Chapter 4

Elliptic Curves over Finite Fields

Let $\mathbf{F}$ be a finite field and let E be an elliptic curve defined over $\mathbf{F}$. Since there are only finitely many pairs (x, y) with $x, y \in \mathbf{F}$, the group $E(\mathbf{F})$ is finite. Various properties of this group, for example, its order, turn out to be important in many contexts. In this chapter, we present the basic theory of elliptic curves over finite fields. Not only are the results interesting in their own right, but also they are the starting points for the cryptographic applications discussed in Chapter 6.

4.1 Examples

First, let's consider some examples.

Example 4.1

Let E be the curve $y^2 = x^3 + x + 1$ over $\mathbf{F}_5$. To count points on E, we make a list of the possible values of x, then of $x^3 + x + 1 \pmod 5$, then of the square roots y of $x^3 + x + 1 \pmod 5$. This yields the points on E.

x	$x^3 + x + 1$	y	Points
0	1	± 1	$(0,1), (0,4)$
1	3	–	–
2	1	± 1	$(2,1), (2,4)$
3	1	± 1	$(3,1), (3,4)$
4	4	± 2	$(4,2), (4,3)$
∞		∞	∞

Therefore, $E(\mathbf{F}_5)$ has order 9.

Let's compute $(3,1)+(2,4)$ on E. The slope of the line through the two points is

$$\frac{4-1}{2-3} \equiv 2 \pmod 5.$$

The line is therefore $y = 2(x-3)+1 \equiv 2x$. Substituting this into $y^2 = x^3+x+1$ and rearranging yields

$$0 = x^3 - 4x^2 + x + 1.$$

The sum of the roots is 4, and we know the roots 3 and 2. Therefore the remaining root is $x = 4$. Since $y = 2x$, we have $y \equiv 3$. Reflecting across the x-axis yields the sum:

$$(3,1)+(2,4) = (4,2).$$

(Of course, we could have used the formulas of Section 2.2 directly.) A little calculation shows that $E(\mathbf{F}_5)$ is cyclic, generated by $(0,1)$ (Exercise 4.1). □

Example 4.2

Let E be the elliptic curve $y^2 = x^3+2$ over $\mathbf{F}_7$. Then

$$E(\mathbf{F}_7) = \{\infty,\ (0,3),\ (0,4),\ (3,1),\ (3,6),\ (5,1),\ (5,6),\ (6,1),\ (6,6)\}.$$

An easy calculation shows that all of these points P satisfy $3P = \infty$, so the group is isomorphic to $\mathbf{Z}_3 \oplus \mathbf{Z}_3$. □

Example 4.3

Let's consider the elliptic curve E given by $y^2 + xy = x^3 + 1$ defined over $\mathbf{F}_2$. We can find the points as before and obtain

$$E(\mathbf{F}_2) = \{\infty,\ (0,1),\ (1,0),\ (1,1)\}.$$

This is a cyclic group of order 4. The points $(1,0), (1,1)$ have order 4 and the point $(0,1)$ has order 2.

Now let's look at $E(\mathbf{F}_4)$. Recall that $\mathbf{F}_4$ is the finite field with 4 elements. We can write it as $\mathbf{F}_4 = \{0,1,\omega,\omega^2\}$, with the relation $\omega^2+\omega+1 = 0$ (which implies, after multiplying by $\omega+1$, that $\omega^3 = 1$). Let's list the elements of $E(\mathbf{F}_4)$.

$$\begin{aligned}
&x = 0 \Rightarrow y^2 = 1 \Rightarrow y = 1\\
&x = 1 \Rightarrow y^2 + y = 0 \Rightarrow y = 0,1\\
&x = \omega \Rightarrow y^2 + \omega y = 0 \Rightarrow y = 0,\omega\\
&x = \omega^2 \Rightarrow y^2 + \omega^2 y = 0 \Rightarrow y = 0,\omega^2\\
&x = \infty \Rightarrow y = \infty.
\end{aligned}$$

Therefore

$$E(\mathbf{F}_4) = \big\{\infty,\ (0,1),\ (1,0),\ (1,1),\ (\omega,0),\ (\omega,\omega),\ (\omega^2,0),\ (\omega^2,\omega^2)\big\}.$$

Since we are in characteristic 2, there is at most one point of order 2 (see Proposition 3.1). In fact, $(0, 1)$ has order 2. Therefore, $E(\mathbf{F}_4)$ is cyclic of order 8. Any one of the four points containing ω or ω^2 is a generator. This may be verified by direct calculation, or by observing that they do not lie in the order 4 subgroup $E(\mathbf{F}_2)$. Let $\phi_2(x, y) = (x^2, y^2)$ be the Frobenius map. It is easy to see that ϕ_2 permutes the elements of $E(\mathbf{F}_4)$, and

$$E(\mathbf{F}_2) = \{(x, y) \in E(\mathbf{F}_4) \mid \phi_2(x, y) = (x, y)\}.$$

In general, for any elliptic curve E defined over $\mathbf{F}_q$ and any extension $\mathbf{F}$ of $\mathbf{F}_q$, the Frobenius map ϕ_q permutes the elements of $E(\mathbf{F})$ and is the identity on the subgroup $E(\mathbf{F}_q)$. See Lemma 4.5. □

Two main restrictions on the groups $E(\mathbf{F}_q)$ are given in the next two theorems.

THEOREM 4.1

Let E be an elliptic curve over the finite field $\mathbf{F}_q$. Then

$$E(\mathbf{F}_q) \simeq \mathbf{Z}_n \quad \textit{or} \quad \mathbf{Z}_{n_1} \oplus \mathbf{Z}_{n_2}$$

for some integer $n \geq 1$, or for some integers $n_1, n_2 \geq 1$ with n_1 dividing n_2.

PROOF A basic result in group theory (see Appendix B) says that a finite abelian group is isomorphic to a direct sum of cyclic groups

$$\mathbf{Z}_{n_1} \oplus \mathbf{Z}_{n_2} \oplus \cdots \oplus \mathbf{Z}_{n_r},$$

with $n_i | n_{i+1}$ for $i \geq 1$. Since, for each i, the group $\mathbf{Z}_{n_i}$ has n_1 elements of order dividing n_1, we find that $E(\mathbf{F}_q)$ has n_1^r elements of order dividing n_1. By Theorem 3.2, there are at most n_1^2 such points (even if we allow coordinates in the algebraic closure of $\mathbf{F}_q$). Therefore $r \leq 2$. This is the desired result (the group is trivial if $r = 0$; this case is covered by $n = 1$ in the theorem). ■

THEOREM 4.2 (Hasse)

Let E be an elliptic curve over the finite field $\mathbf{F}_q$. Then the order of $E(\mathbf{F}_q)$ satisfies

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

The proof will be given in Section 4.2.

A natural question is what groups can actually occur as groups $E(\mathbf{F}_q)$. The answer is given in the following two results, which are proved in [130] and [93], respectively.

THEOREM 4.3

Let $q = p^n$ be a power of a prime p and let $N = q+1-a$. There is an elliptic curve E defined over $\mathbf{F}_q$ such that $\#E(\mathbf{F}_q) = N$ if and only if $|a| \leq 2\sqrt{q}$ and a satisfies one of the following:

1. $\gcd(a, p) = 1$
2. *n is even and $a = \pm 2\sqrt{q}$*
3. *n is even, $p \not\equiv 1 \pmod 3$, and $a = \pm\sqrt{q}$*
4. *n is odd, $p = 2$ or 3, and $a = \pm p^{(n+1)/2}$*
5. *n is even, $p \not\equiv 1 \pmod 4$, and $a = 0$*
6. *n is odd and $a = 0$.*

THEOREM 4.4

Let N be an integer that occurs as the order of an elliptic curve over a finite field $\mathbf{F}_q$, as in Theorem 4.3. Write $N = p^e n_1 n_2$ with $p \nmid n_1 n_2$ and $n_1 | n_2$ (possibly $n_1 = 1$). There is an elliptic curve E over $\mathbf{F}_q$ such that

$$E(\mathbf{F}_q) \simeq \mathbf{Z}_{p^e} \oplus \mathbf{Z}_{n_1} \oplus \mathbf{Z}_{n_2}$$

if and only if

1. *$n_1 | q-1$ in cases (1), (3), (4), (5), (6) of Theorem 4.3*
2. *$n_1 = n_2$ in case (2) of Theorem 4.3.*

These are the only groups that occur as groups $E(\mathbf{F}_q)$.

4.2 The Frobenius Endomorphism

Let $\mathbf{F}_q$ be a finite field with algebraic closure $\overline{\mathbf{F}}_q$ and let

$$\begin{aligned} \phi_q : \overline{\mathbf{F}}_q &\longrightarrow \overline{\mathbf{F}}_q, \\ x &\mapsto x^q \end{aligned}$$

be the Frobenius map for $\mathbf{F}_q$ (see Appendix C for a review of finite fields). Let E be an elliptic curve defined over $\mathbf{F}_q$. Then ϕ_q acts on the coordinates of points in $E(\overline{\mathbf{F}}_q)$:

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

LEMMA 4.5

Let E be defined over $\mathbf{F}_q$, and let $(x, y) \in E(\overline{\mathbf{F}}_q)$.

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

PROOF One fact we need is that $(a + b)^q = a^q + b^q$ when q is a power of the characteristic of the field. We also need that $a^q = a$ for all $a \in \mathbf{F}_q$. See Appendix C.

Since the proof is the same for the Weierstrass and the generalized Weierstrass equations, we work with the general form. We have

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

with $a_i \in \mathbf{F}_q$. Raise the equation to the qth power to obtain

$$(y^q)^2 + a_1(x^qy^q) + a_3(y^q) = (x^q)^3 + a_2(x^q)^2 + a_4(x^q) + a_6.$$

This means that (x^q, y^q) lies on E, which proves (1).

For (2), again recall that $x \in \mathbf{F}_q$ if and only if $\phi_q(x) = x$ (see Appendix C), and similarly for y. Therefore

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

▮

LEMMA 4.6

Let E be an elliptic curve defined over $\mathbf{F}_q$. Then ϕ_q is an endomorphism of E of degree q, and ϕ_q is not separable.

This is the same as Lemma 2.20.

Note that the kernel of the endomorphism ϕ_q is trivial. This is related to the fact that ϕ_q is not separable. See Proposition 2.21.

The following result is the key to counting points on elliptic curves over finite fields. Since ϕ_q is an endomorphism of E, so are $\phi_q^2 = \phi_q \circ \phi_q$ and also $\phi_q^n = \phi_q \circ \phi_q \circ \cdots \circ \phi_q$ for every $n \geq 1$. Since multiplication by -1 is also an endomorphism, the sum $\phi_q^n - 1$ is an endomorphism of E.

PROPOSITION 4.7

Let E be defined over $\mathbf{F}_q$ and let $n \geq 1$.

1. *$Ker(\phi_q^n - 1) = E(\mathbf{F}_{q^n})$.*

2. $\phi_q^n - 1$ *is a separable endomorphism, so* $\#E(\mathbf{F}_{q^n}) = \deg(\phi_q^n - 1)$.

PROOF Since ϕ_q^n is the Frobenius map for the field $\mathbf{F}_{q^n}$, part (1) is just a restatement of Lemma 4.5. The fact that $\phi_q^n - 1$ is separable was proved in Proposition 2.29. Therefore (2) follows from Proposition 2.21. ▮

Proof of Hasse's theorem:
We can now prove Hasse's theorem (Theorem 4.2). Let

$$a = q + 1 - \#E(\mathbf{F}_q) = q + 1 - \deg(\phi_q - 1). \tag{4.1}$$

We want to show that $|a| \le 2\sqrt{q}$. We need the following.

LEMMA 4.8
Let r, s *be integers with* $\gcd(s,q) = 1$. *Then* $\deg(r\phi_q - s) = r^2q + s^2 - rsa$.

PROOF Proposition 3.16 implies that

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

Since $\deg(\phi_q) = q$ and $\deg(-1) = 1$, the result follows from (4.1). ▮

REMARK 4.9 The assumption that $\gcd(s,q) = 1$ is not needed. We include it since we have proved Proposition 3.16 not in general, but only when the endomorphisms are separable or ϕ_q. ▮

We can now finish the proof of Hasse's theorem. Since $\deg(r\phi_q - s) \ge 0$, the lemma implies that

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

for all r, s with $\gcd(s,q) = 1$. The set of rational numbers r/s such that $\gcd(s,q) = 1$ is dense in $\mathbf{R}$. (*Proof:* Take s to be a power of 2 or a power of 3, one of which must be relatively prime with q. The rationals of the form $r/2^m$ and those of the form $r/3^m$ are easily seen to be dense in $\mathbf{R}$.) Therefore,

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

for all real numbers x. Therefore the discriminant of the polynomial is negative or 0, which means that $a^2 - 4q \le 0$, hence $|a| \le 2\sqrt{q}$. This completes the proof of Hasse's theorem. ▮

There are several major ingredients of the above proof. One is that we can identify $E(\mathbf{F}_q)$ as the kernel of $\phi_q - 1$. Another is that $\phi_q - 1$ is separable, so the order of the kernel is the degree of $\phi_q - 1$. A third major ingredient is the Weil pairing, especially part (6) of Theorem 3.9, and its consequence, Proposition 3.16.

Proposition 4.7 has another very useful consequence.

THEOREM 4.10

Let E be an elliptic curve defined over $\mathbf{F}_q$. Let a be as in Equation 4.1. Then

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

as endomorphisms of E, and a is the unique integer k such that

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

In other words, if $(x, y) \in E(\overline{\mathbf{F}}_q)$, then

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

and a is the unique integer such that this relation holds for all $(x, y) \in E(\overline{\mathbf{F}}_q)$. Moreover, a is the unique integer satisfying

$$a \equiv \text{Trace}((\phi_q)_m) \mod m$$

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

PROOF If $\phi_q^2 - a\phi_q + q$ is not the zero endomorphism, then its kernel is finite (Proposition 2.21). We'll show that the kernel is infinite, hence the endomorphism is 0.

Let $m \geq 1$ be an integer with $\gcd(m, q) = 1$. Recall that 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 2.29, Propositions 2.21 and 3.15 imply that

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

By Proposition 3.15, $sv - tu = \det((\phi_q)_m) \equiv q \pmod{m}$. By (4.1), $\#\text{Ker}(\phi_q - 1) = q + 1 - a$. Therefore,

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

By the Cayley-Hamilton theorem of linear algebra, or by a straightforward calculation (substituting the matrix into the polynomial), we have

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

where I is the 2×2 identity matrix. (Note that $X^2 - aX + q$ is the characteristic polynomial of $(\phi_q)_m$.) 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, so the endomorphism is 0.

