PART I. ELLIPTIC CURVES

Contents

Some useful references

[1] I. Blake, G. Seroussi and N. Smart, *Elliptic curves in cryptography*, London Mathematical Society Lecture Note Series **265**, Cambridge University Press (1999)

[2] H. Cohen and G. Frey (eds.), *Handbook of elliptic and hyperelliptic curve cryptography*, Discrete Mathematics and its Applications **34**, Chapman & Hall/CRC (2005)

[3] N. Koblitz, *Algebraic aspects of cryptography*, Algorithms and Computation in Mathematics **3**, Springer-Verlag (1997)

[4] P. Nguyen, *Public-key cryptanalysis*, a chapter in I. Luengo, *Recent trends in cryptography*, Contemporary Mathematics series **477**, AMS-RSME (2009)

[5] J. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics **106**, Springer-Verlag (1986)

The most down-to-earth text is [3]. The standard reference on elliptic curves is [5], for which some experience with algebraic geometry is recommended (the first two chapters give a good introduction). The most up-to-date account is the extensive [2], of which a second edition will appear in the near future. Reference [4] is mainly about RSA instead of elliptic curve cryptography.

1. Introduction to elliptic curves

1.1. **Definition.** Throughout, let k be a field of characteristic not equal to 2 or 3, and let $\overline{k}$ be an algebraic closure. An *elliptic curve* E over k is a plane projective curve of the form

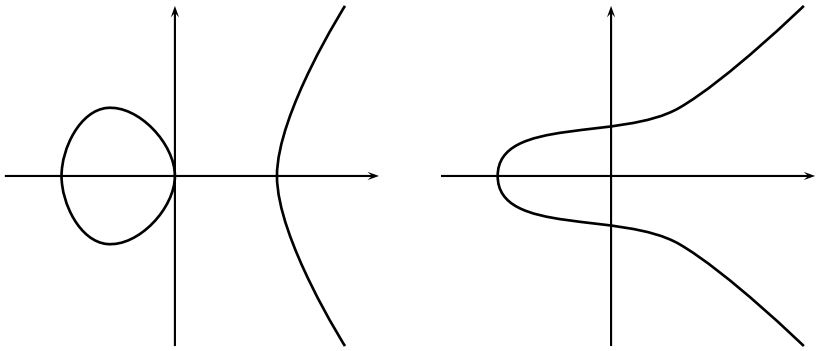
$$y^2z = x^3 + Axz^2 + Bz^3,$$

where $A, B \in k$ are such that $4A^3 + 27B^2 \neq 0$. By a *point* we always mean a point with coordinates in $\overline{k}$:

$$E = \{(x_0, y_0, z_0) \in \mathbb{P}^2_{\overline{k}} \,|\, y_0^2 z_0 = x_0^3 + Ax_0z_0^2 + Bz_0^3\}.$$

A point that can be written as (x_0, y_0, z_0) with $x_0, y_0, z_0 \in k$ is called a *rational point*. The set of rational points is denoted by $E(k)$. Similarly, for each intermediate field $k \subset k' \subset \overline{k}$, we have the set of *$k'$-rational points* $E(k')$. The point $(0, 1, 0)$ is the only point on the line $z = 0$. It is called *the point at infinity*, and we denote it by $\mathcal{O}$.

When $k = \mathbb{R}$, we can draw pictures. Two typical graphs are



depending on whether $x^3 + Ax + B$ has one resp. three real roots. The point $\mathcal{O}$ can be thought of lying infinitely far up north. When $k = \mathbb{C}$, the picture becomes two-dimensional (topologically spoken): the curve then has the structure of a *Riemann surface*. The topological picture is that of a torus (the surface of a donut), i.e. a Riemann surface of *genus* one. (We will make a digression on this in Section 1.5.)

Exercise 1.1. Prove that an elliptic curve never has singular points, i.e. points at which the three partial derivatives of $f(x, y, z) = y^2z - x^3 - Axz^2 - Bz^3$ vanish simultaneously. Show that over a field of characteristic 2, a curve defined by such an equation is always singular.

This implies that every point $(x_0, y_0, z_0) \in E$ has a well-defined tangent line

$$\frac{\partial f}{\partial x}(x_0, y_0, z_0) \cdot x + \frac{\partial f}{\partial y}(x_0, y_0, z_0) \cdot y + \frac{\partial f}{\partial z}(x_0, y_0, z_0) \cdot z = 0.$$

The point at infinity is an *inflection point*: its tangent line ($z = 0$) intersects the curve with multiplicity 3.

1.2. **The group law.** We will now endow E with a binary operator

$$\oplus : E \times E \to E,$$

whose construction is closely related to the geometry of E. For each pair of points $\mathcal{P}_1, \mathcal{P}_2$ in E, the composition $\mathcal{P}_1 \oplus \mathcal{P}_2$ is obtained as follows:

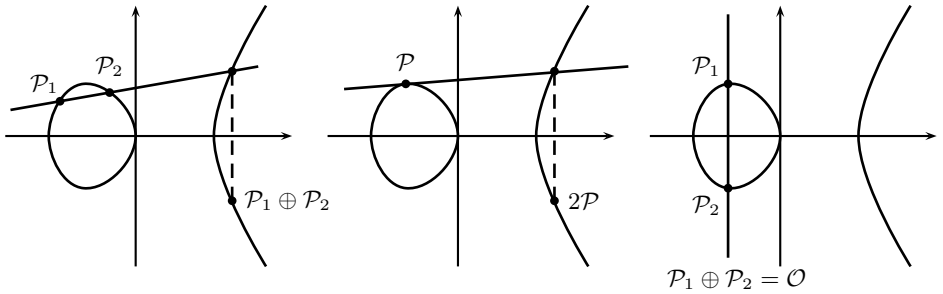
(1) let ℓ be the line connecting $\mathcal{P}_1$ and $\mathcal{P}_2$ (tangent line if $\mathcal{P}_1 = \mathcal{P}_2$), then ℓ intersects E in a third point $\mathcal{R}$ (counting multiplicities);
(2) let m be the line connecting $\mathcal{R}$ and $\mathcal{O}$ (tangent line if $\mathcal{R} = \mathcal{O}$), then m intersects E in a third point $\mathcal{Q}$ (counting multiplicities);
(3) then $\mathcal{P}_1 \oplus \mathcal{P}_2 = \mathcal{Q}$.

Exercise 1.2. Prove that $\oplus$ is a commutative operator, with respect to which $\mathcal{O}$ behaves as a neutral element, and with respect to which each point $\mathcal{P}$ has an inverse $-\mathcal{P}$.

It is less obvious that $\oplus$ is associative. The most down-to-earth proof is a long but straightforward calculation, using the explicit formulas below. In Sections 1.3 and 3.11, we will sketch two more conceptual proofs.

Theorem 1.3. *$E, \oplus$ is an abelian group, with $\mathcal{O}$ as neutral element.*

Note that if $\mathcal{R}$ is an affine point (x_0, y_0), then m is the line $y = y_0$, whose third point of intersection with E (besides $\mathcal{R}$ and $\mathcal{O}$) is $(x_0, -y_0)$. Thus, step (2) can be thought of as reflection over the x-axis. Here are pictures visualizing the group law for $k = \mathbb{R}$, in case $\mathcal{P}_1$ and $\mathcal{P}_2$ are two affine points in $E(\mathbb{R})$.



