COUNTING POINTS ON ELLIPTIC CURVES OVER $\mathbb{F}_q$

RENYI TANG

Abstract. In this expository paper, we introduce elliptic curves over finite fields and the problem of counting the number of rational points on a curve. To solve this problem, we study finite fields, endomorphisms, Frobenius endomorphisms, torsion groups, and division polynomials. We prove several useful intermediate results and finally prove Hasse's theorem, which gives a bound to the number of rational points on a curve, and prove the legitimacy of Schoof's algorithm, which offers an efficient way to count this number precisely.

Contents

1. Introduction 1
2. Preliminaries 2
2.1. Properties of elliptic curves 2
2.2. Finite fields 3
3. Endomorphisms and Frobenius Endomorphisms 5
3.1. Separability of endomorphisms of the form $r\phi_q + s$ 9
3.2. Degree of endomorphisms of the form $a\alpha + b\beta$ 11
3.3. Characteristic equation of Frobenius endomorphisms 12
3.4. Bounding $\#E(\mathbb{F}_q)$: Hasse'e theorem 13
4. Schoof's algorithm 14
4.1. Division polynomials 14
4.2. Proof and summary of Schoof's algorithm 15
4.3. An example that applies Schoof's algorithm 18
Acknowledgment 19
References 19

1. Introduction

Elliptic curves play an important role in cryptography and number theory. The two common applications of the theory of elliptic curves are solving discrete logarithm problems (DLP) and factorizing large integer primes, both of which have been widely used in current encryption techniques. DLP uses the fact that it is hard to reverse-engineer the element in a group whose n-th power is a another element in the group. In general, the harder a DLP is designed to solve, the more secure the encryption technique that uses it is. In order to make a DLP harder, a major step is to compute the number of points on an elliptic curve whose coordinates are in the same field. For some fields such as $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$, some useful results in mathematics have been found. This paper concerns the two significant results for finite fields

Date: August 2018.

$\mathbb{F}_q$, the most commonly used fields in cryptography. First, Hasse's theorem gives a strong bound for the number of points on an elliptic curve whose coordinates are in a finite field. Second, Schoof's algorithm outlines a mathematically legitimate and by far one of the most time-efficient algorithms to count the exact number of such points.

2. Preliminaries

2.1. **Properties of elliptic curves.** The formal definition of elliptic curves requires some background in algebraic geometry. In order to understand the major concepts of elliptic curves in this paper, it is sufficient to define them in elementary algebra and geometry.

Over $\mathbb{R}$, an elliptic curve is a curve given by an equation of the form $y^2 = x^3 + Ax + B$, where A and B are real constants. In this case, x, y, A and B belong to $\mathbb{R}$, but they can belong to any set. They will usually taken to be elements of a field K, such as $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, or a finite field $\mathbb{F}_q$.

Definition 2.1. An elliptic curve E defined over a field K is the graph of an equation of the form

$$y^2 = x^3 + Ax + B,$$

where A, B are constants and $A, B, x, y \in K$.

This will be referred to as the **Weierstrass equation** for an elliptic curve.

For technical reasons, it is useful to add a **point at infinity** to an elliptic curve. It is easiest to regard it as a point (∞, ∞), usually denoted simply by ∞, sitting at the top of the y-axis. It will be a formal symbol satisfying certain computational rules. For example, a vertical line is said to pass ∞. With the point at infinity, the set $\{(x, y) \mid y^2 = x^3 + Ax + B\} \cup \{\infty\}$ is a group under the group law defined below.

Definition 2.2 (Group Law)**.** Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be elements in E with $P_1, P_2 \neq \infty$. Define $(x_3, y_3) = P_3 = P_1 + P_2$ as follows:

(1) If $x_1 \neq x_2$, then

$$x_3 = m^2 - x_1 - x_2,\ y_3 = m(x_1 - x_3) - y_1, \text{ where } m = \frac{y_2 - y_1}{x_2 - x_1}.$$

(2) If $x_1 = x_2$ and $y_1 \neq y_2$, then $P_1 + P_2 = \infty$.

(3) If $P_1 = P_2$ and $y_1 \neq 0$, then

$$x_3 = m^2 - 2x_1,\ y_3 = m(x_1 - x_3) - y_1, \text{ where } m = \frac{3x_1^2 + A}{2y_1}.$$

(4) If $P_1 = P_2$ and $y_1 = 0$, then $P_1 + P_2 = \infty$.

Moreover, define $P + \infty = P$ for all P in E. We also require that the curve is non-singular. Algebraically, this holds if and only if the discriminant $4A^3 + 27B^2$ is not equal to zero.

Geometrically, the group law can be interpreted as follows:

(1) The line connecting two distinct points on the curve must have another intersection with the curve. The proof can be found in [2]. Suppose the line generated by P_1 and P_2 intersects with the curve at P_3'. Since the curve is symmetric with respect to the x-axis, the point reflected by P_3' is also on the curve, and is defined as $P_3 = P_1 + P_2$.

(2) The sum of a point and its reflection point with respect to the x-axis is defined to be ∞.
(3) If P_1 and P_2 coincide and $y_1 = y_2 \neq 0$, then the line is defined to be the tangent line at P. P_3 is then defined in a similar way as in the first case.
(4) If P_1 and P_2 coincide and $y_1 = y_2 = 0$, their sum is defined to be ∞.

Theorem 2.3 (Group properties)**.** *The addition of points on an elliptic curve E satisfies the following properties:*

(1) $P_1 + P_2 = P_2 + P_1$ (commutativity)
(2) $P + \infty = P$ for all $P \in E$ (existence of identity)
(3) For any $P \in E$, there exists $P' \in E$ with $P + P' = \infty$. P' is denoted by $-P$ (existence of inverses)
(4) $(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3)$ for all $P_1, P_2, P_3 \in E$ (associativity).

In other words, the points in E form an abelian group with ∞ as the identity element.

Proof. All four are rather obvious except associativity. It can be verified by brute force calculation with the formulas in Definition 2.2. Another approach uses projective space, which we will not delve into in this paper. It can be found in [1] Chapter 2. □

For an elliptic curve E defined over K, it is useful to consider points with coordinates in some field $L \supseteq K$.

Definition 2.4. Let E be defined over K. The **L-rational points** of E is the set of all points in E with coordinates in a field $L \supseteq K$ and the point at infinity.

$$E(L) = \{(x, y) \in L \times L \mid y^2 = x^3 + Ax + B\} \cup \{\infty\}.$$

Theorem 2.5. *$E(L)$ is a subgroup of E.*

Proof. It is sufficient to prove that $E(L)$ is a nonempty subset of the group E and that it is closed under addition and inverse. Suppose $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ are in $E(L)$. We have $P_1 + P_2 = P_3 = (x_3, y_3)$ and $-P_1 = (x_1, -y_1)$. By the curve equation, $(-y_1)^2 = x_1^3 + Ax_1 + B$, which means $-P_1 \in E(L)$. By applying the group law, (x_3, y_3) has 3 possible choices,

(1) $x_3 = m^2 - x_1 - x_2$, $y_3 = m(x_1 - x_3) - y_1$, where $m = \frac{y_2 - y_1}{x_2 - x_1}$ (if $x_1 \neq x_2$)
(2) $x_3 = m^2 - 2x_1$, $y_3 = m(x_1 - x_3) - y_1$, where $m = \frac{3x_1^2 + A}{2y_1}$ (if $P_1 = P_2$ and $y_1 \neq 0$)
(3) ∞ (if $x_1 = y_2$ and $y_1 \neq y_2$, or when $P_1 = P_2$ and $y_1 = 0$).