Suppose $a_1 \neq a$ satisfies $\phi_q^2 - a_1\phi_q + q = 0$. Then

$$(a - a_1)\phi_q = (\phi_q^2 - a_1\phi_q + q) - (\phi_q^2 - a\phi_q + q) = 0.$$

By Theorem 2.22, $\phi_q : E(\overline{\mathbf{F}}_q) \to E(\overline{\mathbf{F}}_q)$ is surjective. Therefore, $(a - a_1)$ annihilates $E(\overline{\mathbf{F}}_q)$. In particular, $(a - a_1)$ annihilates $E[m]$ for every $m \geq 1$. Since there are points in $E[m]$ of order m when $\gcd(m, q) = 1$, we find that $a - a_1 \equiv 0 \pmod{m}$ for such m. Therefore $a - a_1 = 0$, so a is unique. ▮

We single out the following result, which was proved during the proof of Theorem 4.10.

PROPOSITION 4.11

Let E be an elliptic curve over $\mathbf{F}_q$ and let $(\phi_q)_m$ denote the matrix giving the action of the Frobenius ϕ_q on $E[m]$. Let $a = q + 1 - \#E(\mathbf{F}_q)$. Then

$$\mathrm{Trace}((\phi_q)_m) \equiv a \pmod{m}, \qquad \det((\phi_q)_m) \equiv q \pmod{m}.$$

The polynomial $X^2 - aX + q$ is often called the **characteristic polynomial of Frobenius**.

4.3 Determining the Group Order

Hasse's theorem gives bounds for the group of points on an elliptic curve over a finite field. In this section and in Section 4.5, we'll discuss some methods for actually determining the order of the group.

4.3.1 Subfield Curves

Sometimes we have an elliptic curve E defined over a small finite field $\mathbf{F}_q$ and we want to know the order of $E(\mathbf{F}_{q^n})$ for some n. We can determine the order of $E(\mathbf{F}_{q^n})$ when $n = 1$ by listing the points or by some other elementary procedure. The amazing fact is that this allows us to determine the order for all n.

THEOREM 4.12

Let $\#E(\mathbf{F}_q) = q + 1 - a$. Write $X^2 - aX + q = (X - \alpha)(X - \beta)$. Then

$$\#E(\mathbf{F}_{q^n}) = q^n + 1 - (\alpha^n + \beta^n)$$

for all $n \geq 1$.

PROOF First, we need the fact that $\alpha^n + \beta^n$ is an integer. This could be proved by remarking that it is an algebraic integer and is also a rational number. However, it can also be proved by more elementary means.

LEMMA 4.13

Let $s_n = \alpha^n + \beta^n$. Then $s_0 = 2$, $s_1 = a$, and $s_{n+1} = as_n - qs_{n-1}$ for all $n \geq 1$.

PROOF Multiply the relation $\alpha^2 - a\alpha + q = 0$ by α^{n-1} to obtain $\alpha^{n+1} = a\alpha^n - q\alpha^{n-1}$. There is a similar relation for β. Add the two relations to obtain the lemma. ▮

It follows immediately from the lemma that $\alpha^n + \beta^n$ is an integer for all $n \geq 0$.

Let

$$f(X) = (X^n - \alpha^n)(X^n - \beta^n) = X^{2n} - (\alpha^n + \beta^n)X^n + q^n.$$

Then $X^2 - aX + q = (X - \alpha)(X - \beta)$ divides $f(X)$. It follows immediately from the standard algorithm for dividing polynomials that the quotient is a polynomial $Q(X)$ with integer coefficients (the main points are that the leading coefficient of $X^2 - aX + q$ is 1 and that this polynomial and $f(X)$ have integer coefficients). Therefore

$$(\phi_q^n)^2 - (\alpha^n + \beta^n)\phi_q^n + q^n = f(\phi_q) = Q(\phi_q)(\phi_q^2 - a\phi_q + q) = 0,$$

as endomorphisms of E, by Theorem 4.10. Note that $\phi_q^n = \phi_{q^n}$. By Theorem 4.10, there is only one integer k such that $\phi_{q^n}^2 - k\phi_{q^n} + q^n = 0$, and such a k is determined by $k = q^n + 1 - \#E(\mathbf{F}_{q^n})$. Therefore,

$$\alpha^n + \beta^n = q^n + 1 - \#E(\mathbf{F}_{q^n}).$$

This completes the proof of Theorem 4.12. ▮

Example 4.4

In Example 4.3, we showed that the elliptic curve E given by $y^2+xy = x^3+1$ over $\mathbf{F}_2$ satisfies $\#E(\mathbf{F}_2) = 4$. Therefore, $a = 2+1-4 = -1$, and we obtain the polynomial

$$X^2 + X + 2 = \left(X - \frac{-1+\sqrt{-7}}{2}\right)\left(X - \frac{-1-\sqrt{-7}}{2}\right).$$

Theorem 4.12 says that

$$\#E(\mathbf{F}_4) = 4 + 1 - \left(\frac{-1+\sqrt{-7}}{2}\right)^2 - \left(\frac{-1-\sqrt{-7}}{2}\right)^2.$$

Rather than computing the last expression directly, we can use the recurrence in Lemma 4.13:

$$s_2 = as_1 - 2s_0 = -(-1) - 2(2) = -3.$$

It follows that $\#E(\mathbf{F}_4) = 4+1-(-3) = 8$, which is what we calculated by listing points.

Similarly, using the recurrence or using sufficiently high precision floating point arithmetic yields

$$\left(\frac{-1+\sqrt{-7}}{2}\right)^{101} + \left(\frac{-1-\sqrt{-7}}{2}\right)^{101} = 2969292210605269.$$

Therefore,

$$\begin{aligned}\#E(\mathbf{F}_{2^{101}}) &= 2^{101} + 1 - 2969292210605269 \\ &= 2535301200456455833701195805484.\end{aligned}$$

□

The advantage of Theorem 4.12 is that it allows us to determine the group order for certain curves very quickly. The disadvantage is that it requires the curve to be defined over a small finite field.

4.3.2 Legendre Symbols

To make a list of points on $y^2 = x^3 + Ax + B$ over a finite field, we tried each possible value of x, then found the square roots y of $x^3 + Ax + B$, if they existed. This procedure is the basis for a simple point counting algorithm.

Recall the **Legendre symbol** $\left(\frac{x}{p}\right)$ for an odd prime p, which is defined as follows:

$$\left(\frac{x}{p}\right) = \begin{cases} +1 \text{ if } t^2 \equiv x \pmod p \text{ has a solution } t \not\equiv 0 \pmod p, \\ -1 \text{ if } t^2 \equiv x \pmod p \text{ has no solution } t \\ \ \ 0 \text{ if } x \equiv 0 \pmod p. \end{cases}$$

This can be generalized to any finite field $\mathbf{F}_q$ with q odd by defining, for $x \in \mathbf{F}_q$,

$$\left(\frac{x}{\mathbf{F}_q}\right) = \begin{cases} +1 \text{ if } t^2 = x \text{ has a solution } t \in \mathbf{F}_q^\times, \\ -1 \text{ if } t^2 = x \text{ has no solution } t \in \mathbf{F}_q, \\ \ \ 0 \text{ if } x = 0. \end{cases}$$

THEOREM 4.14

Let E be an elliptic curve defined by $y^2 = x^3 + Ax + B$ over $\mathbf{F}_q$. Then

$$\#E(\mathbf{F}_q) = q + 1 + \sum_{x \in \mathbf{F}_q} \left(\frac{x^3 + Ax + B}{\mathbf{F}_q}\right).$$

PROOF For a given x_0, there are two points (x, y) with x-coordinate x_0 if $x_0^3 + Ax_0 + B$ is a nonzero square in $\mathbf{F}_q$, one such point if it is zero, and no points if it is not a square. Therefore, the number of points with x-coordinate x_0 equals $1 + \left(\frac{x_0^3+Ax_0+B}{\mathbf{F}_q}\right)$. Summing over all $x_0 \in \mathbf{F}_q$, and including 1 for the point ∞, yields

$$\#E(\mathbf{F}_q) = 1 + \sum_{x \in \mathbf{F}_q} \left(1 + \left(\frac{x^3 + Ax + B}{\mathbf{F}_q}\right)\right).$$

Collecting the term 1 from each of the q summands yields the desired formula. ▮

COROLLARY 4.15

Let $x^3 + Ax + B$ be a polynomial with $A, B \in \mathbf{F}_q$, where q is odd. Then

$$\left| \sum_{x \in \mathbf{F}_q} \left(\frac{x^3 + Ax + B}{\mathbf{F}_q}\right) \right| \le 2\sqrt{q}.$$

PROOF When $x^3 + Ax + B$ has no repeated roots, $y^2 = x^3 + Ax + B$ gives an elliptic curve, so Theorem 4.14 says that

$$q + 1 - \#E(\mathbf{F}_q) = - \sum_{x \in \mathbf{F}_q} \left(\frac{x^3 + Ax + B}{\mathbf{F}_q}\right).$$

The result now follows from Hasse's theorem.

The case where $x^3 + Ax + B$ has repeated roots follows from Exercise 4.3. ▮

Example 4.5

Let E be the curve $y^2 = x^3 + x + 1$ over $\mathbf{F}_5$, as in Example 4.1. The nonzero squares mod 5 are 1 and 4. Therefore

$$\begin{aligned}
\#E(\mathbf{F}_5) &= 5 + 1 + \sum_{x=0}^{4} \left(\frac{x^3 + x + 1}{5} \right) \\
&= 6 + \left(\frac{1}{5}\right) + \left(\frac{3}{5}\right) + \left(\frac{1}{5}\right) + \left(\frac{1}{5}\right) + \left(\frac{4}{5}\right) \\
&= 6 + 1 - 1 + 1 + 1 + 1 = 9.
\end{aligned}$$

□

When using Theorem 4.14, it is possible to compute each individual generalized Legendre symbol quickly (see Exercise 4.4), but it is more efficient to square all the elements of $\mathbf{F}_q^\times$ and store the list of squares. For simplicity, consider the case of $\mathbf{F}_p$. Make a vector with p entries, one for each element of $\mathbf{F}_p$. Initially, all entries in the vector are set equal to -1. For each j with $1 \le j \le (p-1)/2$, square j and reduce to get $k \mod p$. Change the kth entry in the vector to $+1$. Finally, change the 0th entry in the vector to 0. The resulting vector will be a list of the values of the Legendre symbol.

Theorem 4.14, which is sometimes known as the Lang-Trotter method, works quickly for small values of q, perhaps $q < 100$, but is slow for larger q, and is impossible to use when q is around 10^{100} or larger.

4.3.3 Orders of Points

Let $P \in E(\mathbf{F}_q)$. The **order** of P is the smallest positive integer k such that $kP = \infty$. A fundamental result from group theory (a corollary of Lagrange's theorem) is that the order of a point always divides the order of the group $E(\mathbf{F}_q)$. Also, for an integer n, we have $nP = \infty$ if and only if the order of P divides n. By Hasse's theorem, $\#E(\mathbf{F}_q)$ lies in an interval of length $4\sqrt{q}$. Therefore, if we can find a point of order greater than $4\sqrt{q}$, there can be only one multiple of this order in the correct interval, and it must be $\#E(\mathbf{F}_q)$. Even if the order of the point is smaller than $4\sqrt{q}$, we obtain a small list of possibilities for $\#E(\mathbf{F}_q)$. Using a few more points often shortens the list enough that there is a unique possibility for $\#E(\mathbf{F}_q)$. For an addiitonal trick that helps in this situation, see Proposition 4.18.

How do we find the order of a point? If we know the order of the full group of points, then we can look at factors of this order. But, at present, the order of the group is what we're trying to find. In Section 4.3.4, we'll discuss a method (Baby Step, Giant Step) for finding the order of a point.

Example 4.6

Let E be the curve $y^2 = x^3 + 7x + 1$ over $\mathbf{F}_{101}$. It is possible to show that the point $(0, 1)$ has order 116, so $N_{101} = \#E(\mathbf{F}_{101})$ is a multiple of 116. Hasse's theorem says that

$$101 + 1 - 2\sqrt{101} \leq N_{101} \leq 101 + 1 + 2\sqrt{101},$$

which means that $82 \leq N_{101} \leq 122$. The only multiple of 116 in this range is 116, so $N_{101} = 116$. As a corollary, we find that the group of points is cyclic of order 116, generated by (0,1). □

Example 4.7

Let E be the elliptic curve $y^2 = x^3 - 10x + 21$ over $\mathbf{F}_{557}$. The point $(2, 3)$ can be shown to have order 189. Hasse's theorem implies that $511 \leq N_{557} \leq 605$. The only multiple of 189 in this range is $3 \cdot 189 = 567$. Therefore $N_{557} = 567$. □

Example 4.8

Let E be the elliptic curve $y^2 = x^3 + 7x + 12$ over $\mathbf{F}_{103}$. The point $(-1, 2)$ has order 13 and the point $(19, 0)$ has order 2. Therefore the order N_{103} of $E(\mathbf{F}_{103})$ is a multiple of 26. Hasse's theorem implies that $84 \leq N_{103} \leq 124$. The only multiple of 26 in that range is 104, so $N_{103} = 104$. □

Example 4.9

Let E be the elliptic curve $y^2 = x^3 + 2$ over $\mathbf{F}_7$, as in Example 4.2. The group of points $E(\mathbf{F}_7)$ is isomorphic to $\mathbf{Z}_3 \oplus \mathbf{Z}_3$. Every point, except ∞, has order 3, so the best we can conclude with the present method is that the order N_7 of the group is a multiple of 3. Hasse's theorem says that $3 \leq N_7 \leq 13$, so the order is 3, 6, 9, or 12. Of course, if we find two independent points of order 3 (that is, one is not a multiple of the other), then they generate a subgroup of order 9. This means that the order of the full group is a multiple of 9, hence is 9. □

The situation of the last example, where $E(\mathbf{F}_q) \simeq \mathbf{Z}_n \oplus \mathbf{Z}_n$, makes it more difficult to find the order of the group of points, but is fairly rare, as the next result shows.

PROPOSITION 4.16

Let E be an elliptic curve over $\mathbf{F}_q$ and suppose

$$E(\mathbf{F}_q) \simeq \mathbf{Z}_n \oplus \mathbf{Z}_n$$

for some integer n. Then either $q = n^2 + 1$ or $q = n^2 \pm n + 1$ or $q = (n \pm 1)^2$.

PROOF By Hasse's theorem, $n^2 = q + 1 - a$, with $|a| \le 2\sqrt{q}$. To prove the proposition, we use the following lemma, which puts a severe restriction on a.

LEMMA 4.17
$a \equiv 2 \pmod{n}$.

PROOF Let p be the characteristic of $\mathbf{F}_q$. Then $p \nmid n$; otherwise, there would be p^2 points in $E[p]$, which is impossible in characteristic p by Theorem 3.2.