The same line of reasoning gives:

Lemma 1.4. *The inverse of an affine point $\mathcal{P} = (x_0, y_0)$ is the affine point $-\mathcal{P} = (x_0, -y_0)$.*

One can compute the following explicit formulas (do the exercise!):

Exercise 1.5. Let $\mathcal{P}_1 = (x_1, y_1)$ and $\mathcal{P}_2 = (x_2, y_2)$ be two affine points of E. Then

(1) if $x_1 \neq x_2$ then $\mathcal{P}_1 \oplus \mathcal{P}_2 = (x_3, y_3)$ with

$$\begin{aligned} x_3 &= \left(\tfrac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2; \\ y_3 &= -y_1 + \left(\tfrac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3). \end{aligned}$$

(2) if $x_1 = x_2$ then
   (a) if $y_1 = -y_2$ then $\mathcal{P}_1 \oplus \mathcal{P}_2 = \mathcal{O}$,
   (b) if $y_1 \neq -y_2$ then $2\mathcal{P}_1 = (x_3, y_3)$ with

$$\begin{aligned} x_3 &= \left(\tfrac{3x_1^2 + A}{2y_1}\right)^2 - 2x_1; \\ y_3 &= -y_1 + \left(\tfrac{3x_1^2 + A}{2y_1}\right)(x_1 - x_3). \end{aligned}$$

Note that if $\mathcal{P}_1, \mathcal{P}_2 \in E(k)$, then also $\mathcal{P}_1 \oplus \mathcal{P}_2 \in E(k)$. More generally, we have the important fact:

Theorem 1.6. *For each intermediate field $k \subset k' \subset \overline{k}$, we have that $E(k')$ is a subgroup of $E = E(\overline{k})$.*

Our main groups of interest will be the finite groups $E(\mathbb{F}_q)$, where E is an elliptic curve over a finite field $\mathbb{F}_q$ (where q is coprime to 6).

Exercise 1.7. The whizzkids are invited to play around with Magma, a computer algebra package. Unfortunately it is licensed, but for short computations (less than 20 seconds) one can use the demo `http://magma.maths.usyd.edu.au/calc/`. There is an online manual. The code

```
Fq := FiniteField(5^70);
A := Random(Fq); B := Random(Fq);
E := EllipticCurve([A,B]); #E;
```

outputs the number of rational points on a random elliptic curve over $\mathbb{F}_{5^{70}}$. Note that it goes very fast (increase the field size to push the limit)! The code

```
E := EllipticCurve([2,13]);
P := E ! [2,5,1];
for k in [1..12] do print Denominator((k*P)[1]); end for;
```

defines the elliptic curve $E : y^2 = x^3 + 2x + 13$ over $\mathbb{Q}$ along with the point $\mathcal{P} = (2, 5, 1)$. It then computes $\mathcal{P}, 2\mathcal{P}, \ldots, 12\mathcal{P}$ and prints the denominator of the x-coordinate. What do you notice? Check your hypothesis for other pairs $E, \mathcal{P}$. For a few lines of comment on this phenomenon, see Exercise 1.11 and below.

1.3. **A geometric explanation for associativity.** Proving associativity using the above explicit formulas is not very enlightening. With a little more machinery, one can do better. A nice argument uses the *ninth point lemma*. Although it is tedious to turn it into a rigorous proof (we will only give a sketch), it gives a first idea about *why* associativity should hold.

Theorem 1.8 (ninth point lemma, generic case)**.** *Let two projective curves of degree* 3 *(possibly reducible) have* 9 *distinct points $\mathcal{P}_1, \ldots, \mathcal{P}_9$ in common. Then any other projective curve of degree* 3 *(possibly reducible) containing $\mathcal{P}_1, \ldots, \mathcal{P}_8$, automatically contains $\mathcal{P}_9$.*

Proof (rough idea): The space of homogeneous polynomials of degree 3 in variables x, y, z is 10-dimensional (indeed, there are 10 monomials

$$x^3, x^2y, x^2z, xy^2, xyz, xz^2, y^3, y^2z, yz^2, z^3$$

to be equipped with a coefficient). This means that the space of plane projective curves of degree 3 can be identified with $\mathbb{P}^9_{\overline{k}}$. Each of the 9 conditions 'the curve contains $\mathcal{P}_i$' corresponds to a hyperplane. These hyperplanes cannot intersect in a single point, since there exist at least two distinct curves satisfying all nine conditions. This already proves that at least one of the conditions must be a consequence of the eight others. The complete proof is then about showing that 8 of these conditions are always independent. ∎

Let $\mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_3 \in E$ and write $\mathcal{P}_{12} = \mathcal{P}_1 \oplus \mathcal{P}_2$, $\mathcal{P}_{23} = \mathcal{P}_2 \oplus \mathcal{P}_3$, $\mathcal{P}_{(12)3} = \mathcal{P}_{12} \oplus \mathcal{P}_3$ and $\mathcal{P}_{1(23)} = \mathcal{P}_1 \oplus \mathcal{P}_{23}$. Then the aim is to show that $\mathcal{P}_{(12)3} = \mathcal{P}_{1(23)}$. Here's how it goes (make a picture!). Let ℓ_{12} be the line connecting $\mathcal{P}_1$ and $\mathcal{P}_2$ and let m_{12} be the line connecting $-\mathcal{P}_{12}$ and $\mathcal{P}_{12}$. Similarly, define lines ℓ_{23}, m_{23}, $\ell_{(12)3}$, $m_{(12)3}$, $\ell_{1(23)}$ and $m_{1(23)}$. Our elliptic curve E and the (reducible) curve $\ell_{12} \cup m_{23} \cup \ell_{(12)3}$

intersect in the nine points

$$\underbrace{\mathcal{P}_1, \mathcal{P}_2, -\mathcal{P}_{12}}_{E \cap \ell_{12}}, \quad \underbrace{\mathcal{O}, -\mathcal{P}_{23}, \mathcal{P}_{23}}_{E \cap m_{23}}, \quad \underbrace{\mathcal{P}_{12}, \mathcal{P}_3, -\mathcal{P}_{(12)3}}_{E \cap \ell_{(12)3}}.$$

Suppose for ease that these are all distinct, to meet the hypotheses of Theorem 1.8. Now E intersects $\ell_{23} \cup m_{12} \cup \ell_{1(23)}$ in the nine points

$$\underbrace{\mathcal{P}_2, \mathcal{P}_3, -\mathcal{P}_{23}}_{E \cap \ell_{23}}, \quad \underbrace{\mathcal{O}, -\mathcal{P}_{12}, \mathcal{P}_{12}}_{E \cap m_{12}}, \quad \underbrace{\mathcal{P}_1, \mathcal{P}_{23}, -\mathcal{P}_{1(23)}}_{E \cap \ell_{1(23)}}.$$

We have an overlap of at least 8 points. Therefore, also the ninth points must be equal. Thus $-\mathcal{P}_{(12)3} = -\mathcal{P}_{1(23)}$, from which associativity follows.

Exercise 1.9. Verify that the construction of $\oplus$, and the proof (sketch in the case of associativity) that $E, \oplus$ is an abelian group, only uses that E is a nonsingular cubic. Thus *any* nonsingular cubic $C \subset \mathbb{P}^2_k$ and *any* choice of $\mathcal{O} \in C$ give rise to an abelian group $C, \oplus$ in which $\mathcal{O}$ serves as neutral element (even if $\operatorname{char} k = 2, 3$). Give a geometric construction for the inverse of a point $\mathcal{P} \in C$ (in general it is no longer the third point of intersection with C of the line connecting $\mathcal{P}$ and $\mathcal{O}$).

One can prove that if $\operatorname{char} k \neq 2, 3$ then for every nonsingular cubic C/k and every point $\mathcal{O}_C \in C(k)$, there is an elliptic curve E and a *k-isomorphism* $C \to E$ such that $\mathcal{O}_C$ is mapped to $\mathcal{O}$. If you are not familiar with this notion: the conclusion is that the above construction does not provide new groups.

1.4. **Elliptic curves over $\mathbb{Q}$.** Elliptic curves are among the most enigmatic and intriguing objects in the mathematical world. They have shown up in various, sometimes truly surprising branches of pure and applied mathematics. In this and the two next sections, we will make a cultural detour that is devoted to the ubiquity of elliptic curves. I will mainly do some cheap statement-dropping, without references (see google, wikipedia, and the references in front).

