations is slightly different, but $\ell(D_1)$ remains the same: in this case, we have $L(D_1) = \{a + bz \mid a, b \in \mathbb{C}\} = \langle 1, z \rangle$, and $\ell(D_1) = 2$.

Suppose $D_2 = (s_1) + (s_2)$ on $\mathbb{C} \cup \{\infty\}$. We leave it to the reader to show that $L(D_2) = \langle 1, \frac{1}{z-s_1}, \frac{1}{z-s_2} \rangle$ (or $\frac{1}{(z-s_1)^2}$ if $s_1 = s_2$), and that $\ell(D_2) = 3$, with the usual adjustments if either s_1 or s_2 is ∞ (in particular, if they are both ∞, then $L(D_2) = \langle 1, z, z^2 \rangle$). Similarly, $\ell((s_1) + (s_2) + (s_3)) = 4$, and so on.

A more interesting case is the case $D_1' = (s_1) + (s_2) - (s_3)$. We see directly from the definition that $L(D_1') \subset L(D_2)$. However, the presence of the $-(s_3)$ term means that $\operatorname{div}(f) + D_1'$ will never be positive unless f has a root at s_3. Thus, we find that $L(D_1')$ is the subset of $L(D_2)$ consisting of functions having a root at s_3. In fact, the linear transformation $T \colon L(D_2) \to L(D_1')$ defined by $T(f(z)) = f(z) - f(s_3)$ is surjective, since T is the identity on $L(D_1') \subset L(D_2)$, and the kernel of T is equal to the space of constant functions. It follows that $\ell(D_1') = 1$.

We summarize our findings in Figure 2.1. Notice in particular the direct numerical relationship between $\deg(D)$ and $\ell(D)$.

Example 2.4.5. We examine the behavior of the divisors on an elliptic curve $\mathbb{C}/\Lambda$. If $D_0 = \emptyset$, then $L(D_0)$ consists of constant functions as before, and $\ell(D_0) = 1$. However, a degree 0 divisor such as $D_0' = (s_1) - (s_2)$, with $s_1 \neq s_2$, admits no functions in $L(D_0')$ by Proposition 2.4.1. Thus, in this case, a degree 0 divisor D on $\mathbb{C}/\Lambda$ can have $\ell(D)$ equal to either 0 or 1.

For a divisor of the form $D_1 = (s)$, the set of functions f such that $\operatorname{div}(f) + (s)$ is positive equals the set of constant functions, by Proposition 2.4.1. Therefore $L(D_1) = \langle 1 \rangle$ and $\ell(D) = 1$.

Divisors of the form $D_2 = (s_1) + (s_2)$ represent the first really difficult case that we encounter. Clearly the constant functions always belong to $L(D_2)$, since constant functions have empty divisor. We claim that there always exists a non-constant function lying within $L(D_2)$. The proof of this claim will require consideration of a number of successively more general cases, as follows.

1. Suppose that $s_1 = s_2 = 0$. In Example 2.3.4, we found that $\operatorname{div}(\mathfrak{p}) = -2(0) + (r) + (-r)$, so $\mathfrak{p}$ is a non-constant function inside $L(D_2)$.

[2]Recall that empty divisors are considered positive. We will not see fit to remind the reader of this fact again.

2. Suppose that $s_1 = s_2 \neq 0$. Then the function $\mathfrak{p}(z - s_1)$ lies inside $L(D_2)$.

3. Suppose that $s_1 = r$ and $s_2 = -r$, or vice versa. Then $\operatorname{div}(1/\mathfrak{p}) = -\operatorname{div}(\mathfrak{p}) = -(r) - (-r) + 2(0)$ since div is a group homomorphism, so $1/\mathfrak{p} \in L(D_2)$.

4. Suppose that $s_1 = -s_2$, and $s_1 \neq s_2$. Then $f(z) = \mathfrak{p}(z) - \mathfrak{p}(s_1)$ has a double pole at 0, and no other poles, so it must have two zeros (since $\deg \operatorname{div}(f) = 0$). Those two zeros are at $z = s_1$ and $z = -s_1$, so $\operatorname{div}(f) = (s_1) + (-s_1) - 2(0)$. It follows that $1/f \in L(D_2)$.

5. Suppose that $s_2 = 0$, and $s_1 \neq s_2$. Let $f(z) = \mathfrak{p}(z) - \mathfrak{p}(s_1)$ as in the previous case. Then, making use of Example 2.3.5, we have

$$\operatorname{div}\left(\frac{\mathfrak{p}'(z)}{f(z)}\right) = -(s_1) - (-s_1) - (0) + \text{positive terms}$$
$$\operatorname{div}\left(\frac{1}{f(z)}\right) = -(s_1) - (-s_1) + \text{positive terms}$$

   From the above equations, we know that any linear combination of $\frac{\mathfrak{p}'(z)}{f(z)}$ and $\frac{1}{f(z)}$ will not have any poles except possibly at the three points 0, s_1, and $-s_1$. In particular,

$$\operatorname{div}\left(\left[\operatorname{Res}_{-s_1}\left(\frac{1}{f(z)}\right)\right]\cdot\left(\frac{\mathfrak{p}'(z)}{f(z)}\right) - \left[\operatorname{Res}_{-s_1}\left(\frac{\mathfrak{p}'(z)}{f(z)}\right)\right]\cdot\left(\frac{1}{f(z)}\right)\right) = -(s_1) - (0) + \text{positive terms},$$

   since this particular linear combination is constructed in such a way as to have no pole at $-s_1$. Hence, this linear combination represents a nonconstant function in $L(D_2)$.

6. Suppose $s_1 \neq s_2$. Apply the previous case to the pair $(s_1', s_2') = (s_1 - s_2, 0)$, and translate the resulting function by s_2.

In all cases, the conclusion that we draw is that $L(D_2)$ has dimension at least 2. We now proceed to show that $L(D_2)$ has dimension exactly 2. For this, we have to prove that any function $g \in L(D_2)$ is contained within the span of 1 and f, where f is the nonconstant function that we constructed above. We first assume that $s_1 = s_2$. In this case we may, by translating if necessary, assume that $s_1 = s_2 = 0$. The hypothesis $g \in L(2(0))$ implies that g must have a double pole at 0 or else g is constant by Proposition 2.4.1. Write

$$g(z) = \frac{c_{-2}}{z^2} + \frac{c_{-1}}{z} + c_0 + c_1 z + c_2 z^2 + \cdots,$$

and consider the function $g(z) - c_{-2}\mathfrak{p}(z)$. This elliptic function has at most a simple pole at $z = 0$, and it has no other poles since $g(z)$ and $\mathfrak{p}(z)$ are both well defined on $\mathbb{C}$ away from 0. By Proposition 2.4.1, the function $g(z) - c_{-2}\mathfrak{p}(z)$ must be constant. This proves our claim that $L(D_2) = \langle 1, \mathfrak{p}\rangle$.

If $s_1 \neq s_2$, then we have

$$\operatorname{div}(f) = -(s_1) - (s_2) + \text{positive terms}$$
$$\operatorname{div}(g) = -(s_1) - (s_2) + \text{positive terms}$$

where f is the nonconstant function that we constructed in $L(D_2)$, and g is any other function in $L(D_2)$. Observe that the assumption $s_1 \neq s_2$ guarantees that f and g both have at worst simple poles at s_2. Therefore the linear combination

$$h(z) = [\operatorname{Res}_{s_2}(g)]\cdot f(z) - [\operatorname{Res}_{s_2}(f)]\cdot g(z)$$

has no pole at s_2, so $\operatorname{div}(h)$ is of the form $\operatorname{div}(h) = -(s_1) + \text{positive terms}$. By Proposition 2.4.1, we conclude that $h(z)$ is constant, which proves that $g \in \langle 1, f\rangle$, as desired. This concludes our proof that $\ell(D_2) = 2$ for all divisors D_2 of the form $(s_1) + (s_2)$.

At this point, we possess in principle all the technical tools needed to compute $L(D)$ and $\ell(D)$ by hand for any particular divisor on an elliptic curve. For example, if $D_1' = (s_1) + (s_2) - (s_3)$, then just as in Example 2.4.4, we find that $L(D_1') \subset L(D_2)$ and that the map $f(z) \mapsto f(z) - f(s_3)$ is a surjective linear transformation, equal to the identity when restricted to $L(D_1')$, with kernel consisting of the constant functions, so $\ell(D_1') = 1$. However, rather than repeating the same laborious calculations whenever we want to compute a linear space, we now state (and prove) the Riemann-Roch theorem, which provides a formula relating the degree of a divisor to the dimension of the linear space of that divisor.

Theorem 2.4.6 (Riemann-Roch)**.** *Let D be a divisor on an algebraic curve C. There exists an integer g, depending only on the curve C, such that the following equations hold.*

(Riemann) If $\deg(D) \geq 0$*, then*

$$\deg(D) + 1 \geq \ell(D) \geq \deg(D) + 1 - g.$$

(Roch) If $\deg(D) > 2g - 2$*, then*

$$\ell(D) = \deg(D) + 1 - g.$$

The integer g is called the genus *of the curve C.*

Note that when $\deg(D) < 0$, the dimension of the linear space $L(D)$ is always equal to zero, which is why the statement of the Riemann-Roch theorem does not need to mention the case $\deg(D) < 0$.

2.5 Proof of the Riemann-Roch theorem

We will prove Riemann-Roch in the case of elliptic curves over $\mathbb{C}$. Our approach will be to prove the theorem for $\mathbb{C}/\Lambda$, and then appeal to Theorems 2.3.7 and 2.3.8 to argue that the proof for $\mathbb{C}/\Lambda$ automatically implies the corresponding result for the corresponding elliptic curve $y^2 = x^3 - (15G_4)x - (35G_6)$. This suffices to prove the theorem for all elliptic curves originating from lattices, because the statement of Riemann-Roch only depends on the divisors and the linear spaces, and Theorems 2.3.7 and 2.3.8 imply that the divisors, meromorphic functions, and linear spaces in the two cases are identical.

We emphasize once again that we do not prove that every complex elliptic curve originates from a lattice. Those who are curious can find a proof of this fact in [6, §1.4]. We also will not prove the Riemann-Roch theorem for curves other than elliptic curves, although we do discuss the case of the extended complex plane. It should be mentioned that the proof of Riemann-Roch in the case of the extended complex plane is easier than the case of elliptic curves, and a well motivated student who has gotten to this point should have no problem producing the proof for that case.