These expressions are well defined since we are working over a field L. This means $x_3, y_3 \in L$ and thus $(x_3, y_3) \in E(L)$. □

2.2. **Finite fields.** We will review some basic properties of finite fields and prove several useful results.

Definition 2.6. A finite field $\mathbb{F}_q$ is a field that contains a finite number of elements.

Definition 2.7. The characteristic of a field is the smallest number of times one must use the field's multiplicative identity (1) in a sum to get the additive identity (0) if the sum does indeed eventually attain 0. If the sum never attains 0, the characteristic is defined to be 0.

Proposition 2.8. *A field with non-zero characteristic must have prime characteristic.*

Proof. Let $n > 0$ be the characteristic of K. If n is a composite number, then $n = ab$ for some $a, b \geq 2$. Since $a, b < n$, then $a, b \neq 0$, but we have $n = ab = 0$, hence a contradiction because K is a field. □

Theorem 2.9. *A finite field of order q exists if and only if $q = p^k$, where p is a prime number and k is a positive integer.*

Proposition 2.10. *In a finite field of order p^k, the characteristic of the field is p.*

Proposition 2.11. *In a finite field of order q, the polynomial $X^q - X$ has all q elements of the finite field as roots.*

Proof. Clearly $x = 0$ satisfies this relation. The nonzero elements of $\mathbb{F}_q$ form a group under multiplication. Therefore, for every $x \neq 0$, its order divides $q - 1$, hence $x^{q-1} = x$ and therefore $x^q = x$ for all $x \in \mathbb{F}_q^\times$. □

Notation 2.12. We write a finite field with $k = 1$ as $\mathbb{F}_p$, and with $k > 1$ as $\mathbb{F}_q$ or $\mathbb{F}_{p^k}$.

Proposition 2.13. *Given a finite field $\mathbb{F}_q$ of characteristic p, $(x + y)^p = x^p + y^p$ for any x, y in $\mathbb{F}_q$.*

Proof. We know p is a prime. Binomial expansion gives coefficients of the form

$$\binom{p}{k} = \frac{p!}{k!(p-k)!}, \text{ which can be rearranged as}$$
$$k!\binom{p}{k} = p(p-1)(p-2)\dots(p-k+1).$$

Since p is a prime, p must either divide $k!$ or $\binom{p}{k}$, but p cannot divide $k!$ unless $k = p$ or 0. Therefore, $p \mid \binom{p}{k}$ for all $0 < k < q$. All terms in the binomial expansion are 0 except x^p and y^p. □

Remark 2.14. By induction, $(x_1 + x_2 + \cdots + x_n)^p = x_1^p + x_2^p + \cdots + x_n^p$ for all x_i in $\mathbb{F}_q$ with $0 < i < q$.

Theorem 2.15. *Let $\mathbb{F}_q$ be a finite field and $\overline{\mathbb{F}}_q$ be its algebraic closure. Then*

$$\mathbb{F}_q = \{\alpha \in \overline{\mathbb{F}}_q \mid \alpha^q = \alpha\}.$$

Proof. The group $\mathbb{F}_q^\times$ of nonzero elements of $\mathbb{F}_q$ forms a group of order $q - 1$. By Lagrange's theorem, $\alpha^{q-1} = 1$ for all nonzero $\alpha \in \mathbb{F}_q$. Therefore, $\alpha^q = \alpha$ for all nonzero $\alpha \in \mathbb{F}_q$.

A polynomial has multiple roots if and only if it shares a common root with its derivative. The polynomial $X^q - X$ has no multiple roots since $\frac{d}{dX}(X^q - X) = qX^{q-1} - 1 = -1$. Therefore, there are q distinct $\alpha \in \overline{\mathbb{F}}_p$ such that $\alpha^q = \alpha$.

Since both sets in the statement of the theorem have q elements and the former is contained in the later, they are equal. □

3. Endomorphisms and Frobenius Endomorphisms

Endomorphisms and **Frobenius endomorphisms** are important in the proof of Hasse's theorem.

Definition 3.1. Let E be an elliptic curve defined over K. An **endomorphism** of E is a homomorphism $\alpha : E(\overline{K}) \to E(\overline{K})$ that is given by rational functions, where $\overline{K}$ is the algebraic closure of K. In other words, $\alpha(P_1+P_2) = \alpha(P_1)+\alpha(P_2)$, and there are rational functions (quotients of polynomials) $R_1(x,y), R_2(x,y)$ with coefficients in $\overline{K}$ such that

$$\alpha(x,y) = (R_1(x,y), R_2(x,y)) \text{ for all } (x,y) \text{ in } E(\overline{K}).$$

In addition, we define $\alpha(\infty) = \infty$. We will also assume that α is nontrivial; that is, $\alpha(x,y)$ is not always ∞. The trivial endomorphism is denoted by 0. The rational functions may not be defined in some situations, i.e. the denominator is 0. We will deal with these situations later.

The curve equation gives a relation between x and y, and so we can use it to get a more uniform form for R_1 and R_2. We can replace any even power of y with a polynomial in x and any odd power of y with a polynomial in x times y. Therefore, we may assume that

$$R(x,y) = \frac{p_1(x) + p_2(x)y}{p_3(x) + p_4(x)y}.$$

Then multiply both numerator and denominator by $p_3(x) - p_4(x)y$, and we get a nice form

$$R(x,y) = \frac{q_1(x) + q_2(x)y}{q_3(x)}. \tag{3.2}$$

In order to further simply it, consider the endomorphism

$$\alpha(x,y) = (R_1(x,y), R_2(x,y)).$$

Since α is also a homomorphism,

$$\alpha(x,-y) = \alpha(-(x,y)) = -\alpha(x,y).$$

This means that

$$R_1(x,-y) = R_1(x,y)\ ,\ R_2(x,-y) = -R_2(x,y).$$

By (3.2), $q_2 = 0$ for R_1 and $q_1 = 0$ for R_2. Therefore, we can assume that

$$\alpha(x,y) = (r_1(x), r_2(x)y)$$

with r_1, r_2 being rational functions.

Definition 3.3. The **degree** of a nontrivial endomorphism α is defined to be

$$\deg(\alpha) = \max\{\deg(p(x)), \deg(q(x))\},$$

where $\alpha(x,y) = (r_1(x), r_2(x)y)$ and $p(x)/q(x) = r_1(x)$.

Definition 3.4. An endomorphism $\alpha \neq 0$ is **separable** if the derivative $r_1'(x)$ is not identically zero.

Proposition 3.5. *Let $\alpha(x,y) = (p(x)/q(x), ys(x)/t(x))$ be an endomorphism of the elliptic curve E over K given by $y^2 = x^3 + Ax + B$, where p, q, s, t are polynomials such that p and q have no common roots and s and t have no common roots. If $t(x_0) = 0$, then $q(x_0) = 0$. In other words, if $q(x_0) \neq 0$, then both p/q and s/t are defined and so is $\alpha(x,y)$.*

Proof. We first show that

$$\frac{(x^3 + Ax + B)s(x)^2}{t(x)^2} = \frac{u(x)}{q(x)^3}$$

for some polynomial $u(x)$ such that q and u have no common roots.

By the group law formulas in Definition 2.2,

$$\frac{y^2 s^2}{t^2} = \frac{p^3}{q^3} + A\frac{p}{q} + B$$
$$\frac{(x^3 + Ax + B)s(x)^2}{t(x)^2} = \frac{p(x)^3 + Ap(x)q(x)^2 + Bq(x)^3}{q(x)^3}.$$

If $p^3 + Apq^2 + Bq^3$ has a common root with q^3, p must have a common root with q. This is a contradiction.