Since $E[n] \subseteq E(\mathbf{F}_q)$, Corollary 3.11 implies that the nth roots of unity are in $\mathbf{F}_q$, so $q - 1$ must be a multiple of n (see Appendix C). Therefore, $a = q + 1 - n^2 \equiv 2 \pmod{n}$. ▮

Write $a = 2 + kn$ for some integer k. Then

$$n^2 = q + 1 - a = q - 1 - kn, \quad \text{so} \quad q = n^2 + kn + 1.$$

By Hasse's theorem,

$$|2 + kn| \le 2\sqrt{q}.$$

Squaring this last inequality yields

$$4 + 4kn + k^2n^2 \le 4q = 4(n^2 + kn + 1).$$

Therefore, $|k| \le 2$. The possibilities $k = 0, \pm 1, \pm 2$ give the values of q listed in the proposition. This completes the proof of Proposition 4.16. ▮

Most values of q are not of the form given in the proposition, and even for such q most elliptic curves do not have $E(\mathbf{F}_q) \simeq \mathbf{Z}_n \oplus \mathbf{Z}_n$ (only a small fraction have order n^2), so we can regard $\mathbf{Z}_n \oplus \mathbf{Z}_n$ as rare.

More generally, most q are such that all elliptic curves over $\mathbf{F}_q$ have points of order greater than $4\sqrt{q}$ (Exercise 4.6). Therefore, with a little luck, we can usually find points with orders that allow us to determine $\#E(\mathbf{F}_q)$.

The following result of Mestre shows that for E defined over $\mathbf{F}_p$, there is a point of sufficiently high order on either E or its quadratic twist. The quadratic twist of E is defined as follows. Let $d \in \mathbf{F}_p^\times$ be a quadratic nonresidue mod p. If E has equation $y^2 = x^3 + Ax + B$, then the quadratic twist E' has the equation $y^2 = x^3 + Ad^2x + Bd^3$ (see Exercise 2.23). By Exercise 4.10, if $\#E(\mathbf{F}_p) = p + 1 - a$ then E' has $p + 1 + a$ points. Once we know the order of one of these two groups, we know a and therefore know the order of both groups.

PROPOSITION 4.18

Let $p > 229$ be prime and let E be an elliptic curve over $\mathbf{F}_p$. Either E or its quadratic twist E' has a point P whose order has only one multiple in the interval $\left(p+1-2\sqrt{p},\, p+1+2\sqrt{p}\right)$.

PROOF Let

$$E(\mathbf{F}_p) \simeq \mathbf{Z}_m \oplus \mathbf{Z}_M, \quad E'(\mathbf{F}_p) \simeq \mathbf{Z}_n \oplus \mathbf{Z}_N,$$

with $m|M$ and $n|N$. If $mM = \#E(\mathbf{F}_p) = p+1-a$, then $nN = \#E'(\mathbf{F}_p) = p+1+a$. Since $m|M$ and $n|N$, we have $m^2|p+1-a$ and $n^2|p+1+a$. Therefore, $\gcd(m^2,n^2)|2a$.

Since $E[m] \subseteq E(\mathbf{F}_p)$, then $\mu_m \subseteq \mathbf{F}_p^\times$ by Corollary 3.11, so $p \equiv 1 \pmod{m}$. Therefore, $2-a \equiv p+1-a \equiv 0 \pmod{m}$. Similarly, $2+a \equiv 0 \pmod{n}$. Therefore, $\gcd(m,n)|(2-a)+(2+a)=4$, and $\gcd(m^2,n^2)|16$.

If $4|m$ and $4|n$, then $16|\gcd(m^2,n^2)$, which divides $2a$. Then $8|a$, which is impossible since then $2-a \equiv 0 \pmod{m}$ implies $2-0 \equiv 0 \pmod{4}$. Therefore, $\gcd(m^2,n^2)|4$. This implies that the least common multiple of m^2 and n^2 is a multiple of $m^2n^2/4$.

Let ϕ be the pth power Frobenius endomorphism for E. Since $E[n] \subseteq E(\mathbf{F}_p)$, it follows that ϕ acts trivially on $E[n]$. Choose a basis for $E[n^2]$. The action of ϕ on $E[n^2]$ is given by a matrix of the form

$$\begin{pmatrix} 1+sn & tn \\ un & 1+vn \end{pmatrix}.$$

By Proposition 4.11, we have $a \equiv 2+(s+v)n \pmod{n^2}$ and $p \equiv 1+(s+v)n \pmod{n^2}$. Therefore, $4p-a^2 \equiv 0 \pmod{n^2}$. Similarly, $4p-a^2 \equiv 0 \pmod{m^2}$.

It follows that the least common multiple of m^2 and n^2 divides $4p-a^2$, so

$$\frac{m^2n^2}{4} \le 4p-a^2.$$

Suppose that both M and N are less than $4\sqrt{p}$. Then, since $a^2 < 4p$,

$$\begin{aligned}(p-1)^2 < (p+1)^2 - a^2 &= (p+1-a)(p+1+a) = mMnN \\ &< \left(4(4p-a^2)\right)^{1/2}(4\sqrt{p})^2 \le 64p^{3/2}.\end{aligned}$$

A straightforward calculation shows that this implies that $p < 4100$. We have therefore shown that if $p > 4100$, then either M or N must be greater than $4\sqrt{p}$. This means that either E or E' has a point of order greater than $4\sqrt{p}$. Therefore, there can be at most one multiple of this order in the interval $\left(p+1-2\sqrt{p}, p+1+2\sqrt{p}\right)$. This proves the theorem for $p > 4100$.

Suppose now that $457 < p < 4100$. A straightforward computation shows that there are no integers a, m, n with $|a| < 2\sqrt{p}$ such that

1. $m^2 | p+1-a$
2. $n^2 | p+1+a$
3. $(p+1-a)/m < 4\sqrt{p}$
4. $(p+1+a)/n < 4\sqrt{p}$.

Therefore, the theorem is true for $p > 457$.

For $p = 457$, we may take $a = 10$, $m = 8$, $n = 6$, which correspond to the groups $\mathbf{Z}_8 \oplus \mathbf{Z}_{56}$ and $\mathbf{Z}_6 \oplus \mathbf{Z}_{78}$ (and can be realized by the curves $E : y^2 = x^3 - 125$ and its quadratic twist $E' : y^2 = x^3 - 1$). Note, however, that the only multiple of 56 in the interval $\left(457 + 1 - 2\sqrt{457},\ 457 + 1 + 2\sqrt{457}\right) = (415.2,\ 500.8)$ is 448, which is the order of $E(\mathbf{F}_{457})$. Similarly, the only multiple of 78 in this interval is 468, which is the order of $E'(\mathbf{F}_{457})$. Therefore, the theorem still holds in this case.

In fact, the search for a, m, n can be extended in this way to $229 < p \leq 457$, with conditions (3) and (4) replaced by

3'. there is more than one multiple of $(p+1-a)/m$ in the interval $\left(p+1-2\sqrt{p},\ p+1+2\sqrt{p}\right)$

4'. there is more than one multiple of $(p+1+a)/m$ in the interval $\left(p+1-2\sqrt{p},\ p+1+2\sqrt{p}\right)$.

No values of a, m, n exist satisfying these conditions, so the theorem holds. ▮

Example 4.10

The theorem is false for $p = 229$. Consider the curve $E : y^2 = x^3 - 1$. A calculation shows that $E(\mathbf{F}_{229}) \simeq \mathbf{Z}_6 \oplus \mathbf{Z}_{42}$. Therefore, $42P = \infty$ for all $P \in E(\mathbf{F}_{229})$. The Hasse bound says that $200 \leq \#E(\mathbf{F}_{229}) \leq 260$, so the existence of a point of order 42 allows both the values 210 and 252. Since 2 is a quadratic nonresidue mod 229, the curve $E' : y^2 = x^3 - 8$ is the quadratic twist of E. A calculation shows that $E'(\mathbf{F}_{229}) \simeq \mathbf{Z}_4 \oplus \mathbf{Z}_{52}$. Therefore, $52P = \infty$ for all $P \in E'(\mathbf{F}_{229})$. The existence of a point of order 52 allows both the values 208 and 260. Therefore, neither E nor its quadratic twist E' has a point whose order has only one multiple in the Hasse interval. □

Suppose $E(\mathbf{F}_q) \simeq \mathbf{Z}_{n_1} \oplus \mathbf{Z}_{n_2}$ with $n_1 | n_2$. Then the order of every element divides n_2. If we choose some random points and compute their orders, what is the chance that the least common multiple of these orders is n_2? Let P_1, P_2 be points of orders n_1, n_2 such that every $P \in E(\mathbf{F}_q)$ is uniquely expressible in the form $P = a_1 P_1 + a_2 P_2$ with $0 \leq a_i < n_i$. Let p be a prime dividing n_2. If we take a random point P, then the probability is $1 - 1/p$ that $p \nmid a_2$. If $p \nmid a_2$, then the order of P contains the highest power of p possible. If p is large, then this means that it is very likely that the order of one randomly chosen point will contribute the correct power of p to the least common multiple of the orders of the points. If p is small, say $p = 2$, then the probability is at least 1/2. This means that if we choose several randomly chosen points, the least common multiples of their orders should still have the correct power of p. The conclusion is that if we choose several random points and compute the least common multiple of their orders, it is very likely that we will obtain n_2, which is as large as possible.

The following result of Cremona and Harley shows that knowledge of n_2 usually determines the group structure.

PROPOSITION 4.19

Let E be an elliptic curve over $\mathbf{F}_q$. Write $E(\mathbf{F}_q) \simeq \mathbf{Z}_{n_1} \oplus \mathbf{Z}_{n_2}$ with $n_1|n_2$. Suppose that q is not one of the following:

$$3, 4, 5, 7, 9, 11, 13, 17, 19, 23, 25, 27, 29, 31, 37,$$
$$43, 61, 73, 181, 331, 547.$$

Then n_2 uniquely determines n_1.

PROOF Fix q and suppose there exist n_2, x, y (regard x, y as two possible values of n_1) with

1. $x, y|n_2$
2. $\left(\sqrt{q}-1\right)^2 \le n_2x < n_2y \le \left(\sqrt{q}+1\right)^2$

(so the groups of order n_2x and n_2y satisfy the bounds in Hasse's theorem). Our first goal is to show that if n_2, x, y satisfying (1) and (2) exist then $q \le 4612$.

Let $d = \gcd(x, y)$. Then $n_2' = dn_2, x' = x/d, y' = y/d$ also satisfy (1), (2). So we may assume that $\gcd(x, y) = 1$. Since $n_2y - n_2x > 0$,

$$n_2 \le n_2y - n_2x \le \left(\sqrt{q}+1\right)^2 - \left(\sqrt{q}-1\right)^2 = 4\sqrt{q}.$$

Since $x, y|n_2$, we have $xy|n_2$, hence $xy \le n_2$. Therefore,

$$x^2 \le xy \le n_2 \le 4\sqrt{q},$$

which implies that

$$\left(\sqrt{q}-1\right)^2 \le n_2x \le \left(4\sqrt{q}\right)\left(4\sqrt{q}\right)^{1/2}.$$

But $\left(\sqrt{q}-1\right)^2 > 8q^{3/4}$ when $q \ge 4613$. Therefore, we must have $q \le 4612$.

The values of $q \le 4612$ can be checked on a computer to get a much smaller list of possibilities for q. However, we can speed up the search with the following observations.

First, $\left(\sqrt{q}-1\right)^2 \le n_2 x \le 4\sqrt{q}x$ implies that $x > \left(\sqrt{q}-2\right)/4$. Second, $y^2 \le n_2 y \le \left(\sqrt{q}+1\right)^2$. Third, $xy^2 = (xy)y \le n_2 y \le \left(\sqrt{q}+1\right)^2$. Finally, $n_1 | q-1$ (by Corollary 3.11), so $x, y | q-1$.

Therefore, we should look for values of $q \le 4612$ that are primes or prime powers and such that $q-1$ has divisors x, y with

1. $\gcd(x, y) = 1$
2. $\left(\sqrt{q}-2\right)/4 < x < y \le \sqrt{q}+1$
3. $xy^2 \le \left(\sqrt{q}+1\right)^2$.

The values of q for which such x, y exist are those on the list in the statement of the theorem, plus the five values $q = 49, 81, 121, 169, 841$. Therefore, for all other q, a number n_2 cannot have two possible values x, y for n_1, so n_1 is uniquely determined.

We need to eliminate the remaining five values. For example, consider $q = 49$. One solution is $x = 2, y = 3, n_2 = 18$, which corresponds to $\#E(\mathbf{F}_q) = 36$ and 54. By Theorem 4.4, or by Exercise 4.14, if $\#E(\mathbf{F}_q) = \left(\sqrt{q}-1\right)^2$, then $E(\mathbf{F}_q) \simeq \mathbf{Z}_{\sqrt{q}-1} \oplus \mathbf{Z}_{\sqrt{q}-1}$. Therefore, if $\#E(\mathbf{F}_{49}) = 36$, we must have $n_1 = n_2 = 6$. This arises from $x = 2$ after multiplying by 3 (recall that we removed $d = \gcd(x, y)$ from x, y in order to make them relatively prime). Multiplying $y = 3$ by $d = 3$ yields $n_1 = 9, n_2 = 6$, which does not satisfy $n_1 | n_2$. Therefore, the solution $x = 2, y = 3$ for $q = 49$ is eliminated. Similarly, all solutions for all of the five values $q = 49, 81, 121, 169, 841$ can be eliminated. This completes the proof. ∎

.

4.3.4 Baby Step, Giant Step

Let $P \in E(\mathbf{F}_q)$. We want to find the order of P. First, we want to find an integer k such that $kP = \infty$. Let $\#E(\mathbf{F}_q) = N$. By Lagrange's theorem, $NP = \infty$. Of course, we might not know N yet, but we know that $q+1-2\sqrt{q} \le N \le q+1+2\sqrt{q}$. We could try all values of N in this range and see which ones satisfy $NP = \infty$. This takes around $4\sqrt{q}$ steps. However, it is possible to speed this up to around $4q^{1/4}$ steps by the following algorithm.

1. Compute $Q = (q+1)P$.
2. Choose an integer m with $m > q^{1/4}$. Compute and store the points jP for $j = 0, 1, 2, \ldots, m$.
3. Compute the points

$$Q + k(2mP) \text{ for } k = -m, -(m-1), \ldots, m$$

until there is a match $Q + k(2mP) = \pm jP$ with a point (or its negative) on the stored list.

4. Conclude that $(q + 1 + 2mk \mp j)P = \infty$. Let $M = q + 1 + 2mk \mp j$.
5. Factor M. Let $p_1, \ldots, p_r$ be the distinct prime factors of M.
6. Compute $(M/p_i)P$ for $i = 1, \ldots, r$. If $(M/p_i)P = \infty$ for some i, replace M with M/p_i and go back to step (5). If $(M/p_i)P \neq \infty$ for all i then M is the order of the point P.
7. If we are looking for the $\#E(\mathbf{F}_q)$, then repeat steps (1)-(6) with randomly chosen points in $E(\mathbf{F}_q)$ until the least common multiple of the orders divides only one integer N with $q+1-2\sqrt{q} \leq N \leq q+1+2\sqrt{q}$. Then $N = \#E(\mathbf{F}_q)$.