We first observe that the genus g of an elliptic curve must be equal to 1. This value can be surmised from our previous computations indicating that $\ell((s)) = 1$ and $\ell((s_1) + (s_2)) = 2$; moreover, it is the only value of g that is consistent with what we will prove below. Compare this to the case of the extended complex plane $\mathbb{C} \cup \{\infty\}$, where the genus g is 0. Our task is thus to prove that $\deg(D) + 1 \geq \ell(D)$ for degree 0 divisors D, and $\ell(D) = \deg(D)$ in general whenever $\deg(D) > 0$.

The following definition of linear equivalence massively facilitates the task of proving the Riemann-Roch theorem.

Definition 2.5.1. Two divisors D_1 and D_2 are *linearly equivalent* (denoted by $D_1 \sim D_2$) if there exists a nonzero meromorphic function f such that

$$D_1 = D_2 + \operatorname{div}(f).$$

In other words, two divisors are linearly equivalent if and only if their difference is a principal divisor.

Linear equivalence is the geometric analogue of the algebraic notion of equivalence of ideals modulo principal ideals [3, p. 22]. From the equations $\operatorname{div}(fg) = \operatorname{div}(f) + \operatorname{div}(g)$ and $\operatorname{div}(1/f) = -\operatorname{div}(f)$, it is evident that $\sim$ is an equivalence relation.

Proof of Riemann-Roch for elliptic curves. We begin by observing that if D_1 is linearly equivalent to D_2, and Riemann-Roch holds for D_1, then Riemann-Roch holds for D_2. This observation drastically reduces the number of cases that we have to consider. The proof of this observation is quite simple. Suppose $D_1 \sim D_2$, with $D_1 = D_2 + \operatorname{div}(g)$. It suffices to show that $\deg(D_1) = \deg(D_2)$ and $\ell(D_1) = \ell(D_2)$. Moreover, the first equality is obvious since $\deg \operatorname{div}(g) = 0$. Now let $f \in L(D_1)$, so that $\operatorname{div}(f) + D_1 =$ positive terms. Then $\operatorname{div}(f) + \operatorname{div}(g) + D_2 =$ positive terms, so $fg \in L(D_2)$. Therefore, multiplication by g is an injection from $L(D_1)$ to $L(D_2)$. We conclude that $\ell(D_1) \leq \ell(D_2)$. However, since $\sim$ is an equivalence relation, we can use the symmetry property of equivalence relations to conclude that $\ell(D_2) \leq \ell(D_1)$, so the two are equal.

Before continuing with the proof, we prove the following useful lemma.

Lemma 2.5.2. *Let $s_1, s_2, s_3, s_4 \in \mathbb{C}/\Lambda$. Then $(s_1) + (s_2) \sim (s_3) + (s_4)$ if and only if $s_1 + s_2 = s_3 + s_4$.*

Proof. By definition of linear equivalence, $(s_1) + (s_2) \sim (s_3) + (s_4)$ if and only if there exists a nonzero meromorphic function f such that $\operatorname{div}(f) = (s_1) + (s_2) - (s_3) - (s_4)$. Theorem 2.2.5(c) applied to f proves the only if direction. To prove the if direction, we may assume that neither of s_1 or s_2 is equal to either s_3 or s_4 (otherwise, Proposition 2.4.1 suffices to prove the theorem). Choose a nonconstant elliptic function $g(z)$ such that $\operatorname{div}(g) = -(s_3) - (s_4) +$ positive terms. Such a function was constructed in Example 2.4.5. Consider the elliptic function

$$h(z) = g(z) - g(s_1).$$

The degree of $\operatorname{div}(h)$ is 0 and h has poles at s_3 and s_4, a zero at s_1, and no other poles. Hence

$$\operatorname{div}(h) = -(s_3) - (s_4) + (s_1) + (r)$$

for some $r \in \mathbb{C}/\Lambda$. By Theorem 2.2.5(c), we must have $r = s_3 + s_4 - s_1$. But $s_1 + s_2 = s_3 + s_4$ by hypothesis, so we obtain $r = s_2$, as desired. □

We can now prove the Riemann-Roch theorem for degree 0 divisors. Let

$$D_0 = \sum_{i=1}^{n} (r_i) - \sum_{j=1}^{n} (s_j)$$

be any degree 0 divisor. We proceed by induction on n. If $n = 0$ or $n = 1$, the theorem is true by what we did in Example 2.4.5. If $n \geq 2$, then Lemma 2.5.2 implies $(r_{n-1}) + (r_n) - (s_n) \sim (r_{n-1} + r_n - s_n)$. Hence

$$D_0 \sim \sum_{i=1}^{n-2} (r_i) + (r_{n-1} + r_n - s_n) - \sum_{j=1}^{n-1} (s_j),$$

and the theorem is true for the right hand side by induction, so the theorem is also true for D_0.

The proof for degree 1 divisors is similar. Let

$$D_1 = \sum_{i=1}^{n+1} (r_i) - \sum_{j=1}^{n} (s_j)$$

be a degree 1 divisor. We prove Riemann-Roch by induction on n. For $n = 0$ the result was already proved in Example 2.4.5. For $n \geq 1$, we have

$$D_1 \sim \sum_{i=1}^{n-1} (r_i) + (r_n + r_{n+1} - s_n) - \sum_{j=1}^{n-1} (s_j),$$

so the theorem follows by induction.

We now proceed to the general case. Let

$$D_k = \sum_{i=1}^{n+k} (r_i) - \sum_{i=1}^{n} (s_i)$$

be a degree k divisor. By repeated application of the relation $(r_{n+k-1})+(r_{n+k})-(s_k) \sim (r_{n+k-1}+r_{n+k}-s_k)$, we may assume $n = 0$. In this case,

$$D_k = \sum_{i=1}^{k} (r_i),$$

and now we apply the relation $(r_{k-1}) + (r_k) \sim (0) + (r_{k-1} + r_k)$ to reduce to the case

$$D_k = (k-1)(0) + (r_1 + r_2 + \cdots + r_k).$$

For simplicity, let ρ denote $\sum_i r_i$ and D denote D_k, so that $D = D_k = (k-1)(0) + (\rho)$. We will consider separately the cases $\rho = 0$ and $\rho \neq 0$.

Consider the case when $\rho = 0$. We first show that $L(D)$ contains at least k linearly independent elements. Write x for $\mathfrak{p}$ and y for $-\mathfrak{p}'/2$. The functions

$$1, x, x^2, x^3, x^4, x^5, \ldots$$

have poles of order $0, 2, 4, 6, 8, 10, \ldots$ at $z = 0$, and no other poles. The functions

$$y, xy, x^2y, x^3y, x^4y, \ldots$$

have poles of order $3, 5, 7, 9, 11, \ldots$ at $z = 0$, and no other poles. Furthermore, these functions are all linearly independent over $\mathbb{C}$, by the proof of Corollary 2.3.9. Consequently, we find that $L(D)$ for a degree k divisor D contains k linearly independent elements out of these two lists alone. To ease notation, we denote these elements by $f_0, f_2, f_3, \ldots, f_k$, where $\mathrm{ord}_0(f_i) = -i$. To finish the proof, it suffices to show that these elements f_i span $L(D)$. Let g be any other function in $L(D)$. We proceed by induction on $\mathrm{ord}_0(g)$. If $\mathrm{ord}_0(g) = 0$, then g has no poles and is constant. We skip the case of $\mathrm{ord}_0(g) = -1$ since this case is impossible by Proposition 2.4.1. When $\mathrm{ord}_0(g) = i \leq -2$, we have

$$g(z) = \frac{c_{-i}}{z^i} + \text{higher order terms},$$

and

$$g(z) - c_{-i} f_i(z) = \frac{0}{z_i} + \text{higher order terms},$$

so by the induction hypothesis, $g(z) - c_{-i} f_i(z)$ lies in $\langle f_0, f_2, \ldots, f_k \rangle$, and hence $g(z)$ does as well.

The final step in the proof is to show that the theorem holds when $D = (k-1)(0) + (\rho)$, and $\rho \neq 0$. For this, we let $D' = (k-1)(0)$ and observe that $L(D') \subset L(D)$. This shows that $\ell(D) \geq k - 1$. Let f be a nonconstant function having simple poles at 0 and ρ and no other poles. Such a function exists by Example 2.4.5. Then f is an element of $L(D)$ which does not lie in $L(D')$, so $\ell(D) \geq k$. To finish the proof, we only need to show that the functions $\{f, f_0, f_2, \ldots, f_{k-1}\}$ span $L(D)$. Let g be any element of $L(D)$, and consider as usual the function

$$h(z) = [\mathrm{Res}_\rho(f)] \cdot g(z) - [\mathrm{Res}_\rho(g)] \cdot f(z).$$

Then h lies in $L(D)$ and h has no pole at $z = \rho$, so h in fact lies in $L(D')$. We conclude that $h \in \langle f_0, f_2, \ldots, f_{k-1} \rangle$, from which it follows that $g \in \langle f, f_0, f_2, \ldots, f_{k-1} \rangle$. Therefore $\ell(D) = k$, and the Riemann-Roch theorem for elliptic curves is proved. $\square$

Chapter 3

Arithmetic of Elliptic Curves

In this chapter, we switch perspectives and consider elliptic curves over fields other than the field of complex numbers, with emphasis on finite fields. We will make liberal use of results such as the Riemann-Roch theorem, even though up to this point we have only proved the corresponding results in the case of elliptic curves over the complex numbers. Although this practice is to some extent unfair to the reader, we believe that it is superior to any of the available alternatives. For example, it is certainly better to give a proof for the complex case than to give no proof at all; on the other hand, to present a full-blown proof in the general case would require far more resources than are available to us in a short treatise such as this one.

The unsatisfying aspects of the previous paragraph can be mitigated in a number of ways. First of all, it must be emphasized that in the vast majority of such cases, the complex geometry actually provides the proper intuition for dealing with elliptic curves over (say) finite fields, even if the actual proof in the case of finite fields is quite different from the proof for complex numbers. Second, in a great many situations, the proof of a given result for elliptic curves over complex numbers actually implies the same result for finite fields. One example is the proof of associativity of geometric addition on an elliptic curve—because the statement of associativity constitutes an equality of two rational functions, proving that the functions are equal over $\mathbb{C}$ suffices to prove that they are equal over any field. Finally, as we remarked in the beginning of the book, there are a number of algorithms in pairing based cryptography that depend directly on elliptic curves over the complex numbers, so even those readers who are purely interested in cryptography can rest assured that a proper understanding of the complex number case is necessary as a foundation for further progress in this area.