If E is an elliptic curve over $\mathbb{Q}$ then, due to a theorem of Mordell (1922),

$$E(\mathbb{Q}) \cong T \times \mathbb{Z}^r, \qquad \text{for some } r \in \mathbb{Z}_{\geq 0},$$

where T is the torsion subgroup of $E(\mathbb{Q})$. A deep theorem by Mazur (1977) gives a precise description of the possible structures of T, in particular one has $\#T \leq 16$.

Opposed to that, the *algebraic rank* r is a big question mark. For instance, it is unknown whether r can be arbitrarily large or not. The current record is a rank 28 curve that was discovered by Elkies (2006). But the most famous open problem concerning the rank is certainly the *Birch & Swinnerton-Dyer conjecture*. Namely, there is also an analytic way of associating a rank to an elliptic curve over $\mathbb{Q}$ (this is more complicated, it is the order of vanishing at $s = 1$ of a certain complex meromorphic function). The conjecture states that this analytic rank is always equal to the algebraic rank. The Clay Mathematics Institute offers $\$1,000,000$ to the first person proving it (at work!).

A surprising appearance of elliptic curves over $\mathbb{Q}$ was made in Wiles' 1994 proof of *Fermat's last theorem*, the main line of thought being that a counterexample

$a^p + b^p = c^p$ can be used to construct an elliptic curve[1]

$$y^2 = x^3 - 432(a^{2p} + a^p b^p + b^{2p})x - 432(8a^{3p} + 12a^{2p}b^p - 12a^p b^{2p} - 8b^{3p}),$$

which has impossible properties (it cannot be *modular*, thereby violating the nowadays proven Taniyama-Weil conjecture).

Another remarkable role is played in partial breakthroughs concerning *Hilberts tenth problem*, which is about finding an algorithm that decides whether a given polynomial $f \in R[x_1, \ldots, x_n]$ has a zero in R^n or not (where R is a ring). This was proven undecidable (i.e. no such algorithm can exist) for $R = \mathbb{Z}$ by Matijasevic in 1970, but it is still an open problem over $R = \mathbb{Q}$.

Yet another application of elliptic curves over $\mathbb{Q}$ appears in the *congruent number problem*: given a positive integer N, does there exist a right triangle with rational sides whose area is N? For instance, 6 is a congruent number, due to the well-known 3-4-5 triangle.

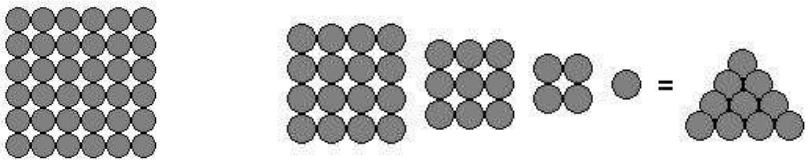
Exercise 1.10. Show that N is a congruent number if and only if the elliptic curve

$$y^2 = x^3 - N^2 x$$

has a $\mathbb{Q}$-rational point different from $\mathcal{O}, (0,0,1), (\pm N, 0, 1)$. For a hint, see this footnote[2].

Tunnell (1983) gave a fast algorithm to determine whether a given integer is congruent or not, but the proof of correctness assumes the conjecture of Birch and Swinnerton-Dyer.

We end this section with the following cannonball riddle. Is it possible to select n cannonballs such that they can be arranged in a plane square, but also in a pyramid with square base? For instance, 36 cannonballs can be arranged in a square, 30 cannonballs can be arranged in a pyramid (pictures are taken from Ed Eikenberg's webpage):



However, it's easy to see that 30 cannonballs cannot be arranged in a square, and neither can 36 cannonballs be arranged in a pyramid.

Exercise 1.11. Show that this boils down to finding integral solutions to

$$E: \ y^2 = \frac{1}{6}x(x+1)(2x+1).$$

Although this does not meet our definition of an elliptic curve, the whole theory works as well for this and more general types of cubics, see Exercise 1.9. But if you wish, you can do an affine change of variables to obtain $y^2 = x^3 - \frac{1}{36}x$, where now we are looking for rational solutions whose denominators are divisors of 3.

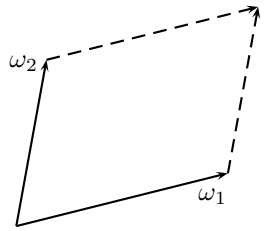
---

[1] In fact, $y^2 = x(x - a^p)(x + b^p)$ is a much simpler and more well-known form. A horizontal translation $x \leftarrow x - (b^p - a^p)/3$ then takes it to the form $y^2 = x^3 + Ax + B$.

[2] If a-b-c is a right triangle (where c is the length of the hypothenuse), then let $x = (c/2)^2$ and $y = (b^2 - a^2)c/8$.

From Exercise 1.7, you may have experienced that points with small denominators are rare; this can be made precise (Siegel's theorem, 1929). In fact, one can prove that apart from the trivial solutions $n = 0$, $n = 1$, the only solution is $n = 4900$, corresponding to the point $(24, 70)$ on E, which can be realized as $(0, 0) \oplus 2(1, 1)$.

1.5. **Elliptic curves over $\mathbb{C}$.** Over $\mathbb{C}$, the group structure has a very explicit description. Let ω_1, ω_2 be generators of $\mathbb{C}$ as an $\mathbb{R}$-vector space, and let $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ (this is called a *lattice*). The group $\mathbb{C}/L$ has the topological structure of a parallelogram



of which the opposite sides are identified. By folding, one sees that $\mathbb{C}/L$ is homeomorphic to a torus. Now there always exists a natural bijective map (called the Weierstrass $\wp$-map) sending $\mathbb{C}/L$ to an elliptic curve E over $\mathbb{C}$. This bijection is in fact an isomorphism of groups! Conversely, every elliptic curve E over $\mathbb{C}$ arises as the image of some $\mathbb{C}/L$.

Exercise 1.12. Using the above, prove Theorem 2.7 for elliptic curves over $\mathbb{C}$.

A 19^{th} century definition for an elliptic curve over $\mathbb{C}$ is an equation of the form

$$y^2 = h(x),$$

with $h(x) \in \mathbb{C}[x]$ squarefree of degree 3 or 4.

Exercise 1.13. Prove that such an equation is always algebraically transformable to the form $y^2 = x^3 + Ax + B$. By an algebraic transformation, we mean a substitution of the form $x \leftarrow g_1(x, y)$, $y \leftarrow g_2(x, y)$ that can be undone by a similar substitution. Here, g_1 and g_2 are rational functions with coefficients in $\mathbb{C}$.

An *elliptic integral* is an integral of the form

$$\int_a^b R(x, y)dx$$

where $R(x, y)$ is a rational function in x and $y = \sqrt{h(x)}$. Such integrals appear in a variety of applications, and are generally hard to compute symbolically.

Exercise 1.14. Consider an ellipse $x^2/a^2 + y^2/b^2 = 1$ (suppose $a \geq b$). Prove that the arc length of its upper half part is given by the elliptic integral

$$a \int_{-1}^{1} \frac{1 - k^2x^2}{\sqrt{(1 - x^2)(1 - k^2x^2)}} dx,$$

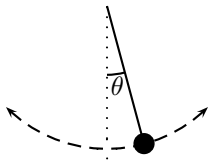
where $k^2 = 1 - b^2/a^2$. Hence the name elliptic integral, **hence the name elliptic curve**!

Another appearance of elliptic integrals is in the computation of the *arithmetic-geometric mean* of two numbers $a, b \in \mathbb{R}_{\geq 0}$, $a \geq b > 0$. The arithmetic mean $a_1 = (a+b)/2$ and the geometric mean $b_1 = \sqrt{ab}$ may of course be different, but one has $0 \leq a_1 - b_1 \leq (a-b)/2$ (verify this!). Hence repeating this process over and over again, one obtains two sequences $a, a_1, a_2, \ldots$ and $b, b_1, b_2, \ldots$ converging to the same number. This is the arithmetic-geometric mean $M(a,b)$ of a and b. Remarkably enough, $M(a,b)$ can be expressed in terms of a and b using an elliptic integral. One instance of this is

$$\frac{\pi}{2} M(\sqrt{2}, 1) = \int_0^1 \frac{1}{\sqrt{1-x^4}} dx,$$

a formula due to Gauss (1799).