Suppose $t(x_0) = 0$ for x_0. Then x_0 are two roots of $t(x_0)^2$. Since $x^3 + Ax + B$ has no multiple roots by definition and s and t share no common roots, q must share at least one x_0 with t. □

Theorem 3.6. *Let $\alpha \neq 0$ be a separable endomorphism of an elliptic curve E defined over K. Then*

$$\deg(\alpha) = \#\ker(\alpha),$$

where $\ker(\alpha)$ is the kernel of the homomorphism $\alpha : E(\overline{K}) \to E(\overline{K})$.

If $\alpha \neq 0$ is not separable, then

$$\deg(\alpha) > \#\ker(\alpha).$$

Proof. Write $\alpha(x,y) = (r_1(x), yr_2(x))$ with $r_1(x) = p(x)/q(x)$, as above. If α is separable, $r_1' \neq 0$. So $p'q - pq'$ is not the zero polynomial. Let

$$S = \{x \in \overline{K} \mid (pq' - p'q)(x)q(x) = 0\}.$$

Let $(a,b) \in E(\overline{K})$ be such that

(1) $a \neq 0, b \neq 0, (a,b) \neq \infty$,
(2) $\deg(p(x) - aq(x)) = \max\{\deg(p(x)), \deg(q(x))\} = \deg(\alpha)$,
(3) $\alpha \notin r_1(S)$, and
(4) $(a,b) \in \alpha(E(\overline{K}))$.

The reason why such a (a,b) exists is as follows:

(1) Since $pq' - p'q$ is not identically zero, S is a finite set. Hence its image under α, $\alpha(S)$, is finite.
(2) The function $r_1(x)$ is easily seen to take on infinitely many distinct values as x runs through $\overline{K}$.
(3) Since for each x, there is a point $(x,y) \in E(\overline{K})$, $\alpha(E(\overline{K}))$ is an infinite set.

We claim that there are exactly $\deg(\alpha)$ points $(x_1, y_1) \in E(\overline{K})$ such that $\alpha(x_1, y_1) = (a,b)$. For such a point (x_1, y_1) we have

$$\frac{p(x_1)}{q(x_1)} = a,\ y_1 r_2(x_1) = b.$$

Since $(a,b) \neq \infty$, $q(x_1) \neq 0$. By Proposition 3.5, $r_2(x_1)$ is defined. Since $b \neq 0$ and $y_1 r_2(x_1) = b$, we must have $y_1 = b/r_2(x_1)$. Therefore x_1 determines y_1 in this case. So we only need to count values of x_1.

By assumption (2), $p(x) - aq(x)$ has $\deg(\alpha)$, and so $p(x) - aq(x) = 0$ has $\deg(\alpha)$ roots, counting multiplicities. However, we need to show that it does not have multiple roots because the homomorphism α acts on the group $E(\overline{K})$, whose elements are all distinct. Suppose that x_0 is a multiple root. Then

$$p(x_0) = aq(x_0) \text{ and } p'(x_0) = aq'(x_0).$$

Multiplying them yields

$$ap(x_0)q'(x_0) = ap'(x_0)q(x_0).$$

Since $a \neq 0$, this implies that x_0 is a root of $(pq' - p'q)(x)$, so $x_0 \in S$. Thus, $a = r_1(x_0) \in r_1(S)$, which is contrary to assumption (3). Therefore, there are exactly $\deg(\alpha)$ points $(x_1, y_1) \in E(\overline{K})$ such that $\alpha(x_1, y_1) = (a, b)$. In addition, we know that for a homomorphism $\alpha : G \to G$, $\#\ker(\alpha)$ is equal to the size of the preimage of any element in G. Therefore, $\deg(\alpha) = \#\ker(\alpha)$.

If α is not separable, then the above proof still holds except that $p' - aq'$ is identically zero. This means $p(x) - aq(x) = 0$ always has multiple roots and therefore the kernel size is smaller than $\deg(\alpha)$. □

Lemma 3.7. *Let $\alpha \neq 0$ be an endomorphism of E defined over K. Then $\alpha : E(\overline{K}) \to E(\overline{K})$ is surjective.*

Proof. Choose a random point $(a,b) \in E(\overline{K})$. Since $\alpha(\infty) = \infty$, we may assume that $(a,b) \neq \infty$. Let $r_1(x) = p(x)/q(x)$ be as in Theorem 3.6. If $p(x) - aq(x)$ is not a constant polynomial, then it has a root x_0. Since p and q do not have common roots, $q(x_0) \neq 0$. Choose $y_0 \in \overline{K}$ to be either square root of $x_0^3 + Ax_0 + B$. By Lemma 3.21, $\alpha(x_0, y_0)$ is defined and thus equals (a, b') for some b'. Then we have $b'^2 = x^3 + Ax + B = b^2$. If $b = b'$, then $\alpha(x_0, y_0) = (a, b') = (a, b)$. This means we have successfully found an inverse image for (a, b). If $b' = -b$, then $\alpha(x_0, -y_0) = (a, -b') = (a, b)$. So $(x_0, -y_0)$ is an inverse image.

We need to consider the case when $p - aq$ is a constant polynomial. By Theorem 3.6, the kernel of α is finite, and so only finitely many points of $E(\overline{K})$ can map to a point with a given x-coordinate. Therefore, either $p(x)$ or $q(x)$ is not constant. Otherwise, there are infinitely many x that map to the same a. Thus p and q are two nonconstant polynomials. There is at most one constant a such that $p - aq$ is constant (if a' is another such number, then $(a'-a)q = (p-aq)-(p-a'q)$ is constant and $(a'-a)p = a'(p-aq)-a(p-a'q)$ is constant, which means p is constant and thus q as well. Therefore, there are at most two points, (a, b) and $(a, -b)$ for some b, that are not in the range of α. Let (a_1, b_1) be any other point. Then $\alpha(P_1) = (a_1, b_1)$ for some P_1. We can choose (a_1, b_1) such that $(a_1, b_1) + (a, b) \neq (a, \pm b)$, so there exists P_2 with $\alpha(P_2) = (a_1, b_1) + (a, b)$. Then $\alpha(P_2 - P_1) = (a, b)$, and $\alpha(P_1 - P_2) = (a, -b)$. Therefore α is surjective. □

Definition 3.8. Let $\mathbb{F}_q$ be a finite field with algebraic closure $\overline{\mathbb{F}}_q$. Let

$$\phi : \overline{\mathbb{F}}_q \to \overline{\mathbb{F}}_q,\ x \mapsto x^q.$$

ϕ is called the **Frobenius map** of $\mathbb{F}_q$.

Proposition 3.9. *Let ϕ be a Frobenius map of $\mathbb{F}_q$. Let $\alpha \in \overline{\mathbb{F}}_q$. Then*

$$\alpha \in \mathbb{F}_q \iff \phi(\alpha) = \alpha.$$

Proof. This is a restatement of Theorem 2.15. □

Definition 3.10. Let E be defined over $\mathbb{F}_q$, whose algebraic closure is $\overline{\mathbb{F}}_q$. The **Frobenius endomorphism** of E of **degree** q is

$$\phi_q : E(\overline{\mathbb{F}}_q) \to E(\overline{\mathbb{F}}_q), (x, y) \mapsto (x^q, y^q).$$

In addition, we define $\phi_q(\infty) = \infty$.

Proposition 3.11. *Let E be defined over $\mathbb{F}_q$. Let ϕ_q be a Frobenius endomorphism of E. Consider the points $(x, y) \in E(\overline{\mathbb{F}}_q)$. Then*

(1) $\phi_q(x, y) \in E(\overline{\mathbb{F}}_q)$.
(2) $(x, y) \in E(\mathbb{F}_q)$ if and only if $\phi_q(x, y) = (x, y)$.

Proof. Raise both sides of the curve equation to the qth power, and we get

$$(y^q)^2 = (x^q)^3 + A(x^q) + B.$$

This means that $(x^q, y^q) \in E(\overline{\mathbb{F}}_q)$.

