Elliptic curves: exercise sheet 8

Due: 12th November 2013

Mastermath / DIAMANT, Fall 2013

René Schoof and Peter Stevenhagen

Exercise 11. Let k be any field of characteristic unequal to 11. Show that the point $(0,0)$ of the elliptic curve over k given by $Y^2 + Y = X^3 - X^2$ has order 5.

Exercise 12. Let E be the elliptic curve over $\mathbf{Q}$ given by the equation $Y^2 + Y = X^3$. Compute the coordinates of its 2-torsion points and of its 3-torsion points.

Exercise 13. Let $\zeta \in \mathbf{F}_4$ denote a 3rd root of unity. Let E be the elliptic curve over $\mathbf{F}_4$ defined by the equation $Y^2 + Y = X^3$. Let $f : E \to E$ be given by $f(x,y) = (\zeta x, y)$ and let $g : E \to E$ be given by $g(x,y) = (x+1, y+x+\zeta)$. Show that f and g are automorphisms of E and show that they do not commute. Therefore the ring $\mathrm{End}\, E$ is not commutative in this case.

Exercise 14. Let E be the elliptic curve given over $\mathbf{F}_2$ by $Y^2 + Y = X^3$. Compute the dual of its Frobenius endomorphism.

Exercise 15. Let k be a field and let C be the parabola given by the equation $y = x^2$ in $\mathbf{A}^2$. We define a composition of points of C as follows: given two points P and Q on C, we let l be the line passing through them and m be the line parallel to l, passing through the point $(1,1)$. Then the composition of P and Q is the second point of intersection of m and C. (if $P = Q$, take for l the tangent line ... etc).

(a) Compute the coordinates of the composition of the points (x, x^2) and (x', x'^2) of C.

(b) Show that this composition turns the points of C into a commutative group with neutral element $(1,1)$.

(c) Show that the set of points of C with coordinates in k is a group isomorphic to the additive group k.

Exercise 16. Let E be the elliptic curve over $\mathbf{Q}$ given by $Y^2 + Y = X^3$ and let Q denote the point $(0,0)$. Let $\tau : E \longrightarrow E$ denote translation by Q. In other words $\tau(P) = P + Q$ for P a point on E.

(a) Show that τ is an automorphism of E of order 3. For an arbitrary point $P = (x,y)$ of E compute $\tau\, P$ and $\tau^2 P$.

(b) Let H be the subgroup generated by Q and let E' denote the elliptic curve over $\mathbf{Q}$ given by $Y^2 + 3Y = X^3 - 9$. Show that $\phi(x,y) = (x + \frac{1}{x^2}, y - 1 - \frac{2y+1}{x^3})$ defines an isogeny $\phi : E \longrightarrow E'$ whose kernel is H.

Exercise 17. Let k be a field and let E be an elliptic curve over k.

(a) Show that for $m \geq 3$ prime to $\operatorname{char} k$, the natural map $\operatorname{Aut} E \longrightarrow \operatorname{Aut}(E[m])$ is injective, while for $m = 2$ its kernel is $\pm\mathrm{id}$. (Silverman Exercise III.3.12).

(b) Show that the order of $\operatorname{Aut} E$ is at most 12 when $\operatorname{char} k \neq 2$, while it is at most 48 when $\operatorname{char} k = 2$. (it is actually ≤ 24).

(c) Show that the order of any automorphism of E is at most 6.

Exercise 18. Let k be a field of characteristic different from 2. Suppose that k contains i, a square root of -1. Let E be the elliptic curve over k given by $Y^2 = X^3 - X$.

(a) Show that the map $[i](x, y) = (-x, iy)$ defines an endomorphism $[i] : E \longrightarrow E$ and that $[i]$ satisfies $[i]^2 + \mathrm{id} = 0$ in $\operatorname{End}(E)$.

(b) For $a, b \in \mathbf{Z}$, show that the degree of the endomorphism $a + b[i]$ of E is equal to $a^2 + b^2$.

Exercise 19. Let k be a field and let E be an elliptic curve over k. Let l be a prime different from $\operatorname{char} k$. The *l-adic Tate module* $T_l(E)$ of E is the projective limit of the groups of l^n-torsion points $E(\overline{k})[l^n]$. Show that the natural map $\operatorname{End}(E) \longrightarrow \operatorname{End}(T_l(E))$ is injective. (Silverman Exercise III.3.14)

***Exercise 20.** Learn about the Weil pairing and make Exercise III.3.31 of Silverman, i.e. prove that the dual of the sum of two isogenies is equal to the sum of their duals.