There are two points that must be addressed.

I. Assuming that there is a match, this method clearly produces an integer that annihilates P. But why is there a match?

LEMMA 4.20

Let a be an integer with $|a| \leq 2m^2$. There exist integers a_0 and a_1 with $-m < a_0 \leq m$ and $-m \leq a_1 \leq m$ such that

$$a = a_0 + 2ma_1.$$

PROOF Let $a_0 \equiv a \pmod{2m}$, with $-m < a_0 \leq m$ and $a_1 = (a - a_0)/2m$. Then

$$|a_1| \leq (2m^2 + m)/2m < m + 1.$$

▮

Let $a = a_0 + 2ma_1$ be as in the lemma and let $k = -a_1$. Then

$$\begin{aligned} Q + k(2mP) &= (q + 1 - 2ma_1)P \\ = (q + 1 - a + a_0)P &= NP + a_0P \\ &= a_0P = \pm jP, \end{aligned}$$

where $j = |a_0|$. Therefore, there is a match.

II. Why does step (6) yield the order of P?

LEMMA 4.21

Let G be an additive group (with identity element 0) and let $g \in G$. Suppose $Mg = 0$ for some positive integer M. Let $p_1, \ldots, p_r$ be the distinct primes dividing M. If $(M/p_i)g \neq 0$ for all i, then M is the order of g.

PROOF Let k be the order of g. Then $k|M$. Suppose $k \neq M$. Let p_i be a prime dividing M/k. Then $p_i k|M$, so $k|(M/p_i)$. Therefore, $(M/p_i)g = 0$, contrary to assumption. Therefore $k = M$. ▮

Therefore, step (6) finds the order of P.

REMARK 4.22 (1) To save storage space, it might be more efficient to store only the x coordinates of the points jP (along with the corresponding integer j), since looking for a match with $\pm jP$ only requires the x-coordinate (assuming we are working with a Weierstrass equation). When a match is found, the two possible y-coordinates can be recomputed.

(2) Computing $Q + k(2mP)$ can be done by computing Q and $2mP$ once for all. To get from $Q+k(2mP)$ to $Q+(k+1)(2mP)$, simply add $2mP$ rather than recomputing everything. Similarly, once jP has been computed, add P to get $(j+1)P$.

(3) We are assuming that we can factor M. If not, we can at least find all the small prime factors p_i and check that $(M/p_i)P \neq \infty$ for these. Then M will be a good candidate for the order of P.

(4) Why is the method called "Baby Step, Giant Step"? The **baby steps** are from a point jP to $(j+1)P$. The **giant steps** are from a point $k(2mP)$ to $(k+1)(2mP)$, since we take the "bigger" step $2mP$. ▮

Example 4.11

Let E be the elliptic curve $y^2 = x^3 - 10x + 21$ over $\mathbf{F}_{557}$, as in Example 4.7. Let $P = (2, 3)$. We follow the procedure above.

1. $Q = 558P = (418, 33)$.

2. Let $m = 5$, which is greater than $557^{1/4}$. The list of jP is

$$\infty,\ (2,3),\ (58,164),\ (44,294),\ (56,339),\ (132,364).$$

3. When $k = 1$, we have $Q + k(2mP) = (2, 3)$, which matches the point on our list for $j = 1$.

4. We have $(q + 1 + 2mk - j)P = 567P = \infty$.

5. Factor $567 = 3^4 \cdot 7$. Compute $(567/3)P = 189P = \infty$. We now have 189 as a candidate for the order of P.

6. Factor $189 = 3^3 7$. Compute $(189/3)P = (38, 535) \neq \infty$ and $(189/7)P = (136, 360) \neq \infty$. Therefore 189 is the order of P.

As pointed out in Example 4.7, this suffices to determine that $\#E(\mathbf{F}_{557}) = 567$. □

4.4 A Family of Curves

In this section we give an explicit formula for the number of points in $E(\mathbf{F}_p)$, where E is the elliptic curve

$$y^2 = x^3 - kx,$$

and $k \not\equiv 0 \pmod{p}$. Counting the points on this curve mod a prime p has a long history, going back at least to Gauss.

THEOREM 4.23
Let p be an odd prime and let $k \not\equiv 0 \pmod{p}$. Let $N_p = \#E(\mathbf{F}_p)$, where E is the elliptic curve

$$y^2 = x^3 - kx.$$

1. *If $p \equiv 3 \pmod{4}$, then $N_p = p + 1$.*
2. *If $p \equiv 1 \pmod{4}$, write $p = a^2 + b^2$, where a, b are integers with b even and $a + b \equiv 1 \pmod{4}$. Then*

$$N_p = \begin{cases} p + 1 - 2a & \textit{if } k \textit{ is a fourth power mod } p \\ p + 1 + 2a & \textit{if } k \textit{ is a square mod } p \textit{ but not a 4th power mod } p \\ p + 1 \pm 2b & \textit{if } k \textit{ is not a square mod } p. \end{cases}$$

The proof of the theorem will take the rest of this section.

The integer a is uniquely determined by the conditions in the theorem, and b is uniquely determined up to sign. When k is not a square mod p, the proof below does not determine the sign of b. This is a much more delicate problem and we omit it.

Example 4.12
Let $p = 61 = (-5)^2 + 6^2$, where we chose the negative sign on 5 so that $-5 + 6 \equiv 1 \pmod{4}$. Since $k = 1$ is a fourth power, the number of points on $y^2 = x^3 - x$ is $p + 1 - 2(-5) = 72$. □

It is well known that every prime $p \equiv 1 \pmod{4}$ is a sum of two squares (this follows from Proposition 4.27 below). The next lemma shows that a and b are uniquely determined up to order and sign.

LEMMA 4.24
Suppose p is prime and a, b, c, d are integers such that $a^2 + b^2 = p = c^2 + d^2$. Then $a = \pm c$ and $b = \pm d$, or $a = \pm d$ and $b = \pm c$.

PROOF We have $(a/b)^2+1 \equiv 0 \equiv (c/d)^2+1 \pmod p$, so $a/b \equiv \pm(c/d)$. By changing the sign of c if necessary, we may assume that $a/b \equiv c/d \pmod p$, hence $ad - bc \equiv 0 \pmod p$. A quick calculation shows that

$$p^2 = (ac + bd)^2 + (bc - ad)^2. \tag{4.2}$$

Suppose $ad = bc$. Then (4.2) implies that $ac + bd = \pm p$, so

$$\pm ap = a^2c + abd = a^2c + b^2c = pc.$$

Hence, $\pm a = c$. It follows that $b = \pm d$.

Now suppose $ad \neq bc$. Since $ad - bc \equiv 0 \pmod p$, we have $(ad - bc)^2 \geq p^2$. Since $(ac + bd)^2 \geq 0$, it follows from (4.2) that $ad - bc = \pm p$ and $ac + bd = 0$. Therefore,

$$\pm cp = acd - bc^2 = -bd^2 - bc^2 = -bp,$$

so $c = \pm b$. This implies that $d = \pm a$. ∎

If we require that a is odd and b is even, then a and b are uniquely determined up to sign. Suppose $b \equiv 2 \pmod 4$. Then $a + b \equiv 1 \pmod 4$ for a unique choice of the sign of a. Similarly, if $b \equiv 0 \pmod 4$, there is a unique choice of the sign of a that makes $a + b \equiv 1 \pmod 4$. Therefore, the integer a in the lemma is uniquely determined by p if we require that a is odd and $a + b \equiv 1 \pmod 4$.

The main part of the proof of Theorem 4.23 involves the case $p \equiv 1 \pmod 4$, so let's treat the case $p \equiv 3 \pmod 4$ first. The main point is that -1 is not a square mod p (*Proof:* if $x^2 \equiv -1$, then $1 \equiv x^{p-1} \equiv (x^2)^{(p-1)/2} \equiv (-1)^{(p-1)/2} \equiv (-1)^{\text{odd}} = -1$, contradiction). Moreover, a nonsquare times a nonsquare is a square mod p. Therefore $x^3 - kx$ is a nonzero square mod p if and only if $(-x)^3 - k(-x) = -(x^3 - kx)$ is not a square mod p. Let's count points on E. Whenever $x^3 - kx = 0$, we obtain one point $(x, 0)$. For the remaining values of x, we pair up x and $-x$. One of these gives two points (the one that makes $x^3 - kx$ a square) and the other gives no points. Therefore, each pair $x, -x$ gives two points. Therefore, we obtain a total of p points. The point ∞ gives one more, so we have $p + 1$ points.

Now assume $p \equiv 1 \pmod 4$. The proof, which takes the rest of this section, involves several steps and counts the points in terms of Jacobi sums. Rather than count the points on E directly, we make the transformation (see Theorem 2.17)

$$x = \frac{2(v+1)}{u^2}, \quad y = \frac{4(v+1)}{u^3},$$

which changes E into the curve C given by

$$v^2 = (k/4)u^4 + 1.$$

The inverse transformation is

$$u = \frac{2x}{y}, \quad v = -1 + \frac{2x^3}{y^2}.$$

We'll count the points on C mod p.

First, there are a few special points for the transformation from E to C. The point ∞ on E corresponds to $(0, 1)$ on C. The point $(0, 0)$ on E corresponds to $(0, -1)$ on C (see Theorem 2.17). If k is a square mod p, then the two 2-torsion points $(\pm\sqrt{k}, 0)$ correspond to the point at infinity on C. Therefore,

$$\#E(\mathbf{F}_p) = \#\{(u, v) \in \mathbf{F}_p \times \mathbf{F}_p \,|\, v^2 = (k/4)u^4 + 1\} + \delta,$$

where

$$\delta = \begin{cases} 2 & \text{if } k \text{ is a square mod } p \\ 0 & \text{if not.} \end{cases}$$

Let g be a primitive root mod p, which means that

$$\mathbf{F}_p^\times = \{g^j \,|\, 0 \le j < p - 1\}.$$

Let $i = \sqrt{-1} \in \mathbf{C}$. Define

$$\chi_2(g^j) = (-1)^j \quad \text{and} \quad \chi_4(g^j) = i^j.$$

Then χ_2 and χ_4 can be regarded as homomorphisms from $\mathbf{F}_p^\times$ to $\{\pm 1, \pm i\}$. Note that $\chi_4^2 = \chi_2$. The following lemma gets us started.

LEMMA 4.25

Let $p \equiv 1 \pmod 4$ be prime and let $x \in \mathbf{F}_p^\times$. Then

$$\#\{u \in \mathbf{F}_p^\times \,|\, u^2 = x\} = \sum_{\ell=0}^{1} \chi_2(x)^\ell,$$

and

$$\#\{u \in \mathbf{F}_p^\times \,|\, u^4 = x\} = \sum_{\ell=0}^{3} \chi_4(x)^\ell.$$

PROOF Since $p \equiv 1 \pmod 4$, there are 4 fourth roots of 1 in $\mathbf{F}_p^\times$. Therefore, if there is a solution to $u^4 \equiv x$, there are 4 solutions. Write $x \equiv g^j \pmod p$. Then x is a fourth power mod p if and only if $j \equiv 0 \pmod 4$. We have

$$\sum_{\ell=0}^{3} \chi_4(x)^\ell = \sum_{\ell=0}^{3} i^{j\ell} = \begin{cases} 4 \text{ if } j \equiv 0 & \pmod 4 \\ 0 \text{ if } j \not\equiv 0 & \pmod 4, \end{cases}$$

which is exactly the number of u with $u^4 \equiv x$. This proves the second half of the lemma. The proof of the first half is similar. ▮

If, instead, we sum over the elements of $\mathbf{F}_p^\times$, we have the following result.

LEMMA 4.26

Let $p \equiv 1 \pmod 4$ *be prime. Then*

$$\sum_{b \in \mathbf{F}_p^\times} \chi_4(b)^\ell = \begin{cases} p-1 & \text{if} \quad \ell \equiv 0 \pmod 4 \\ 0 & \text{if} \quad \ell \not\equiv 0 \pmod 4. \end{cases}$$

PROOF If $\ell \equiv 0 \pmod 4$, all the terms in the sum are 1, so the sum is $p-1$. If $\ell \not\equiv 0 \pmod 4$, then $\chi_4(g)^\ell \neq 1$. Multiplying by g permutes the elements of $\mathbf{F}_p^\times$, so

$$\chi_4(g)^\ell \sum_{b \in \mathbf{F}_p^\times} \chi_4(b)^\ell = \sum_{b \in \mathbf{F}_p^\times} \chi_4(gb)^\ell = \sum_{c \in \mathbf{F}_p^\times} \chi_4(c)^\ell,$$

which is the original sum. Since $\chi_4(g)^\ell \neq 1$, the sum must be 0. ▮

Define the **Jacobi sums** by

$$J(\chi_2^j, \chi_4^\ell) = \sum_{\substack{a \in \mathbf{F}_p^\times \\ a \neq 1}} \chi_2(a)^j \chi_4(1-a)^\ell.$$

PROPOSITION 4.27

$J(\chi_2, \chi_4^2) = -1$ *and* $|J(\chi_2, \chi_4)|^2 = p$.

PROOF The first equality is proved as follows.

$$J(\chi_2, \chi_4^2) = \sum_{\substack{a \in \mathbf{F}_p^\times \\ a \neq 1}} \chi_2(a)\chi_4(1-a)^2 = \sum_{a \neq 0,1} \chi_2(a)\chi_2(1-a),$$

since $\chi_4^2 = \chi_2$. Since $\chi_2(a) = \pm 1$, we have $\chi_2(a) = \chi_2(a)^{-1}$ so the sum equals

$$\sum_{a \neq 0,1} \chi_2(a)^{-1}\chi_2(1-a) = \sum_{a \neq 0,1} \chi_2\left(\frac{1-a}{a}\right).$$

The map $x \mapsto 1 - \frac{1}{x}$ gives a permutation of the set of $x \in \mathbf{F}_p$, $x \neq 0, 1$. Therefore, letting $c = 1 - 1/a$, we obtain

$$\sum_{a \neq 0,1} \chi_2\left(\frac{1}{a} - 1\right) = \sum_{c \neq 0,1} \chi_2(-c) = -\chi_2(-1),$$

by Lemma 4.26. Since $g^{(p-1)/2} \equiv -1 \pmod p$ (both have order 2 in the cyclic group $\mathbf{F}_p^\times$), we have

$$1 = (\pm 1)^2 = \chi_2(g^{(p-1)/4})^2 = \chi_2(g^{(p-1)/2}) = \chi_2(-1).$$

This yields the first equality of the proposition.

