Elliptic curves: exercise sheet 7

Due: 29th October 2013

Mastermath / DIAMANT, Fall 2013

René Schoof and Peter Stevenhagen

Exercise 1. Let E be the elliptic curve over $\mathbf{F}_2$ given by the equation $Y^2 + Y = X^3$.

(a) Compute the zeta function of E.

(b) For every $m \geq 1$ compute the number of points of E over $\mathbf{F}_{2^m}$.

Exercise 2. Let E be the elliptic curve over $\mathbf{F}_5$ defined by the equation $Y^2 = X^3 - X - 2$. Show that the complex zeroes of the ζ-function of E are given by

$$\frac{1}{2} \pm \frac{\arctan(\frac{\sqrt{11}}{3}) + 2\pi k}{\log 5} i, \qquad (k \in \mathbf{Z}).$$

Exercise 3. Let E be the elliptic curve over $\mathbf{F}_2$ given by the equation $Y^2 + Y = X^3$. For $a \geq 0$, let $L_a = \{f \in \mathbf{F}_2(E) : f \text{ has a pole of order} \leq a \text{ at } \infty\}$. For $a, b \geq 0$, let $L_a^2 L_b$ denote the $\mathbf{F}_2$-vector space generated by the functions $f^2 g$ where $f \in L_a$ and $g \in L_b$.

(a) Compute the dimension of $L_a^2 L_b$ for $(a, b) = (4, 1)$ and $(3, 3)$.

(b) Compute the dimension of $L_a^2 L_b$ for $a = 2$ and $b \geq 0$.

Exercise 4. Let E be the elliptic curve over $\mathbf{Q}$ defined by the equation $Y^2 = X^3 + X + 1$. Let P and Q denote the points $(+i, 1)$ and $(-i, 1)$ in $E(\mathbf{Q}(i))$ and let D denote the divisor $P + Q$. Find a function f on E and a point $R \in E(\mathbf{Q})$ for which

$$D + (f) \;=\; R + (\infty).$$

Exercise 5. Let p be a prime congruent to $2 \pmod 3$ and let E be the elliptic curve over $\mathbf{F}_p$ given by $y^2 - y = x^3$.

(a) Show that for every $y \in \mathbf{F}_p$ there is precisely one $x \in \mathbf{F}_p$ for which $(x, y) \in E(\mathbf{F}_p)$.

(b) Show that $\#E(\mathbf{F}_p) = p + 1$ and $\#E(\mathbf{F}_{p^2}) = (p + 1)^2$.

Exercise 6. Let p be a prime congruent to $3 \pmod 4$ and let E be the elliptic curve over $\mathbf{F}_p$ given by $y^2 = x^3 - x$.

(a) Let $x \in \mathbf{F}_p - \{0, \pm 1\}$. Show that for precisely one of $\pm x$ there is a $y \in \mathbf{F}_p$ for which $(x, y) \in E(\mathbf{F}_p)$.

(b) Show that $\#E(\mathbf{F}_p) = p + 1$ and $\#E(\mathbf{F}_{p^2}) = (p+1)^2$.

Exercise 7. Let $\mathbf{F}_q$ be a finite field of characteristic $p \neq 2$. Let E be an elliptic curve given by the

(a) Weierstrass equation $Y^2 = X^3 + b_2X^2 + b_4X + b_6$. Let $g \in \mathbf{F}_q$ be a non-square. Find a Weierstrass equation for the "twisted" elliptic curve E' given by $gY^2 = X^3 + b_2X^2 + b_4X + b_6$.

(b) Suppose that $\#E(\mathbf{F}_q) = q + 1 - t$. Prove that $\#E'(\mathbf{F}_q) = q + 1 + t$.

Exercise 8. Let k be a finite fields of q elements and let $k \subset k'$ be a finite extension.

(a) Show that $\{y^q - y : y \in k'\}$ is a sub-k-vector space of k' of codimension 1.

(b) Let $x \in k'$. Show that $\operatorname{Tr} x = 0$ if and only if $x = y^q - y$ for some $y \in k'$.

Exercise 9. Let $q = 2^m$ and let $z \in \mathbf{C}$ be a zero of the polynomial $t^2 + t + 2$.

(a) Let E be the elliptic curve $Y^2 + XY = X^3 + X$ over $\mathbf{F}_2$. Show that $\#E(\mathbf{F}_q)$ is equal to $q + 1 - z^m - \overline{z}^m$.

(b) Let $\operatorname{Tr} : \mathbf{F}_q \to \mathbf{F}_2$ denote the trace map and consider the vector

$$\left(\operatorname{Tr}(x + \frac{1}{x})\right)_{x \in \mathbf{F}_q^*} \in \mathbf{F}_2^{q-1}.$$

Show that precisely $\frac{1}{2}(q - 1 + z^m + \overline{z}^m)$ of its coordinates are equal to 1 (the others are equal to zero).

Exercise 10. By Hasse's Theorem an elliptic curve E over $\mathbf{F}_q$ satisfies $\#E(\mathbf{F}_q) \leq q + 1 + 2\sqrt{q}$.

(a) Show that if equality holds, then q is a square.

The converse is also true: for every q that is a square there exists an elliptic curve over $\mathbf{F}_q$ for which equality holds. When the characteristic p of $\mathbf{F}_q$ is not congruent to $1 \pmod{12}$ this is relatively easy to prove.

(b)* Show that there exists an elliptic curve over $\mathbf{F}_q$ for which equality holds when $q = p^2$ and p is a prime $\not\equiv 1 \pmod{12}$. (Hint: exercises 5 and 6.)

(c)* Show that there exists an elliptic curve over $\mathbf{F}_q$ for which equality holds when q is an even power of a prime $p \not\equiv 1 \pmod{12}$. (Hint: exercise 7.)