By Proposition 3.9, $x \in \mathbb{F}_q$ if and only if $\phi(x) = x$, and similarly for y. Therefore

$$\begin{aligned}(x, y) \in E(\mathbb{F}_q) &\Leftrightarrow x, y \in \mathbb{F}_q \\ &\Leftrightarrow \phi(x) = x \text{ and } \phi(y) = y \\ &\Leftrightarrow \phi_q(x, y) = (x, y).\end{aligned}$$

□

Lemma 3.12. *Let E be defined over $\mathbb{F}_q$. Let ϕ_q be a Frobenius endomorphism of E.*

(1) ϕ_q is an endomorphism of $E(\overline{\mathbb{F}}_q)$.
(2) ϕ_q is not separable.

Proof. By its definition, ϕ_q is given by rational functions. We only need to prove that ϕ_q is a homomorphism. Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ in $\overline{\mathbb{F}}_q$ with $x_1 \neq x_2$. By the group law, $P_3 = P_1 + P_2 = (x_3, y_3)$ with

$$x_3 = m^2 - x_1 - x_2,\ y_3 = m(x_1 - x_3) - y_1, \text{ where } m = \frac{y_2 - y_1}{x_2 - x_1}.$$

Raise everything to the qth power to obtain

$$x_3^q = (m')^2 - x_1^q - x_2^q,\ y_3^q = m'(x_1^q - x_3^q) - y_1^q, \text{ where } m' = \frac{y_2^q - y_1^q}{x_2^q - x_1^q}.$$

This means that

$$\phi_q(x_3, y_3) = \phi_q(x_1, y_1) + \phi_q(x_2, y_2).$$

The cases where $x_1 = x_2$ but $y_1 \neq y_2$, or where $P_1 = P_2$ and $y_1 = 0$, or where one of the points is ∞ are checked similarly. One subtlety arises in the case where $P_1 = P_2$ and $y_1 \neq 0$. In this case,

$$x_3 = m^2 - 2x_1,\ y_3 = m(x_1 - x_3) - y_1, \text{ where } m = \frac{3x_1^2 + A}{2y_1}.$$

After raising them to the qth power, we obtain

$$x_3^q = (m')^2 - 2x_1^q,\ y_3^q = m'(x_1^q - x_3^q) - y_1^q, \text{ where } m' = \frac{3^q(x_1^q)^2 + A}{2^q y_1^q}.$$

Since $2, 3, A \in \mathbb{F}_q$, $2^q = 2, 3^q = 3, A^q = A$. Thus $2, 3, A$ remain the same in m' and $\phi_q(x_3, y_3) = \phi_q(x_1, y_1) + \phi_q(x_2, y_2)$ still holds. In any case, ϕ_q is a homomorphism.

ϕ_q is not separable because $q = 0$ in $\mathbb{F}_q$ and so the derivative of x^q is identically zero. □

3.1. **Separability of endomorphisms of the form $r\phi_q + s$.** The Frobenius endomorphism is not separable, but the separability of $r\phi_q + s$ is to be examined. We need a convenient criterion for separability. As we will see in the last theorem of this section, the endomorphism $r\phi_q + s$ is separable if and only if $p \nmid s$, where p is the characteristic of the finite field on which the curve is defined.

Here are some preliminaries. If (x, y) is a variable point, differentiating y with respect to x yields

$$2yy' = 3x^2 + A.$$

We can also differentiate a rational function $f(x, y)$ with respect to x,

$$\frac{d}{dx}f(x, y) = \frac{\partial f(x, y)}{\partial x} + \frac{\partial f(x, y)}{\partial y}y'.$$

Lemma 3.13. *Let E be the elliptic curve $y^2 = x^3 + Ax + B$. Fix a point (u, v) on E. Write*

$$(x, y) + (u, v) = (f(x, y), g(x, y)),$$

where $f(x, y)$ and $g(x, y)$ are rational functions of x, y (the coefficients depend on (u, v). Then

$$\frac{d}{dx}f(x, y) = \frac{g(x, y)}{y}.$$

Proof. The group law gives

$$f(x, y) = \left(\frac{y - v}{x - u}\right)^2 - x - u$$

$$g(x, y) = \frac{-(y - v)^3 + x(y - v)(x - u)^2 + 2u(y - v)(x - u)^2 - v(x - u)^3}{(x - u)^3}$$

$$\frac{d}{dx}f(x, y) = \frac{2y'(y - v)(x - u) - 2(y - v)^2 - (x - u)^3}{(x - u)^3}.$$

A lengthy calculation, using $2yy' = 3x^2 + A$, yields that

$$(x - u)^3(y\frac{d}{dx}f(x, y) - g(x, y)) =$$
$$v(Au + u^3 - v^2 - Ax - x^3 + y^2) + y(-Au - u^3 + v^2 + Ax + x^3 - y^2).$$

Since (x, y) and (u, v) are on E, we have $v^2 = u^3 + Au + B$ and $y^2 = x^3 + Ax + B$. Therefore, the right side of the above expression is 0. Therefore, $\frac{d}{dx}f(x, y) = \frac{g(x,y)}{y}$. □

Lemma 3.14. *Let $\alpha_1, \alpha_2, \alpha_3$ be nonzero endomorphisms of an elliptic curve E with $\alpha_1 + \alpha_2 = \alpha_3$. Write*

$$\alpha_i(x, y) = (R_{\alpha_i}(x), yS_{\alpha_i}(x)).$$

Suppose there are constants c_{α_1}, c_{α_2} such that

$$\frac{R'_{\alpha_1}(x)}{S_{\alpha_1}(x)} = c_{\alpha_1} \text{ and } \frac{R'_{\alpha_2}(x)}{S_{\alpha_2}(x)} = c_{\alpha_2}.$$

Then

$$\frac{R'_{\alpha_3}(x)}{S_{\alpha_3}(x)} = c_{\alpha_1} + c_{\alpha_2}.$$

Proof. Let (x_1, y_1) and (x_2, y_2) be variable points on E. Write

$$(x_3, y_3) = (x_1, y_1) + (x_2, y_2),$$

where

$$(x_1, y_1) = \alpha_1(x, y),\ (x_2, y_2) = \alpha_2(x, y).$$

By Lemma 3.7, such α_1 and α_2 must exist. By the group law, x_3 and y_3 are rational functions of x_1, y_1, x_2, y_2, which are in turn rational functions of x, y. By Lemma 3.13, with $(u, v) = (x_2, y_2)$,

$$\frac{\partial x_3}{\partial x_1} = \frac{y_3}{y_1}.$$

Similarly, with $(u, v) = (x_1, y_1)$,

$$\frac{\partial x_3}{\partial x_2} = \frac{y_3}{y_2}.$$

By assumption,

$$\frac{\partial x_i}{\partial x} = c_{\alpha_i}\frac{y_i}{y}$$

for $i = 1, 2$. By the chain rule,

$$\begin{aligned}\frac{dx_3}{dx} &= \frac{\partial x_3}{\partial x_1}\frac{\partial x_1}{\partial x} + \frac{\partial x_3}{\partial x_2}\frac{\partial x_2}{\partial x} \\ &= \frac{y_3}{y_1}\frac{y_1}{y}c_{\alpha_1} + \frac{y_3}{y_2}\frac{y_2}{y}c_{\alpha_2} \\ &= (c_{\alpha_1} + c_{\alpha_2})\frac{y_3}{y}.\end{aligned}$$

Dividing by y_3/y yields the result. □

Proposition 3.15. *Let E be an elliptic curve defined over a field K, and let n be a nonzero integer. Suppose that multiplication by n on E is given by*

$$n(x, y) = (R_n(x), yS_n(x))$$

for all $(x, y) \in E(\overline{K})$, where R_n and S_n are rational functions. Then

$$\frac{R'_n(x)}{S_n(x)} = n.$$

Proof. Since $R_{-n} = R_n$ and $S_{-n} = -S_n$, we have $R'_{-n}/S_{-n} = -R'_n/S_n$. Therefore, we only need to consider positive n.