Elliptic integrals also appear in classical physics, for instance in describing the pendulum motion



obeying $d^2\theta/dt = -k^2 \sin\theta$ (t is the time). One can verify that $\tan\theta$ and t are related through an elliptic integral. In school books, this is usually circumvented by the approximation $\sin\theta \approx \theta$.

1.6. **Elliptic curves over finite fields.** This is the third kind of base fields over which elliptic curves pop up in a variety of applications. The number one application is of course elliptic curve cryptography: this course is devoted to it. Further on, we will also spend some words on two other applications that have cryptographic relevance:

(1) a method due to Lenstra for factoring integers (1987),
(2) a proof by Maurer & Wolf of the equivalence between the Diffie-Hellman problem (DHP) and the discrete logarithm problem (DLP), modulo a plausible conjecture (2000).

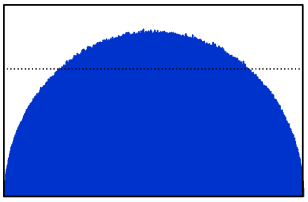
It should be emphasized that both applications are really surprising: although connected with *cryptography*, these problems have a priori nothing to do with *elliptic curve cryptography*.

There are also many fascinating open problems concerning elliptic curves over finite fields. An important example is *the Sato-Tate conjecture*, although Taylor et al. recently proved it in virtually all cases (2008). Take an equation

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

with $A, B \in \mathbb{Z}_{\geq 1}$. Then modulo any prime $p \neq 2, 3$ that does not divide $4A^3 + 27B^2$, this equation defines an elliptic curve over $\mathbb{F}_p$. We will see below that its number of rational points is contained in $[p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p}]$. Hence subtracting $p+1$ and dividing by $2\sqrt{p}$ results in an element $t_p \in [-1, 1]$. If p varies, then how is t_p distributed across this interval? The Sato-Tate conjecture states that, modulo some well-understood exceptions, the t_p are distributed according to the semicircular measure $\frac{2}{\pi}\sqrt{1-t^2}dt$. Here is some experimental evidence for $y^2 =$

$x^3 + 314159x + 271828$, namely a histogram for all primes $< 2^{27}$ (taken from a paper by Kedlaya-Sutherland):



2. Torsion on elliptic curves

2.1. **m-torsion subgroups.** For any $m \in \mathbb{Z}_{\geq 1}$, define

$$E[m] = \{\mathcal{P} \in E \,|\, m\mathcal{P} = \mathcal{O}\}\,.$$

Exercise 2.1. Prove that for coprime m, m', one has $E[mm'] \cong E[m] \times E[m']$.

Exercise 2.2. Prove that $\#E[1] = 1$, that $\#E[2] = 4$ and that $\#E[3] = 9$.

For the latter, you should make use of the following classical result:

Theorem 2.3 (Hessian criterion)**.** *Let $f(x,y,z) \in k[x,y,z]$ define a nonsingular curve C in $\mathbb{P}^2_k$. A point $\mathcal{P} \in C$ is an inflection point if and only if*

$$H_f = \det \begin{pmatrix} \frac{\partial^2 f}{\partial x^2} & \frac{\partial^2 f}{\partial x \partial y} & \frac{\partial^2 f}{\partial x \partial z} \\ \frac{\partial^2 f}{\partial x \partial y} & \frac{\partial^2 f}{\partial y^2} & \frac{\partial^2 f}{\partial y \partial z} \\ \frac{\partial^2 f}{\partial x \partial z} & \frac{\partial^2 f}{\partial y \partial z} & \frac{\partial^2 f}{\partial z^2} \end{pmatrix}$$

vanishes at $\mathcal{P}$.

Proof. The vanishing of H_f at $\mathcal{P}$ is not affected by projective transformations, so we may assume that $\mathcal{P} = (0,0,1)$ and that the corresponding tangent line is $y = 0$. Hence we may write

$$f(x,y,1) = x^2 \cdot g(x) + y \cdot h(x,y).$$

Write $x^2 \cdot g(x) = a_2 x^2 + a_3 x^3 + \ldots$ and $h(x,y) = b_{00} + b_{10}x + b_{01}y + \ldots$ Note that $b_{00} \neq 0$ (since C is nonsingular) and that $a_2 = 0$ if and only if $\mathcal{P}$ is an inflection point. Now $H_f(\mathcal{P})$ is

$$\det \begin{pmatrix} 2a_2 & b_{10} & 0 \\ b_{10} & 2b_{01} & b_{00} \\ 0 & b_{00} & 0 \end{pmatrix} = -2b_{00}^2 a_2$$

and the criterion follows. ∎

Note that the exercise implies $E[2] \cong \mathbb{Z}/(2) \times \mathbb{Z}/(2)$ and $E[3] \cong \mathbb{Z}/(3) \times \mathbb{Z}/(3)$.

2.2. **Division polynomials.** Let us have another look at the doubling formulas from Exercise 1.5(2.b):

$$\begin{aligned} x_3 &= \left(\tfrac{3x_1^2 + A}{2y_1}\right)^2 - 2x_1; \\ y_3 &= -y_1 + \left(\tfrac{3x_1^2 + A}{2y_1}\right)(x_1 - x_3). \end{aligned}$$

We cannot evaluate these formulas at points where $y_1 = 0$. This is not surprising, since the affine points for which $y_1 = 0$ double to $\mathcal{O}$. But it is nice that the formulas

work everywhere else, i.e. the exceptional points are *exactly those that double to* $\mathcal{O}$. Also note that we can rewrite

$$x_3 \quad = \quad \left(\frac{3x_1^2+A}{2y_1}\right)^2 - 2x_1 \quad = \quad \frac{(3x_1^2+A)^2}{(4x_1^3+4Ax_1+4B)} - 2x_1 \qquad \in k(x_1)$$

using the equation of the curve. That makes sense:

Exercise 2.4. Let $\mathcal{P} \in E$ and let $m \in \mathbb{Z}_{\geq 1}$ such that $m\mathcal{P} \neq \mathcal{O}$. Then the x-coordinate of $m\mathcal{P}$ only depends on the x-coordinate of $\mathcal{P}$.

General facts from commutative algebra then guarantee that one can write the x-coordinate of $m\mathcal{P}$ as a rational function in the x-coordinate of $\mathcal{P}$.

One can combine the doubling formulas with the addition formulas to obtain the following tripling formulas (not an attractive job!):

$$\begin{array}{rcl} x_3 & = & \frac{x(3x_1^4+6Ax_1^2+12Bx_1-A^2)^2-8(x_1^3+Ax+B)(x^6+5Ax^4+20Bx^3-5A^2x^2-4ABx-8B^2-A^3)}{(3x_1^4+6Ax_1^2+12Bx_1-A^2)^2} \\ y_3 & = & y_1 \cdot \frac{\text{horrible degree 12 polynomial in } x_1}{(3x_1^4+6Ax_1^2+12Bx_1-A^2)^3} \end{array}$$

Note that again $x_3 \in k(x_1)$. We cannot evaluate these formulas whenever $3x_1^4 + 6Ax_1^2+12Bx_1-A^2 = 0$. If you did Exercise 2.2, you might recognize this polynomial: its roots are the four x-coordinates of the eight affine 3-torsion points. Thus, the affine points at which these tripling formulas cannot be evaluated are *exactly those that triple to* $\mathcal{O}$.

The story continues. One can compute formulas for $(x_3, y_3) = m(x_1, y_1)$ for $m = 4, 5, \ldots$ The formulas are excruciating, but at each step we end up with an expression

$$x_3 = \frac{\chi_m(x_1)}{\phi_m(x_1)} \qquad \in k(x_1)$$

whose denominator $\phi_m(x_1)$ becomes zero *exactly at the points whose* m*-uple is* $\mathcal{O}$. Of course, there is a systematic way of proving this. A guideline can be found in Silverman's book [5, Cor.III.6.4(b),Ex.III.3.7].

