Problem Set 2

PAWS 2025

Nathaniel Hurst

1

Let $a \in K$ and consider the (affine plane) curve C (not elliptic curve since $4a^3 + 27b^2$ is not necessarily 0 in this exercise), defined by $y^2 = x^3 + ax + b$.

(a) Show that $4a^3 + 27b^2 = 0$ if and only if the polynomial $f = x^3 + ax + b$ has a repeated root.

(b) A point P on an affine plane curve is a singularity if and only if both partial derivatives $\frac{\partial f}{\partial x}$ and $\frac{\partial f}{\partial y}$ vanish at P; otherwise P is called a smooth point. Use this definition and part (a) to show that all points P on C are smooth if and only if $4a^3 + 27b^2 \neq 0$.

A

2

Consider the elliptic curve $E : y^2 = x^3 - 3x + 1$ defined over $\mathbb{F}_{13}$ and let

$$P_1 = (0, 1) \in E(\mathbb{F}_{13})$$

(a) Compute $[2] \cdot P_1$. Is there any relation to the point P_2 of Example 3.8 in the lecture notes?

(b) Compute $[12] \cdot P_1$. Try to use as few elliptic curve additions as possible.

A

3

Given an elliptic curve E over K, a point $P \in E(K)$ and an integer N. Show that Algorithm 4 computes $[N] \cdot P$ using at most $2 \log_2(N)$ elliptic curve additions (a doubling $[2] \cdot P$ is counted as one addition $P + P$).

A

4

Consider $E : y^2 = x^3 - 2x + 5$ over $\mathbb{F}_{19}$. Let $P = (2, 3)$ and $Q = (10, 4)$. (Note: See the SageMath documentation for how to construct elliptic curves and points on elliptic curves.)

(a) Check that P and Q are points on E.

(b) Calculate $P + Q$, without using SageMath.

(c) Calculate $[5] \cdot P$ using the double-and-add algorithm (Algorithm 4 of the lecture notes).

(d) Calculate $[7] \cdot Q$. What does this tell you about the order of Q?

A

5

Let $E : y^2 = x^3 + ax + b$ be an elliptic curve defined over a field of characteristic $\neq 2, 3$. In this exercise, you are asked to show that $\#E[3] = 9$ by describing how to compute the points.

(a) Use the description of the group law (in Theorem 3.7 of the lecture notes) to construct a polynomial φ such that $\varphi(x) = 0$ if and only if $[3] \cdot P = \infty$, where $P = (x, y)$ is a point on the (affine) curve.

(b) Show that φ has no repeated roots. (Hint: Show that φ and its derivative cannot share any roots.)

A

6

For each of the following elliptic curves and finite fields $\mathbb{F}_p$, list the points in $E(\mathbb{F}_p)$ and check that the number of points is within the Hasse bound:

(a) $E : y^2 = x^3 + 7x - 3$ over $\mathbb{F}_{13}$.

(b) $E : y^2 = x^3 + 11x + 2$ over $\mathbb{F}_{17}$.

A

7

Let $p > 3$ be a prime, and consider two elliptic curves:

$$E : y^2 = x^3 + ax + b \quad \text{and} \quad \overline{E} : y^2 = x^3 + ax - b$$

defined over $\mathbb{F}_p$.

(a) Assume that $p \equiv 1 \pmod 4$. Show that

$$\#E(\mathbb{F}_p) = \#\overline{E}(\mathbb{F}_p)$$

(b)Assume that $p \equiv 3 \pmod 4$. Show that

$$\#E(\mathbb{F}_p) + \#\overline{E}(\mathbb{F}_p) = 2p + 2.$$

Some hints: **1)** Check if -1 is a square in $\mathbb{F}_p$. **2)** Let $p = (x_0, y_0) \in E(\mathbb{F}_p)$. Is there a point $\overline{P} = (x_0, \star) \in \overline{E}(\mathbb{F}_p)$? What about $\overline{P} = (-x_0, \star) \in \overline{E}(\mathbb{F}_p)$?