The proposition is obviously true for $n = 1$. If it is true for n, then Lemma 3.14 implies that it is true for $n + 1$, the sum of n and 1. Thus the statement is true for all n. □

Theorem 3.16. *Let E be defined over $\mathbb{F}_q$. Let r and s integers, not both 0. The endomorphism $r\phi_q + s$ is separable if and only if $p \nmid s$, where p is the characteristic of $\mathbb{F}_q$.*

Proof. Write the multiplication by r endomorphism as

$$r(x,y) = (R_r(x), yS_r(x)).$$

Then

$$\begin{aligned}(R_{r\phi_q}(x), yS_{r\phi_q}(x)) &= (r\phi_q)(x,y)\\ &= (R_r^q(x), y^q S_r^q(x))\\ &= (R_r^q(x), y(x^3+Ax+B)^{(q-1)/2} S_r^q(x)).\end{aligned}$$

This means that we can apply Proposition 3.15. Therefore,

$$c_{r\phi_q} = R'_{r\phi_q}/S_{r\phi_q} = qR_r^{q-1}R'_r/S_{r\phi_q} = 0.$$

Also, by Proposition 3.15, $c_s = R'_s/S_s = s$. By Lemma 3.14,

$$R'_{r\phi_q+s}/S_{r\phi_q+s} = c_{r\phi_q+s} = c_{r\phi_q} + c_s = 0 + s = s.$$

Therefore, $R'_{r\phi_q+s} \neq 0$ if and only if $p \nmid s$. □

3.2. **Degree of endomorphisms of the form $a\alpha + b\beta$.**

Definition 3.17. Let E be an elliptic curve over a field K. Let n be a positive integer. The **torsion points** of E of order n is the set

$$E[n] = \{P \in E(\overline{K}) \mid nP = \infty\}.$$

Remark 3.18. $E[n]$ may contain points in $E(\overline{K})$. It may also be empty.

Theorem 3.19. *Let E be an elliptic curve over a field K and let n be a positive integer. If the characteristic of K does not divide n, or is 0, then*

$$E[n] \backsimeq \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}.$$

Proof. The proof can be found in [1] Chapter 3. □

Remark 3.20. This theorem implies that we can choose a basis $\{\beta_1, \beta_2\}$ for $E[n] \backsimeq \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$. This means that every element of $E[n]$ can be expressed in the form $m_1\beta_1 + m_2\beta_2$, where m_1, m_2 are integers that are uniquely determined mod n. Let $\alpha : E(\overline{K}) \to E(\overline{K})$ be a homomorphism (not necessarily an endomorphism). Then α maps $E[n]$ to $E[n]$. Therefore, there are integers $a, b, c, d \in \mathbb{Z}/n\mathbb{Z}$ such that

$$\alpha(\beta_1) = a\beta_1 + c\beta_2,\ \alpha(\beta_2) = b\beta_1 + d\beta_2.$$

Thus, each homomorphism $\alpha : E(\overline{K}) \to E(\overline{K})$ can be represented by a 2×2 matrix

$$\alpha_M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

It follows that composition of homomorphisms corresponds to multiplication of the corresponding matrices.

In many cases, the homomorphism α will be taken to be an endomorphism, which means a homomorphism that is given by rational functions.

Lemma 3.21. *Let M and N be 2×2 matrices. Then*

$$\det(aM + bN) - a^2 \det M - b^2 \det N = ab(\det(M+N) - \det M - \det N)$$

for all scalars a, b.

Proof. Let

$$N = \begin{pmatrix} w & x \\ y & z \end{pmatrix} \quad N' = \begin{pmatrix} z & -x \\ -y & w \end{pmatrix} \quad M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

We first show that

$$\text{Trace}(MN') = \det(M+N) - \det M - \det N.$$

A straightforward calculation yields that both sides equal $az - by + dw - cx$. The left side of the statement becomes

$$\begin{aligned} \det(aM+bN) - \det(aM) - \det(bN) &= \text{Trace}(aM(bN)') \\ &= ab\text{Trace}(MN') \\ &= ab(\det(M+N) - \det M - \det N). \end{aligned}$$

□

Proposition 3.22. *Let α be an endomorphism of an elliptic curve E defined over a field K. Let n be a positive integer not divisible by the characteristic of K. Then* $\det(\alpha_M) \equiv \deg(\alpha) \pmod{n}$.

Proof. The proof needs the construction of Weil pairings, which we will not delve into. It can be found in [1] Chapter 3. □

Lemma 3.23. *Let a, b be scalars and α, β be endomorphisms of an elliptic curve E defined over a field K. Then*

$$\deg(a\alpha + b\beta) = a^2\deg(\alpha) + b^2\deg(\beta) + ab(\deg(\alpha+\beta) - \deg(\alpha) - \deg(\beta)).$$

Proof. By Lemma 3.21,

$$\begin{aligned} \deg(a\alpha+b\beta) &= \det(a\alpha_M + b\beta_M) \\ &= a^2\det(\alpha_M) + b^2\det(\beta_M) + ab(\det(\alpha_M+\beta_M) - \det\alpha_M - \det\beta_M) \end{aligned}$$

for any matrices α_M, β_M. By Proposition 3.22,

$$\deg(a\alpha+b\beta) \equiv a^2\deg(\alpha)+b^2\deg(\beta)+ab(\deg(\alpha+\beta)-\deg(\alpha)-\deg(\beta)) \pmod{n}.$$

This is true for any positive integer n not divisible by the characteristic of K, i.e. infinitely many n. Therefore it must be an equality. □

3.3. **Characteristic equation of Frobenius endomorphisms.** The following theorem is crucial in the proof of Schoof's algorithm, the last section of this paper.

Theorem 3.24. *Let E be an elliptic curve defined over $\mathbb{F}_q$. Let a be $q+1-\#E(\mathbb{F}_q)$. Then*

$$\phi_q^2 - a\phi_q + q = 0$$

as endomorphisms of E for all (x, y). Moreover,

$$a \equiv \textit{Trace}\,((\phi_q)_m) \pmod{m}$$

for all m with gcd$(m, q) = 1$.

Proof. First, $\phi_q^2 - a\phi_q + q$ is an endomorphism. By Theorem 3.6, if an endomorphism is not 0, its kernel size is finite. If we prove that its kernel size is infinite, then it is 0. Let $m \geq 1$ be an integer with $\gcd(m, q)=1$. ϕ_q induces a matrix $(\phi_q)_m$ that describes the action of ϕ_q on $E[m]$. Let

$$(\phi_q)_m = \begin{pmatrix} s & t \\ u & v \end{pmatrix}.$$

Since $\phi_q - 1$ is separable by Proposition 3.25, Theorem 3.6 and Proposition 3.22,

$$\begin{aligned}\#\ker(\phi_q - 1) = \deg(\phi_q - 1) &\equiv \det((\phi_q)_m - I) \\ &= sv - tu - (s + v) + 1 \pmod m.\end{aligned}$$

By Proposition 3.22, $sv - tu = \det((\phi_q)_m) \equiv q \pmod m$. We also know that $\#\ker(\phi_q - 1) = q + 1 - a$. Therefore,

$$\text{Trace } ((\phi_q)_m) = s + v \equiv a \pmod m.$$

By the Cayley-Hamilton theorem of linear algebra, we have

$$(\phi_q)_m^2 - a(\phi_q)_m + qI \equiv 0 \pmod m,$$

where I is the 2×2 identity matrix. This means that the endomorphism $\phi_q^2 - a\phi_q + q$ is identically zero on $E[m]$. Since there are infinitely many choices for m, the kernel of $\phi_q^2 - a\phi_q + q$ is infinite, and so the endomorphism is 0. □

3.4. **Bounding $\#E(\mathbb{F}_q)$: Hasse'e theorem.** We are now ready to prove Hasse's theorem, which bounds the size of $E(\mathbb{F}_q)$. First, we consider the endomorphism $\phi_q - 1$ and prove that $E(\mathbb{F}_q)$ and the kernel of $\phi_p - 1$ have the same size. Second, we prove that $\phi_q - 1$ is separable, and we find that $\#E(\mathbb{F}_q)$ is equal to $\deg(\phi_q - 1))$. Finally, we will use the fact that $\deg(r\phi_q - s) \geq 0$ to get a non-negative discriminant that involves $\deg(\phi_q - 1)$. This non-negative discriminant will bound $\deg(\phi_q - 1)$.