To prove the second equality, multiply the Jacobi sum by its complex conjugate to obtain

$$\begin{aligned}|J(\chi_2,\chi_4)|^2 &= \sum_{a\neq 0,1}\chi_2(a)\chi_4(1-a)\overline{\sum_{b\neq 0,1}\chi_2(b)\chi_4(1-b)}\\ &= \sum_{a\neq 0,1}\sum_{b\neq 0,1}\chi_2\left(\frac{a}{b}\right)\chi_4\left(\frac{1-a}{1-b}\right).\end{aligned}$$

We have used the fact that $\overline{\chi_4(x)} = \chi_4(x)^{-1}$. We now need the following.

LEMMA 4.28

Let $S = \{(x,y)\,|\,x,y\in \mathbf{F}_p^\times;\ x,y\neq 1;\ x\neq y\}$. The map

$$\sigma : (x,y) \mapsto \left(\frac{x}{y}, \frac{1-x}{1-y}\right)$$

is a permutation of S.

PROOF Let $c = x/y$ and $d = (1-x)/(1-y)$. Then $x\neq 0$ yields $c\neq 0$ and $x\neq 1$ yields $d\neq 0$. The assumption that $x\neq y$ yields $c,d\neq 1$ and $c\neq d$. Therefore, $(c,d)\in S$.

To show that σ is surjective, let $c,d\in S$. Let

$$x = c\frac{d-1}{d-c}, \quad y = \frac{d-1}{d-c}.$$

It is easily verified that $(c,d)\in S$ implies $(x,y)\in S$ and that $\sigma(x,y) = (c,d)$. ∎

Returning to the proof of the proposition, we find that

$$\begin{aligned}|J(\chi_2,\chi_4)|^2 &= \sum_{a=b}\chi_2\left(\frac{a}{b}\right)\chi_4\left(\frac{1-a}{1-b}\right) + \sum_{(a,b)\in S}\chi_2\left(\frac{a}{b}\right)\chi_4\left(\frac{1-a}{1-b}\right)\\ &= (p-2) + \sum_{(c,d)\in S}\chi_2(c)\chi_4(d)\\ &= (p-2) + \sum_{d\neq 0,1}\chi_4(d)\left(\sum_{c\in\mathbf{F}_p^\times}\chi_2(c) - \chi_2(1) - \chi_2(d)\right)\\ &= (p-2) + \sum_{d\neq 0,1}\chi_4(d)(0-1-\chi_4(d)^2)\\ &= (p-2) - \sum_{d\neq 0,1}\chi_4(d) - \sum_{d\neq 0,1}\chi_4(d)^3\\ &= (p-2) + \chi_4(1) + \chi_4(1)^3 = p.\end{aligned}$$

This completes the proof of the second equality of Proposition 4.27. ∎

We now show that the number of points on $v^2 = (k/4)u^4 + 1$ can be expressed in terms of Jacobi sums. By separating out the terms with $u = 0$ and the terms with $v = 0$, we obtain that the number of points is

$$\#\{v \,|\, v^2 = 1\} + \#\{u \,|\, u^4 = -4/k\}$$

$$+ \sum_{\substack{a+b=1\\ a,b\neq 0}} \#\{v \,|\, v^2 = a\} \, \#\{u \,|\, u^4 = -4b/k\}$$

$$\begin{aligned} &= \sum_{j=0}^{1} \chi_2(1)^j + \sum_{\ell=0}^{3} \chi_4(-4/k)^\ell + \sum_{\substack{a+b=1\\ a,b\neq 0}} \sum_{j=0}^{1} \chi_2(a)^j \sum_{\ell=0}^{3} \chi_4(-4b/k)^\ell \\ &= \sum_{j=0}^{1} \chi_2(1)^j + \sum_{\ell=0}^{3} \chi_4(-4/k)^\ell + \sum_{b\neq 0,1} \sum_{\ell=0}^{3} \chi_4(-4b/k)^\ell \\ &\quad + \sum_{a\neq 0,1} \sum_{j=0}^{1} \chi_2(a)^j \,-\, (p-2) \\ &\quad + \chi_4(-4/k)^2 J(\chi_2, \chi_4^2) + \chi_4(-4/k) J(\chi_2, \chi_4) + \chi_4(-4/k)^3 J(\chi_2, \chi_4^3) \end{aligned}$$

(Separate out the terms with $j = 0$ and $\ell = 0$. These yield the sums over ℓ and over j, respectively. The terms with $j = \ell = 0$, which sum to $p - 2$, are counted twice, so subtract $p - 2$. The terms with $j, \ell \neq 0$ contribute to the Jacobi sums.)

$$\begin{aligned} &= \sum_{j=0}^{1} \sum_{a\neq 0} \chi_2(a)^j + \sum_{\ell=0}^{3} \sum_{b\neq 0} \chi_4(-4b/k)^\ell \,-\, (p-2) \\ &\quad -\chi_2(-4/k) + \chi_4(-4/k) J(\chi_2, \chi_4) + \chi_4(-4/k)^3 J(\chi_2, \chi_4^3) \end{aligned}$$

$$\begin{aligned} &= (p-1) + (p-1) - (p-2) \\ &\quad -\chi_2(-4/k) + \chi_4(-4/k) J(\chi_2, \chi_4) + \chi_4(-4/k)^3 J(\chi_2, \chi_4^3) \\ &\quad \text{(by Lemma 4.26)} \end{aligned}$$

$$= p + 1 - \delta + \chi_4(-4/k) J(\chi_2, \chi_4) + \chi_4(-4/k)^3 J(\chi_2, \chi_4^3).$$

For the last equality, we used the fact that

$$1 + \chi_2(-4/k) = 1 + \chi_2(1/k) = \begin{cases} 0 \text{ if } k \text{ is not a square} \\ 2 \text{ if } k \text{ is a square mod } p, \end{cases}$$

hence $1+\chi_2(-4/k)=\delta$. Therefore,

$$\begin{aligned}\#E(\mathbf{F}_p) &= \#\{(u,v)\in\mathbf{F}_p\times\mathbf{F}_p \mid v^2=(k/4)u^4+1\}+\delta\\ &= p+1-\alpha-\overline{\alpha},\end{aligned}$$

where

$$\alpha=-\chi_4(-4/k)J(\chi_2,\chi_4)\in\mathbf{Z}[i].$$

If we write $\alpha=a+bi$, then $\alpha+\overline{\alpha}=2a$. Proposition 4.27 implies that $a^2+b^2=p$, so we have almost proved Theorem 4.23. It remains to evaluate a mod 4.

Let $x_1+y_1i,\ x_2+y_2i\in\mathbf{Z}[i]$. We say that

$$x_1+y_1i\equiv x_2+y_2i \pmod{2+2i}$$

if

$$(x_1-x_2)+(y_1-y_2)i=(x_3+y_3i)(2+2i)$$

for some $x_3+y_3i\in\mathbf{Z}[i]$. Clearly $-2i\equiv 2 \pmod{2+2i}$. Since $2i-2=i(2+2i)$ and $-2=2+(-1+i)(2+2i)$, we have

$$2i\equiv 2\equiv -2\equiv -2i \pmod{2+2i}.$$

It follows easily that

$$2\chi_4(a)\equiv 2 \pmod{2+2i} \tag{4.3}$$

for all a. Since $p-1$ is a multiple of $4=(1-i)(2+2i)$, we have $p\equiv 1$ $\pmod{2+2i}$.

LEMMA 4.29

Let $p\equiv 1 \pmod 4$ be prime. Then

$$J(\chi_2,\chi_4)\equiv -1 \pmod{2+2i}.$$

PROOF Let $S=\{x\in\mathbf{F}_p^\times \mid x\neq 1\}$. Let

$$\tau: S\to S,\quad x\mapsto \frac{x}{x-1}.$$

It is easy to check that $\tau(\tau(x))=x$ for all $x\in S$ and that $x=2$ is the only value of x such that $\tau(x)=x$. Put the elements of S, other than 2, into pairs $(x,\tau(x))$. Note that if x is paired with $y=\tau(x)$, then y is paired with $\tau(y)=\tau(\tau(x))=x$. This divides S into $(p-3)/2$ pairs plus the element 2, which is not in a pair. We have

$$J(\chi_2,\chi_4)=\sum_{a\neq 0,1}\chi_2(a)\chi_4(1-a)=$$

$$\chi_2(2)\chi_4(1-2)+\sum_{(a,\tau(a))}\left(\chi_2(a)\chi_4(1-a)+\chi_2\left(\frac{a}{a-1}\right)\chi_4\left(1-\frac{a}{a-1}\right)\right),$$

where the sum is over pairs $(a, \tau(a))$. Note that since $\chi_2\chi_4 = \chi_4^{-1}$, we have

$$\chi_2\left(\frac{a}{a-1}\right)\chi_4\left(1-\frac{a}{a-1}\right) = \frac{\chi_2(a)}{\chi_2(a-1)}\frac{\chi_4(-1)}{\chi_4(a-1)}$$
$$= \chi_2(a)\chi_4(-1)\chi_4(a-1) = \chi_2(a)\chi_4(1-a).$$

Therefore, since $\chi_2(2) = \chi_4(2)^2 = \chi_4(4)$,

$$\begin{aligned} J(\chi_2, \chi_4) &= \chi_4(-4) + 2\sum_{(a,\tau(a))} \chi_2(a)\chi_4(1-a) \\ &\equiv \chi_4(-4) + \sum_{(a,\tau(a))} 2 \quad \text{(by (4.3))} \\ &\equiv \chi_4(-4) + (p-3) \equiv \chi_4(-4) - 2 \pmod{2+2i}. \end{aligned}$$

Suppose $p \equiv 1 \pmod 8$. Since $g^{(p-1)/2} \equiv -1 \pmod p$, we have that -1 is a fourth power. It is well known that 2 is a square mod p if and only if $p \equiv \pm 1 \pmod 8$ (this is one of the supplementary laws for quadratic reciprocity and is covered in most elementary number theory texts). Therefore 4 is a fourth power when $p \equiv 1 \pmod 8$. It follows that $\chi_4(-4) = 1$.

Now suppose $p \equiv 5 \pmod 8$. Then 2 is not a square mod p, so $2 \equiv g^j \pmod p$ with j odd. Therefore

$$-4 \equiv g^{2j+(p-1)/2} \pmod p.$$

Since $2j \equiv 2 \pmod 4$ and $(p-1)/2 \equiv 2 \pmod 4$, it follows that -4 is a fourth power mod p. Therefore, $\chi_4(-4) = 1$.

In both cases, we obtain $J(\chi_2, \chi_4) \equiv \chi_4(-4) - 2 \equiv -1 \pmod{2+2i}$. ∎

Since we just proved that $\chi_4(-4) = 1$, the lemma implies that

$$\alpha = -\chi_4(-4/k)J(\chi_2, \chi_4) = -\chi_4(1/k)J(\chi_2, \chi_4) \equiv \chi_4(k)^3 \pmod{2+2i}.$$

LEMMA 4.30

Let $\alpha = x + yi \in \mathbf{Z}[i]$.

1. *If $\alpha \equiv 1 \pmod{2+2i}$, then x is odd and $x + y \equiv 1 \pmod 4$.*
2. *If $\alpha \equiv -1 \pmod{2+2i}$, then x is odd and $x + y \equiv 3 \pmod 4$.*
3. *If $\alpha \equiv \pm i \pmod{2+2i}$, then x is even.*

PROOF Suppose $\alpha \equiv 1 \pmod{2+2i}$, so $\alpha - 1 = (u+iv)(2+2i)$ for some u, v. Since $(1-i)(2+2i) = 4$, we have

$$(x+y-1) + (y+1-x)i = (1-i)(\alpha-1) = 4u + 4vi.$$

Therefore, $x + y \equiv 1 \pmod 4$ and $x - y \equiv 1 \pmod 4$. It follows that y is even. This proves (1). The proofs of (2) and (3) are similar. ▮

If k is a fourth power mod p, then $\chi_4(k) = 1$, so $\alpha \equiv 1 \pmod{2 + 2i}$. The lemma yields $\alpha = a + bi$ with b even and $a + b \equiv 1 \pmod 4$. This proves part of part (2) of Theorem 4.23. The other parts are proved similarly. This completes the proof of Theorem 4.23.

4.5 Schoof's Algorithm

In 1985, Schoof [97] published an algorithm for computing the number of points on elliptic curves over finite fields $\mathbf{F}_q$ that runs much faster than existing algorithms, at least for very large q. In particular, it requires at most a constant times $\log^8 q$ bit operations, in contrast to the $q^{1/4}$ used in Baby Step, Giant Step, for example. Subsequently, Atkin and Elkies refined and improved Schoof's method (see Section 12.4). It has now been used successfully when q has several hundred decimal digits. In the following, we'll give Schoof's method. For details of the method of Atkins and Elkies, see [12] and [99]. For other methods for counting points, see [60] and [94].

Suppose E is an elliptic curve given by $y^2 = x^3 + Ax + B$ over $\mathbf{F}_q$. We know, by Hasse's theorem, that

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

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

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

If we can determine $a \bmod \ell$ for each prime $\ell \in S$, then we know $a \bmod \prod \ell$, and therefore a is uniquely determined.

Let ℓ be prime. For simplicity, we assume $\ell \neq p$, where p is the characteristic of $\mathbf{F}_q$. We also assume that q is odd. We want to compute $a \pmod \ell$.

If $\ell = 2$, this is easy. If $x^3 + Ax + B$ has a root $e \in \mathbf{F}_q$, then $(e, 0) \in E[2]$ and $(e, 0) \in E(\mathbf{F}_q)$, so $E(\mathbf{F}_q)$ has even order. In this case, $q + 1 - a \equiv 0 \pmod 2$, so a is even. If $x^3 + Ax + B$ has no roots in $\mathbf{F}_q$, then $E(\mathbf{F}_q)$ has no points of order 2, and a is odd. To determine whether $x^3 + Ax + B$ has a root in $\mathbf{F}_q$, we could try all the elements in $\mathbf{F}_q$, but there is a faster way. Recall (see Appendix C) that the roots of $x^q - x$ are exactly the elements of $\mathbf{F}_q$. Therefore, $x^3 + Ax + B$ has a root in $\mathbf{F}_q$ if and only if it has a root in common with $x^q - x$. The Euclidean algorithm, applied to polynomials, yields the gcd of the two polynomials.

If q is very large, the polynomial x^q has very large degree. Therefore, it is more efficient to compute $x_q \equiv x^q \pmod{x^3 + Ax + B}$ by successive squaring (cf. Section 2.2), and then use the result to compute

$$\gcd(x_q - x,\, x^3 + Ax + B) = \gcd(x^q - x,\, x^3 + Ax + B).$$

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. This finishes the case $\ell = 2$.