A

8

Let $p > 2$ be a prime number and let $E : y^2 = x^3 + Ax + B$ be an elliptic curve over $\mathbb{F}_p$, and denote with $E(\mathbb{F}_p)$ all points of E with coordinates in $\mathbb{F}_p$. Further, let $\left(\frac{a}{b}\right)$ be the Legendre symbol.

(a) Show that

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

(b) Let $d \in \mathbb{F}_p$ be such that $\left(\frac{d}{p}\right) = -1$ and $E' : dy^2 = x^3 + Ax + B$. Show that

$$|E(\mathbb{F}_p)| + |E'(\mathbb{F}_p)| = 2p + 2.$$

(c) Let p be a prime such that $p \equiv 3 \pmod 4$ and $E : y^2 = x^3 + Ax$. Show that $|E(\mathbb{F}_p)| = p + 1$.

A

9

Compute the group structure of $E(\mathbb{F}_p)$ for the given elliptic curves E and primes p. (Can you also find generators?)

(a) $E : y^2 = x^3 + 1$ for $p = 5$

(b) $E : y^2 = x^3 + x$ for $p = 7$

(c) $E : y^2 = x^3 - 1$ for $p = 7$

(d) $E : y^2 = x^3 + 3x + 1$ for $p = 11$

(e) For $p = 13$, compute the group structures of $E(\mathbb{F}_p)$ for all elliptic curves over $\mathbb{F}_p$. (You can use the command .abelian_group() for this.)

A

10

In this exercise we will outline a proof of Hasse's theorem (Theorem 3.16 of the lecture notes): Let E be an elliptic curve over $\mathbb{F}_q$. Then:

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

We first introduce the q-power Frobenius endomorphism,

$$\pi_q : E \longrightarrow E, \quad (x, y) \mapsto (x^q, y^q), \quad \infty \mapsto \infty.$$

(Note: Endomorphisms have not been defined in the lecture! An endomorphism is a rational map from an elliptic curve to itself, which maps ∞ to ∞. Multiplication by N for an integer N is an example of an endomorphism. One can show that an endomorphism is a group homomorphism.)

(a) Show that $\pi_q : E \longrightarrow E$ is a group homomorphism.

(b) Show that $\#E(\mathbb{F}_q) = \#\ker(1 - \pi_q)$, where 1 is the identity map on E.

(c) A **binary quadratic form** on an abelian group A, $Q : A \longrightarrow \mathbb{Z}$, is a function satisfying the properties:

1) $Q(x) = Q(-x)$ for all $x \in A$,

2) The pairing $(x, y) = Q(x + y) - Q(x) - Q(y)$ is bilinear. It is further called **positive definite** if $Q(x) \geq 0$ for all $x \in A$ and $Q(x) = 0$ if and only if $x = 0$.

(i) Prove that for a positive definite quadratic form Q,

$$|Q(x - y) - Q(x) - Q(y)| \leq 2\sqrt{Q(x)Q(y)}$$

for all $x, y \in A$.

(d) For an endomorphism $\varphi : E \longrightarrow E$, when $p \nmid \#\ker(\varphi)$ (more generally, when φ is separable), we define the degree of φ to be the size of its kernel and denote it by $\deg(\varphi)$. It is a fact that $1 - \pi_q$ is separable (see Silverman's **The Arithmetic of Elliptic Curves**, III.5.5), so $\#\ker(1 - \pi_q) = \deg(1 - \pi_q)$.

Then the proof of Hasse's Theorem reduces to proving that the degree map $\deg : \mathrm{End}(E) \longrightarrow \mathbb{Z}$ is a positive definite binary quadratic form and applying the preceding result in part (c).

(i) (Practice with the definition.) Let $p \nmid N$. What is $\deg([N])$, where $[N]$ is the multiplication-by-N map on E?

(ii) Prove that the degree map is a positive definite binary quadratic form. (Hard part: bilinearity of the pairing.)

(iii) Apply the result in part (c) to the degree map to show that

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

A