

### Exercises for week 13

Hand in three of the four exercises below.

In the lecture the *Hilbert class polynomial* for a quadratic discriminant  $D$  was defined as

$$H_D = \prod_{\Lambda} (X - j(\Lambda)),$$

where  $\Lambda$  runs over the set of isomorphism classes of lattices having  $\mathcal{O}(\Lambda) \cong \mathcal{O}_D$ . This polynomial has integer coefficients. The set of isomorphism classes of such lattices  $\Lambda$  can be enumerated as in last week's exercises.

The  $j$ -function on the upper half plane  $\mathbf{H}$  is defined by

$$j(\tau) = j(\mathbf{Z} + \tau\mathbf{Z}) \quad \text{for } \tau \in \mathbf{H}.$$

This function can be computed in PARI using the command `ellj`.

For an elliptic curve  $E$  over a field  $\mathbf{F}_p$  of  $p$  elements, the *Frobenius endomorphism* of  $E$  is defined as

$$\begin{aligned} \pi: E &\rightarrow E \\ (x, y) &\mapsto (x^p, y^p). \end{aligned}$$

It satisfies a quadratic equation of the form

$$\pi^2 - t\pi + p = 0.$$

with  $t$  an integer such that  $|t| \leq 2\sqrt{p}$ ; this  $t$  is called the *trace of Frobenius* of  $E$ . The number of points of  $E$  over  $\mathbf{F}_p$  equals

$$\#E(\mathbf{F}_p) = N(\pi - 1) = p + 1 - t.$$

For any prime number  $p$  and for any  $t \in \mathbf{Z}$  with  $|t| \leq 2\sqrt{p}$ , there exists an elliptic curve  $E$  over  $\mathbf{F}_p$  with trace of Frobenius  $t$ . Moreover, all the zeroes of  $H_D$  in the field  $\mathbf{F}_p$  are  $j$ -invariants of such curves  $E$ , where

$$D = t^2 - 4p.$$

For any given  $j_0$  different from 0 and 1728, one can construct an elliptic curve having  $j$ -invariant  $j_0$  as follows: the  $j$ -invariant of an elliptic curve  $E$  of the form

$$E: y^2 = x^3 + ax + a$$

is given by the formula

$$j(E) = 1728 \frac{4a}{4a + 27}$$

and the equation  $j(E) = j_0$  is easily solved for  $a$ .

For any prime number  $p \neq 2, 3$  and any element  $j_0 \in \mathbf{F}_p$  different from 0 and 1728, there are two isomorphism classes over  $\mathbf{F}_p$  of curves having  $j$ -invariant  $j_0$ ; they are represented by the curves

$$y^2 = x^3 + ax + a$$

and

$$y^2 = x^3 + c^2ax + c^3a,$$

where  $a$  is as above and  $c$  is an element of  $\mathbf{F}_p^\times \setminus \mathbf{F}_p^{\times 2}$ .

1. (a) Determine all prime numbers  $p$  for which there exists an elliptic curve over  $\mathbf{F}_p$  having exactly 8 points over  $\mathbf{F}_p$ .  
 (b) For all  $p$  as in (a), write down an elliptic curve over  $\mathbf{F}_p$  with exactly 8 points over  $\mathbf{F}_p$ , using a suitable Hilbert class polynomial. Prove that your answer is correct.
2. Write down an elliptic curve over a finite field  $\mathbf{F}_p$  having exactly 174 points over  $\mathbf{F}_p$ , using a suitable Hilbert class polynomial. Prove that your answer is correct.

3. Consider the elliptic curve

$$E: y^2 = x^3 + x$$

over a finite field  $\mathbf{F}_p$  with  $p \equiv 1 \pmod{4}$ . Choose an element  $i \in \mathbf{F}_p$  with  $i^2 = -1$ . The curve  $E$  has an endomorphism

$$\begin{aligned} I: E &\rightarrow E \\ (x, y) &\mapsto (-x, iy), \end{aligned}$$

which clearly satisfies  $I^2 = -1$  in the endomorphism ring  $\text{End}(E)$ . It turns out that  $I$  generates the endomorphism ring  $\text{End}(E)$  over  $\mathbf{Z}$  and therefore the ring  $\text{End}(E)$  is isomorphic to the ring of Gaussian integers. This implies that the Frobenius endomorphism  $\pi \in \text{End}(E)$  can be written as

$$\pi = r + sI$$

with  $r, s \in \mathbf{Z}$ . Note that  $r^2 + s^2 = p$ . There are four ways to write  $p$  in this way, up to the sign of  $s$ , so there are four possibilities for the trace  $t = 2r$ . The goal of this exercise is to find out which is the correct one for this curve.

- (a) Prove that  $E(\mathbf{F}_p)$  has four 2-torsion points, and conclude that  $r$  is odd.
- (b) Prove that  $r \equiv 1 \pmod{4}$ . [*Hint*: look at (non-)existence of a point of order 4.]

4. Now consider the curve

$$E: y^2 = x^3 + x$$

over a finite field  $\mathbf{F}_p$  with  $p \equiv 3 \pmod{4}$ . Let  $i$  be a square root of  $-1$  in the field  $\mathbf{F}_{p^2}$  of  $p^2$  elements, and consider the endomorphism  $I$  of  $E$  defined as in the previous exercise.

- (a) Prove that  $\pi \circ I = -I \circ \pi$ .
- (b) Show that  $I^{-1} \circ \pi \circ I$  is (like  $\pi$ ) a zero of the quadratic polynomial  $X^2 - tX + p$ , and conclude that  $\#E(\mathbf{F}_p) = p + 1$ .