Elliptic curves: homework 9
Mastermath / DIAMANT, Spring 2019
Martin Bright and Marco Streng
Deadline: 9 April

Hand in exercises 2 and 4.

1. Let $\zeta \in \mathbb{F}_4$ denote a primitive 3rd root of unity. Let E be the elliptic curve over $\mathbb{F}_4$ defined by the equation

$$Y^2 + Y = X^3.$$

Let $f\colon E \to E$ 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 $\operatorname{End} E$ is not commutative in this case.

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

(a) Show that τ is a *curve automorphism* of E of order 3, but not an elliptic curve automorphism.

(b) Give a formula for the point $\tau(P)$ in terms of the coordinates x and y of $P = (x, y)$. Also give a formula for $\tau^2(P)$.

(c) Let H be the subgroup generated by Q and let E' denote the elliptic curve over $\mathbb{Q}$ given by $Y^2 + 3Y = X^3 - 9$. Show that

$$\phi(x, y) = \left(x + \frac{1}{x^2}, y - 1 - \frac{2y + 1}{x^3} \right)$$

defines an isogeny $\phi\colon E \to E'$ whose kernel is H. (You may use a computer for part (c).)

3. (Silverman, 3.9) Let E/k be an elliptic curve given by a homogeneous Weierstrass equation $F(X_0, X_1, X_2) = 0$. Let $P \in E$. Assume that $\operatorname{char}(k) \neq 2, 3$.

(a) Show that $[3]P = O$ if and only if the tangent line to E at P intersects E only at P.

(b) Show that $[3]P = O$ if and only if the Hessian matrix

$$\big((\partial^2 F/\partial X_i \partial X_j)(P)\big)_{0 \le i,j \le 2}$$

has determinant 0.

(c) Show that $E[3]$ consists of 9 points.

4. Let E be the elliptic curve over $\mathbb{Q}$ given by the Weierstrass equation $Y^2 + Y = X^3$. Compute the coordinates of its 2-torsion points and of its 3-torsion points in $E(\bar{\mathbb{Q}})$.

5. (Silverman, Exercise 3.30) Let A be an abelian group and $r \geq 0$ and $N \geq 1$ integers. Suppose that $\#A[d] = d^r$ for all $d \mid N$, where $A[d]$ denotes the subgroup of elements of order dividing d. Show $A[N] \cong (\mathbb{Z}/N\mathbb{Z})^r$.