**Elliptic curves: homework 11**
Mastermath / DIAMANT, Spring 2019
Martin Bright and Marco Streng
**Deadline: 30 April**

Hand in exercises 1 and 2.

**1.** Let $E(\mathbb{C})$ be the group of points of a complex elliptic curve. Show that $E(\mathbb{C})$ contains subgroups $H$, each of countably infinite cardinality, such that:

(a) $H$ is a torsion group and $H/2H$ is trivial;

(b) $H$ is torsion-free and $H/2H$ is trivial;

(c) $H$ is torsion-free and $H/2H$ is infinite.

**2.** Let $E$ be the elliptic curve over $\mathbb{Q}$ defined by

$$y^2 = x(x^2 + 13).$$

Find a minimal set of generators for $E(\mathbb{Q})/2E(\mathbb{Q})$.

**3.** Let $E$ be the elliptic curve over $\mathbb{Q}$ defined by

$$y^2 = x(x^2 + 17).$$

Try (hard) to find a minimal set of generators for $E(\mathbb{Q})/2E(\mathbb{Q})$. Describe the problem you encounter.

**4.** (Cassels §14, Exercise 3) Let

$$E : y^2 = x(x^2 + ax + b), \quad E' : y^2 = x(x^2 + a_1x + b_1)$$

be two elliptic curves over $\mathbb{Q}$, with $a_1 = -2a$ and $b_1 = a^2 - 4b$.

(a) Show that the groups $E(\mathbb{Q})$ and $E'(\mathbb{Q})$ have isomorphic odd-order torsion.

(b) Assuming the Mordell–Weil theorem, show that $E(\mathbb{Q})$ and $E'(\mathbb{Q})$ have the same rank.

(c) Give an example to show that the 2-power torsion groups of $E(\mathbb{Q})$ and $E'(\mathbb{Q})$ need not be isomorphic.

**5.** Consider the equation

$$2Y^2 = X^4 - 17Z^4 \tag{1}$$

which appeared during exercise 3.

(a) Show that, if (1) has a non-zero integer solution $(x, y, z)$, then we may assume that $x, z$ are coprime and that $y$ is positive.

(b) Given such a solution, show that 17 does not divide $y$.

(c) Use quadratic reciprocity to show that, if $p \neq 17$ is an odd prime dividing $y$, then $p$ is a square modulo 17. Deduce that $y$ is a square modulo 17.

(d) Show that 2 is not a fourth power modulo 17, and conclude that (1) has no non-zero integer solutions.