Elliptic curves: problem sheet 6
These problems do not count for your grade, but it is still important that you solve them.
Mastermath / DIAMANT, Spring 2019
Martin Bright and Marco Streng

In problems 1 and 2, *only* use the result that for integers m, elliptic curves E and primes $p \nmid m$ of good reduction, the reduction map $E(\mathbb{Q})[m] \to E(\mathbb{F}_p)$ is injective [Silverman, VII.3.1].

Problem 1. Let E be the elliptic curve over $\mathbb{Q}$ defined by the Weierstrass equation

$$y^2 = x^3 + 2x + 6.$$

(a) Show that E has good reduction at both 3 and 5.

(b) Find the number of points of the reduction of E over $\mathbb{F}_3$ and over $\mathbb{F}_5$.

(c) Deduce that $E(\mathbb{Q})$ is torsion-free.

Problem 2 (optional)**.** For each of the following elliptic curves E over $\mathbb{Q}$, using only [Silverman, VII.3.1], find the torsion subgroup of $E(\mathbb{Q})$. (That is, give the coordinates of the torsion points and describe the group structure on them.)

(a) $y^2 = x^3 + 1$,

(b) $y^2 = x^3 - 43x + 166$ [Silverman, Exercise 8.12(g)],

(c) $y^2 = x(x-1)(x-2)$.

Problem 3. Let E be a curve given by a general Weierstrass equation with coefficients in $\mathbb{Z}$.

(a) Show that every point $Q \in E(\mathbb{Q}) \setminus \{O\}$ can be written in a unique way as

$$Q = \left(\frac{A}{B^2}, \frac{C}{B^3}\right) \qquad \text{with} \qquad A, B, C \in \mathbb{Z}, B > 0, \text{and } \gcd(A, B, C) = 1.$$

For a point of infinite order $P \in E^{\mathrm{ns}}(\mathbb{Q})$, we define the *elliptic divisibility sequence (EDS)* $B_1, B_2, B_3, \ldots$ associated to P by $B_n = B(nP)$, that is, B_n is the number B as above when we take $Q = nP$. If you would like to see an example, see (f) below and compute the first few terms by hand.

(b) Show that every EDS is a *divisibility sequence* in the sense that if $m \mid n$, then $B_m \mid B_n$.

(c) Show that every EDS is a *strong divisibility sequence* in the sense that for all $m, n \in \mathbb{Z}_{>0}$, we have $B_{\gcd(m,n)} = \gcd(B_m, B_n)$.

(d) Show that if p is a prime and n is a positive integer such that $p \mid B_n$, then $B_{pn} = p^a \cdot B_n \cdot C$ for some $a, C \in \mathbb{Z}_{>0}$ with $\gcd(C, pB_n) = 1$.

(e) (Optional, using results from the lecture/book that were not proven in the lecture.) Show that if $p \neq 2$ or $p^2 \mid B_n$, then $a = 1$ in (d). [Hint: [Silverman, IV.6.4(b) and VII.2.2].]

(f) (Optional, lot of work, I haven't tried it yet.) Let E be the singular curve $E : y^2 = x^3 + 5x^2$ and take $P = (-4, 4)$. Show that for all $n \in \mathbb{Z}_{>0}$, we have

$$B_n = \begin{cases} \frac{1}{2}F_n & \text{if } 3 \mid n, \\ F_n & \text{otherwise,} \end{cases}$$

where F_n is the n-th Fibonacci number. [Hint: use an isomorphism $\overline{\mathbb{Q}}^* \to E^{\mathrm{ns}}(\overline{\mathbb{Q}})$.]

[Elliptic divisibility sequences can be seen as higher-genus analogues of the Fibonacci sequence. The degenerate cases given by additive Weierstrass equations (with cusps) are related to arithmetic progressions, and the degenerate cases given by multiplicative Weierstrass equations (with nodes) are related to Lucas and Lehmer sequences.]

Problem 4 (Alternative to [Silverman (2nd edition), Lemma VII.2.1.1] and details for [Milne, page 59, the phrase "Since [...] lines reduce to lines"])**.** Let K be a field and let L and $C \neq L$ be a line and a curve defined over K in $\mathbb{P}^2$.

(0) Show that the intersection points and their multiplicities do not depend on any of the choices made in Problem 7 of Homework 5 (such as the choice of ϕ).

Now suppose that K, R, π, v and k are as in the lecture and that C is given by an equation $F = 0$ with $F \in R[X, Y, Z]$ such that $\widetilde{F}$ is irreducible in $\overline{k}[X, Y, Z]$. Suppose that all intersection points of L and C over $\overline{K}$ are defined over K. Let $P_1, P_2, \ldots, P_d \in C(K)$ be the intersection points, listed with their appropriate multiplicities.

(i) Show that we can choose ϕ in Problem 7 of Homework 5 such that for both $i \in \{0, 1\}$ we have x_i, y_i, $z_i \in R$ with at least one of $\widetilde{x_i}$, $\widetilde{y_i}$, $\widetilde{z_i}$ in k^*, and such that $(\widetilde{x_0}, \widetilde{y_0}, \widetilde{z_0}) \neq (\widetilde{x_1}, \widetilde{y_1}, \widetilde{z_1})$.

(ii) Show that this gives an isomorphism $\widetilde{\phi} : \mathbb{P}^1 \to \widetilde{L}$.

(iii) Show that we have

$$F \circ \phi = \prod_{i=1}^{d} (\beta_i s - \alpha_i t)$$

with α_i, $\beta_j \in R$ and for every $i = 1, 2, \ldots, d$ at least one of $\widetilde{\alpha_i}$, $\widetilde{\beta_i}$ in k^*.
[Hint: show first $F \circ \phi = u \prod_{i=1}^{d} (\beta_i s - \alpha_i t)$ with $u \in K^*$, then show $v(u) = 0$.]

(iv) Show that $\widetilde{P_1}, \widetilde{P_2}, \ldots, \widetilde{P_d}$ are the intersection points of $\widetilde{L}$ with $\widetilde{C}$ listed with their multiplicities.

(iv) Now suppose that C is given by a Weierstrass equation with coefficients in R. Let $C_0(K)$ be the set of $P \in C(K)$ such that $\widetilde{P}$ is not a singular point of $\widetilde{C}$. Show that $C_0(K)$ is a subgroup of $C^{\mathrm{ns}}(K)$ and that the map

$$\begin{aligned} C_0(K) &\longrightarrow \widetilde{C}^{\mathrm{ns}}(k) \\ P &\longmapsto \widetilde{P} \end{aligned}$$

is a homomorphism.

Problem 5 (Only if this was not already done in class)**.** (i) Let $p \neq q$ be prime numbers such and let E be an elliptic curve over $\mathbb{Q}$ that has good reduction at both p and q. Show that reduction gives an injective homomorphism $E(\mathbb{Q})^{\mathrm{tors}} \to \widetilde{E}(\mathbf{F}_p) \times \widetilde{E}(\mathbf{F}_q)$.

(ii) