Elliptic Curves over Finite Fields

Kenneth Giuliani

6 December 1999
1 Introduction

Elliptic curves over various fields have studied for quite a long time. However, only recently have they been considered for use in cryptographic systems. In the mid-1980's, Miller [9] and Koblitz [5] both realized that the group structure of elliptic curves over finite fields supply a very natural instance of a “discrete logarithm problem” which is very difficult to solve. This makes them very attractive for use in cryptographic protocols. Thus, this paper will examine elliptic curves over finite fields in more detail.

This paper is divided into two parts. First, we examine the structure of elliptic curves over finite fields. Second, we display an algorithm due to Schoof [10] which calculates the group order of an elliptic curve. One thing to keep in mind throughout this exposition is that elliptic curves have a very rich theory. In fact, Lang [6] has been quoted as saying, “It is possible to write endlessly on elliptic curves. (This is not a threat).” Thus, in the interest of brevity, some of the less prevalent facts will be stated without proof with the emphasis on the reader to look them up from other references. Still, a great deal of the theory will be exposed.

2 The Basic Setup

We will restrict our attention to the following scenario: Let $p > 3$ be a prime and consider the field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Let $a, b \in \mathbb{F}_p$ such that $p \not| 4a^3 + 27b^2$. The set of points $E(\mathbb{F}_p)$ defined by

$$E : Y^2 = X^3 + aX + b$$

is an elliptic curve over the field $\mathbb{F}_p$. It forms a group with point at infinity denoted $P_\infty$. (Note that the condition $p \not| 4a^3 + 27b^2$ ensures that the curve is nonsingular.)

Let $\overline{\mathbb{F}_p} = \bigcup_{i \geq 1} \mathbb{F}_{p^i}$ be the algebraic closure of $\mathbb{F}_p$. Then $E(\overline{\mathbb{F}_p})$ is also a group and contains $E(\mathbb{F}_p)$ as a subgroup. If we wished to, we could examine $E(\mathbb{F}_q)$ over any such finite field where $q = p^i$ was a prime power. However, we will restrict our attention to $E(\mathbb{F}_p)$ since all the results shown in this paper generalize easily.

Please note that for every point $P = (x, y)$, its inverse is $-P = (x, -y)$. We see that $P + P_\infty = P$ and $P + (-P) = P_\infty$ for all $P \in E(\overline{\mathbb{F}_p})$. In addition, for all other cases, the addition law for two points $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ are given in table 1.

3 Endomorphisms

In this section, we will examine the endomorphisms of $E(\overline{\mathbb{F}_p})$, i.e., the group homomorphisms of from $E(\overline{\mathbb{F}_p})$ to itself.
\[ x_3 = \begin{cases} 
\left( \frac{y_2 - y_1}{x_2 - x_1} \right)^2 - x_1 - x_2 & \text{if } P \neq Q \\
\left( \frac{3x_1^2 + a}{2y} \right)^2 - 2x_1 & \text{if } P = Q 
\end{cases} \]

\[ y_3 = \begin{cases} 
\left( \frac{y_2 - y_1}{x_2 - x_1} \right)(x_3 - x_1) - y_1 & \text{if } P \neq Q \\
\frac{-3x_1^2 + a}{2y}(x_3 - x_1) - y_1 & \text{if } P = Q 
\end{cases} \]

Table 1: Addition Formulae for the Curve \( y^2 = x^3 + ax + b \)

**Example 1:** Let \( m \in \mathbb{Z} \). Then the map

\[ [m] : E(\mathbb{F}_p) \rightarrow E(\mathbb{F}_p) 
Q \mapsto mQ \]

is an endomorphism of \( E(\mathbb{F}_p) \). This is called the **multiplication-by-\( m \) endomorphism** and applies to any group. Observe that \([0]\) is the zero map while \([1]\) is the identity.

**Example 2:** Since we are working with fields of characteristic \( p \), we see that \((x_1 + x_2)^p = x_1^p + x_2^p \) and \((x_1x_2)^p = x_1^px_2^p \) for any field elements \( x_1, x_2 \in \mathbb{F}_p \). This allows us to define the **\( p \)-th power Frobenius endomorphism** \( \phi_p \) as

\[ \phi_p : E(\mathbb{F}_p) \rightarrow E(\mathbb{F}_p) 
(x : y : z) \mapsto (x^p : y^p : z^p) \]

Note that we are using projective coordinates in this definition. The point at infinity \( P_{\infty} \) is represented by \((0 : 1 : 0)\) and hence is fixed by \( \phi_p \). This can be shown to be an endomorphism. It is not equal to \([m]\) for any \( m \in \mathbb{Z} \). When the prime \( p \) is known, we will write \( \phi \) instead of \( \phi_p \).

Let \( \text{End}(E) \) denote the set of endomorphisms of \( E(\mathbb{F}_p) \). Suppose \( \varphi, \psi \in \text{End}(E) \). Then, clearly, we see that \( \varphi \circ \psi \) is also an endomorphism of \( E(\mathbb{F}_p) \).

It is also easy to see that \( \varphi + \psi \) is an endomorphism of \( E(\mathbb{F}_p) \), where we define \((\varphi + \psi)(P) = \varphi(P) + \gamma(P)\). From these properties, we have that \((\text{End}(E), +, \circ)\) is a ring.

If this ring is commutative, then the elliptic curve is said to be ordinary. If it is non-commutative, then the elliptic curve is called supersingular. Now, it is easy to determine the group order and structure of supersingular curves over \( E(\mathbb{F}_p) \). In addition, these curves are unsuitable for cryptographic implementation [8]. Thus, for the remainder of this paper, we will deal only with ordinary elliptic curves.
4 Elliptic Function Fields, the Degree Map, and the Dual Endomorphisms

This section will present some theoretical background needed to examine the group structure in more depth. The results here will be stated without proof. The reader is referred either to Silverman [11], Husomoller [4], or Tate [12] for a more thorough exposition of elliptic curves.

Let $E$ denote the polynomial $Y^2 - X^3 - aX - b$ in $\mathbb{F}_p[X, Y]$. Now,

$$ \mathbb{F}_p[E] = \frac{\mathbb{F}_p[X, Y]}{(E)} $$

is an integral domain. Let $\mathbb{F}_p(E)$ denote its field of fractions. Every nonzero endomorphism $\varphi \in \text{End}(E)$ induces a natural field homomorphism

$$ \varphi^* : \mathbb{F}_p(E) \to \mathbb{F}_p(E) $$

$$ f \mapsto f \circ \varphi $$

It can further be shown that the index $[\mathbb{F}_p(E) : \text{Im } \varphi^*]$ is finite. We use these facts to make the following definition.

**Definition 1** We define the **degree** of a nonzero endomorphism $\varphi \in \text{End}(E)$ to be the degree of the corresponding function field extension, i.e.

$$ \deg \varphi = [\mathbb{F}_p(E) : \text{Im } \varphi^*] $$

The degree of $[0]$ is defined to be $0$. The **separable** (inseparable) degree of $\varphi$ denoted $\deg_s, \varphi$ (deg, $\varphi$) is defined to be the separable (inseparable) degree of the above field extension. $\varphi$ is said to be separable (inseparable, purely inseparable) if the above field extension is separable (inseparable, purely inseparable).

**Remarks: 1)** Let $m \in \mathbb{Z}$ with $p \nmid m$. Then $[m]$ is separable and

$$ \deg[m] = \deg_s[m] = m^2 $$

2) Let $e \geq 1$ be an integer. Then $[p^e]$ is inseparable with

$$ \deg[p^e] = p^2e $$

and

$$ \deg_s[p^e] = \deg[p^e] = p^e $$

3) The Frobenius endomorphism $\phi$ is purely inseparable with

$$ \deg \phi = \deg_\phi = p $$

4) The endomorphism $[1] - \phi$ (which will come into play later) is a separable endomorphism.

5) From remarks 1) and 2) and the fact that $[m] \neq [-m]$ if $m \neq 0$, we see that $[m] = [n]$ implies that $m = n$.

The reason for introducing the degree function is shown by the following theorem.
Theorem 1 Let \( \varphi \in \text{End}(E) \) be a nonzero endomorphism. Then the size of the kernel of \( \varphi \) is equal to its separable degree, i.e.

\[ |\ker \varphi| = \deg \varphi \]

This fact is essential to the proof of Hasse’s Theorem in the next section. We now state some other useful properties of the degree function. We start by introducing the concept of a quadratic form.

Definition 2 Let \( A \) be an abelian group. A function

\[ d : A \to \mathbb{R} \]

is a quadratic form if

1) \( d(\alpha) = d(-\alpha) \) for all \( \alpha \in A \) and
2) the pairing

\[ A \times A \to \mathbb{R} \]

\[ (\alpha, \beta) \mapsto d(\alpha + \beta) - d(\alpha) - d(\beta) \]

is bilinear.

\( d \) is said to positive definite if

3) \( d(\alpha) \geq 0 \) for all \( \alpha \in A \) and
4) \( d(\alpha) = 0 \) if and only if \( \alpha = 0 \).

Proposition 1 The degree function

\[ \deg : \text{End}(E) \to \mathbb{Z} \]

is a positive definite quadratic form.

One property which will prove useful is the following.

Lemma 1 Let \( A \) be an abelian group and

\[ d : A \to \mathbb{Z} \]

a positive definite quadratic form. Then for all \( \alpha, \beta \in A \),

\[ |d(\alpha - \beta) - d(\alpha) - d(\beta)| \leq 2 \sqrt{d(\alpha)d(\beta)} \]

We now introduce the concept of the dual of an endomorphism. Its existence is shown by the following theorem.

Theorem 2 Let \( \varphi \in \text{End}(E) \) have degree \( m \). Then there exists a unique endomorphism \( \hat{\varphi} \) such that

\[ \hat{\varphi} \circ \varphi = \varphi \circ \hat{\varphi} = [m] \]

This endomorphism is called the dual endomorphism of \( \varphi \).
Remark: We define the dual of the zero endomorphism to be itself, i.e. \( [0] = [0] \).
Dual endomorphisms have the following properties.

**Lemma 2** Let \( \varphi, \gamma \in \text{End}(E) \). Then
1) \( \widehat{\varphi} = \varphi \)
2) \( \deg \varphi = \deg \varphi \)
3) \( \varphi + \gamma = \widehat{\varphi + \gamma} \)
4) \( \varphi \circ \gamma = \widehat{\varphi} \circ \widehat{\gamma} \)
5) \( \varphi + \widehat{\varphi} = [t] \) for some \( t \in \mathbb{Z} \)
6) \( [m] = [m] \) for all \( m \in \mathbb{Z} \)

Remark: Observe that although the degree of an endomorphism is equal to the degree of its dual, the same is not necessarily true about the separable and inseparable degrees. In particular, the Frobenius endomorphism \( \phi \) has \( \deg_{s} \phi = 1 \neq p = \deg_{s} \widehat{\phi} \) and \( \deg_{i} \phi = p \neq 1 = \deg_{i} \widehat{\phi} \).

5 The Structure of Elliptic Curves over Finite Fields

What is the structure of \( E(\mathbb{F}_p) \) and how large is it? An easy upper bound on the number of points in \( E(\mathbb{F}_p) \) is \( 2p + 1 \). To arrive at this value, we note that we have a single point at infinity and each \( x \)-coordinate corresponds to at most 2 \( y \)-coordinates on the curve. Hasse's Theorem gives a better bound.

**Theorem 3 (Hasse)** Recall that \( \phi \) is the Frobenius endomorphism.
1) \( p + 1 - 2\sqrt{p} \leq |E(\mathbb{F}_p)| \leq p + 1 + 2\sqrt{p} \)
2) \( \phi \circ \phi = [t] \circ \phi + [p] = [0] \) where \( |E(\mathbb{F}_p)| = p + 1 - t \).

**Proof:**
For this proof and beyond we will drop the braces \([,]\) around the multiplication-by-\( m \) endomorphisms.
1) Observe that \( E(\mathbb{F}_p) \) are exactly those points of \( E(\mathbb{F}_p) \) which are fixed by the Frobenus. Hence,

\[
|E(\mathbb{F}_p)| = | \{ P \in E(\mathbb{F}_p) \mid \phi(P) = P \} | = | \ker (1 - \phi) | = \deg_{s}(1 - \phi) \text{ from Theorem } 1
= \deg(1 - \phi) \text{ since } 1 - \phi \text{ is separable}
\]

Now since the degree function is a positive definite quadratic form, we get from lemma 1,

\[
|\deg(1 - \phi) - \deg(1) - \deg(\phi)| \leq 2\sqrt{\deg(1)\deg(\phi)}
\]
Substituting $\deg(1) = 1$ and $\deg(\phi) = p$ as shown from the remarks after definition 1, we get

$$|E(\mathbb{F}_p) - 1 - p| \leq 2\sqrt{p}$$

which proves the first part.

2) From remark 5) following definition 1, we may consider $End(E)$ as an extension of the ring $\mathbb{Z}$. Now, from lemma 2, we can define the polynomial $f \in End(E)[X]$ as

$$f(X) = (X - \phi)(X - \hat{\phi}) = X^2 - (\phi + \hat{\phi})X + \phi\hat{\phi} = X^2 - tX + p$$

for some $t \in \mathbb{Z}$. Hence $f \in \mathbb{Z}[X]$. By construction, $\phi$ is a root of this polynomial and so

$$f(\phi) = \phi^2 - t\phi + p = 0$$

To determine what the value $t$ can be, we consider $f(1)$ which gives us on one hand

$$f(1) = 1 - t + p$$

and on the other hand,

$$f(1) = (1 - \phi)(1 - \hat{\phi}) = (1 - \phi)(1 - \hat{\phi}) = \deg(1 - \phi) = |E(\mathbb{F}_p)|$$

which proves the second part. \hfill \Box

Remark: The bounds given by Hasse’s Theorem are sharp. Elliptic curves can be found whose order are either of the extreme values.

Now that we have established the order of an elliptic curve to the best of our abilities, let us examine its structure.

**Definition 3** Let $m \in \mathbb{Z}$, $m \geq 1$. A point $Q \in E(\mathbb{F}_p)$ is said to be an $m$-torsion point if $mQ = P_\infty$. The set of $m$-torsion points form a subgroup of $E(\mathbb{F}_p)$ which is denoted by $E[m]$.

**Theorem 4** Let $m \in \mathbb{Z}$, $m \geq 1$. Then if $p \nmid m$, then

$$E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

If $m = p^c$ for integer $c \geq 1$, then

$$E[m] \cong \mathbb{Z}/p^c\mathbb{Z}$$

**Proof:**

Suppose that $m$ is a prime not equal to $p$. Then, since the multiplication-by-$m$ endomorphism is separable and its degree is $m^2$, its kernel is of size $m^2$. The result for this case is now established by the fact that $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ is the only abelian group (up to isomorphism) with $m^2$ points of order dividing $m$.  

6
Now suppose that \( m = l^d \) where \( l \) is a prime not equal to \( p \) and \( d \geq 2 \) is an integer. Then by the same argument as above, the multiplication-by-\( m \) map has a kernel of size \( m^2 = l^2d^2 \). Thus, \( E[m] \) is isomorphic to group of the form

\[
E[m] \simeq \mathbb{Z}/l^d\mathbb{Z} \times \mathbb{Z}/l^d\mathbb{Z} \times \cdots \times \mathbb{Z}/l^d\mathbb{Z}
\]

for some positive integer \( r \) where \( 0 \leq d_1, d_2, \ldots, d_r \leq d \) and \( d_1 + d_2 + \cdots + d_r = 2d \). We may suppose, without loss of generality that \( d_1 \geq d_2 \geq \cdots \geq d_r \). Now if \( d_3 \geq 1 \), then that would imply that we would have at least \( l^2 \) \( l \)-torsion points which contradicts the first case. Thus, the only possibility is if \( d_1 = d_2 = d \) and \( d_3 = \cdots = d_r = 0 \) which establishes the result for this case.

If \( m \) is a composite number not divisible by \( p \), we may simply decompose \( m \) into maximal prime powers, use the previous case for each prime power and then stitch everything back together to get the result.

Now suppose \( m = p^r \). Then \( | \ker p^r | = \deg_r(p^r) = p^r \). Following the same argument as with the previous cases, we establish the result for this case. \( \square \)

**Corollary 1**

\[
E(\mathbb{F}_p) \simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}
\]

where \( n_2 | n_1 \).

**Proof:**

Let \( n_1 \) be a point of maximum order in \( E(\mathbb{F}_p) \). Then every point in \( E(\mathbb{F}_p) \) must divide \( n_1 \) and hence \( E(\mathbb{F}_p) \) must be a subgroup of \( E[n_1] \). The result now follows from the previous proposition. \( \square \)

### 6 Schoof’s Algorithm

How can one compute the order of an elliptic curve over a finite field? One can simply use an exhaustive search to do this. However, given that elliptic curves used in industry today use a prime \( p \approx 2^{160} \), this is a very inefficient way of doing so. In 1985, Schoof presented an algorithm to calculate the order of an elliptic curve by using the second part of Hasse’s Theorem. Observe that to calculate the order of the group, it suffices to compute \( t \). The remainder of this paper will describe this algorithm.

Schoof’s algorithm is based upon two observations. First, suppose that \( l \) is a prime number not equal to \( p \) and \( Q \in E[l] \) is not the point of infinity. Suppose further that for some \( t' \in \mathbb{Z} \), we have that

\[
\phi^2(Q) - t' \phi(Q) + pQ = P_{\infty}
\]

We know, from the second part of Hasse’s Theorem, that

\[
\phi^2(Q) - t \phi(Q) + pQ = P_{\infty}
\]
Putting these two together gives us

\[ P_\infty = (t' - t)\phi(Q) = \phi((t' - t)Q) \]

since the endomorphism ring is commutative (we are working with ordinary curves). But since the only point in the kernel of \( \phi \) is \( P_\infty \), we see that \((t' - t)Q = P_\infty \) and since \( Q \) was chosen as a nontrivial \( l \)-torsion point, we must have that \( t' \equiv t \pmod{l} \).

The second observation to be made is that the value \( t \) lives only within a range of size \( 4\sqrt{p} + 1 \). Hence, if we can determine \( t \) modulo \( K \) for some positive integer \( K \geq 4\sqrt{p} \), then we can uniquely determine \( t \) and hence the order of the group.

The strategy for determining \( t \) that immediately lends itself from these two observations is this: determine \( t \) modulo \( l \) for enough small primes \( l \) so that the product of these primes is greater than \( 4\sqrt{p} \), and then use the Chinese Remainder Theorem to find \( t \) uniquely.

## 7 Division Polynomials

The key problem we are faced with is finding \( l \)-torsion points \( Q \in E(\mathbb{F}_p) \). To find them, we will probably have to extend the field and work in \( E(\mathbb{F}_q) \) for various prime powers \( q = p^r \). This is very undesirable. It is much more preferable to work only within the field \( \mathbb{F}_p \).