For the rest of this book, we will assume without comment that properties of elliptic curves over complex numbers carry through without change to other fields such as finite fields. Of course, there are some properties that do **not** carry through as expected (such as the structure of p-torsion points in supersingular curves), and in such cases we will of course make a special comment to alert the reader to this fact.

3.1 Elliptic curves and addition

We first define what an elliptic curve is over a general finite field. Afterwards, we give the geometric definition of the group law on an elliptic curve. Readers having prior experience with elliptic curves will of course be familiar with the group law, but our goal here is to discuss the group law from the perspective of divisors and the Riemann-Roch theorem.

Definition 3.1.1. Let K be a field of characteristic not equal to 2. An *elliptic curve* E over K, denoted E/K or $E(K)$, is the set of solutions $(x, y) \in K^2$ to an equation of the form

$$y^2 = x^3 + a_2x^2 + a_4x + a_6,$$

where the cubic polynomial has no repeated roots in an algebraic closure of K, together with a formal point at infinity, denoted ∞.

Definition 3.1.2. Let E/K be an elliptic curve. The *geometric sum* or *point sum* of two points P and Q in E is defined as follows.

- If $Q = \infty$, then $P + Q = P$.
- If $P = \infty$, then $P + Q = Q$.
- If $P = (x, y)$ and $Q = (x, -y)$ for some $x, y \in K$, then $P + Q = \infty$.
- In all other cases:
  - If $P = Q = (x, y)$, then draw the tangent line L to E in the x, y-plane passing through the point P. This line L intersects E in exactly one other point $R = (x', y')$. Define $P + Q = (x', -y')$. In other words, $P + Q = (x_2, y_2)$ where

$$x_2 = \frac{x^4 - 2a_4x^2 - 8a_6x + (a_4^2 - 4a_2a_6)}{4(x^3 + a_2x^2 + a_4x + a_6)}$$
$$y_2 = \frac{x^3 - a_4x - 2a_6}{2y} - \frac{(x^4 - 2a_4x^2 - 8a_6x + (a_4^2 - 4a_2a_6))(3x^2 + 2a_2x + a_4)}{8(x^3 + a_2x^2 + a_4x + a_6)y}$$

  - If $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ with $P \neq Q$, then draw the line L in the x, y-plane passing through P and Q. This line L intersects E in exactly one other point $R = (x', y')$. Define $P + Q = (x', -y')$. In other words, $P + Q = (x_3, y_3)$ where

$$x_3 = \frac{(y_2 - y_1)^2}{(x_2 - x_1)^2} - x_1 - x_2 - a_2$$
$$y_3 = \frac{x_1y_2 - x_2y_1}{x_2 - x_1} - \left(\frac{y_2 - y_1}{x_2 - x_1}\right)\left(\frac{(y_2 - y_1)^2}{(x_2 - x_1)^2} - x_1 - x_2 - a_2\right)$$

It is not obvious from the definition of geometric sum that the operation is associative—other group properties, such as existence of identity, inverses, and even commutativity, are obvious, but associativity is not. Our immediate goal is to prove that the operation is associative, and we will do so using Riemann-Roch. We give this argument in some detail because everything that we prove along the way will also turn out to be necessary for defining cryptographic pairings.

Lemma 3.1.3. *Let P and Q be points on an elliptic curve E. The divisors (P) and (Q) are linearly equivalent if and only if $P = Q$; that is, $(P) \sim (Q) \iff P = Q$.*

Proof. The $\Leftarrow$ direction is obvious. To prove the $\Rightarrow$ direction, suppose $(P) \sim (Q)$. By definition of $\sim$, there exists a rational function f such that $\mathrm{div}(f) = (P) - (Q) = -(Q) + (P)$. By definition of linear space, it follows that $f \in L((Q))$. By Riemann-Roch, the dimension of $L((Q))$ is equal to 1, implying that $L((Q))$ consists only of the constant functions. Hence f is a constant function, and $(P) - (Q) = \mathrm{div}(f) = \emptyset$. The only way this can happen is if $P = Q$. □

Theorem 3.1.4. *For every degree zero divisor D on E, there exists a unique point $P \in E$ such that $D \sim (P) - (\infty)$.*

Proof. The divisor $D + (\infty)$ has degree 1. By Riemann-Roch, the linear space $L(D + (\infty))$ has dimension 1. Let $\{f\}$ be a basis for $L(D + (\infty))$, consisting of one element. By definition of linear space, the divisor $D' = \mathrm{div}(f) + D + (\infty)$ consists only of positive terms. However, D' also has degree 1. The only way a positive divisor can have degree 1 is if the divisor consists of one single term, i.e. $D' = (P)$ for some point $P \in E$. We have proven that

$$(P) = \mathrm{div}(f) + D + (\infty),$$

which is the same thing as saying that $D \sim (P) - (\infty)$. This establishes the existence of P.

To show uniqueness, suppose $(P) - (\infty) \sim (P') - (\infty)$. Then $(P) \sim (P')$ as well, so Lemma 3.1.3 implies $P = P'$. □

Theorem 3.1.5. *For any two points $P, Q \in E$,*

$$(P) - (\infty) + (Q) - (\infty) \sim (P + Q) - (\infty),$$

where the addition sign on the right hand side denotes geometric addition.

Proof. We will prove the theorem in the case where P and Q are distinct points not equalling ∞. The proof for the other cases is no harder, but the variations are somewhat tedious to write down.

Let $ax + by + c$ be the equation of the line passing through the points P and Q, and let $x - d$ be the equation of the vertical line passing through $P + Q$. These two lines intersect at a common point R lying on the elliptic curve.

We have

$$\begin{aligned} \operatorname{div}(ax + by + c) &= (P) + (Q) + (R) - 3(\infty), \\ \operatorname{div}(x - d) &= (R) + (P + Q) - 2(\infty), \\ \operatorname{div}\left(\frac{ax + by + c}{x - d}\right) &= (P) + (Q) - (P + Q) - (\infty), \end{aligned}$$

implying that $(P) - (\infty) + (Q) - (\infty) - [(P + Q) - (\infty)]$ is a principal divisor, as required. □

We remark in passing that this theorem together with Theorem 3.1.4 and Lemma 2.5.2 implies that the map ϕ of Theorem 2.3.7 is an isomorphism of additive groups between $\mathbb{C}/\Lambda$ and E.

Theorem 3.1.6. *Elliptic curve geometric addition is associative, i.e.,*

$$(P + Q) + R = P + (Q + R)$$

for all $P, Q, R \in E$.

Proof. By applying Theorem 3.1.5 four times, we find that

$$((P + Q) + R) - (\infty) \sim (P) - (\infty) + (Q) - (\infty) + (R) - (\infty) \sim (P + (Q + R)) - (\infty).$$

The equality of $(P + Q) + R$ and $P + (Q + R)$ now follows from Theorem 3.1.4. □

Theorem 3.1.7. *Let $D = \sum a_P(P)$ be any degree zero divisor on E. Then*

$$D \sim \left(\sum a_P P\right) - (\infty),$$

where the interior sum denotes elliptic curve point addition.

Proof. Since D has degree zero, the equation

$$D = \sum a_P[(P) - (\infty)]$$

holds. Now apply Theorem 3.1.5 repeatedly. □

3.2 Weil pairing

We are now in a position to define the Weil pairing, which is nowadays regarded as one of the fundamental mathematical primitives of modern elliptic curve cryptography (although its status as such constitutes a relatively recent development).

Definition 3.2.1. Let E/K be an elliptic curve and let $n > 0$ be an integer. The set of *n-torsion points* of E, denoted $E[n]$, is given by

$$E[n] := \left\{ P \in E(\bar{K}) \mid nP = \infty \right\},$$

where $\bar{K}$ denotes the algebraic closure of K. The set $E[n]$ is always a subgroup of $E(\bar{K})$.

If the characteristic of K does not divide n, then the group $E[n]$ is isomorphic as a group to $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. This is easy to see in the case of elliptic curves defined over the complex numbers, for in this case $E[n]$ is generated by the two points w_1/n and w_2/n in $\mathbb{C}/\Lambda$, and these two points evidently generate a subgroup of $\mathbb{C}/\Lambda$ isomorphic to $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

Definition 3.2.2. Let f be a rational function and let $D = \sum a_P(P)$ be a degree zero divisor on E. The value of f at D, denoted $f(D)$, is the element

$$f(D) := \prod f(P)^{a_P} \in K.$$

Definition 3.2.3. Let E be an elliptic curve over K. Fix an integer $n > 0$ such that $\mathrm{char}(K) \nmid n$ and $E[n] \subset E(K)$. For any two points $P, Q \in E[n]$, let A_P be any divisor linearly equivalent to $(P) - (\infty)$ (and similarly for A_Q). By Theorem 3.1.7, the divisor nA_P is linearly equivalent to $(nP) - (n\infty) = \emptyset$. Hence nA_P is a principal divisor. Let f_P be any rational function having divisor equal to nA_P (and similarly for f_Q).

The *Weil pairing* of P and Q is given by the formula

$$e(P, Q) = \frac{f_P(A_Q)}{f_Q(A_P)},$$

valid whenever the expression is defined (i.e., neither the numerator nor the denominator nor the overall fraction involves a division by zero).

Proposition 3.2.4. *The Weil pairing is well defined for any pair of points $P, Q \in E[n]$.*

Proof. The definition of Weil pairing involves a choice of divisors A_P, A_Q and a choice of rational functions f_P, f_Q. In order to prove the proposition, we need to show that for any two points P, Q there exists a choice such that $e(P, Q)$ is defined, and that any other set of choices for which $e(P, Q)$ is defined leads to the same value.

We will begin by proving the second part. To start with, the choice of f_P does not affect the value of $e(P, Q)$, since for any other function $\hat{f}_P$ sharing the same divisor, we have

$$\mathrm{div}(\hat{f}_P / f_P) = \emptyset,$$

which means $\hat{f}_P = c f_P$ for some nonzero constant $c \in K$. It follows then that $\hat{f}_P(A_Q) = f_P(A_Q)$, since A_Q has degree zero, and therefore the factors of c cancel out in the formula of Definition 3.2.2.