Definition 2.5. *The squarefree part* $\psi_m \in \mathbb{Z}[A, B, x_1]$ *of* ϕ_m *is called the* m^{th} *division polynomial.*

One can prove the following facts about ψ_m:

(1) if m is odd, then
$$\psi_m = m x_1^{(m^2-1)/2} + \ldots$$
(2) if m is even, then
$$\psi_m = (x_1^3 + Ax_1 + B) \cdot \left(m x_1^{(m^2-4)/2} + \ldots \right).$$
(3) for each field k of characteristic ($\neq 2, 3$) not dividing m, and each pair $A, B \in k$ such that $4A^3 + 27B^2 \neq 0$, the natural specialization of ψ_m to a polynomial in $k(x_1)$ remains squarefree.

Moreover, there is an efficient recursive method for computing ϕ_m (and hence ψ_m).

Exercise 2.6. Using the above information, prove part (1) of the following theorem.

Theorem 2.7. (1) *If* m *is not a multiple of the field characteristic, then*
$$E[m] \cong \mathbb{Z}/(m) \times \mathbb{Z}/(m).$$

(2) *In characteristic $p > 0$, one has either $E[p^r] \cong \mathbb{Z}/(p^r)$ (for all $r \geq 1$) or $E[p^r] = 0$ (for all $r \geq 1$).*

If $E[p^r] = 0$ holds (which is rare), then E is called *supersingular*.

Exercise 2.6 is not entirely honest, as one typically needs Theorem 2.7 to prove the above results on division polynomials. In any case, an interesting corollary is:

Exercise 2.8. Prove that for an elliptic curve E over a finite field $\mathbb{F}_q$ ($\gcd(q, 6) = 1$), the group $E(\mathbb{F}_q)$ has at most two generators. More precisely:

$$E(\mathbb{F}_q) \cong \mathbb{Z}/(k) \times \mathbb{Z}/(\ell)$$

with $\ell \mid k$.

Later on, we will see that additionally $q \equiv 1 \bmod \ell$ and $k\ell \in [q + 1 - 2\sqrt{q}, q + 1 + 2\sqrt{q}]$.

Exercise 2.9. In Magma (see Exercise 1.7), experiment with the following code

```
Q<A,B> := FunctionField(Rationals(),2);
E := EllipticCurve([A,B]);
psi := DivisionPolynomial(E,4);
psi; Factorization(psi);
```

which first defines a universal elliptic curve $y^2 = x^3 + Ax + B$ over $\mathbb{Q}(A, B)$ (this allows us to work symbolically), and then prints ψ_4 along with its factorization (the latter omits leading coefficients). Try to see what happens with ψ_5 in characteristic 5, and with ψ_7 in characteristic 7.

3. Functions and divisors

3.1. **Divisors of functions.** The *function field* $\overline{k}(E)$ of an elliptic curve $E : y^2 = x^3 + Ax + B$ over k is the field of fractions of

$$\frac{\overline{k}[x, y]}{(y^2 - x^3 - Ax - B)}.$$

A *function* on E is an element of the function field. A *divisor* on E is an element of the free abelian group generated by the points of E:

$$\mathrm{Div}(E) = \left\{ \sum_{\mathcal{P} \in E} n_{\mathcal{P}}[\mathcal{P}] \;\middle|\; n_{\mathcal{P}} = 0 \text{ for all but a finite number of } \mathcal{P} \right\}.$$

The *degree* of a divisor is the sum of the $n_{\mathcal{P}}$. If all $n_{\mathcal{P}} \geq 0$, then the divisor is called *effective*. The finite set of points $\mathcal{P} \in E$ for which $n_{\mathcal{P}} \neq 0$ is called the *support* of the divisor. The divisors of degree 0 form a subgroup of $\mathrm{Div}(E)$, denoted $\mathrm{Div}^0(E)$.

Now to a function $\varphi \in \overline{k}(E)^\times$, one can associate a divisor as follows: write

$$\varphi = \frac{g(x, y)}{h(x, y)}$$

as a quotient of two nonzero polynomials (nonzero modulo $y^2 - x^3 - Ax - B$, that is). Homogenize this quotient with respect to a third variable z, such that numerator and denominator have the same degree d (by adjoining additional factors z if necessary). By Bezout's theorem, the numerator defines a (possibly reducible)

projective curve that intersects E in $3d$ points (counting multiplicities). This defines an effective degree $3d$ divisor

$$D_+ = \sum_{\mathcal{P} \in E} (\text{intersection multiplicity at } \mathcal{P})[\mathcal{P}].$$

Similarly, the denominator defines an effective degree $3d$ divisor D_-. Then the divisor of φ is

$$\text{div}\varphi = D_+ - D_-,$$

which is of degree 0. This is well-defined, i.e. it does not depend on the choice of $g(x, y)$ and $h(x, y)$.

Remark 3.1. Filling in the details of the above exposure requires a good understanding of the notion *intersection multiplicity*, which is not entirely trivial. For now, the intuitive idea suffices (in many cases, we will have $d = 1$ where the notion is clear).

Write

$$\text{div}\varphi = D_0 - D_\infty$$

as a difference of effective divisors, such that D_0 and D_∞ have minimal degree (note that not necessarily $D_0 = D_+$ and $D_\infty = D_-$: there might be some cancellation). Points in the support of D_0 are called *zeroes* of φ. Points in the support of D_∞ are called *poles* of φ.

Exercise 3.2. Consider the elliptic curve $E : y^2 = x^3 + 2x + 1$ over $\mathbb{Q}$. Show that $\text{div}(x - 1) = [(1, 2)] + [(1, -2)] - 2[\mathcal{O}]$.

If $\mathcal{P}$ is not a pole of φ, then we can consider the *evaluation* $\varphi(\mathcal{P}) \in \overline{k}$. Intuitively, if

$$\varphi = \frac{g(x, y)}{h(x, y)}$$

and $\mathcal{P} = (x_0, y_0)$, then $\varphi(\mathcal{P}) = f(x_0, y_0)/g(x_0, y_0)$. (You can take the homogenized version to evaluate at $\mathcal{O} = (0, 1, 0)$.) But there are some subtleties due to cancellation:

Example 3.3. Consider $E : y^2 = x^3 - x$ over $\mathbb{Q}$, and let $\varphi = \frac{x}{y}$. Then

$$\text{div}\varphi = 2[(0, 0)] + [\mathcal{O}] - [(0, 0)] - [(1, 0)] - [(-1, 0)] = [(0, 0)] + [\mathcal{O}] - [(1, 0)] - [(-1, 0)].$$

In particular, φ has no pole at $\mathcal{P} = (0, 0)$, so it should be possible to compute $\varphi(\mathcal{P})$, although $\frac{0}{0}$ makes no sense. But we can rewrite $\varphi = \frac{y}{x^2 - 1}$ (verify this!), and now we can indeed compute $\varphi(\mathcal{P}) = \frac{0}{-1} = 0$. It can be proven that such a trick always applies.

One can also *evaluate* φ *at divisors* whose support contains no zeroes or poles of φ. Write

$$D = \sum_{\mathcal{P} \in E} n_{\mathcal{P}}[\mathcal{P}],$$

then

$$\varphi(D) = \prod_{\mathcal{P} \in E} \varphi(\mathcal{P})^{n_{\mathcal{P}}} \qquad (\text{if } D = 0 \text{ then } \varphi(D) = 1).$$

We will now formulate the most fundamental tool in dealing with functions and divisors, namely the Riemann-Roch theorem (without proof). To each divisor D on E, associate its *Riemann-Roch space*

$$\mathcal{L}(D) = \left\{\varphi \in \overline{k}(E)^\times \,|\, \mathrm{div}\varphi + D \text{ is effective}\right\} \cup \{0\}.$$

This is a $\overline{k}$-vector space (again, this is not surprising, but again, there are some subtleties in proving this due to cancellation).

