Elliptic curves: homework 10
Mastermath / DIAMANT, Spring 2019
Martin Bright and Marco Streng

1. 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 $[i](x, y) = (-x, iy)$ defines an endomorphism $[i] : E \longrightarrow E$ and that $[i]$ satisfies $[i]^2 + [1] = 0$ in $\mathrm{End}(E)$.

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

(c) Compute formulas for the isogeny $\phi = [1] + [i]$.

(d) Compute the points in $\ker(\phi)$ for $\phi = [1] + [i]$. [Note: this can easily be done without doing (c).]

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

3. (Inspired by Silverman, Exercise 3.32) Let $\phi \in \mathrm{End}(E)$ be an endomorphism and let

$$d = \deg(\phi), \quad \text{and} \quad t = 1 + \deg(\phi) - \deg(1 - \phi) \in \mathbb{Z}.$$

(a) Prove $t = \phi + \widehat{\phi}$ and $\phi^2 - t\phi + d = 0$ in $\mathrm{End}(E)$.

(b) Give a formula for $\deg(m\phi - n)$ in terms of m, n, d, t.

(c) Prove $|t| \leq 2\sqrt{d}$. [Hint: use $\deg(m\phi - n) \geq 0$ for all $m, n \in \mathbb{Z}$.]

(d) Prove *Hasse's theorem*, which states that for $E/\mathbb{F}_q$ an elliptic curve, we have

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

[Hint: show that $E(\mathbb{F}_q) = \ker(1 - \mathrm{Frob}_q)$.]

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

(a) Show that for $m \geq 3$ not divisible by $\mathrm{char}\, k$, the natural map $\mathrm{Aut}\, E \to \mathrm{Aut}(E[m])$ is injective, while for $m = 2$ its kernel is $\{\pm \mathrm{id}\}$. [Notes: this is [Silverman, Exercise 3.12], and you are not allowed to use [Silverman, Theorem III.10.1]. Hint for one approach to this problem: use Problem 3(c).]

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

(c) Show that the order of an automorphism of E is 1, 2, 3, 4 or 6. [Hint: use Problems 3(a) and 3(b).]