We now prove that the choice of A_P does not affect the value of $e(P, Q)$; the proof for A_Q is similar. If $\hat{A}_P$ is another divisor linearly equivalent to A_P, then $\hat{A}_P = A_P + \mathrm{div}(g)$ for some rational function g. It follows that $\hat{f}_P := f_P \cdot g^n$ is a rational function whose divisor is equal to $n\hat{A}_P$. The value of $e(P, Q)$ under this choice of divisor is equal to

$$\hat{e}(P, Q) = \frac{\hat{f}_P(A_Q)}{f_Q(\hat{A}_P)} = \frac{f_P(A_Q) g(A_Q)^n}{f_Q(A_P) f_Q(\mathrm{div}(g))} = \frac{f_P(A_Q)}{f_Q(A_P)} \, \frac{g(nA_Q)}{f_Q(\mathrm{div}(g))} = e(P, Q) \, \frac{g(\mathrm{div}(f_Q))}{f_Q(\mathrm{div}(g))}.$$

The fraction on the right hand side is equal to one by the *Weil reciprocity formula*, a proof of which can be found in [2]. We limit our remarks here to the observation that the Weil reciprocity formula is relatively easy to prove for rational functions in $\mathbb{C} \cup \{\infty\}$, i.e., rational functions in one variable.

To complete the proof, we need to show that there exists a choice of divisors A_P and A_Q for which the calculation of $e(P, Q)$ does not involve division by zero. The naive choice of $A_P = (P)-(\infty)$, $A_Q = (Q)-(\infty)$ does not work whenever $Q \neq \infty$, because in this case $\mathrm{div}(f_Q) = n(Q) - n(\infty)$, so f_Q has a pole at ∞, and consequently

$$f_Q(A_P) = \frac{f_Q(P)}{f_Q(\infty)} = 0.$$

To fix this problem, let R be any point in $E(\bar{K})$ not equal to any of the four points Q, ∞, $-P$, $Q - P$. Here $\bar{K}$ denotes the algebraic closure of K, over which E has infinitely many points, guaranteeing that such an R exists. Set $A_P = (P + R) - (R)$. Then A_P is linearly equivalent to $(P) - (\infty)$, and

$$f_Q(A_P) = \frac{f_Q(P + R)}{f_Q(R)} \in K^*,$$

since $\mathrm{div}(f_Q) = n(Q) - n(\infty)$, and we have chosen R in such a way that neither R nor $P + R$ coincides with either Q or ∞. Similarly, we find that

$$f_P(A_Q) = \frac{f_P(Q)}{f_P(\infty)} \in K^*,$$

because $\mathrm{div}(f_P) = n(P + R) - n(R)$, and neither Q nor ∞ coincides with R or $P + R$. □

Theorem 3.2.5. *The Weil pairing satisfies the following properties.*

- $e(P_1 + P_2, Q) = e(P_1, Q)\ e(P_2, Q)$ *and* $e(P, Q_1 + Q_2) = e(P, Q_1)\ e(P, Q_2)$ *(bilinearity)*
- $e(aP, Q) = e(P, aQ) = e(P, Q)^a$*, for all* $a \in \mathbb{Z}$
- $e(P, \infty) = e(\infty, Q) = 1$
- $e(P, Q)^n = 1$
- $e(P, Q) = e(Q, P)^{-1}$ *and* $e(P, P) = 1$ *(anti-symmetry)*
- *If* $P \neq \infty$ *and* K *is algebraically closed, there exists* $Q \in E$ *such that* $e(P, Q) \neq 1$ *(non-degeneracy)*

Proof. We begin with bilinearity. Suppose $P_1, P_2, Q \in E[n]$. Observe that

$$A_{P_1+P_2} \sim (P_1 + P_2) - (\infty) \sim (P_1) - (\infty) + (P_2) - (\infty) \sim A_{P_1} + A_{P_2}$$

by Theorem 3.1.5. Hence we may use $A_{P_1} + A_{P_2}$ as our choice of $A_{P_1+P_2}$. Moreover, if f_{P_1} and f_{P_2} are rational functions having divisor nA_{P_1} and nA_{P_2} respectively, then

$$\mathrm{div}(f_{P_1} f_{P_2}) = \mathrm{div}(f_{P_1}) + \mathrm{div}(f_{P_2}) = nA_{P_1} + nA_{P_2} = nA_{P_1+P_2}.$$

Accordingly, we may take $f_{P_1+P_2}$ to be equal to $f_{P_1} f_{P_2}$. Therefore,

$$e(P_1 + P_2, Q) = \frac{f_{P_1+P_2}(A_Q)}{f_Q(A_{P_1+P_2})} = \frac{(f_{P_1} f_{P_2})(A_Q)}{f_Q(A_{P_1} + A_{P_2})} = \frac{f_{P_1}(A_Q) f_{P_2}(A_Q)}{f_Q(A_{P_1}) f_Q(A_{P_2})} = e(P_1, Q)\ e(P_2, Q),$$

as desired. The proof that $e(P, Q_1 + Q_2) = e(P, Q_1)\ e(P, Q_2)$ is similar.

The property $e(aP, Q) = e(P, aQ) = e(P, Q)^a$ follows from bilinearity, and $e(P, \infty) = e(\infty, Q) = 1$ is a consequence of the definition of the Weil pairing. These two facts together imply that $e(P, Q)^n = e(nP, Q) = e(\infty, Q) = 1$.

Anti-symmetry follows from the definition of the Weil pairing, since

$$e(P, Q) = \frac{f_P(A_Q)}{f_Q(A_P)} = \left(\frac{f_Q(A_P)}{f_P(A_Q)}\right)^{-1} = e(Q, P)^{-1}.$$

We will not prove non-degeneracy, since it can be easily verified in practice via computation. A proof of non-degeneracy can be found in [2]. □

3.3 Tate pairing

The Tate pairing is a non-degenerate bilinear pairing which shares much in common with the Weil pairing. It is generally preferred over the Weil pairing in most implementations of cryptographic protocols, because it can be computed more efficiently.

Definition 3.3.1. Let E be an elliptic curve over a field K. Fix an integer $n > 0$ for which $\mathrm{char}(K) \nmid n$ and $E[n] \subset E(K)$. For any two points $P, Q \in E[n]$, the *Tate proto-pairing* of P and Q, denoted $\langle P, Q \rangle$, is given by the formula

$$\langle P, Q \rangle := f_P(A_Q) \in K^*/K^{*n},$$

valid whenever the expression $f_P(A_Q)$ is defined and nonzero.

Proposition 3.3.2. *The value of the Tate proto-pairing is well defined, independent of the choices of A_P, A_Q, and f_P.*

Proof. As in the case of the Weil pairing, the choice of f_P is irrelevant once A_P is fixed. We may thus take $A_P = (P) - (\infty)$ and $A_Q = (Q + R) - (R)$ where $R \neq P, \infty, -Q, P - Q$. For this choice of A_P and A_Q, the expression $f_P(A_Q)$ will be a nonzero element of K.

We now show that $\langle P, Q \rangle$ takes on the same value independent of the choice of A_P and A_Q. If a different value of A_Q is chosen, say $\hat{A}_Q = A_Q + \mathrm{div}(g)$, then, using Weil reciprocity, we find that

$$\widehat{\langle P, Q \rangle} = f_P(\hat{A}_Q) = f_P(A_Q)\ f_P(\mathrm{div}(g)) = f_P(A_Q)\ g(\mathrm{div}(f_P)) = f_P(A_Q)\ g(nA_P) = f_P(A_Q)\ g(A_P)^n.$$

The latter expression is equal to $\langle P, Q \rangle = f_P(A_Q)$ in the quotient group K^*/K^{*n}. Likewise, if a different divisor $\hat{A}_P = A_P + \mathrm{div}(g)$ is used, then $n\hat{A}_P = \mathrm{div}(f_P \cdot g^n)$, so

$$\widehat{\langle P, Q \rangle} = \hat{f}_P(A_Q) = f_P(A_Q)g(A_Q)^n \equiv f_P(A_Q) \pmod{K^{*n}}.$$

□

Theorem 3.3.3. *The Tate proto-pairing satisfies the following properties.*

- $\langle P_1 + P_2, Q \rangle = \langle P_1, Q \rangle\ \langle P_2, Q \rangle$ *and* $\langle P, Q_1 + Q_2 \rangle = \langle P, Q_1 \rangle\ \langle P, Q_2 \rangle$ *(bilinearity)*
- $\langle aP, Q \rangle = \langle P, aQ \rangle = \langle P, Q \rangle^a$ *for all* $a \in \mathbb{Z}$
- $\langle P, \infty \rangle = \langle \infty, Q \rangle = 1$
- $\langle P, Q \rangle^n = 1$
- *If $P \neq \infty$, and K is algebraically closed, there exists $Q \in E[n]$ such that $\langle P, Q \rangle \neq 1$ (non-degeneracy)*

Note that the Tate proto-pairing is **not** anti-symmetric.

Proof. As in the case of the Weil pairing, we may take $A_{Q_1+Q_2}$ to be $A_{Q_1} + A_{Q_2}$, and $f_{P_1+P_2}$ to be $f_{P_1} f_{P_2}$. In this case,

$$\langle P_1 + P_2, Q \rangle = f_{P_1+P_2}(A_Q) = f_{P_1}(A_Q)\ f_{P_2}(A_Q) = \langle P_1, Q \rangle\ \langle P_2, Q \rangle,$$
$$\langle P, Q_1 + Q_2 \rangle = f_P(A_{Q_1} + A_{Q_2}) = f_P(A_{Q_1})\ f_P(A_{Q_2}) = \langle P, Q_1 \rangle\ \langle P, Q_2 \rangle.$$

All of the other properties (except for non-degeneracy) follow from bilinearity and the definition of the pairing. We will not prove non-degeneracy (see [2]). □

Definition 3.3.4. Let $K = \mathbb{F}_q$ be a finite field of q elements. Let n be an integer dividing $q - 1$, and fix two points $P, Q \in E[n]$. The *Tate pairing* $T(P, Q)$ of P and Q is the value

$$T(P, Q) = \langle P, Q \rangle^{\frac{q-1}{n}} \in \mathbb{F}_q^*.$$

Theorem 3.3.5. *The Tate pairing satisfies all the properties of Theorem 3.3.3.*

Proof. Exponentiation by $\frac{q-1}{n}$ is an isomorphism from $\mathbb{F}_q^*/\mathbb{F}_q^{*n}$ to $\left(\mathbb{F}_q^*\right)^{\frac{q-1}{n}}$, so all of the properties in Theorem 3.3.3 hold for the Tate pairing. □

3.4 Calculating pairings

The calculation of Weil and Tate pairings on an elliptic curve $E/\mathbb{F}_q$ can be performed in a number of field operations polynomial in $\log(n)$, thanks to the following algorithm discovered by Victor Miller [4], which we present here.