Theorem 3.4 (Riemann-Roch for elliptic curves)**.** *For each divisor D on E, the Riemann-Roch space $\mathcal{L}(D)$ is finite-dimensional. Moreover,*

$$\dim \mathcal{L}(D) = \deg D + \dim \mathcal{L}(-D).$$

Exercise 3.5. Use the Riemann-Roch theorem to prove the following facts:

(1) if $\deg D < 0$, then $\mathcal{L}(D) = 0$,
(2) if $\deg D > 0$, then $\dim \mathcal{L}(D) = \deg D$,
(3) if $\deg D = 0$, then $\dim \mathcal{L}(D) \in \{0, 1\}$,
(4) if $D = 0$, then $\dim \mathcal{L}(D) = 1$.

For this, the following obvious property can be useful: for any $D \in \mathrm{Div}(E)$ and any $\mathcal{P} \in E$, one has $\mathcal{L}(D) \subset \mathcal{L}(D + [\mathcal{P}])$.

Exercise 3.6. Prove that if $\mathrm{div}\varphi = \mathrm{div}\varphi'$, then $\varphi = c\varphi'$ for some $c \in \overline{k}^\times$.

Exercise 3.7. Prove that if $D \in \mathrm{Div}^0(E)$, then $\varphi(D)$ only depends on $\mathrm{div}\varphi$ and D.

3.2. **The divisor class group of degree** 0**.** We begin with the following observation.

Exercise 3.8. Show that the map $\mathrm{div} : \overline{k}(E)^\times \to \mathrm{Div}^0(E) : \varphi \mapsto \mathrm{div}\varphi$ is a morphism of groups.

The image of this map is called the subgroup of *principal divisors*, denoted $\mathrm{Prin}(E)$. Two divisors are called *linearly equivalent* if their difference is a principal divisor.

Exercise 3.9. Let $\mathcal{P}_1, \mathcal{P}_2 \in E$, not necessarily distinct. Prove that $[\mathcal{P}_1] + [\mathcal{P}_2]$ is linearly equivalent to $[\mathcal{P}_1 \oplus \mathcal{P}_2] + [\mathcal{O}]$.

Exercise 3.10. Use the foregoing exercise to prove that every divisor $D \in \mathrm{Div}^0(E)$ is linearly equivalent with a divisor of the form $[\mathcal{P}] - [\mathcal{O}]$. To this end, first reduce D to a divisor of the form $D' - (\deg D')[\mathcal{O}]$, where D' is an effective divisor.

Consider the quotient group

$$\mathrm{Pic}^0(E) = \frac{\mathrm{Div}^0(E)}{\mathrm{Prin}(E)}$$

of equivalence classes of divisors of degree 0.

Theorem 3.11. *The map*

$$E \to \mathrm{Pic}^0(E) : \mathcal{P} \mapsto [\mathcal{P}] - [\mathcal{O}]$$

is an isomorphism of groups.

PROOF. Exercise 3.9 can be rephrased as

$$[\mathcal{P}_1] - [\mathcal{O}] \ + \ [\mathcal{P}_2] - [\mathcal{O}] \ \sim \ [\mathcal{P}_1 \oplus \mathcal{P}_2] - [\mathcal{O}],$$

which implies that the map is a group homomorphism. By Exercise 3.10, it is surjective. So it remains to prove injectivity. Therefore, we need to show that a divisor of the form $[\mathcal{P}] - [\mathcal{O}]$ is never the divisor of a function, unless $\mathcal{P} = \mathcal{O}$. This follows immediately from the Riemann-Roch theorem: such a function would be contained in $\mathcal{L}([\mathcal{O}])$ which is 1-dimensional and hence generated by the constant function 1. In particular, the divisor of this function would be 0, hence $\mathcal{P} = \mathcal{O}$. ■

In fact, one can alter the point of view and *define* our binary operator $\oplus$ as the operator corresponding to $+$ on $\mathrm{Pic}^0(E)$ under the above bijection. As such, one gets associativity for free!

The description of $E, \oplus$ as a divisor class group is the modern way to go. It is very flexible. For instance, we no longer need to restrict to cubics: it makes sense to consider $\mathrm{Pic}^0(C)$ for nonsingular curves C of higher degree. In that case, $\mathrm{Pic}^0(C)$ will no longer be in a natural bijection with C itself, but with a higher-dimensional object called the *Jacobian variety* of C (the dimension will be the genus of C).

3.3. **The Weil pairing.** We have the following result.

Lemma 3.12. *Let E/k be an elliptic curve and let $\mathcal{P} \in E$. Then for any $m \in \mathbb{Z}_{\geq 1}$ there exists a function $\varphi_{m,\mathcal{P}}$ on E such that* $\mathrm{div}\varphi_{m,\mathcal{P}} = m[\mathcal{P}] - [m\mathcal{P}] - (m-1)[\mathcal{O}]$.

PROOF. This is obvious from Theorem 3.11, which implies that $m([\mathcal{P}] - [\mathcal{O}])$ and $[m\mathcal{P}] - [\mathcal{O}]$ are linearly equivalent. We will give a more constructive proof.

We may assume that $\mathcal{P} \neq \mathcal{O}$, otherwise one can take $\varphi = 1$. Similarly, if $m = 1$ then $\varphi = 1$ will do. Now note that if $m, n \in \mathbb{Z}_{\geq 1}$, and $\varphi_{m,\mathcal{P}}$ and $\varphi_{n,\mathcal{P}}$ are functions with divisors

$$m[\mathcal{P}] - [m\mathcal{P}] - (m-1)[\mathcal{O}] \quad \text{and} \quad n[\mathcal{P}] - [n\mathcal{P}] - (n-1)[\mathcal{O}]$$

respectively, then

$$\text{(1)} \quad \mathrm{div}\left(\varphi_{m,\mathcal{P}} \cdot \varphi_{n,\mathcal{P}} \cdot \frac{\ell_{m\mathcal{P},n\mathcal{P}}}{m_{(m+n)\mathcal{P}}}\right) = (m+n)[\mathcal{P}] - [(m+n)\mathcal{P}] - (m+n-1)[\mathcal{O}].$$

Here, $\ell_{m\mathcal{P},n\mathcal{P}}$ is the line connecting $m\mathcal{P}$ and $n\mathcal{P}$, and $m_{(m+n)\mathcal{P}}$ is

(1) the vertical line through $(m+n)\mathcal{P}$ if $(m+n)\mathcal{P} \neq \mathcal{O}$,
(2) the line $z = 0$ if $(m+n)\mathcal{P} = \mathcal{O}$.

(It is straightforward how the quotient can be considered as an element of $\overline{k}(E)^\times$.) The theorem follows by applying (1) inductively. ■

Corollary 3.13. *If $\mathcal{P}$ is an m-torsion point, then* $\mathrm{div}\varphi_{m,\mathcal{P}} = m[\mathcal{P}] - m[\mathcal{O}]$.

For any $m \in \mathbb{Z}_{\geq 0}$, not divisible by $\mathrm{char}\, k$, the *Weil pairing* of level m on E is then defined as the map

$$e_m : E[m] \times E[m] \to \overline{k}^\times : (\mathcal{P}, \mathcal{Q}) \mapsto \begin{cases} 1 \text{ if } \mathcal{P} = \mathcal{Q},\ \mathcal{P} = \mathcal{O} \text{ or } \mathcal{Q} = \mathcal{O}, \\ \frac{\varphi_{m,\mathcal{P}}([\mathcal{Q}]-[\mathcal{O}])}{\varphi_{m,\mathcal{Q}}([\mathcal{P}]-[\mathcal{O}])} \text{ if } \mathcal{P} \neq \mathcal{Q}. \end{cases}$$

Note that, by Exercise 3.7, this does not depend on the choice of $\varphi_{m,\mathcal{P}}$ and $\varphi_{m,\mathcal{Q}}$.

One can prove the following facts about the Weil pairing:

Theorem 3.14. (1) *e_m takes values in the m^{th} roots of unity of $\overline{k}$,*

(2) *it is* bilinear*, meaning that*

$$e_m(\mathcal{P}_1 \oplus \mathcal{P}_2, \mathcal{Q}) = e_m(\mathcal{P}_1, \mathcal{Q}) e_m(\mathcal{P}_2, \mathcal{Q}) \quad \text{and} \quad e_m(\mathcal{P}, \mathcal{Q}_1 \oplus \mathcal{Q}_2) = e_m(\mathcal{P}, \mathcal{Q}_1) e_m(\mathcal{P}, \mathcal{Q}_2),$$

(3) *it is* alternating*, in the sense that*

$$e_m(\mathcal{P}, \mathcal{Q}) = e_m(\mathcal{Q}, \mathcal{P})^{-1}$$

(4) *it is* nondegenerate*: if $e_m(\mathcal{P}, \mathcal{Q}) = 1$ for all $\mathcal{P} \in E[m]$, then $\mathcal{Q} = \mathcal{O}$.*

The proof is not so straightforward, and we will omit it; see Silverman [5, III.§8,Ex.3.16]. Note however that (3) is immediate from the definition, and that (1) is a consequence of (2). Instead, we will verify the theorem for e_2: although somewhat trivial, it is already enlightening.

Example 3.15. The affine 2-torsion points are of the form $(x_1, 0)$, $(x_2, 0)$, $(x_3, 0)$. It is obvious that we can take $\varphi_{2,(x_i,0)} = x - x_i$. Hence for $i \neq j$ we have

$$e_2((x_i, 0), (x_j, 0)) = \frac{x_j - x_i}{x_i - x_j}.$$

So two different affine 2-torsion points pair to -1. In all other cases, the pairing gives 1. The fact that we indeed obtain a 2^{nd} root of unity comes from the obvious fact that plugging in x_j in $x - x_i$ or plugging in x_i in $x - x_j$ are closely related. This close connection exists in general, due to a phenomenon called *Weil reciprocity*: if φ and φ' are functions whose divisors have disjoint supports, then

$$\varphi(\text{div}\varphi') = \varphi'(\text{div}\varphi).$$

See [5, Ex.2.11] for guidelines towards proving Weil reciprocity.

Lemma 3.16. *e_m is surjective on the set of m^{th} roots of unity.*

Proof. Let $\mathcal{Q} \in E[m]$ be a point of order m, which exists due to Theorem 2.7. By bilinearity, the set

$$\{e_m(\mathcal{P}, \mathcal{Q}) \mid \mathcal{Q} \in E[m]\}$$

is a subgroup of μ_m, hence of the form μ_d for $d \mid m$. But then for all $\mathcal{P}$ in $E[m]$ we have

$$e_m(\mathcal{P}, d\mathcal{Q}) = e_m(\mathcal{P}, \mathcal{Q})^d = 1,$$

so by nondegeneracy one has $d\mathcal{Q} = \mathcal{O}$. Thus $m = d$ and e_m is surjective. ∎

A surprising corollary is:

Corollary 3.17. *Let E be an elliptic curve over a finite field $\mathbb{F}_q$ ($\gcd(q, 6) = 1$) and let $m \in \mathbb{Z}_{\geq 1}$ be coprime to q. If $E[m] \subset E(\mathbb{F}_q)$, then $q \equiv 1 \bmod m$.*

Proof. From the constructive proof of Lemma 3.12, one sees that if $E[m] \subset E(\mathbb{F}_q)$ then e_m takes values in $\mathbb{F}_q$. On the other hand, by the above lemma it maps onto μ_m. Hence $\mu_m \subset \mathbb{F}_q^\times, \cdot$. Thus there is a $g \in \mathbb{F}_q^\times$ of order m. So $m \mid q - 1$ or $q \equiv 1 \bmod m$. ∎

Exercise 3.18. Refine the statement in Exercise 2.8 and prove that $q \equiv 1 \bmod \ell$.

4. Elliptic curves over finite fields

Throughout, let $\mathbb{F}_q$ be a fixed finite field of characteristic $\neq 2, 3$.

4.1. **Hasse's theorem.** If E is an elliptic curve over a $\mathbb{F}_q$, we obtain a finite group $E(\mathbb{F}_q)$.

Exercise 4.1. Prove that $1 \leq \#E(\mathbb{F}_q) \leq 2q+1$.

Exercise 4.2. Suppose $q \equiv 3 \bmod 4$, then show that the elliptic curve $y^2 = x^3 + x$ over $\mathbb{F}_q$ has $q+1$ rational points.

One can do better than the bound in Exercise 4.1: a theorem by Hasse states that $\#E(\mathbb{F}_q)$ is contained in

$$[q+1-2\sqrt{q}, q+1+2\sqrt{q}]\,,$$

which is called the *Hasse interval*.

We can now formulate

Theorem 4.3 (structure theorem)**.** *Any elliptic curve E over a finite field $\mathbb{F}_q$ satisfies*

$$E(\mathbb{F}_q) = \mathbb{Z}/(k) \times \mathbb{Z}/(\ell)$$

with $\ell | k$, $q \equiv 1 \bmod \ell$ and $k\ell \in [q+1-2\sqrt{q}, q+1+2\sqrt{q}]$.

Proof. Exercise 2.8, Exercise 3.18 and Hasse's theorem. ∎

The proof of Hasse's theorem is beautiful, but would lead us too far. It builds on a thorough analysis of the *Frobenius endomorphism*

$$\mathcal{F}_q : E \to E : (x,y) \mapsto (x^q, y^q) \text{ and } \mathcal{O} \mapsto \mathcal{O},$$

which is well defined because E is defined over $\mathbb{F}_q$. Note that

$$\mathcal{P} \in E(\mathbb{F}_q) \quad \text{ if and only if } \quad \mathcal{F}_q(\mathcal{P}) = \mathcal{P}.$$

Hence $\#E(\mathbb{F}_q)$ is the number of elements in the kernel of

$$1 - \mathcal{F}_q : E \to E : \mathcal{P} \mapsto \mathcal{P} \oplus -\mathcal{F}_q(\mathcal{P}).$$

Now there is a natural notion of *degree* $\deg \sigma$ one can associate to an endomorphism σ (it is the index inside $\overline{k}(E)$ of the pull-back of $\overline{k}(E)$ along σ), which generically matches with the cardinality of its kernel. In particular, it turns out to match for $1 - \mathcal{F}_q$. Hasse's theorem then follows from a version of the Cauchy-Schwartz inequality connecting the degrees of 1, $\mathcal{F}_q$, and $1 - \mathcal{F}_q$:

$$|\deg(1-\mathcal{F}_q) - \deg 1 - \deg \mathcal{F}_q| \leq 2\sqrt{\deg \mathcal{F}_q \cdot \deg 1}$$

(along with $\deg \mathcal{F}_q = q$ and $\deg 1 = 1$).

An amusing, though rarely useful property is:

Exercise 4.4. Let $\mathbb{F}_p$ be a prime field and let E be an elliptic curve over $\mathbb{F}_p$. Let $c \in \mathbb{F}_p$ be the coefficient of x^{p-1} in the expansion of

$$\left(x^3 + Ax + B\right)^{(p-1)/2}.$$

Then show that $\#E(\mathbb{F}_p) \equiv -c \bmod p$. Hint: first show that

$$\#E(\mathbb{F}_p) = \sum_{x \in \mathbb{F}_p} \left(1 + \left(x^3 + Ax + B\right)^{(p-1)/2}\right).$$

4.2. **The Frobenius action on $E[m]$.** In this section, we will justify the following definition (without proof):

Definition 4.5. *$t = \#E(\mathbb{F}_q) - (q+1)$ is called* the trace of Frobenius *of E.*

Exercise 4.6. For any $m \in \mathbb{Z}_{\geq 1}$, prove that $\mathcal{F}_q(m\mathcal{P}) = m\mathcal{F}_q(\mathcal{P})$. In particular, if $\mathcal{P} \in E[m]$, then $\mathcal{F}_q(\mathcal{P}) \in E[m]$.