Proposition 3.25. *Let E be an elliptic curve defined over $\mathbb{F}_q$ and let $n \geq 1$.*

(1) $\ker(\phi_q - 1) = E(\mathbb{F}_q)$
(2) $\phi_q - 1$ *is a separable endomorphism, and* $\#E(\mathbb{F}_q) = \deg(\phi_q - 1)$.

Proof. By Lemma 3.12, $(x, y) \in E(\mathbb{F}_q)$ if and only if $\phi_q(x, y) = (x, y)$. We can multiply the inverse of (x, y) to both sides, and thus $\ker(\phi_q - 1) = E(\mathbb{F}_q)$. Since ϕ_q is an endomorphism, $\phi_q - 1$ is also an endomorphism. By Theorem 3.16, it is separable. Then by Theorem 3.6,

$$\#\ker(\phi_q - 1) = \deg(\phi_q - 1).$$

Therefore $\#E(\mathbb{F}_q) = \deg(\phi_q - 1)$. □

Theorem 3.26 (Hasse'e theorem)**.** *Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$. Then*

$$|\#E(\mathbb{F}_q) - (q + 1)| \leq 2\sqrt{q}.$$

Proof. Let $a = (q + 1) - \#E(\mathbb{F}_q) = (q + 1) - \deg(\phi_q - 1)$ by Proposition 3.25. We want to show that $|a| \leq 2\sqrt{q}$. Let r, s be integers with $\gcd(s, q) = 1$. By Lemma 3.23,

$$\deg(r\phi_q - s) = r^2 \deg(\phi_q) + s^2 \deg(-1) + rs(\deg(\phi_q - 1)) - \deg(\phi_q) - \deg(-1)).$$

Since $\deg(\phi_q) = q$ and $\deg(-1) = 1$,

$$\begin{aligned}\deg(\phi_q - 1)) - \deg(\phi_q) - \deg(-1) &= \deg(\phi_q - 1) - q - 1 \\ &= -a.\end{aligned}$$

Thus

$$\deg(r\phi_q - s) = r^2 q + s^2 - rsa.$$

Since $\deg(r\phi_q - s) \geq 0$,

$$r^2 q + s^2 - rsa \geq 0$$

or equivalently, dividing by s^2,

$$q\left(\frac{r}{s}\right)^2 - a\left(\frac{r}{s}\right) + 1 \geq 0$$

for all r, s with $\gcd(s, q) = 1$. The set of rational numbers such that $\gcd(s, q) = 1$ is dense in $\mathbb{R}$. Therefore,

$$qx^2 - ax + 1 \geq 0$$

for all real numbers x. The discriminant $a^2 - 4q$ must then be less than or equal to 0, hence $|a| \leq 2\sqrt{q}$. □

Remark 3.27. The reason we require $\gcd(s, q) = 1$ is that a proposition in Weil pairings that we used is restricted to this situation.

4. Schoof's algorithm

Schoof's algorithm is an efficient algorithm to compute the number of points in $E(\mathbb{F}_q)$. By Hasse's theorem, $|q + 1 - \#E(\mathbb{F}_q)|$ is bounded by $4\sqrt{q}$. We can know its exact value if we know its modulo by a number greater than $4\sqrt{q}$.

4.1. **Division polynomials.** To prove the mathematical legitimacy of Schoof's algorithm, we need to construct a sequence of complicated polynomials called **division polynomials**. We will only use them and some of the useful results, whose proofs can be found in [1] Chapter 3.

Definition 4.1. Define the division polynomials $\psi_m \in \mathbb{Z}[x, y, A, B]$ by

$$\begin{aligned}
\psi_0 &= 0 \\
\psi_1 &= 1 \\
\psi_2 &= 2y \\
\psi_3 &= 3x^4 + 6Ax^2 + 12Bx - A^2 \\
\psi_4 &= 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3) \\
&\vdots \\
\psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \text{ for } m \geq 2 \\
\psi_{2m} &= (2y)^{-1}(\psi_m)(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2) \text{ for } m \geq 2.
\end{aligned}$$

Additionally, define polynomials

$$\begin{aligned}
\phi_m &= x\psi_m^2 - \psi_{m+1}\psi_{m-1} \\
\omega_m &= (4y)^{-1}(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2).
\end{aligned}$$

Lemma 4.2. *ψ_n is a polynomial in $\mathbb{Z}[x, y^2, A, B]$ when n is odd, and ψ_n is a polynomial in $2y\mathbb{Z}[x, y^2, A, B]$ when n is even.*

Theorem 4.3. *Let $P = (x, y)$ be a point on the elliptic curve $y^2 = x^3 + Ax + B$ (over some field of characteristic not 2), and let n be a positive integer. Then*

$$nP = \left(\frac{\phi_n(x)}{\psi_n^2(x)}, \frac{\omega_n(x, y)}{\psi_n(x, y)^3}\right).$$

Lemma 4.4. *Let E be defined over $\mathbb{F}_q$ and $E[n]$ the torsion group of n. Then when n is odd, ψ_n is a polynomial in x and, for $(x, y) \in E(\overline{\mathbb{F}}_q)$, we have*

$$(x, y) \in E[n] \text{ if and only if } \psi_n(x) = 0.$$

4.2. **Proof and summary of Schoof's algorithm.** Suppose E is an elliptic curve given by $y^2 = x^3 + Ax + B$ over $\mathbb{F}_q$. By Hasse's theorem,

$$\#E(\mathbb{F}_q) = q + 1 - a, \text{ with } |a| \leq 2\sqrt{q}.$$

Let $S = \{2, 3, 5, 7 \cdots L\}$ be a set of primes such that

$$\prod_{l \in S} l > 4\sqrt{q}.$$

If we can determine $a \bmod l$ for each prime l in S, then by the Chinese remainder theorem, we know $a \bmod \prod l$, and therefore a is uniquely determined.

Let l be a prime. We can assume that $l \neq p$, where p is the characteristic of $\mathbb{F}_q$, since there always exists another prime that substitutes p and still makes $\prod l$ greater than $4\sqrt{q}$. We want to compute $a \pmod l$.

The first case is when $l = 2$. If $x^3 + Ax + B$ has a root $r \in \mathbb{F}_q$, then $(r, 0) \in E[2]$ and $(r, 0) \in E(\mathbb{F}_q)$, so $E(\mathbb{F}_q)$ has even order. Then $q+1-a$ is even and so a is even. If $x^3 + Ax + B$ has no roots in $\mathbb{F}_q$, then $E(\mathbb{F}_q)$ has no points of order 2, and a is odd. To determine whether $x^3 + Ax + B$ has a root in $\mathbb{F}_q$, we can try all elements in $\mathbb{F}_q$, but this is very costly. A simpler way is to use the fact that $x^3 + Ax + B$ has a root in $\mathbb{F}_q$ if and only if it has a common root with $x^q - x$, since $x^q - x$ contains and only contains all elements of $\mathbb{F}_q$. The Euclidean algorithm, applied to polynomials, yields the gcd of the two polynomials. If the gcd is 1, then there is no common root and a is odd. If the gcd is not 1, then a is even.