Fix a triple of n-torsion points $P, Q, R \in E[n]$. We assume for simplicity that n is large, since this is the most interesting case from an implementation standpoint. For each integer m between 1 and n, let f_m denote a rational function whose divisor has the form

$$\mathrm{div}(f_m) = m(P+R) - m(R) - (mP) + (\infty).$$

We will first demonstrate an algorithm for calculating $f_n(Q)$, and then show how we can use this algorithm to find $e(P, Q)$.

For any two points $P_1, P_2 \in E[n]$, let $g_{P_1,P_2}(x, y) = ax+by+c$ be the equation of the line passing through the two points P_1 and P_2. In the event that $P_1 = P_2$, we set $g_{P_1,P_2}(x, y)$ to be equal to the tangent line at P_1. If either P_1 or P_2 is equal to ∞, then g_{P_1,P_2} is the equation of the vertical line passing through the other point; and finally, if $P_1 = P_2 = \infty$, then we define $g_{P_1,P_2} = 1$. In all cases,

$$\mathrm{div}(g_{P_1,P_2}) = (P_1) + (P_2) + (-P_1 - P_2) - 3(\infty).$$

To calculate $f_m(Q)$ for $m = 1, 2, \ldots, n$, we proceed by induction on m. If $m = 1$, then the function

$$f_1(x, y) = \frac{g_{P+R,-P-R}(x, y)}{g_{P,R}(x, y)}$$

has divisor equal to $(P + R) - (R) - (P) + (\infty)$. We can evaluate this function at Q to obtain $f_1(Q)$.

For values of m greater than 1, we consider separately the cases of m even and m odd. If m is even, say $m = 2k$, then

$$f_m(Q) = f_k(Q) \cdot \frac{g_{kP,kP}(Q)}{g_{mP,-mP}(Q)},$$

while if m is odd we have

$$f_m(Q) = f_{m-1}(Q) \cdot f_1(Q) \cdot \frac{g_{(m-1)P,P}(Q)}{g_{mP,-mP}(Q)}.$$

Note that every two steps in the induction process reduces the value of m by a factor of 2 or more. This feature is the reason why this method succeeds in calculating $f_n(Q)$ even for very large values of n.

The Tate pairing of two n-torsion points $P, Q \in E[n]$ can now be calculated as follows. Choose two random points $R, R' \in E[n]$. Set $A_P = (P + R) - (R)$ and $A_Q = (Q + R') - (R')$. Using the method above, find the values of $f_n(Q + R')$ and $f_n(R')$. Since $\mathrm{div}(f_n) = n(P + R) - n(R) - (nP) + (\infty) = nA_p = \mathrm{div}(f_P)$, we find that

$$\frac{f_n(Q + R')}{f_n(R')} = \frac{f_P(Q + R')}{f_P(R')} = f_P(A_Q).$$

It is now easy to calculate $T(P, Q) = f_P(A_Q)^{\frac{q-1}{n}}$. To find the Weil pairing, simply repeat the procedure in order to find $f_Q(A_P)$, and divide the two. As long as the integer n is sufficiently large, it is unlikely that the execution of this algorithm will yield a division by zero error. On the rare occasion when such an obstacle does arise, repeat the calculation using a different choice of random points R and R'.

A complete and working implementation of this algorithm in the Magma programming language can be found in Figure 3.1.

```
/* div(g) = (P1) + (P2) + (-P1-P2) - 3(O). This function evaluates g at Q. */
function g(E,P1,P2,Q)
        if ([P1[1],P1[2],P1[3]] eq [0,1,0]) and ([P2[1],P2[2],P2[3]] eq [0,1,0]) then
                return 1;
        elif ([P1[1],P1[2],P1[3]] eq [0,1,0]) then
                return Q[1]-P2[1];
        elif ([P2[1],P2[2],P2[3]] eq [0,1,0]) then
                return Q[1]-P1[1];
        elif (P1 eq P2) then
                return (3*P1[1]^2 + aInvariants(E)[4]) * (Q[1] - P1[1]) -
                        2*P1[2] * (Q[2] - P1[2]);
        else
                return (Q[1]-P1[1]) * (P2[2]-P1[2]) + (Q[2]-P1[2]) * (P1[1]-P2[1]);
        end if;
end function;

/* div(fm) = m(P1+P2) - m (P2) - (m P1) + (O). This function evaluates fm at Q. */
function f(m,E,P1,P2,Q)
        local k;
        if (m eq 1) then
                return g(E,P1+P2,-P1-P2,Q)/g(E,P1,P2,Q);
        elif IsEven(m) then
                k := Integers()!(m/2);
                return (f(k,E,P1,P2,Q))^2 * g(E,k*P1,k*P1,Q)/g(E,m*P1,-m*P1,Q);
        elif IsOdd(m) then
                return f(m-1,E,P1,P2,Q) * f(1,E,P1,P2,Q) *
                       g(E,(m-1)*P1,P1,Q)/g(E,m*P1,-m*P1,Q);
        end if;
end function;

/* Weil pairing of two n-torsion points P and Q over E. */
function Weil(E,P,Q,n)
        local R1,R2;
        R1 := E!((Integers()!(Order(E)/n^2)) * Random(E));
        R2 := E!((Integers()!(Order(E)/n^2)) * Random(E));
        P1 := E!P;
        return (f(n,E,P1,R1,Q+R2) * f(n,E,Q,R2,R1)) /
               (f(n,E,P1,R1,R2) * f(n,E,Q,R2,P1+R1));
end function;

/* Tate pairing of two n-torsion points P and Q over E. */
function Tate(E,P,Q,n)
        local R1,R2,exponent;
        R1 := E!((Integers()!(Order(E)/n^2)) * Random(E));
        R2 := E!((Integers()!(Order(E)/n^2)) * Random(E));
        P1 := E!P;
        exponent := Integers()!((#(Parent(aInvariants(E)[1]))-1)/n);
        return (f(n,E,P1,R1,Q+R2) / f(n,E,P1,R1,R2))^exponent;
end function;
```

Figure 3.1: Implementation of Weil and Tate pairings in the Magma programming language

Chapter 4

Elliptic Curve Cryptography

4.1 Foundations

Recall the ElGamal encryption scheme, which was one of the first public key cryptosystems to be discovered.

ElGamal encryption:

Setup: A finite field $\mathbb{F}_q$, together with an element $g \in (\mathbb{F}_q)^*$.

Key generation: The public key is (g, g^α), for some randomly chosen $\alpha \in_R \mathbb{Z}$. The private key is α.

Encryption: Given a message m, choose $r \in_R \mathbb{Z}$ at random and compute $c = m \oplus (g^\alpha)^r$. Send (g^r, c).

Decryption: Compute $c \oplus (g^r)^\alpha = m$.

The security of the ElGamal encryption scheme is contingent upon the *Diffie-Hellman assumption*, which states that given three elements $g, g^\alpha, g^\beta \in (\mathbb{F}_q)^*$, computing the value of $g^{\alpha\beta} \in (\mathbb{F}_q)^*$ is conjectured to be computationally infeasible. To date, the only known method for computing $g^{\alpha\beta}$ given (g, g^α, g^β) is to compute the value of α and then raise g^β to the α power. The conjecture that α is infeasible to compute given g and g^α is known as the *discrete logarithm assumption*.

In the context of elliptic curves, the discrete logarithm assumption states that given two points $P, \alpha P \in E(\mathbb{F}_q)$, it is in general computationally infeasible to find the value of α. Likewise, the Diffie-Hellman assumption for elliptic curves is the statement that $\alpha\beta P$ cannot feasibly be computed from $P, \alpha P, \beta P \in E(\mathbb{F}_q)$. For both $(\mathbb{F}_q)^*$ and $E(\mathbb{F}_q)$, the status of the discrete logarithm and Diffie-Hellman assumptions remains a major open problem.

Using the Diffie-Hellman assumption for elliptic curves as a starting point, we can construct a version of the ElGamal cryptosystem based upon elliptic curves. Indeed, this construction historically represents one of the first applications of elliptic curve arithmetic to cryptography.

Elliptic curve ElGamal encryption:

Setup: A finite field $\mathbb{F}_q$, an elliptic curve $E/\mathbb{F}_q$, and a point $P \in E(\mathbb{F}_q)$.

Key generation: The public key is $(P, \alpha P)$, for some randomly chosen $\alpha \in_R \mathbb{Z}$. The private key is α.

Encryption: Given a message m, choose $r \in_R \mathbb{Z}$ at random and compute $c = m \oplus r(\alpha P)$. Send (rP, c).

Decryption: Compute $c \oplus \alpha(rP) = m$.

Many other cryptographic primitives have their elliptic curve counterparts as well. We give one example of a public key signature scheme (called the Digital Signature Algorithm, or DSA), together with its elliptic curve counterpart ECDSA; there are many others.

Digital Signature Algorithm (DSA): Let H be a collision resistant hash function which maps messages into integers.

Setup: A cyclic subgroup $G \subset (\mathbb{F}_p)^*$ of size n, generated by $g \in G$.

Key generation: The public key is (g, g^α), for some randomly chosen $\alpha \in_R \mathbb{Z}$. The private key is α.

Signing: Given a message m, choose $k \in_R \mathbb{Z}$. Compute $r = g^k \bmod n$ and $s = \frac{H(m)+\alpha r}{k} \bmod n$. The signature is (r, s).

Verification: Compute $g^{\frac{H(m)}{s}} (g^\alpha)^{\frac{r}{s}}$ and check whether this quantity equals r.

Elliptic Curve Digital Signature Algorithm (ECDSA): Let H be a collision resistant hash function which maps messages into integers.

Setup: A finite field $\mathbb{F}_p$, an elliptic curve $E/\mathbb{F}_p$, and a point $P \in E(\mathbb{F}_p)$.

Key generation: The public key is $(P, \alpha P)$, for some randomly chosen $\alpha \in_R \mathbb{Z}$. The private key is α.

Signing: Given a message m, choose $k \in_R \mathbb{Z}$. Compute $r = x(kP)$ and $s = \frac{H(m)+\alpha r}{k} \bmod p$. The signature is (r, s).

Verification: Compute $x\left[\frac{H(m)}{s} P + \frac{r}{s}(\alpha P)\right]$ and check whether this quantity equals r.