Recall that, if m is coprime to q, we have

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

which is a module over $\mathbb{Z}/(m)$. This module has a basis $\mathcal{P}, \mathcal{Q}$. By the above exercise, there exist expressions

$$\mathcal{F}_q(\mathcal{P}) = \alpha\mathcal{P} \oplus \beta\mathcal{Q}, \quad \mathcal{F}_q(\mathcal{Q}) = \gamma\mathcal{P} \oplus \delta\mathcal{Q}$$

for $\alpha, \beta, \gamma, \delta \in \mathbb{Z}/(m)$. The matrix

$$M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

is called the *matrix of Frobenius* with respect to the basis $\mathcal{P}, \mathcal{Q}$. A very strong result is:

Theorem 4.7. *M has determinant q and trace t (modulo m, that is).*

Exercise 4.8. Use this to give an alternative proof of Corollary 3.17.

Exercise 4.9. Suppose that $E(\mathbb{F}_q)$ has a point of order m. Then prove that 'determinant q' and 'trace t' imply each other.

The *characteristic polynomial of Frobenius mod m* is then the characteristic polynomial of M:

$$X^2 - tX + q \qquad \in \mathbb{Z}/(m)[X].$$

By Cayley-Hamilton, we have that for any point $\mathcal{P} \in E[m]$

$$\mathcal{F}_q(\mathcal{F}_q((\mathcal{P})) \oplus -t\mathcal{F}_q(\mathcal{P}) \oplus q\mathcal{P} = \mathcal{O}, \tag{2}$$

which is a crucial ingredient in Schoof's point counting algorithm.

The parental polynomial $X^2 - tX + q \in \mathbb{Z}[X]$ is simply called the *characteristic polynomial of Frobenius*. One can show that this is again a characteristic polynomial in the true mathematical sense, but now the underlying space is somewhat more complicated (we omit it). Note that an alternative formulation of Hasse's theorem is then: the characteristic polynomial of Frobenius has negative discriminant (verify this).

Write $\chi(X) = X^2 - tX + q = (X - \alpha_1)(X - \alpha_2)$, then α_1, α_2 are called *the eigenvalues of Frobenius*. Note that they are complex conjugates. Hence $|\alpha_1|_{\mathbb{C}} = |\alpha_2|_{\mathbb{C}} = \sqrt{q}$, a statement which is called the *Riemann hypothesis for elliptic curves*. One motivation for this taxonomy is that it is equivalent to $s \mapsto \chi(q^s)$ having its zeroes on the line $\mathfrak{Re}(s) = 1/2$ (verify this), but the analogy goes further than that.

Now, as can be expected from decent eigenvalues, one can prove that the eigenvalues corresponding to $(\mathcal{F}_q)^r = \mathcal{F}_{q^r}$ are given by α_1^r and α_2^r, respectively. In other words,

$$\text{if } \#E(\mathbb{F}_q) = q + 1 - \alpha_1 - \alpha_2, \quad \text{then } \#E(\mathbb{F}_{q^r}) = q + 1 - \alpha_1^r - \alpha_2^r, \tag{3}$$

i.e. the number of $\mathbb{F}_{q^r}$-rational points (for any $r \in \mathbb{Z}_{\geq 1}$) is completely determined by the number of $\mathbb{F}_q$-rational points.

Exercise 4.10. Prove (3) directly from Theorem 4.7 and Hasse's theorem (or the naive bound from Exercise 4.1).

4.3. **Schoof's point counting algorithm.** We end Part I with the following problem. Given an elliptic curve $y^2 = x^3 + Ax + B$ over $\mathbb{F}_q$, can we efficiently compute $\#E(\mathbb{F}_q)$? As we will see in Part II, an affirmative answer is desirable from a cryptographic point of view.

The most naive approach is to check for all $(x, y) \in \mathbb{F}_q^2$ whether they satisfy $y^2 = x^3 + Ax + B$ or not. In cryptography, q is typically a prime power of about 256 binary digits. This means we would need 2^{512} verifications, which we would not be able to complete before the end of the universe. With a little more effort, one can reduce this to 2^{128} verifications, but still this is absolutely hopeless.

In 1985, Schoof (S) presented an algorithm that, also due to non-trivial improvements by Elkies (E) and Atkin (A), performs much better. Optimized versions of this so-called SEA algorithm have now been implemented in various computer algebra packages. Try for instance

```
p := NextPrime(2^256);
Fp := FiniteField(p);
A := Random(Fp); B := Random(Fp);
E := EllipticCurve([A,B]);
time #E;
```

in the Magma calculator: this invokes the SEA algorithm. Compare this with the time needed for point counting over finite fields of comparable size, but small characteristic (e.g. $\operatorname{char} \mathbb{F}_q = 5$): for such fields, even much faster methods exist.

Here are the main ideas of Schoof's original algorithm:

(1) It suffices to compute the trace of Frobenius t, since $\#E(\mathbb{F}_q) = q + 1 - t$.
(2) By Hasse's theorem, $|t| \leq 2\sqrt{q}$. Hence it suffices to compute $t \bmod M$ for some $M > 4\sqrt{q}$.
(3) By the Chinese Remainder Theorem, it suffices to compute $t \bmod \ell$ for the first primes $\ell = 2, 3, \ldots$ (omitting $p = \operatorname{char} k$) so that
$$\prod_{\ell} \ell > 4\sqrt{q}.$$
By the prime number theorem, this concerns a small number of small primes. For instance, for $q \approx 2^{256}$, it suffices check all 28 primes up to $\ell = 103$ (even if p is among these).
(4) As an introductory example, let us first show how to compute $t \bmod 2$. We know that $t \bmod 2 = 0$ if and only if $\#E(\mathbb{F}_q)$ is even (since q is odd), thus if and only if there is a rational point of order 2. Thus, $t \bmod 2 = 0$ if and only if $x^3 + Ax + B$ has a root in $\mathbb{F}_q$, which is equivalent to
$$\gcd(x^q - x, x^3 + Ax + B) \neq 1 \quad \text{in } \mathbb{F}_q[x].$$
Naively verifying this would take a huge amount of time, since $x^q - x$ is of degree $\approx 2^{256}$. But the condition can be rewritten as
$$\gcd(x^q - x \bmod (x^3 + Ax + B), x^3 + Ax + B) \neq 1.$$
So it is all about computing x^q modulo $x^3 + Ax + B$, which can be done quickly by repeated squaring and/or multiplying (depending on the binary expansion of q).

(5) Remark that $x^3 + Ax + B$ is the 2^{nd} division polynomial ψ_2!
(6) Generalizing the above to arbitrary ℓ works by working modulo the ℓ^{th} division polynomial ψ_ℓ. Recall that it vanishes *exactly* at the affine ℓ-torsion points. Also recall that there is an efficient recursive way of computing the polynomials ψ_ℓ. Now by Cayley-Hamilton (2) we know that for all affine points $(x, y) \in E[\ell]$,

$$(x^{q^2}, y^{q^2}) \oplus q(x, y) = t(x^q, y^q).$$

This statement cannot be true for some other value of t mod ℓ (why?). Thus if we find the t mod ℓ for which this relation holds, we are done. Then it is all about computing $x^q, x^{q^2}, y^q, y^{q^2}$, computing $q(x, y)$ using the explicit formulas (1.5), and similarly consecutively computing $t(x^q, y^q)$ until equality is found. All computations are to be done modulo $y^2 - x^3 - Ax - B$ and $\psi_\ell(x)$, since these characterize $E[\ell]$.

The speed-ups by Elkies and Atkin, which we don't discuss here, are necessary to turn the above into a practical algorithm. One problem is that, although the primes ℓ are small, the ψ_ℓ nevertheless become considerably large (recall that they are of degree $(\ell^2 - 1)/2$).