In the following, various expressions such as x^q and x^{q^2} will be used. They will always be computed mod a polynomial in a manner similar to that just done in the case $\ell = 2$

In Section 3.2, we defined the division polynomials ψ_n. When n is odd, ψ_n is a polynomial in x and, for $(x, y) \in E(\overline{\mathbf{F}}_q)$, we have

$$(x, y) \in E[n] \Longleftrightarrow \psi_n(x) = 0.$$

These polynomials play a crucial role in Schoof's algorithm.

Let ϕ_q be the Frobenius endomorphism (not to be confused with the polynomials ϕ_n from Section 3.2, which are not used in this section), so

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

By Theorem 4.10,

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

Let (x, y) be a point of order ℓ. Then

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

Let

$$q_\ell \equiv q \pmod{\ell}, \quad |q_\ell| < \ell/2.$$

Then $q(x, y) = q_\ell(x, y)$, so

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

Since (x^q, y^q) is also a point of order ℓ, this relation determines a mod ℓ. The idea is to compute all the terms except a in this relation, then determine a value of a that makes the relation hold. Note that if the relation holds for one point $(x, y) \in E[\ell]$, then we have determined $a \pmod{\ell}$; hence, it holds for all $(x, y) \in E[\ell]$.

Assume first that $\left(x^{q^2}, y^{q^2}\right) \neq \pm q_\ell(x, y)$ for some $(x, y) \in E[\ell]$. Then

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

so $a \not\equiv 0 \pmod{\ell}$. In this case, the x-coordinates of $\left(x^{q^2}, y^{q^2}\right)$ and $q_\ell(x,y)$ are distinct, so the sum of the two points is found 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. We may compute x_j and y_j using division polynomials, as in Section 3.2. Moreover, $x_j = r_{1,j}(x)$ and $y_j = r_{2,j}(x)y$, as on page 47. We have

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

Writing

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

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

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

First, we look at the x-coordinates. Starting with $(x,y) \in E[\ell]$, we have $(x', y') = \pm(x_j^q, y_j^q)$ if and only if $x' = x_j^q$. As pointed out above, if this happens for one point in $E[\ell]$, it happens for all (finite) points in $E[\ell]$. Since the roots of ψ_ℓ are the x-coordinates of the points in $E[\ell]$, this implies that

$$x' - x_j^q \equiv 0 \pmod{\psi_\ell} \tag{4.4}$$

(this means that the numerator of $x' - x_j^q$ is a multiple of ψ_ℓ). We are using here 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 $\ell^2 - 1$ distinct points of order ℓ, since ℓ is assumed not to be the characteristic of $\mathbf{F}_q$. There are $(\ell^2 - 1)/2$ distinct x-coordinates of these points, and all of them are roots of ψ_ℓ, which has degree $(\ell^2 - 1)/2$. Therefore, the roots of ψ_ℓ must be simple.

Assume now that we have found j such that (4.4) 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

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

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

It remains to consider the case where $\left(x^{q^2}, y^{q^2}\right) = \pm q(x,y)$ for all $(x,y) \in E[\ell]$. 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, $a^2 q \equiv 4q^2 \pmod{\ell}$, so q is a square mod ℓ. If q is not a square mod ℓ, then we cannot be in this case. If q is a square mod ℓ, let $w^2 \equiv q \pmod{\ell}$. We have

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

for all $(x,y) \in E[\ell]$. Let P be any point in $E[\ell]$. 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 $P \in E[\ell]$ with $\phi_q P = \pm wP$.

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

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

so $aw \equiv 2q \equiv 2w^2 \pmod{\ell}$. Therefore, $a \equiv 2w \pmod{\ell}$. Similarly, if there exists P such that $\phi_q P = -wP$, then $a \equiv -2w \pmod{\ell}$. 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 $(x,y) \in E[\ell]$. Therefore, we compute $x^q - x_w$, which is a rational function of x. If

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

then there is some $(x,y) \in E[\ell]$ 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. Looking for 0 $\pmod{\psi_\ell}$ 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 $P \in E[\ell]$. For example, the matrix representing ϕ_q on $E[\ell]$ might not be diagonalizable. It might be $\begin{pmatrix} w & 1 \\ 0 & w \end{pmatrix}$. In this case, the eigenvectors for ϕ_q form a one-dimensional subspace.

If we have $\gcd(\text{numerator}(x^q - x_w),\ \psi_\ell) = 1$, 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 $P \in E[\ell]$. Therefore, $a \equiv 0 \pmod{\ell}$.

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

1. Choose a set of primes $S = \{2, 3, 5, \ldots, L\}$ (with $p \notin S$) such that $\prod_{\ell \in S} \ell > 4\sqrt{q}$.

2. If $\ell = 2$, 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 $\ell \in S$, do the following.

   (a) Let $q_\ell \equiv q \pmod \ell$ with $|q_\ell| < \ell/2$.

   (b) Compute the x-coordinate x' of

   $$(x', y') = \left(x^{q^2}, y^{q^2}\right) + q_\ell(x, y) \bmod \psi_\ell.$$

   (c) For $j = 1, 2, \ldots, (\ell-1)/2$, do the following.

      i. Compute the x-coordinate x_j of $(x_j, y_j) = j(x, y)$.

      ii. If $x' - x_j^q \equiv 0 \pmod{\psi_\ell}$, go to step (iii). If not, try the next value of j (in step (c)). If all values $1 \le j \le (\ell-1)/2$ have been tried, go to step (d).

      iii. Compute y' and y_j. If $(y' - y_j^q)/y \equiv 0 \pmod{\psi_\ell}$, then $a \equiv j \pmod \ell$. If not, then $a \equiv -j \pmod \ell$.

   (d) If all values $1 \le j \le (\ell-1)/2$ have been tried without success, let $w^2 \equiv q \pmod \ell$. If w does not exist, then $a \equiv 0 \pmod \ell$.

   (e) If gcd(numerator($x^q - x_w$), ψ_ℓ) $= 1$, then $a \equiv 0 \pmod \ell$. Otherwise, compute

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

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

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

Example 4.13

Let E be the elliptic curve $y^2 = x^3 + 2x + 1 \bmod 19$. Then

$$\#E(\mathbf{F}_{19}) = 19 + 1 - a.$$

We want to determine a. We'll show that

$$a \equiv \begin{cases} 1 & \pmod 2 \\ 2 & \pmod 3 \\ 3 & \pmod 5. \end{cases}$$

Putting these together yields

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

Since $|a| < 2\sqrt{19} < 9$, we must have $a = -7$.

We start with $\ell = 2$. We compute

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

by successive squaring (cf. Section 2.2) and then use the result to compute

$$\gcd(x^{19} - x,\, x^3 + 2x + 1) = \gcd(x^2 + 12x + 14,\, x^3 + 2x + 1) = 1.$$

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

For $\ell = 3$, we proceed as in Schoof's algorithm and eventually get to $j = 1$. We have $q^2 = 361$ and we have $q \equiv 1 \pmod 3$. Therefore, $q_\ell = 1$ and we need to check whether

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

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 mod ψ_3. The natural way to start is to use the extended Euclidean algorithm to find the inverse of $x^{361} - x \pmod{\psi_3}$. 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 $(8, 4) \in E(\mathbf{F}_{19})$ has order 3. Therefore,

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

so $a \equiv 2 \pmod 3$.

For $\ell = 5$, we follow Schoof's algorithm, eventually arriving at $j = 2$. Note that

$$19 \equiv 4 \equiv -1 \pmod 5,$$

so $q_\ell = -1$ and

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

We need to check whether

$$(x',y') \overset{\text{def}}{=} (x^{361}, y^{361}) + (x,-y) \overset{?}{=} \pm 2(x^{19}, y^{19}) \overset{\text{def}}{=} \pm(x'', y'')$$

for all $(x,y) \in E[5]$. The recurrence of Section 3.2 shows that the fifth division polynomial is

$$\begin{aligned}\psi_5 &= 32(x^3+2x+1)^2(x^6+10x^4+20x^3-20x^2-8x-8-8)-\psi_3^3\\ &= 5x^{12}+10x^{10}+17x^8+5x^7+x^6+9x^5+12x^4+2x^3+5x^2+8x+8.\end{aligned}$$

The equation for the x-coordinates yields

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

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

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

To determine the sign, we look at the y-coordinates. The y-coordinate of $(x',y') = (x^{361}, y^{361}) + (x,-y)$ is computed to be

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

The y-coordinate of $(x'',y'') = 2(x,y)$ 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

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

This means that

$$(x',y') \equiv (x''^{19}, -y''^{19}) = -2(x^q, y^q) \pmod{\psi_5}.$$

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

As we showed above, the information from $\ell = 2, 3, 5$ is sufficient to yield $a = -7$. Therefore, $\#E(\mathbf{F}_{19}) = 27$. □

4.6 Supersingular Curves

An elliptic curve E in characteristic p is called **supersingular** if $E[p] = \{\infty\}$. In other words, there are no points of order p, even with coordinates in an algebraically closed field. Supersingular curves have many interesting properties, some of which we'll discuss in the present section.

Note: Supersingular curves are not singular curves in the sense of Section 2.4. The term "singular" was used classically to describe the j-invariants of elliptic curves with endomorphism rings larger than $\mathbf{Z}$. These rings usually are subrings of quadratic extensions of the rationals. The term "supersingular" refers to j-invariants of curves with even larger rings of endomorphisms, namely, subrings of quaternion algebras. These ideas will be discussed in Chapter 10.

The following result is useful because it gives a simple way of determining whether or not an elliptic curve over a finite field is supersingular.

PROPOSITION 4.31

Let E be an elliptic curve over $\mathbf{F}_q$, where q is a power of the prime number p. Let $a = q + 1 - \#E(\mathbf{F}_q)$. Then E is supersingular if and only if $a \equiv 0 \pmod{p}$, which is if and only if $\#E(\mathbf{F}_q) \equiv 1 \pmod{p}$.

PROOF Write $X^2 - aX + q = (X - \alpha)(X - \beta)$. Theorem 4.12 implies that

$$\#E(\mathbf{F}_{q^n}) = q^n + 1 - (\alpha^n + \beta^n).$$

Lemma 4.13 says that $s_n = \alpha^n + \beta^n$ satisfies the recurrence relation

$$s_0 = 2, \quad s_1 = a, \quad s_{n+1} = as_n - qs_{n-1}.$$

Suppose $a \equiv 0 \pmod{p}$. Then $s_1 = a \equiv 0 \pmod{p}$, and $s_{n+1} \equiv 0 \pmod{p}$ for all $n \geq 1$ by the recurrence. Therefore,

$$\#E(\mathbf{F}_{q^n}) = q^n + 1 - s_n \equiv 1 \pmod{p},$$

so there are no points of order p in $E(\mathbf{F}_{q^n})$ for any $n \geq 1$. Since $\overline{\mathbf{F}}_q = \cup_{n\geq 1}\mathbf{F}_{q^n}$, there are no points of order p in $E(\overline{\mathbf{F}}_q)$. Therefore, E is supersingular.

Now suppose $a \not\equiv 0 \pmod{p}$. The recurrence implies that $s_{n+1} \equiv as_n \pmod{p}$ for $n \geq 1$. Since $s_1 = a$, we have $s_n \equiv a^n \pmod{p}$ for all $n \geq 1$. Therefore

$$\#E(\mathbf{F}_{q^n}) = q^n + 1 - s_n \equiv 1 - a^n \pmod{p}.$$

By Fermat's little theorem, $a^{p-1} \equiv 1 \pmod{p}$. Therefore, $E(\mathbf{F}_{q^{p-1}})$ has order divisible by p, hence contains a point of order p. This means that E is not supersingular.

For the last part of the proposition, note that

$$\#E(\mathbf{F}_q) \equiv q + 1 - a \equiv 1 - a \pmod{p},$$

so $\#E(\mathbf{F}_q) \equiv 1 \pmod{p}$ if and only if $a \equiv 0 \pmod{p}$. ▮

COROLLARY 4.32

Suppose $p \geq 5$ is a prime and E is defined over $\mathbf{F}_p$. Then E is supersingular if and only if $a = 0$, which is the case if and only if $\#E(\mathbf{F}_p) = p + 1$.

PROOF If $a = 0$, then E is supersingular, by the proposition. Conversely, suppose E is supersingular but $a \neq 0$. Then $a \equiv 0 \pmod{p}$ implies that $|a| \geq p$. By Hasse's theorem, $|a| \leq 2\sqrt{p}$, so we have $p \leq 2\sqrt{p}$. This means that $p \leq 4$. ▮

When $p = 2$ or $p = 3$, there are examples of supersingular curves with $a \neq 0$. See Exercise 4.7.

For general finite fields $\mathbf{F}_q$, it can be shown that if E defined over $\mathbf{F}_q$ is supersingular, then a^2 is one of 0, q, $2q$, $3q$, $4q$. See [98], [80], or Theorem 4.3.

In Section 3.1, we saw that the elliptic curve $y^2 + a_3y = x^3 + a_4x + a_6$ in characteristic 2 is supersingular. Also, in characteristic 3, the curve $y^2 = x^3 + a_2x^2 + a_4x + a_6$ is supersingular if and only if $a_2 = 0$. Here is a way to construct supersingular curves in many other characteristics.

PROPOSITION 4.33

Suppose q is odd and $q \equiv 2 \pmod{3}$. Let $B \in \mathbf{F}_q^\times$. Then the elliptic curve E given by $y^2 = x^3 + B$ is supersingular.

PROOF Let $\psi : \mathbf{F}_q^\times \to \mathbf{F}_q^\times$ be the homomorphism defined by $\psi(x) = x^3$. Since $q - 1$ is not a multiple of 3, there are no elements of order 3 in $\mathbf{F}_q^\times$, so the kernel of ψ is trivial. Therefore, ψ is injective, hence must be surjective since it is a map from a finite group to itself. In particular, every element of $\mathbf{F}_q$ has a unique cube root in $\mathbf{F}_q$.

For each $y \in \mathbf{F}_q$, there is exactly one $x \in \mathbf{F}_q$ such that (x, y) lies on the curve, namely, x is the unique cube root of $y^2 - B$. Since there are q values of y, we obtain q points. Including the point ∞ yields

$$\#E(\mathbf{F}_q) = q + 1.$$

Therefore, E is supersingular. ▮

Later (Theorem 4.34), we'll see how to obtain all supersingular elliptic curves over an algebraically closed field.