The reason why elliptic curves are attractive for cryptography is because, at the present time, the best known algorithms for solving calculating discrete logarithms in $(\mathbb{F}_q)^*$ are, in general, asymptotically faster than the best known algorithms for calculating discrete logarithms in $E(\mathbb{F}_q)$. Specifically, if we let $L_n(\sigma, c)$ be the function defined by

$$L_n(\sigma, c) := \exp(c(\log n)^\sigma (\log\log n)^{1-\sigma}),$$

then, roughly speaking, the best known algorithms for computing discrete logarithms in $(\mathbb{F}_q)^*$ require $O(L_q(\frac{1}{3}, c))$ operations, whereas the best known algorithms for computing discrete logarithms in $E(\mathbb{F}_q)$ require $O(\sqrt{q}) = O(L_q(1, \frac{1}{2}))$ operations. Since $L_q(1, \frac{1}{2}) \gg L_q(\frac{1}{3}, c)$, the security of elliptic curve cryptosystems at present is superior to that afforded by traditional cryptosystems based upon the multiplicative group of a finite field.

4.2 Pairing based cryptography

Suppose we have an elliptic curve $E/\mathbb{F}_q$ for which a non-degenerate bilinear pairing exists on some subset $G \subset E$. We call such a pairing a *cryptographic pairing*. We have seen that cryptographic pairings exist whenever $E[n] \subset E(\mathbb{F}_q)$, for in this case we can take $G = E[n]$ and use the Weil pairing or the Tate pairing. When cryptographic pairings exist, it is possible to implement novel cryptographic protocols and primitives which cannot be realized in the absence of bilinear pairings. We give a few examples here in order to help guide our further study of pairings. The reader should keep these examples in mind, as they help to illuminate which of the mathematical properties of pairings are important from the standpoint of designing and implementing cryptosystems.

4.2.1 Identify Based Encryption (IBE)

The most notable feature of pairings is that they enable the practical construction of (conjecturally) secure identity based encryption schemes. An identity based encryption scheme (IBE) is defined to be a public key cryptosystem with the property that any string can be a public key. Unlike traditional public key cryptosystems, for which the use of a trusted third party (perhaps in the role of a Certificate Authority) is optional, IBE requires the use of a trusted third party for key generation.

Boneh-Franklin Identity Based Encryption: Let H be a collision resistant hash function which maps arbitrary strings into points of the group G described in the setup phase.

Setup: A finite field $\mathbb{F}_q$, an elliptic curve $E(\mathbb{F}_q)$, a cryptographic pairing e on $G \subset E(\mathbb{F}_q)$, and a point $P \in G$. The trusted third party generates a random integer $\alpha \in_R \mathbb{Z}$, and publishes αP, while keeping α secret.

Encryption: Let σ be any string. Then σ is a valid public key. To encrypt a message m to σ, choose $r \in_R \mathbb{Z}$ at random. Compute $Q = H(\sigma)$, $c = m \oplus e(\alpha P, rQ)$, and rP. Send (rP, c). Note that encryption can be performed even if the owner of the public key σ has not executed the key generation step.

Key generation: Let σ be any string. The public key is σ and the private key is $\alpha H(\sigma)$. The owner of any particular public key must interact with the trusted third party in order to obtain the corresponding private key.

Decryption: Let $Q = H(\sigma)$. Compute $c \oplus e(rP, \alpha Q) = m$.

The security of the Boneh-Franklin identity based encryption system is conditioned upon the *bilinear Diffie-Hellman assumption*, which states: given four points $P, \alpha P, \beta P, Q \in G$, it is computationally infeasible to calculate $e(P, Q)^{\alpha\beta}$.

4.2.2 One round tri-partite key agreement

In the classical Diffie-Hellman key agreement protocol, two parties A and B agree on a group G generated by an element $g \in G$ and broadcast to each other the quantities g^α and g^β, where α and β are secret integers known only to A and B respectively. Each party can then derive the common quantity $g^{\alpha beta} = (g^\alpha)^\beta = (g^\beta)^\alpha$ knowing only one of the two integers α, β. An eavesdropper to the communication will not know the value of either α or β, and will not be able to determine the quantity $g^{\alpha\beta}$ unless the Diffie-Hellman assumption is false.

A variant of this protocol, based on pairings, allows for three parties A, B, and C to broadcast public information in such a way that the three participants can derive a common value which is known only to them and not to outsiders. To do this, the parties choose a group G which admits a bilinear pairing e, and a point $P \in G$. Each participant chooses respectively a secret integer α, β, and γ, and broadcasts respectively αP, βP, and γP. The quantity $e(P, P)^{\alpha\beta\gamma} = e(\alpha P, \beta P)^\gamma = \cdots$ can now be calculated by anyone who has knowledge of at least one of the secret exponents α, β, γ, while an eavesdropper without access to any secret exponent would have to break the bilinear Diffie-Hellman assumption in order to learn the common value.

The one round tri-partite key agreement protocol is most suitable for use with the Tate pairing, since the anti-symmetry property of the Weil pairing forces $e(P, P)$ to equal 1. Another option is to use distortion maps on supersingular curves to change the Weil pairing into a modified pairing which lacks the anti-symmetry property.

4.2.3 Short signatures

Bilinear pairings on elliptic curves can be used to construct a public key signature system with very short signatures relative to the level of security that the scheme provides. As an example, we present the signature scheme of Boneh, Lynn, and Shacham, which is based upon the Boneh-Franklin identity based encryption scheme given above.

It is no accident that the Boneh-Franklin IBE scheme yields a public key signature scheme. As once remarked by Boneh, every identity based encryption scheme trivially yields a signature scheme, wherein a string is signed by publishing the private key corresponding to a given string. Verification of a signature consists of simply encrypting an arbitrary message to the given string, and checking whether the purported signature correctly decrypts the encryption.

Boneh-Lynn-Shacham Signature Scheme: Let H be a collision resistant hash function which maps arbitrary strings into points of the group G described in the setup phase.

Setup: A finite field $\mathbb{F}_q$, an elliptic curve $E(\mathbb{F}_q)$, a cryptographic pairing e on $G \subset E(\mathbb{F}_q)$, and a point $P \in G$.

Key generation: The public key is $(P, \alpha P)$, for some randomly chosen $\alpha \in_R \mathbb{Z}$. The private key is α.

Signing: Given a message m, let $Q = H(m)$. The signature is $s = \alpha Q$.

Verification: Given a message m and signature s, let $Q = H(m)$ and check whether $e(P, s) = e(\alpha P, Q)$.

Note that short signatures are secure under the regular Diffie-Hellman assumption, as opposed to the bilinear Diffie-Hellman assumption that was required for the previous two systems.

The advantage of BLS short signatures over ECDSA is that the signature consists of only one group element, rather than two. One offsetting disadvantage is that we must work with a subgroup G of $E(\mathbb{F}_q)$ rather than the full group $E(\mathbb{F}_q)$. The security implications of this and other differences between the schemes will be examined in the next few sections.

4.3 Discrete logarithms

We turn away from the construction of cryptosystems for a moment in order to consider the question of how difficult it is to compute discrete logarithms. To compute a discrete logarithm means to find the value of an integer α given two group elements (g, g^α), or for an additive group $(P, \alpha P)$. This question is in some sense fundamental because all of the systems that we have discussed so far require the assumption that computing discrete logarithms is infeasible. To put it another way, any attacker who succeeds in solving a discrete logarithm would be able to obtain the private key in any of the cryptosystems that we have described above.

The landscape of attacks against discrete logarithms is quite varied, and no simple answer can completely sum up the difficulty of performing a discrete logarithm computation even if we limit ourselves to the context of known groups and known attacks. Here we will describe the most important attacks on discrete logarithms and indicate where each attack works and how fast it runs.

It is critical to keep in mind that, if more than one attack applies to a given system, then the faster of the two attacks must be taken into account when designing system parameters. For example, the Digital Signature Algorithm can be broken in $O(\sqrt{n})$ operations using Pollard rho, or $O(L_p(\frac{1}{3}, c))$ operations using index calculus. If $\log n$ is much smaller than $\log p$, then the Pollard rho algorithm will be faster. Likewise, if $\log n$ is near $\log p$, then the index calculus algorithm will be faster. Practical implementations of DSA usually employ values of n and p for which the complexity of the two attacks is similar, for example $n \approx 2^{160}$ and $p \approx 2^{1024}$.

Pollard's rho algorithm. Pollard's rho algorithm (also known as the Pollard rho algorithm) is a probabilistic algorithm[1] which applies to any cyclic group of order n. It can compute the discrete logarithm of a group element in a number of group operations equal to $O(\sqrt{n})$.

Pohlig-Hellman algorithm. Given any cyclic group G of order n, let B be the largest prime factor of n. The Pohlig-Hellman algorithm computes discrete logarithms in G in $O(\sqrt{B})$ operations.

Index calculus algorithm. Let G be a cyclic subgroup of a finite field $\mathbb{F}_q$ where $q = p^d$. As before, we define the function $L_n(\sigma, c)$ by the formula

$$L_n(\sigma, c) := \exp(c(\log n)^\sigma (\log\log n)^{1-\sigma}).$$

[1] All discrete logarithm algorithms presented here are probabilistic.

This function is intended to interpolate between polynomial and exponential running times as σ ranges between 0 and 1. Indeed, one can see from the definition that $L_n(0,c) = (\log n)^c$ and $L_n(1,c) = n^c$.

For most values of q encountered in practice, there exists an absolute constant c (independent of q) such that the index calculus algorithm can solve discrete logarithms in G in a number of operations equal to $O(L_q(\frac{1}{3}, c))$. The exception is when $\sqrt{\log p} < d < (\log p)^2$, in which case only some of the finite fields $\mathbb{F}_{p^d}$ are vulnerable to index calculus methods at the present time.

Weil descent attacks. Let G be a cyclic subgroup of an elliptic curve defined over $\mathbb{F}_q$, where $q = p^d$. If p is very small, and d is composite, then in some situations the Weil descent attack of Gaudry, Hess, and Smart can determine discrete logarithms in G in a subexponential number of operations.

Transfer to $\mathbb{F}_q$. Let G be a cyclic subgroup of an elliptic curve defined over $\mathbb{F}_q$. If the number of points in $E/\mathbb{F}_q$ is equal to q, then the transfer attack of N. Smart allows one to find discrete logarithms in G in polynomial time.