It turns out that we can indeed work within the field \( \mathbb{F}_p \) if we use polynomials to represent \( l \)-torsion points. To that end, we introduce the set of division polynomials \( \Psi_n(X, Y) \in \mathbb{F}_p[X, Y] \) defined as follows:

\[
\Psi_{-1}(X, Y) = -1, \quad \Psi_0(X, Y) = 0, \quad \Psi_1(X, Y) = 1, \quad \Psi_2(X, Y) = 2Y, \\
\Psi_3(X, Y) = 3X^4 + 6aX^2 + 12bX - a^2, \\
\Psi_4(X, Y) = 4Y(X^6 + 5aX^4 + 20bX^3 - 5a^2X^2 - 4bX - 8b^2 - a^3), \\
\Psi_{2n}(X, Y) = \Psi_n(\Psi_{n+2}\Psi_{n-1}^2 - \Psi_{n-2}\Psi_{n+1}^2)/2Y \text{ for } n \in \mathbb{Z}_{\geq 1}, \\
\Psi_{2n+1}(X, Y) = \Psi_{n+2}\Psi_n^2 - \Psi_{n-1}\Psi_{n+1}^2 \text{ for } n \in \mathbb{Z}_{\geq 1}.
\]

These polynomials have the property that if \( Q = (x, y) \in E(\mathbb{F}_p) \), then \( Q \in E[n] \) if and only if \( \Psi_n(Q) = 0 \). Now, we may substitute the relation \( Y^2 = X^3 + aX + b \) into each division polynomial \( \Psi_n \) to get equivalent polynomials \( \Psi'_n \) with no monomial containing a \( Y \) exponent of 2 or higher. These new polynomials have the property that \( \Psi'_n(X, Y) \) is in \( \mathbb{F}_p[X] \) if \( n \) is odd and \( Y^\mathbb{F}_p[X] \) if \( n \) is even.
if $n$ is even. We can thus define polynomials $f_n(X) \in \mathbb{F}_p[X]$ only in the variable $X$ as

$$f_n(X) = \Psi_n(X, Y) \text{ if } n \text{ is odd}$$

$$f_n(X) = \Psi_n(X, Y)/Y \text{ if } n \text{ is even}$$

These new polynomials retain the same properties as the original division polynomials $\Psi_n$ with the exception that $f_n(X)$ is no longer zero at the $2$-torsion points if $n$ is even. This is not a concern for the algorithm, though.

One of the key uses for these polynomials comes from the following lemma.

**Lemma 3** Let $Q = (x, y) \in E(\mathbb{F}_p)$ not be a $2$-torsion point, and $n$ be a positive integer so that $nQ \neq P_\infty$. Then,

$$nQ = \begin{cases} 
(x - \frac{f_{n+1}(x)f_{n-1}(x)(x^2+ax+b)}{f_n(x)^2}, \frac{f_{n+1}(x)f_{n-1}(x)^2 - f_{n+2}(x)f_{n-2}(x)(x^2+ax+b)}{4f_n(x)^3}) & \text{if } n \text{ is odd} \\
(x - \frac{f_{n+1}(x)f_{n-1}(x)}{f_n(x)^2(x^2+ax+b)}, \frac{f_{n+2}(x)f_{n-2}(x)^2 - f_{n+1}(x)(x^2+ax+b)}{4g_n(x)^3x^2+ax+b}) & \text{if } n \text{ is even}
\end{cases}$$

8 Implementing the Algorithm

Let $l$ be a prime different from $2$ and $p$ and $Q = (x, y) \in E(\mathbb{F}_p)[l]$. Let $k \equiv p \pmod{l}$ with $0 \leq k < p$. Our aim is to find a number $t'$ so that

$$\phi^2(Q) + kQ = t'\phi(Q)$$

Let us now consider the coordinates of $Q$ as indeterminates in $X$ and $Y$. Applying lemma 3 and the equations in table 1 together with the Frobenius map would give rational functions in $X$ and $Y$ for each coordinate on the left and right hand sides of the above equation. If substituting $Q$ into these relations gives equality for a specified choice of $t'$ then we have found our value $t' \equiv t \pmod{l}$. To test whether there is such a point $Q$ satisfying the above relations, we merely take the gcd of $f_l$ and the resulting polynomial creating by clearing out the denominator of the given rational function. This will be illustrated as we progress through the algorithm in more detail.