An attractive feature of supersingular curves is that computations involving an integer times a point can sometimes be done faster than might be expected. Suppose E is a supersingular elliptic curve defined over $\mathbf{F}_q$ and let $P = (x, y)$ be a point in $E(\mathbf{F}_{q^n})$ for some $n \geq 1$. Usually n is large. Let k be a positive integer. We want to compute kP. This can be done quickly by successive doubling, but it is possible to do even better. Let's assume that $a = 0$. Then

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

by Theorem 4.10. Therefore

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

The calculations of x^{q^2} and y^{q^2} involve finite field arithmetic, which is generally faster than elliptic curve calculations. Moreover, if x and y are expressed in terms of a normal basis of $\mathbf{F}_{q^n}$ over $\mathbf{F}_q$, then x^{q^2} and y^{q^2} are computed by shift operations (see Appendix C). The procedure is now as follows:

1. Expand k in base q:

$$k = k_0 + k_1 q + k_2 q^2 + \cdots + k_r q^r,$$

with $0 \leq k_i < q$.

2. Compute $k_i P = (x_i, y_i)$ for each i.

3. Compute $q^i k_i P = (x_i^{q^{2i}}, (-1)^i y_i^{q^{2i}})$.

4. Sum the points $q^i k_i P$ for $0 \leq i \leq r$.

The main savings is in step (3), where elliptic curve calculations are replaced by finite field computations.

We now show how to obtain all supersingular curves over $\overline{\mathbf{F}}_q$. Note that supersingularity means that there are no points of order p with coordinates in the algebraic closure; hence, it is really a property of an elliptic curve over an algebraically closed field. If we have two elliptic curves E_1 and E_2 defined over a field such that E_1 can be transformed into E_2 by a change of variables defined over some extension field, then E_1 is supersingular if and only if E_2 is supersingular.

For example, in Proposition 4.33, the curve $y_1^2 = x_1^3 + B$ can be changed into $y_2^2 = x_2^3 + 1$ via $x_2 = x_1/B^{1/3}$, $y_2 = y_1/B^{1/2}$. Therefore, it would have sufficed to prove the proposition for the curve $y^2 = x^3 + 1$.

Recall (Section 2.5.1) that an elliptic curve E over an algebraically closed field of characteristic not 2 can be put into the Legendre form $y^2 = x(x-1)(x-\lambda)$ with $\lambda \neq 0, 1$.

THEOREM 4.34

Let p be an odd prime. Define the polynomial

$$H_p(T) = \sum_{i=0}^{(p-1)/2} \binom{(p-1)/2}{i}^2 T^i.$$

The elliptic curve E given by $y^2 = x(x-1)(x-\lambda)$ with $\lambda \in \overline{\mathbf{F}}_p$ is supersingular if and only if $H_p(\lambda) = 0$.

PROOF Since $\overline{\mathbf{F}}_p = \cup_{n\geq 1}\mathbf{F}_{p^n}$, we have $\lambda \in \mathbf{F}_q = \mathbf{F}_{p^n}$ for some n. So E is defined over $\mathbf{F}_q$. To determine supersingularity, it suffices to count points in $E(\mathbf{F}_q)$, by Proposition 4.31. We know (Exercise 4.4) that

$$\left(\frac{x}{\mathbf{F}_q}\right) = x^{(q-1)/2}$$

in $\mathbf{F}_q$. Therefore, by Theorem 4.14,

$$\#E(\mathbf{F}_q) = q + 1 + \sum_{x\in\mathbf{F}_q} \left(x(x-1)(x-\lambda)\right)^{(q-1)/2},$$

where this is now an equality in $\mathbf{F}_q$. The integers in this formula are regarded as elements of $\mathbf{F}_p \subseteq \mathbf{F}_q$. The following lemma allows us to simplify the sum.

LEMMA 4.35

Let $i > 0$ be an integer. Then

$$\sum_{x\in\mathbf{F}_q} x^i = \begin{cases} 0 & \text{if } q-1 \nmid i \\ -1 & \text{if } q-1 | i. \end{cases}$$

PROOF If $q-1|i$ then $x^i = 1$ for all nonzero x, so the sum equals $q-1$, which equals -1 in $\mathbf{F}_q$. The group $\mathbf{F}_q^\times$ is cyclic of order $q-1$. Let g be a generator. Then every nonzero element of $\mathbf{F}_q$ can be written in the form g^j with $0 \leq j \leq q-2$. Therefore, if $q-1 \nmid i$,

$$\sum_{x\in\mathbf{F}_q} x^i = 0 + \sum_{x\in\mathbf{F}_q^\times} x^i = \sum_{j=0}^{q-2} (g^j)^i = \sum_{j=0}^{q-2} (g^i)^j = \frac{(g^i)^{q-1} - 1}{g^i - 1} = 0,$$

since $g^{q-1} = 1$. ∎

Expand $(x(x-1)(x-\lambda))^{(q-1)/2}$ into a polynomial of degree $3(q-1)/2$. There is no constant term, so the only term x^i with $q-1|i$ is x^{q-1}. Let A_q be the coefficient of x^{q-1}. By the lemma,

$$\sum_{x\in\mathbf{F}_q} \left(x(x-1)(x-\lambda)\right)^{(q-1)/2} = -A_q,$$

since all the powers of x except for x^{q-1} sum to 0. Therefore,

$$\#E(\mathbf{F}_q) = 1 - A_q \quad \text{in } \mathbf{F}_q.$$

By Proposition 4.31, E is supersingular if and only if $A_q = 0$ in $\mathbf{F}_q$. The following lemma allows us to relate A_q to A_p.

LEMMA 4.36

Let $f(x) = x^3 + c_2x^2 + c_1x + c_0$ be a cubic polynomial with coefficients in a field of characteristic p. For each $r \geq 1$, let A_{p^r} be the coefficient of x^{p^r-1} in $f(x)^{(p^r-1)/2}$. Then

$$A_{p^r} = A_p^{1+p+p^2+\cdots+p^{r-1}}.$$

PROOF We have

$$\begin{aligned}(f(x)^{(p-1)/2})^{p^r} &= (x^{3(p-1)/2} + \cdots + A_p x^{p-1} + \cdots)^{p^r} \\ &= x^{3(p-1)p^r/2} + \cdots + A_p^{p^r} x^{p^r(p-1)} + \cdots .\end{aligned}$$

Therefore,

$$\begin{aligned}f(x)^{(p^{r+1}-1)/2} &= f(x)^{(p^r-1)/2}\left(f(x)^{(p-1)/2}\right)^{p^r} \\ &= (x^{3(p^r-1)/2} + \cdots + A_{p^r} x^{p^r-1} + \cdots) \\ &\quad \cdot (x^{3(p-1)p^r/2} + \cdots + A_p^{p^r} x^{p^r(p-1)} + \cdots).\end{aligned}$$

To obtain the coefficient of $x^{p^{r+1}-1}$, choose indices i and j with $i + j = p^{r+1} - 1$, multiply the corresponding coefficients from the first and second factors in the above product, and sum over all such pairs i, j. A term with $0 \leq i \leq 3(p^r - 1)/2$ from the first factor requires a term with

$$p^{r+1} - 1 \geq j \geq (p^{r+1} - 1) - \frac{3}{2}(p^r - 1) > (p-2)p^r$$

from the second factor. Since all of the exponents in the second factor are multiples of p^r, the only index j in this range that has a nonzero exponent is $j = (p-1)p^r$. The corresponding index i is $p^r - 1$. The product of the coefficients yields

$$A_{p^{r+1}} = A_{p^r} A_p^{p^r}.$$

The formula of the lemma is trivially true for $r = 1$. It now follows by an easy induction for all r. ▮

From the lemma, we now see that E is supersingular if and only if $A_p = 0$. This is significant progress, since A_p depends on p but not on which power of p is used to get q.

It remains to express A_p as a polynomial in λ. The coefficient A_p of x^{p-1} in $(x(x-1)(x-\lambda))^{(p-1)/2}$ is the coefficient of $x^{(p-1)/2}$ in

$$((x-1)(x-\lambda))^{(p-1)/2}.$$

By the binomial theorem,

$$(x-1)^{(p-1)/2} = \sum_i \binom{(p-1)/2}{i} x^i (-1)^{(p-1)/2-i}$$
$$(x-\lambda)^{(p-1)/2} = \sum_j \binom{(p-1)/2}{j} x^{(p-1)/2-j} (-\lambda)^j.$$

The coefficient A_p of $x^{(p-1)/2}$ in $(x-1)^{(p-1)/2}(x-\lambda)^{(p-1)/2}$ is

$$(-1)^{(p-1)/2} \sum_{k=0}^{(p-1)/2} \binom{(p-1)/2}{k}^2 \lambda^k = (-1)^{(p-1)/2} H_p(\lambda).$$

Therefore, E is supersingular if and only if $H_p(\lambda) = 0$. This completes the proof of Theorem 4.34. ∎

It is possible to use the method of the preceding proof to determine when certain curves are supersingular.

PROPOSITION 4.37

Let $p \geq 5$ be prime. Then the elliptic curve $y^2 = x^3 + 1$ over $\mathbf{F}_p$ is supersingular if and only if $p \equiv 2 \pmod 3$, and the elliptic curve $y^2 = x^3 + x$ over $\mathbf{F}_p$ is supersingular if and only if $p \equiv 3 \pmod 4$.

PROOF The coefficient of x^{p-1} in $(x^3+1)^{(p-1)/2}$ is 0 if $p \equiv 2 \pmod 3$ (since we only get exponents that are multiples of 3), and is $\binom{(p-1)/2}{(p-1)/3} \not\equiv 0 \pmod p$ when $p \equiv 1 \pmod 3$ (since the binomial coefficient contains no factors of p). Since the coefficient of x^{p-1} is zero mod p if and only if the curve is supersingular, this proves the first part.

The coefficient of x^{p-1} in $(x^3+x)^{(p-1)/2}$ is the coefficient of $x^{(p-1)/2}$ in $(x^2+1)^{(p-1)/2}$. All exponents appearing in this last expression are even, so $x^{(p-1)/2}$ doesn't appear when $p \equiv 3 \pmod 4$. When $p \equiv 1 \pmod 4$, the coefficient is $\binom{(p-1)/2}{(p-1)/4} \not\equiv 0 \pmod p$. This proves the second part of the proposition. ∎

If E is an elliptic curve defined over $\mathbf{Z}$ with complex multiplication (see Chapter 10) by a subring of $\mathbf{Q}(\sqrt{-d})$, and p is an odd prime number not dividing d for which $E \pmod p$ is an elliptic curve, then $E \pmod p$ is supersingular if and only if $-d$ is not a square mod p. Therefore, for such an E, the curve $E \pmod p$ is supersingular for approximately half of the primes. In the proposition, the curve $y^2 = x^3 + 1$ has complex multiplication by $\mathbf{Z}[(1+\sqrt{-3})/2]$, and -3 is a square mod p if and only if $p \equiv 1 \pmod 3$. The curve $y^2 = x^3 + x$ has complex multiplication by $\mathbf{Z}[\sqrt{-1}]$, and -1 is a square mod p if and only if $p \equiv 1 \pmod 4$.

If E does not have complex multiplication, the set of primes for which $E \pmod p$ is supersingular is much more sparse. Elkies [37] proved in 1986 that, for each E, the set of such primes is infinite. Wan [126], improving on an argument of Serre, showed that, for each $\epsilon > 0$, the number of such $p < x$ for which $E \pmod p$ is supersingular is less than $C_\epsilon x/\ln^{2-\epsilon}(x)$ for some constant C_ϵ depending on ϵ. Since the number of primes less than x is approximately $x/\ln x$, this shows that substantially less than half of the primes are supersingular for E. It has been conjectured by Lang and Trotter that the number of supersingular p is asymptotic to $C'\sqrt{x}/\ln x$ (as $x \to \infty$) for some constant C' depending on E. This has been shown to be true "on the average" by Fouvry and Murty [39].

We now change our viewpoint and fix p and count supersingular E over $\overline{\mathbf{F}}_p$. This essentially amounts to counting distinct zeros of $H_p(T)$. The values $\lambda = 0, 1$ are not allowed in the Legendre form of an elliptic curve. Moreover, they also don't appear as zeros of $H_p(T)$. It is easy to see that $H_p(0) = 1$. For $H_p(1)$, observe that the coefficient of $x^{(p-1)/2}$ in

$$(x+1)^{p-1} = (x+1)^{(p-1)/2}(x+1)^{(p-1)/2}$$

is

$$\binom{p-1}{(p-1)/2} = \sum_k \binom{(p-1)/2}{k}\binom{(p-1)/2}{(p-1)/2-k} = H_p(1),$$

(use the identity $\binom{n}{k} = \binom{n}{n-k}$). Since $\binom{p-1}{(p-1)/2}$ contains no factors p, it is nonzero mod p. Therefore, $H_p(1) \neq 0$.

PROPOSITION 4.38

$H_p(T)$ has $(p-1)/2$ distinct roots in $\overline{\mathbf{F}}_p$.

PROOF We claim that

$$4T(1-T)H_p''(T) + 4(1-2T)H_p'(T) - H_p(T) \equiv 0 \pmod p. \qquad (4.5)$$

Write $H_p(T) = \sum_k b_k T^k$. The coefficient of T^k on the left side of (4.5) is

$$\begin{aligned} &4(k+1)kb_{k+1} - 4k(k-1)b_k + 4(k+1)b_{k+1} - 8kb_k - b_k \\ &\quad = 4(k+1)^2 b_{k+1} - (2k+1)^2 b_k. \end{aligned}$$

Using the fact that

$$\begin{aligned} b_{k+1} &= \binom{(p-1)/2}{k+1}^2 \\ &= \left(\frac{((p-1)/2)!}{(k+1)!(((p-1)/2)-k-1)!}\right)^2 \\ &= \left(\frac{((p-1)/2)-k}{k+1}\right)^2 b_k, \end{aligned}$$

we find that the coefficient of T^k is

$$\left(4\left(((p-1)/2)-k\right)^2-(2k+1)^2\right) b_k = p(p-2-4k)b_k \equiv 0 \pmod{p}.$$

This proves the claim.

Suppose now that $H_p(\lambda)=0$ with $\lambda \in \overline{\mathbf{F}}_p$. Since $H_p(0)\neq 0$ and $H_p(1)\neq 0$, we have $\lambda \neq 0, 1$. Write $H_p(T)=(T-\lambda)^r G(T)$ for some polynomial $G(T)$ with $G(\lambda)\neq 0$. Suppose $r\geq 2$. In (4.5), we have $(T-\lambda)^{r-1}$ dividing the last term and the middle term, but only $(T-\lambda)^{r-2}$ divides the term $4T(1-T)H_p''(T)$. Since the sum of the three terms is 0, this is impossible, so we must have $r=1$. Therefore, λ is a simple root. (*Technical point:* Since the degree of $H_p(T)$ is less than p, we have $r<p$, so the first term of the derivative

$$H_p''(T) = r(r-1)(T-\lambda)^{r-2}G(T) + 2r(T-\lambda)^{r-1}G'(T) + (T-\lambda)^r G''(T)$$

does not disappear in characteristic p. Hence $(T-\lambda)^{r-1}$ does not divide the first term of (4.5).) ▮

REMARK 4.39 The differential equation 4.5 is called a **Picard-Fuchs differential equation**. For a discussion of this equation in the study of families of elliptic curves in characteristic 0, see [24]. Once we know that $H_p(T)$ satisfies this differential equation, the simplicity of the roots follows from a characteristic p version of the uniqueness theorem for second order differential equations. If λ is a multiple root of $H_p(T)$, then $H_p(\lambda)=H_p'(\lambda)=0$. Such a uniqueness theorem would say that $H_p(T)$ must be identically 0, which is a contradiction. Note that we must avoid $\lambda = 0, 1$ because of the coefficient $T(1-T)$ for $H_p''(T)$. ▮

COROLLARY 4.40

Let $p\geq 5$ be prime. The number of $j\in\overline{\mathbf{F}}_p$ that occur as j-invariants of supersingular elliptic curves is

$$\left[\frac{p}{12}\right]+\epsilon_p,$$

where $\epsilon_p = 0, 1, 1, 2$ if $p\equiv 1, 5, 7, 11 \pmod{12}$, respectively.