MOV attack. Let G be a cyclic subgroup of $E(\mathbb{F}_q)$, and suppose G has order n. If $q^k \equiv 1 \bmod n$, then the MOV attack of Menezes, Okamoto, and Vanstone allows one to solve discrete logarithms in G using $O(L_{q^k}(\frac{1}{3}, c))$ operations. We will study the MOV attack in detail later in this chapter.

4.4 Embedding degree

Let us examine the implications of these discrete logarithm attacks in the context of cryptographic pairings. Recall that a pairing requires an elliptic curve E over $\mathbb{F}_q$, for which there exists an integer n such that $E[n] \subset E(\mathbb{F}_q)$. The ambient group G in which the discrete logarithm problem takes place is a subgroup of $E[n]$, and hence has maximum size n. Computing a discrete logarithm under such circumstances requires $O(\sqrt{n})$ operations under Pollard rho, or even fewer under Pohlig-Hellman if n is composite. In order to avoid the Pohlig-Hellman attack, we will usually require n to be prime.

The relationship $E[n] \subset E(\mathbb{F}_q)$ implies that $n^2 \mid \#E(\mathbb{F}_q)$, since $E[n]$ is a subgroup. This requirement presents a couple of problems from an implementation standpoint. First of all, it is usually difficult to arrange for the cardinality of an elliptic curve to be divisible by the square of a large prime number. Second of all, the fact that n^2 divides $\#E(\mathbb{F}_q)$ imposes some loss of efficiency for any pairing based cryptosystem that uses points in $E(\mathbb{F}_q)$, since such points require $\log q$ bits to represent, while the resulting system only achieves a $O(\sqrt{n})$ level of security for $n < \sqrt{q}$. For systems such as identity based encryption, where the primary value of pairings is in enabling the construction of new cryptographic primitives, this efficiency loss is not a big concern, but for systems such as short signatures, where the main goal is efficiency, overcoming the efficiency loss is of primary importance.

In order to address both of these issues, we adopt the following alternative perspective of the situation. Let n be a large prime integer such that n divides the number of points in $E(\mathbb{F}_q)$, but n^2 does not. Note that this convention differs from what we were using before; the change of notation is regrettable, but unavoidable. Instead of requiring cryptographic pairings to exist on $E(\mathbb{F}_q)$, we will ask instead the following question:

> For which values of k does the elliptic curve $E/\mathbb{F}_{q^k}$, defined over the extension field $\mathbb{F}_{q^k}$ of $\mathbb{F}_q$, admit a cryptographic pairing on the subset of n-torsion points in $E(\mathbb{F}_{q^k})$?

Under this interpretation, the extension field $\mathbb{F}_{q^k}$ takes the place of what we had previously denoted $\mathbb{F}_q$. The advantage of viewing things from this angle is that in this situation, there is a subgroup G_0 of $E[n]$, of order n, which is contained in $E(\mathbb{F}_q)$ (**not** $E(\mathbb{F}_{q^k})$). Whereas a random point of $E[n]$ is likely to lie in $E(\mathbb{F}_{q^k}) \setminus E(\mathbb{F}_q)$, and thus requires $O(k \log q)$ bits to represent, the points inside the special subgroup $G_0 \subset E[n]$ are defined over $\mathbb{F}_q$, and hence require only $\log q$ bits to represent. Thus, in situations requiring efficient representations of points (such as short signatures), we can place such efficincy-sensitive points inside the group G_0 to save a factor of k in size.

To answer the question, observe that any non-degenerate bilinear pairing on $E[n]$ with values in $\mathbb{F}_{q^k}$ is of the form $e\colon E[n] \times E[n] \to \left(\mathbb{F}_{q^k}\right)^*$. Since the right hand group has order $q^k - 1$, and elements in the left hand group have order n, a necessary condition for the existence of cryptographic pairings is that $n \mid q^k - 1$; that is to say, the multiplicative order of $q \in (\mathbb{Z}/n\mathbb{Z})^*$ must divide k. If we are trying to minimize k, it makes sense to take k equal to the multiplicative order of q mod n, i.e., $k = \mathrm{ord}_n(q)$.

These observations motivate the following definition.

Definition 4.4.1. Let E be an elliptic curve defined over $\mathbb{F}_q$, and let n be the largest prime factor of $\#E(\mathbb{F}_q)$. The *embedding degree* of $E/\mathbb{F}_q$ is the integer $k = \mathrm{ord}_n(q)$.

It turns out that setting $k = \mathrm{ord}_n(q)$ is also sufficient to ensure the existence of a cryptographic pairing on the subgroup of n-torsion points in $E/\mathbb{F}_{q^k}$. We will not prove this fact, at least not yet, but the necessity of the embedding degree for cryptographic pairings already ought to provide enough motivation for the reader to be interested in the problem of finding embedding degrees of elliptic curves.

We remark that, in Definition 4.4.1, the maximum possible value of n is $O(q)$. This is because the quantities $\#E(\mathbb{F}_q)$ and q must satisfy the relation $\#E(\mathbb{F}_q) = q + 1 - t$ where $|t| \leq 2\sqrt{q}$, a relationship known as the *Hasse-Weil bound*.

Finally, the following definition gives a rough measurement of how efficient a given elliptic curve is from the point of view of pairings. Since the security of an elliptic curve cryptosystem is proportional to $\log n$, while the ciphertext size is proportional to $\log q$, elliptic curves for which the ratio of $\log q$ to $\log n$ equals 1 are more suitable for use whenever the cryptosystem requires short ciphertexts (such as short signatures).

Definition 4.4.2. Let E, q, and n be as in Definition 4.4.1. The *expansion factor* of E is defined to be the real number

$$\rho := \frac{\log q}{\log n}.$$

4.5 Optimizing the embedding degree

If the embedding degree k of an elliptic curve $E/\mathbb{F}_q$ is too large, the Weil and Tate pairings become infeasible to implement. Indeed, for most random choices of E and q, the value of $\mathrm{ord}_n(q)$ in general is not much smaller than n itself, so most of the time we have $k = O(n)$ and $q^k \approx q^n$. Storing even a single element of $\mathbb{F}_{q^k}$ in this case requires $O(n \log q)$ bits, which is infeasible for the values of n which arise in cryptography (typically, $n > 2^{160}$). For this reason, it is necessary to construct curves with small embedding degree before pairing based cryptosystems can be implemented. Moreover, all else being equal, implementors of pairing based cryptosystems generally prefer small embedding degrees whenever possible.

On the other hand, if the embedding degree is too small, then the discrete logarithm problem on $E(\mathbb{F}_q)$ becomes vulnerable to an application of the index calculus algorithm in $\mathbb{F}_{q^k}$, which for small values of k is noticeably faster than any other algorithm. This attack is known as the MOV attack, which was already mentioned in Section 4.3. The attack works as follows: Given $P, \alpha P \in E(\mathbb{F}_q)$, pick a point $Q \in E(\mathbb{F}_{q^k})$ for which the value of the pairing $e(P, Q)$ is nontrivial. Set $g = e(P, Q) \in \left(\mathbb{F}_{q^k}\right)^*$, and observe that g^α can be computed via the equation $e(P, \alpha Q) = g^\alpha$. The index calculus algorithm, applied to the pair $g, g^\alpha \in \left(\mathbb{F}_{q^k}\right)^*$, can determine the value of α in $O(L_{q^k}(\frac{1}{3}, c))$ operations.

In general, for any value of k, the value of $L_{q^k}(\frac{1}{3}, c)$ is equal to

$$L_{q^k}\left(\frac{1}{3}, c\right) = \exp(c(\log q^k)^{\frac{1}{3}}(\log\log q)^{\frac{2}{3}}) = \exp(c\, k^{\frac{1}{3}}(\log q)^{\frac{1}{3}}(\log\log q)^{\frac{2}{3}}).$$

Comparing this value to $\sqrt{n} = O(\sqrt{q}) = O\left(\exp\left(\frac{1}{2}\log q\right)\right)$, we find that, ignoring constant factors and factors of $\log\log q$, the index calculus algorithm on $\left(\mathbb{F}_{q^k}\right)^*$ is faster than the Pollard rho algorithm on $E(\mathbb{F}_q)$ if and only if $k < O((\log q)^2)$. Embedding degrees satisfying the property $k = O((\log q)^2)$ are said to be *optimal*, because they are the smallest possible values of embedding degree that neutralize the MOV attack.

$\log n$	160	224	256	320	384
k	6	10	12	24	36

Figure 4.1: Optimal embedding degrees

Determining the implied constant in the relation $k = O((\log q)^2)$ requires a somewhat detailed analysis which is beyond the scope of this monograph. Figure 4.1 gives a partial list of optimal embedding degrees for some values of n under the assumption that $\log n \approx \log q$.

In order to study embedding degrees of elliptic curves systematically, we fix the following notation. Let E be an elliptic curve over $\mathbb{F}_q$, having a number of points equal to $\#E(\mathbb{F}_q) = mn$ where n is the largest prime factor of $\#E(\mathbb{F}_q)$, and m is the cofactor. Let $t = q + 1 - mn$, and recall that t satisfies the inequality $|t| \leq 2\sqrt{q}$ by the Hasse-Weil theorem (Section 4.4).

Proposition 4.5.1. *For any integer k, the embedding degree of E divides k if and only if n divides $(t-1)^k - 1$.*

Proof. By definition of embedding degree (Definition 4.4.1), the embedding degree of E divides k if and only if $q^k \equiv 1 \bmod n$. Since $t - 1 = q - mn$, we find that

$$q^k \equiv 1 \bmod n \iff (q - mn)^k \equiv 1 \bmod n \iff (t-1)^k \equiv 1 \bmod n \iff (t-1)^k - 1 \equiv 0 \bmod n,$$

which finishes the proof. □

We now proceed to use Proposition 4.5.1 to construct examples of elliptic curves having small embedding degrees.

4.6 Supersingular elliptic curves

Definition 4.6.1. An elliptic curve $E/\mathbb{F}_q$ is said to be *supersingular* if $p \mid t$, where $p = \mathrm{char}(\mathbb{F}_q)$.

We now give some examples of supersingular elliptic curves having small embedding degrees.

Curves of embedding degree 2. We claim that any elliptic curve over $\mathbb{F}_p$ with $t = 0$ has embedding degree 2. By Proposition 4.5.1, we must check that $n \mid f_2(t-1)$, where $f_2(x)$ is the polynomial $x^2 - 1$. But

$$f_2(t-1) = (t-1)^2 - 1 = (0-1)^2 - 1 = 0,$$

so n does indeed divide $f_2(t-1)$. Examples of such elliptic curves include the curves $y^2 = x^3 + ax$ where $a \in (\mathbb{F}_p)^*$ and $p \equiv 3 \bmod 4$.