Let ϕ_q be the Frobenius endomorphism of E, so

$$\phi_q(x, y) = (x^q, y^q).$$

By Theorem 3.24,

$$\phi_q^2 - a\phi_q + q = 0.$$

Let (x, y) be a point of order l, and let

$$q_l \equiv q \pmod l, \ |q_l| < l/2.$$

Then $q(x, y) = q_l(x, y)$, so

$$\left(x^{q^2}, y^{q^2}\right) + q_l(x, y) = a(x^q, y^q).$$

Since $r\phi_q(P) = \phi_q(rP)$ for any integer r and point P, (x^q, y^q) is also a point of order l. Thus, the above relation determines $a \pmod l$. The idea is to compute all terms in this relation and find a value of a that makes this relation hold. Note that by Theorem 3.24, if the relation holds for one point $(x, y) \in E[l]$, then $a \pmod l$ is determined, and thus it holds for all $x, y \in E[l]$.

Assume first that $(x^q, y^q) \neq \pm q_l(x, y)$ for some $(x, y) \in E[l]$. Then

$$(x', y') \stackrel{\text{def}}{=} \left(x^{q^2}, y^{q^2}\right) + q_l(x, y) \neq \infty,$$

so $a \not\equiv 0 \pmod l$. In this case, the x-coordinates of $\left(x^{q^2}, y^{q^2}\right)$ and $q_l(x, y)$ are distinct, so the sum of the two points is determined by the formula using the line through the two points, rather than a tangent line or a vertical line. Write

$$j(x, y) = (x_j, y_j)$$

for integers j. By Theorem 4.3, we may compute x_j and y_j by using division polynomials. Moreover, $x_j = r_{1,j}(x)$ and $y_j = r_{2,j}(x)y$, as x_j and y_j are given by rational functions. We have

$$x' = \left(\frac{y^{q^2} - y_{q_l}}{x^{q^2} - x_{q_l}}\right)^2 - x^{q^2} - x_{q_l}.$$

Writing

$$\begin{aligned}\left(y^{q^2} - y_{q_l}\right)^2 &= y^2\left(y^{q^2-1} - r_{2,q_l}(x)\right)^2 \\ &= (x^3 + Ax + B)\left((x^3 + Ax + B)^{(q^2-1)/2} - r_{2,q_l}(x)\right)^2,\end{aligned}$$

and noting that x_{q_l} is a function of x, we change x' into a rational function of x. Now we want to find j such that

$$(x', y') = (x_j^q, y_j^q).$$

First, we look at the x-coordinates. We want $x' = x_j^q$. As pointed out above, if this happens for one point in $E[l]$, it happens for all points in $E[l]$. By Lemma 4.4, the roots of ψ_l are the x-coordinates of the points in $E[l]$. This implies that

$$x' - x_j^q \equiv 0 \pmod{\psi_l}. \tag{4.5}$$

This means that the numerator of $x' - x_j^q$ is a multiple of ψ_l. We are here using the fact that the roots of ψ_l are simple (otherwise, we would obtain only that ψ_l divides some power of $x' - x_j^q$). This is proved by noting that there are $l^2 - 1$ distinct points of order l, since $E[l] \backsimeq \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ where $n = l$ and $l \neq p$. There are $(l^2 - 1)/2$ distinct x-coordinates of these points, since if P is in $E[n]$, $-P$ is also in $E[n]$. All of the distinct x-coordinates are roots of ψ_l, which has degree $(l^2 - 1)/2$. Therefore, the roots of ψ_l must be simple.

Assume now that we have found j such that eq. (4.5) holds. Then

$$(x', y') = \pm(x_j^q, y_j^q) = (x_j^q, \pm y_j^q).$$

To determine the sign, we need to look at the y-coordinates. Both y'/y and y_j^q/y can be written as functions of x. If

$$(y' - y_j^q)/y \equiv 0 \pmod{\psi_l},$$

then $a \equiv j \pmod{l}$. Otherwise, $a \equiv -j \pmod{l}$. Therefore, we have found $a \pmod{l}$.

The last case left is where $(x^{q^2}, y^{q^2}) = \pm q(x, y)$ for all $(x, y) \in E[l]$. If

$$\phi_q^2(x, y) = \left(x^{q^2}, y^{q^2}\right) = q(x, y),$$

then

$$a\phi_q(x, y) = \phi_q^2(x, y) + q(x, y) = 2q(x, y),$$

hence

$$a^2 q(x, y) = a^2\phi_q^2(x, y) = (2q)^2(x, y).$$

Therefore, $a^2 q \equiv 4q^2 \pmod{l}$, so $a^2 \equiv 2^2 q \pmod{l}$. Thus q is a square mod l. Let $w^2 \equiv q \pmod{l}$. We have

$$(\phi_q + w)(\phi_q - w)(x, y) = (\phi_q^2 - q)(x, y) = \infty$$

for all $(x, y) \in E[l]$. Let P be any point in $E[l]$. Then either $(\phi_q - w)P = \infty$, so $\phi_q P = wP$, or $P' = (\phi_q - w)P$ is a finite point with $(\phi_q + w)P' = \infty$. Therefore, in either case, there exists a point $P \in E[l]$ with $\phi_q P = \pm wP$.

Suppose there exists a point $P \in E[l]$ such that $\phi_q P = wP$. Then

$$\infty = (\phi_q^2 - a\phi_q + q)P = (q - aw + q)P,$$

so $aw \equiv 2q \equiv 2w^2 \pmod{l}$. Therefore, $a \equiv 2w \pmod{l}$. Similarly, if there exists P such that $\phi_q P = -wP$, then $a \equiv -2w \pmod{l}$. We can check whether we are in this case as follows. We need to know whether or not

$$(x^q, y^q) = \pm w(x, y) = \pm(x_w, y_w) = (x_w, \pm y_w)$$

for some $(x, y) \in E[l]$. Therefore, we compute $x^q - x_w$, which is a rational function of x. If

$$\gcd(\text{numerator}(x^q - x_w), \psi_l) \neq 1,$$

then there is some $(x, y) \in E[l]$ such that $\phi_q(x, y) = \pm w(x, y)$. If this happens, then use the y-coordinates to determine the sign.

Why do we use the gcd rather than simply checking whether we have 0 mod ψ_l? The gcd checks for the existence of one point, while looking for 0 $\pmod{\psi_l}$ checks if the relation holds for all points simultaneously. The problem is that we are not guaranteed that $\phi_q P = \pm wP$ for all $P \in E[l]$. For example, the matrix representing ϕ_q on $E[l]$ might not be diagonalizable.

If $\gcd(\text{numerator}(x^q - x_w), \psi_l) = 1$, then we cannot be in the case $\left(x^{q^2}, y^{q^2}\right) = q(x, y)$. So the only remaining case is $\left(x^{q^2}, y^{q^2}\right) = -q(x, y)$. In this case, $aP = (\phi_q^2 + q)P = \infty$ for all $P \in E[l]$. Therefore, $a \equiv 0 \pmod{l}$.

We summarize Schoof's algorithm as follows. We start with an elliptic curve E given by $y^2 = x^3 + Ax + B$ over $\mathbb{F}_q$. We want to compute $\#E(\mathbb{F}_q) = q + 1 - a$.