First, let us add $\phi^2(Q)$ and $kQ$. Observe that neither is $P_\infty$. We must first check whether or not $\phi^2(Q) = \pm kQ$. When considered as an indeterminate, the $x$-coordinate of $\phi^2(Q)$ is $X^p$. Suppose $k$ is odd. The $x$-coordinate of $kQ$ would then be

$$X - \frac{f_{n-1}(x)f_{n+1}(x)(X^3 + aX + b)}{f_n(x)^2}$$

We can now determine whether or not substituting the $x$-coordinate of $Q$ makes these two terms equal by calculating

$$\gcd((X^p - X)f_{k,l}^2(X) + f_{k-1}(X)f_{k+1}(X)(X^3 + aX + b), f_l(X))$$
Suppose that this gcd is not equal to 1. Then some \( E[l] \)-torsion point, WLOG \( Q \), makes the two equal. Then we see that, indeed, \( \phi^2(Q) = \pm kQ \). We can similarly check the \( y \)-coordinate of \( Q \) to determine \(+\) or \(-\).

If \( \phi^2(Q) = -kQ \), then \( t'Q = (-kQ) + kQ = P_\infty \) so \( t' = 0 \). Thus \( t \equiv 0 \) (mod \( l \)). Otherwise, \( \phi^2(Q) = kQ \) and we see that

\[
2kQ = t' \phi(Q)
\]

which means that

\[
\phi(Q) = \frac{2k}{t'} Q
\]

and so

\[
\phi^2(Q) = kQ = \frac{4k^2}{(t')^2}
\]

Thus, \( (t')^2 \equiv 4k \) (mod \( l \)) which means that \( k \) must be a quadratic residue modulo \( l \), i.e. \( k \equiv w^2 \) (mod \( l \)) for some \( w \in \mathbb{F}_p \). This, however, would imply that \( \phi(Q) = \pm wQ \). We may once again use polynomials in the \( x \)-coordinate to solve for \( w \) and then in the \( y \)-coordinate to see if we want \(+\) or \(-\). Then, WLOG, we have that \( \phi(Q) = wQ \) and substituting this into \( (1) \) gives \( t' \equiv 2w \) (mod \( l \)).

Now suppose, that the gcd was 1. The we could then add \( \phi^2(Q) \) and \( kQ \) using the addition laws in table 1 to get rational functions in \( X \) and \( Y \). Then for \( t' = 1, 2, 3, \ldots \), we would use lemma 3 to determine a rational expression for \( t' \phi(Q) \) and then test using gcd’s to see if \( Q \) gives an equal value for them. When we find a \( t' \) that works, then we have found that value of \( t' \) such that \( t' \equiv t \) (mod \( l \)).

If \( k \) was even, we would follow the exact same procedure except with the different equation given in lemma 3.

Once we have found values \( t' \) for sufficiently many primes \( l \), we can use the Chinese Remainder Theorem to determine \( t \).

This algorithm works fairly well in practice. For a prime \( p \) in the range of \( p \approx 2^{160} \), the algorithm will take several hours to run.

9 Final Notes

There have been several improvements made to Schoof’s algorithm over the years. In 1989, Elkies [3] described how to use “good” primes \( l \) to make the algorithm execute more quickly. In 1992, Atkin [1] gave improvements that made Elkies’ ideas more practical. In 1994, Couveignes and Morsin [2] showed how to use prime powers \( l^d \) to speed up the algorithm even further.

Finally, we note that in 1994, Lay and Zimmer [7] described an algorithm to actually construct an elliptic curve with a given group order. They use the orders in imaginary quadratic number fields to construct an element \( \pi \) such that
norm of $1 - \pi$ is the desired group order and the norm of $\pi$ itself is (hopefully) a prime $p$. When this happens, the element $\pi$ corresponds to the Frobenius endomorphism of some curve which can then be determined over the field $\mathbb{F}_p$.

References