Curves of embedding degree 3. Let $q = p^2$, $t = p$. In this case the resulting elliptic curve has embedding degree 3. Indeed, setting $f_3(x) = x^3 - 1$, we find that

$$f_3(t-1) = (p-1)^3 - 1 = p^3 - 3p^2 + 3p - 2 = (p-2)(p^2 - p + 1).$$

Observe that $\#E(\mathbb{F}_q) = q + 1 - t = p^2 - p + 1$, so n divides $p^2 - p + 1$ and hence divides $f_3(t-1)$. Examples of such curves are provided by the family $y^2 = x^3 + a$ where $a \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$ and $p \equiv 2 \bmod 3$.

Curves of embdding degree 6. Let $q = 3^d$, $t = 3^{\frac{d+1}{2}}$. Then

$$(t-1)^6 - 1 = t^6 - 6t^5 + 15t^4 - 20t^3 + 15t^2 - 6t = t(t-2)(t^2 - t + 1)(t^2 - 3t + 3).$$

Note that $t^2 - 3t + 3 = 3^{d+1} - 3t + 3 = 3(q - t + 1)$ is a multiple of n. Hence E has embedding degree at most 6. One can check that $(t-1)^k - 1$ is not a multiple of n whenever $k = 2$ and $k = 3$, so the embedding degree of E is exactly 6. An example of such a curve is $y^2 = x^3 + 2x + 1$ over $\mathbb{F}_{3^d}$.

In general, a theorem of Menezes, Okamoto, and Vanstone states that a supersingular elliptic curve $E/\mathbb{F}_q$ always has embedding degree at most 6. More precisely, the maximum possible embedding degrees are:

- If $q = 2^d$, then $k \leq 4$.
- If $q = 3^d$, then $k \leq 6$.
- If $q = p$, then $k \leq 2$.
- If $q = p^2$ or p^d, then $k \leq 3$.

4.7 Ordinary elliptic curves

From Section 4.5, we know that the optimal choice of embedding degree from a security standpoint is $k \approx O((\log q)^2)$. In particular, any family of curves with embedding degree bounded by a constant (such as supersingular curves, for which $k \leq 6$) will never achieve the ideal value of k. To obtain larger embedding degrees, we need to consider ordinary elliptic curves, which are defined as follows.

Definition 4.7.1. An elliptic curve E defined over a finite field $\mathbb{F}_q$ is *ordinary* if it is not supersingular.

All known constructions of ordinary elliptic curves having small embedding degree rely to some extent on the following algorithm, known as the *Complex Multiplication method* or *CM method*.

Theorem 4.7.2 (Complex Multiplication method)**.** *Let p be any prime, and let t be any integer satisfying the bound $|t| \leq 2\sqrt{p}$. Suppose that there exist integers $D < 0$ and $c > 0$ for which the equation*

$$t^2 - 4p = Dc^2$$

holds. Then there exists an algorithm to produce an elliptic curve $E/\mathbb{F}_p$ having trace equal to t, with running time polynomial in $|D|$ and $\log p$.

We will study several families of ordinary elliptic curves having low embedding degree: the MNT family, the BN family, and the Cocks-Pinch family. All families adopt the approach of constructing integers p and t for which the Complex Multiplication method applies, and then using the CM method in order to produce the curve E.

MNT elliptic curves. The MNT family of elliptic curves was discovered in the early 1990s by Miyaji, Nakabayashi, and Takano. Elliptic curves constructed via this method have embedding degrees equal to 3, 4, or 6. The most important feature of MNT curves is that their expansion factor is 1 (cf. Definition 4.4.2).

Let $f_k(x)$ be the polynomial $x^k - 1$. We will look for pairs (p, t) for which the CM method can be applied. By Proposition 4.5.1, the trace $t - 1$ must satisfy $f_k(t-1) \equiv 0 \bmod n$ in order for E to have embedding degree k. In addition, the polynomials $f_k(x)$ for $k = 3, 4, 6$ factor as

$$\begin{aligned} f_3(x) &= (x-1)(x^2+x+1) \\ f_4(x) &= (x-1)(x+1)(x^2+1) \\ f_6(x) &= (x-1)(x+1)(x^2+x+1)(x^2-x+1) \end{aligned}$$

Since n is prime, it must divide one of the factors of $f_k(t-1)$. Moreover, if we want E to have embedding degree exactly k (as opposed to merely dividing k), then n must divide the last factor in each of the factorizations above. Denoting the last factor by $\Phi_k(x)$, the requirement we need is that $n \mid \Phi_k(x)$, or $nm' = \Phi_k(x)$ for some integer m'.

We therefore have $p = mn + t - 1$, so

$$t^2 - 4p = t^2 - 4(mn + t - 1) = (t-2)^2 - 4mn = (t-2)^2 - 4m\frac{\Phi_k(t-1)}{m'},$$

and this expression is required to equal Dc^2 for some pair of integers D and c. The key observation is that $\Phi_k(x)$ is a quadratic polynomial, so that the equation

$$(t-2)^2 - 4m\frac{\Phi_k(t-1)}{m'} = Dc^2, \tag{4.1}$$

for fixed values of D, m, and m' is a quadratic equation in t and c, which can be reduced to a Pell's equation by a linear change of variables. Indeed, by making the substitutions

$$\begin{aligned}
\tilde{m} &= \begin{cases} 2m + m' & k = 3 \\ m' & k = 4 \\ m' - 2m & k = 6 \end{cases} \\
\bar{m} &= 4m - m' \\
r &= m'\bar{m}D \\
y &= \bar{m}(t-1) + \tilde{m} \\
f &= \tilde{m}^2 - \bar{m}^2
\end{aligned}$$

we can transform Equation (4.1) into the equation $y^2 - rc^2 = f$. In practice, curves are constructed by fixing values of m, m', and D in advance and then solving the equation $y^2 - rc^2 = f$ for pairs (y, c) such that t and n are integers and n and q are primes, where

$$\begin{aligned}
t &= \frac{y - \tilde{m}}{\bar{m}} + 1 \\
n &= \frac{\Phi_k(t-1)}{m'} \\
q &= mn + t - 1.
\end{aligned}$$

For such triplets (t, n, q), the resulting elliptic curves constructed via the CM method will have embedding degree k with an expansion factor close to 1.

Barreto-Naehrig curves We describe here a family of curves discovered by Barreto and Naehrig in 2005, having embedding degree $k = 12$ and an expansion factor of 1. Our goal here is to illustrate how ordinary elliptic curves can exceed the maximum embedding degree of $k = 6$ which is achievable with supersingular curves. It is not our intention here to give an exhaustive list of all known ordinary elliptic curves having small embedding degrees.

Let $t = 6u^2 + 1$. Denote by $\Phi_{12}(x)$ the quartic factor of $x^{12} - 1$. Then $\Phi_{12}(x) = x^4 - x^2 + 1$, and

$$\Phi_{12}(t-1) = (36u^4 + 36u^3 + 18u^2 + 6u + 1)(36u^4 - 36u^3 + 18u^2 - 6u + 1).$$

Set n equal to the first factor above; i.e., $n = 36u^4 + 36u^3 + 18u^2 + 6u + 1$. Set

$$p = n + t - 1 = 36u^4 + 36u^3 + 24u^2 + 6u + 1.$$

Observe that

$$t^2 - 4p = -3(6u^2 + 4u + 1)^2,$$

so that the CM method (with $D = -3$) can always construct elliptic curves $E/\mathbb{F}_p$ having trace equal to t, provided that p is prime. If one starts with a value of u for which both p and n are prime, then E will have expansion factor 1 and embedding degree 12, since n divides $\Phi_{12}(t-1)$ and n does not divide $\Phi_k(t-1)$ for any divisor k of 12.

Cocks-Pinch curves The Cocks-Pinch method produces ordinary elliptic curves having arbitrary embedding degree. The disadvantage of this method is that it typically produces elliptic curves having expansion factor equal to 2.

Fix $k > 0$ and $D < 0$. The method proceeds as follows.

1. Let n be a prime such that $k \mid n - 1$ and $\left(\frac{D}{n}\right) = 1$.
2. Let z be a primitive k-th root of unity in $(\mathbb{Z}/n\mathbb{Z})^*$. Such a z exists because $k \mid n - 1$.

3. Let $t = z + 1$.
4. Let $y = \frac{t-2}{\sqrt{D}} \pmod{n}$.
5. Let $p = (t^2 - Dy^2)/4$.

If p is an integer and prime, then:

- $Dy^2 - (t-2)^2 \equiv 0 \bmod n$, by item 4.
- $t^2 - 4p = Dy^2$, by item 5.
- The previous two facts imply that $4(p + 1 - t) \equiv 0 \bmod n$, so n divides $p + 1 - t$.
- $(t-1)^k - 1 \equiv 0 \bmod n$, and no smaller power of $t - 1$ is congruent to $0 \bmod n$, since $t - 1 = z$ is a primitive k-th root of unity.

We conclude that the CM method produces elliptic curves $E/\mathbb{F}_p$, having trace t, for which the embedding degree of E is equal to k. Observe that in general $t \approx O(n)$ and $y \approx O(n)$, so $q = (t^2 + Dy^2)/4 \approx O(n^2)$. Consequently the expansion factor of elliptic curves E constructed via the Cocks-Pinch method is typically equal to 2.

Chapter 5

Complex Multiplication

5.1 Overview

Our goal in this chapter is to describe the use of the Complex Multiplication method for generating elliptic curves $E/\mathbb{F}_p$ having known values of trace t (Theorem 4.7.2).

Bibliography

[1] Lars V. Ahlfors, *Complex analysis*, 3rd ed., McGraw-Hill Book Co., New York, 1978. An introduction to the theory of analytic functions of one complex variable; International Series in Pure and Applied Mathematics.

[2] Ian F. Blake, Gadiel Seroussi, and Nigel P. Smart (eds.), *Advances in elliptic curve cryptography*, London Mathematical Society Lecture Note Series, vol. 317, Cambridge University Press, Cambridge, 2005.

[3] Serge Lang, *Algebraic number theory*, 2nd ed., Graduate Texts in Mathematics, vol. 110, Springer-Verlag, New York, 1994.

[4] Victor S. Miller, *The Weil pairing, and its efficient calculation*, J. Cryptology **17** (2004), no. 4, 235–261.

[5] Joseph H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1986.

[6] ———, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994.