(1) Choose a set of primes $S = \{2, 3, 5, \ldots, L\}$(with $p \notin S$) such that $\prod_{l \in S} l > 4\sqrt{q}$.
(2) If $l = 2$, we have $a \equiv 0 \pmod{2}$ if and only if $\gcd(x^3 + Ax + B, x^q - x) \neq 1$.
(3) For each odd prime $l \in S$, do the following.
   (a) Let $q_l \equiv q \pmod{l}$ with $|q_l| < l/2$.
   (b) Compute the x-coordinate x' of

$$(x', y') = \left(x^{q^2}, y^{q^2}\right) + q_l(x, y) \pmod{\psi_l}.$$

   (c) For $j = 1, 2, \ldots, (l-1)/2$, do the following.
      i. Compute the x-coordinate x_j of $(x_j, y_j) = j(x, y)$.
      ii. If $x' - x_j^q \equiv 0 \pmod{\psi_l}$, go to step (iii). If not, try the next value of j in step (c). If all values $1 \leq j \leq (l-1)/2$ have been tried, go to step (d).
      iii. Compute y' and y_j. If $(y' - y_j)/y \equiv 0 \pmod{\psi_l}$, then $a \equiv j \pmod{l}$. If not, then $a \equiv -j \pmod{l}$.
   (d) If all values $1 \leq j \leq (l-1)/2$ have been tried without success, let $w^2 \equiv q \pmod{l}$. If w does not exist, then $a \equiv 0 \pmod{l}$.
   (e) If $\gcd(\text{numerator}(x^q - x_w), \psi_l) = 1$, then $a \equiv 0 \pmod{l}$. Otherwise, compute

$$\gcd(\text{numerator}((y^q - y_w)/y), \psi_l).$$

If this gcd is not 1, then $a \equiv 2w \pmod{l}$. Otherwise, $a \equiv -2w \pmod{l}$.

(4) Use $a \pmod{l}$ for each $l \in S$ to compute $a \pmod{\prod l}$. Choose the value of a that satisfies this congruence and such that $|a| \leq 2\sqrt{q}$. The number of points in $E(\mathbb{F}_q)$ is $q + 1 - a$.

4.3. **An example that applies Schoof's algorithm.**

Example 4.6. Let E be the elliptic curve $y^2 = x^3 + 2x + 1 \bmod 19$. By Hasse's theorem,

$$\#E(\mathbb{F}_{19}) = 19 + 1 - a, \text{ where } |a| < 2\sqrt{19} < 9.$$

In order to determine a, we'll show that

$$a \equiv 1 \pmod{2},\ a \equiv 2 \pmod{3},\ a \equiv 3 \pmod{5}.$$

Putting these together yields,

$$a \equiv 23 \pmod{30}.$$

Since $|a| < 9$, we must have $a = -7$. Start with $l = 2$. We compute

$$x^{19} \equiv x^2 + 13x + 14 \pmod{x^3 + 2x + 1}.$$

Then we can use the result to compute

$$\gcd(x^{19} - x, x^3 + 2x + 1) = \gcd(x^2 + 13x + 14, x^3 + 2x + 1) = 1.$$

It follows that $x^3 + 2x + 1$ has no roots in $\mathbb{F}_{19}$. Therefore, there is no 2-torsion in $E(\mathbb{F}_{19})$. So $a \equiv 1 \pmod{2}$.

For $l = 3$, we proceed as in Schoof's algorithm and eventually get to $j = 1$. We have $q^2 = 361$ and $q \equiv 1 \pmod{3}$. By the characteristic equation, we need to check whether

$$\left(x^{361}, y^{361}\right) + (x, y) = \pm\left(x^{19}, y^{19}\right)$$

for $(x, y) \in E[3]$. The third division polynomial is

$$\psi_3 = 3x^4 + 12x^2 + 12x - 4.$$

We compute the x-coordinate of $(x^{361}, y^{361}) + (x, y)$:

$$\left(\frac{y^{361} - y}{x^{361} - x}\right)^2 - x^{361} - x = (x^3 + 2x + 1)\left(\frac{(x^3 + 2x + 1)^{180} - 1}{x^{361} - x}\right)^2 - x^{361} - x,$$

where we have used the relation $y^2 = x^3 + 2x + 1$. We need to reduce this $\pmod{\psi_3}$. However,

$$\gcd(x^{361} - x, \psi_3) = x - 8 \neq 1,$$

so the multiplicative inverse does not exist. We could remove $x - 8$ from the numerator and denominator of

$$\frac{(x^3 + 2x + 1)^{180} - 1}{x^{361} - x},$$

but this is unnecessary. Instead, we realize that since $x = 8$ is a root of ψ_3, the point $(8, 4) \in E(\mathbb{F}_{19})$ has order 3. Therefore,

$$\#E(\mathbb{F}_{19}) = 19 + 1 - a \equiv 0 \pmod{3},$$

so $a \equiv 2 \pmod{3}$.

For $l = 5$, we eventually arrive at $j = 2$ by following Schoof's algorithm. Note that

$$19 \equiv -1 \pmod 5,$$

so $q_l = -1$ and

$$19(x, y) = -(x, y) = (x, -y) \text{ for all } (x, y) \in E[5].$$

We need to check whether

$$(x_1, y_1) \stackrel{\text{def}}{=} \left(x^{361}, y^{361}\right) + (x, -y) \stackrel{?}{=} \pm 2\left(x^{19}, y^{19}\right) \stackrel{\text{def}}{=} \pm(x_2, y_2)$$

for all $(x, y) \in E[5]$. The fifth division polynomial is computed:

$$\psi_5 = 5x^{12} + 10x^{10} + 17x^8 + 5x^7 + x^6 + 9x^5 + 12x^4 + 2x^3 + 5x^2 + 8x + 8.$$

The equation for the x-coordinates yields

$$x_1 = \left(\frac{y^{361} + y}{x^{361} - x}\right)^2 - x^{361} - x \stackrel{?}{=} \left(\frac{3x^{38} + 2}{2y^{19}}\right)^2 - 2x^{19} = x_2 \pmod{\psi_5}.$$

When y^2 is changed to $x^3 + 2x + 1$, this reduces to a polynomial relation in x, which is then verified. Therefore,

$$a \equiv \pm 2 \pmod 5.$$

We look at the y-coordinate to determine the sign. y_1 is computed:

$$y(9x^{11} + 13x^{10} + 15x^9 + 15x^7 + 18x^6 + 17x^5 + 8x^4 + 12x^3 + 8x + 6) \pmod{\psi_5}.$$

The y-coordinate of $(x_2, y_2) = 2(x, y)$ is

$$y(13x^{10} + 15x^9 + 16x^8 + 13x^7 + 8x^6 + 6x^5 + 17x^4 + 18x^3 + 8x + 18) \pmod{\psi_5}.$$

A computation yields

$$(y_1 + y_2^{19})/y \equiv 0 \pmod{\psi_5}.$$

This means that

$$(x_1, y_1) \equiv (x_2^{19}, -y_2^{19}) = -2(x^q, y^q) \pmod{\psi_5}.$$

It follows that $a \equiv -2 \pmod 5$.

Therefore, $\#E(\mathbb{F}_{19}) = 27$.

Acknowledgment

It is my pleasure to thank my mentor, Adan Medrano Martin Del Campo, for his continuous assistance with problems I encountered in the study of elliptic curves. I would also like to thank Peter May for organizing this great REU program at the University of Chicago.

References

[1] Lawrence C. Washington. *Elliptic Curves: Number Theory and Cryptography.* Chapman & Hall/CRC, 2003.

[2] Igor Tolkov. *Counting points on elliptic curves: Hasse's theorem and recent developments.* 2009.