PROOF The j-invariant of $y^2 = x(x-1)(x-\lambda)$ is

$$2^8 \frac{(\lambda^2-\lambda+1)^3}{\lambda^2(\lambda-1)^2}$$

(see Exercise 2.13), so the values of λ yielding a given j are roots of the polynomial

$$P_j(\lambda) = 2^8(\lambda^2-\lambda+1)^3 - j\lambda^2(\lambda-1)^2.$$

The discriminant of this polynomial is $2^{30}(j-1728)^3 j^4$, which is nonzero unless $j = 0$ or 1728. Therefore, there are 6 distinct values of $\lambda \in \overline{\mathbf{F}}_p$ corresponding to each value of $j \neq 0, 1728$. If one of these λ's is a root of $H_p(T)$, then all six must be roots, since the corresponding elliptic curves are all the same (up to changes of variables), and therefore all or none are supersingular.

Since the degree of $H_p(T)$ is $(p-1)/2$, we expect approximately $(p-1)/12$ supersingular j-invariants, with corrections needed for the cases when at least one of $j = 0$ or $j = 1728$ is supersingular.

When $j = 0$, the polynomial $P_j(\lambda)$ becomes $2^8(\lambda^2-\lambda+1)^3$, so there are two values of λ that give $j = 0$. When $j = 1728$, the polynomial becomes $2^8(\lambda-2)^2(\lambda-\frac{1}{2})^2(\lambda+1)^2$, so there are three values of λ yielding $j = 1728$.

A curve with j-invariant 0 can be put into the form $y^2 = x^3 + 1$ over an algebraically closed field. Theorem 4.34 therefore tells us that when $p \equiv 2 \pmod 3$, the two λ's yielding $j = 0$ are roots of $H_p(T)$. Similarly, when $p \equiv 3 \pmod 4$, the three λ yielding $j = 1728$ are roots of $H_p(T)$.

Putting everything together, the total count of roots of $H_p(T)$ is

$$\begin{aligned} 6 \cdot \#\{\text{supersingular}\, j \neq 0, 1728\} &+ 2\delta_{2(3)} + 3\delta_{3(4)} \\ &= \deg H_p(T) = (p-1)/2, \end{aligned}$$

where $\delta_{i(j)} = 1$ if $p \equiv i \pmod j$ and $= 0$ otherwise.

Suppose that $p \equiv 5 \pmod{12}$. Then $\delta_{2(3)} = 1$ and $\delta_{3(4)} = 0$, so the number of supersingular $j \neq 0, 1728$ is

$$\frac{p-1}{12} - \frac{1}{3} = \left[\frac{p}{12}\right].$$

Adding 1 for the case $j = 0$ yields the number given in the proposition. The other cases of $p \pmod{12}$ are similar. ▮

Example 4.14

When $p = 23$, we have

$$\begin{aligned} H_{23}(T) = (T-3)(T-8)(T-21)(T-11)(T-13)(T-16) \\ \cdot(T-2)(T-12)(T+1)(T^2-T+1) \end{aligned}$$

(this is a factorization over $\mathbf{F}_{23}$). The first 6 factors correspond to

$$\{\lambda, \frac{1}{\lambda}, 1-\lambda, \frac{1}{1-\lambda}, \frac{\lambda}{\lambda-1}, \frac{\lambda-1}{\lambda}\},$$

with $\lambda = 3$, hence to the curve $y^2 = x(x-1)(x-3)$. The next three factors correspond to $j = 1728$, hence to the curve $y^2 = x^3 + x$. The last factor corresponds to $j = 0$, hence to $y^2 = x^3 + 1$. Therefore, we have found the three supersingular curves over $\overline{\mathbf{F}}_{23}$. Of course, over $\mathbf{F}_{23}$, there are different forms of these curves. For example, $y^2 = x^3 + 1$ and $y^2 = x^3 + 2$ are different curves over $\mathbf{F}_{23}$, but are the same over $\overline{\mathbf{F}}_{23}$. $\square$

Example 4.15

When $p = 13$,

$$H_{13}(T) \equiv (T^2 + 4T + 9)(T^2 + 12T + 3)(T^2 + 7T + 1).$$

The six roots correspond to one value of j. Since $\lambda = -2 + \sqrt{8}$ is a root of the first factor, the corresponding elliptic curve is

$$y^2 = x(x-1)(x + 2 - \sqrt{8}).$$

$\square$

The appearance of a square root such as $\sqrt{8}$ is fairly common. It is possible to show that a supersingular curve over a perfect field of characteristic p must have its j-invariant in $\mathbf{F}_{p^2}$ (see [109, Theorem V.3.1]). Therefore, a supersingular elliptic curve over $\overline{\mathbf{F}}_q$ can always be transformed via a change of variables (over $\overline{\mathbf{F}}_q$) into a curve defined over $\mathbf{F}_{p^2}$.

Exercises

4.1 Let E be the elliptic curve $y^2 = x^3 + x + 1 \pmod 5$.

(a) Show that $3(0,1) = (2,1)$ on E.

(b) Show that $(0,1)$ generates $E(\mathbf{F}_5)$. (Use the fact that $E(\mathbf{F}_5)$ has order 9 (see Example 4.1), plus the fact that the order of any element of a group divides the order of the group.)

4.2 Let E be the elliptic curve $y^2 + y = x^3$ over $\mathbf{F}_2$. Show that

$$\#E(\mathbf{F}_{2^n}) = \begin{cases} 2^n + 1 & \text{if } n \text{ is odd} \\ 2^n + 1 - 2(-2)^{n/2} & \text{if } n \text{ is even.} \end{cases}$$

4.3 Let $\mathbf{F}_q$ be a finite field with q odd. Since $\mathbf{F}_q^\times$ is cyclic of even order $q-1$, half of the elements of $\mathbf{F}_q^\times$ are squares and half are nonsquares.

(a) Let $u \in \mathbf{F}_q$. Show that

$$\sum_{x \in \mathbf{F}_q} \left(\frac{x+u}{\mathbf{F}_q} \right) = 0.$$

(b) Let $f(x) = (x-r)^2(x-s)$, where $r, s \in \mathbf{F}_q$ with q odd. Show that

$$\sum_{x \in \mathbf{F}_q} \left(\frac{f(x)}{\mathbf{F}_q} \right) = -\left(\frac{r-s}{\mathbf{F}_q} \right).$$

(*Hint:* If $x \neq r$, then $(x-r)^2(x-s)$ is a square exactly when $x-s$ is a square.)

4.4 Let $x \in \mathbf{F}_q$ with q odd. Show that

$$\left(\frac{x}{\mathbf{F}_q} \right) = x^{(q-1)/2}$$

as elements of $\mathbf{F}_q$. (*Remark:* Since the exponentiation on the right can be done quickly, for example, by successive squaring (this is the multiplicative version of the successive doubling in Section 2.2), this shows that the generalized Legendre symbol can be calculated quickly. Of course, the classical Legendre symbol can also be calculated quickly using quadratic reciprocity.)

4.5 Let $p \equiv 1 \pmod 4$ be prime and let E be given by $y^2 = x^3 - kx$, where $k \not\equiv 0 \pmod p$.

(a) Use Theorem 4.23 to show that $\#E(\mathbf{F}_p)$ is a multiple of 4 when k is a square mod p.

(b) Show that when k is a square mod p, then $E(\mathbf{F}_p)$ contains 4 points P satisfying $2P = \infty$. Conclude again that $\#E(\mathbf{F}_p)$ is a multiple of 4.

(c) Show that when k is not a square mod p, then $E(\mathbf{F}_p)$ contains no points of order 4.

(d) Let k be a square but not a fourth power mod p. Show that exactly one of the curves $y^2 = x^3 - x$ and $y^2 = x^3 - kx$ has a point of order 4 defined over $\mathbf{F}_p$.

4.6 Let E be an elliptic curve over $\mathbf{F}_q$ and suppose

$$E(\mathbf{F}_q) \simeq \mathbf{Z}_n \oplus \mathbf{Z}_{mn}.$$

(a) Use the techniques of the proof of Proposition 4.16 to show that $q = mn^2 + kn + 1$ for some integer k.

(b) Use Hasse's theorem in the form $a^2 \leq 4q$ to show that $|k| \leq 2\sqrt{m}$. Therefore, if m is fixed, q occurs as the value of one of finitely many quadratic polynomials.

(c) The prime number theorem implies that the number of prime powers less than x is approximately $x/\ln x$. Use this to show that most prime powers do not occur as values of the finite list of polynomials in (b).

(d) Use Hasse's theorem to show that $mn \geq \sqrt{m}(\sqrt{q}-1)$.

(e) Show that if $m \geq 17$ and q is sufficiently large ($q \geq 1122$ suffices), then $E(\mathbf{F}_q)$ has a point of order greater than $4\sqrt{q}$.

(f) Show that for most values of q, an elliptic curve over $\mathbf{F}_q$ has a point of order greater than $4\sqrt{q}$.

4.7 (a) Let E be defined by $y^2+y = x^3+x$ over $\mathbf{F}_2$. Show that $\#E(\mathbf{F}_2) = 5$.

(b) Let E be defined by $y^2 = x^3-x+2$ over $\mathbf{F}_3$. Show that $\#E(\mathbf{F}_3) = 1$.

(c) Show that the curves in (a) and (b) are supersingular, but that, in each case, $a = p+1-\#E(\mathbf{F}_p) \neq 0$. This shows that the restriction to $p \geq 5$ is needed in Corollary 4.32.

4.8 Let $p \geq 5$ be prime. Use Theorem 4.23 to prove Hasse's theorem for the elliptic curve given by $y^2 = x^3 - kx$ over $\mathbf{F}_p$.

4.9 Let E be an elliptic curve over $\mathbf{F}_q$ with $q = p^{2m}$. Suppose that $\#E(\mathbf{F}_q) = q + 1 - 2\sqrt{q}$.

(a) Let ϕ_q be the Frobenius endomorphism. Show that $(\phi_q - p^m)^2 = 0$.

(b) Show that $\phi_q - p^m = 0$ (*Hint:* Theorem 2.22).

(c) Show that ϕ_q acts as the identity on $E[p^m-1]$, and therefore that $E[p^m-1] \subseteq E(\mathbf{F}_q)$.

(d) Show that $E(\mathbf{F}_q) \simeq \mathbf{Z}_{p^m-1} \oplus \mathbf{Z}_{p^m-1}$.

4.10 Let E be an elliptic curve over $\mathbf{F}_q$ with q odd. Write $\#E(\mathbf{F}_q) = q+1-a$. Let $d \in \mathbf{F}_q^\times$ and let $E^{(d)}$ be the twist of E, as in Exercise 2.23. Show that

$$\#E^{(d)}(\mathbf{F}_q) = q + 1 - \left(\frac{d}{\mathbf{F}_q}\right) a.$$

(*Hint:* Use Exercise 2.23(c) and Theorem 4.14.)

4.11 Let $\mathbf{F}_q$ be a finite field of odd characteristic and let $a, b \in \mathbf{F}_q$ with $a \neq \pm 2b$ and $b \neq 0$. Define the elliptic curve E by

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

(a) Show that the points $(b,\, b\sqrt{a+2b})$ and $(-b,\, -b\sqrt{a-2b})$ have order 4.

(b) Show that at least one of $a+2b$, $a-2b$, a^2-4b^2 is a square in $\mathbf{F}_q$.

(c) Show that if a^2-4b^2 is a square in $\mathbf{F}_q$, then $E[2] \subseteq E(\mathbf{F}_q)$.

(d) (Suyama) Show that $\#E(\mathbf{F}_q)$ is a multiple of 4.

(e) Let E' be defined by $y'^2 = x'^3 - 2ax'^2 + (a^2-4b^2)x'$. Show that $E'[2] \subseteq E'(\mathbf{F}_q)$. Conclude that $\#E'(\mathbf{F}_q)$ is a multiple of 4.

The curve E' is isogenous to E via

$$(x', y') = (y^2/x^2,\ y(b^2-x^2)/x^2)$$

(see the end of Section 8.6 and also Chapter 12). It can be shown that this implies that $\#E(\mathbf{F}_q) = \#E'(\mathbf{F}_q)$. This gives another proof of the result of part (d). The curve E has been used in certain elliptic curve factorization implementations (see [19]).

4.12 Let p be a prime and let E be a supersingular elliptic curve over the finite field $\mathbf{F}_p$. Let ϕ_p be the Frobenius endomorphism. Show that some power of ϕ_p is an integer. (*Note*: This is easy when $p \geq 5$. The cases $p = 2, 3$ can be done by a case-by-case calculation.)

4.13 Let E be an elliptic curve over $\mathbf{F}_q$. Show that Hasse's theorem can be restated as

$$\left| \sqrt{\#E(\mathbf{F}_q)} - \sqrt{q} \right| \leq 1.$$

4.14 Let E be an elliptic curve over $\mathbf{F}_q$. Assume that $q = r^2$ for some integer r. Suppose that $\#E(\mathbf{F}_q) = (r-1)^2$. Let $\phi = \phi_q$ be the qth power Frobenius endomorphism.

(a) Show that $(\phi - r)^2 = 0$.

(b) Show that $\phi - r = 0$. (*Hint:* A nonzero endomorphism is surjective on $E(\overline{\mathbf{F}}_q)$ by Theorem 2.22.)

(c) Show that $(r-1)E(\mathbf{F}_q) = 0$.

(d) Show that $E(\mathbf{F}_q) \simeq \mathbf{Z}_{r-1} \oplus \mathbf{Z}_{r-1}$.

(e) Now suppose E' is an elliptic curve over $\mathbf{F}_q$ with $\#E'(\mathbf{F}_q) = (r+1)^2$ (where $q = r^2$). Show that $E'(\mathbf{F}_q) \simeq \mathbf{Z}_{r+1} \oplus \mathbf{Z}_{r+1}$.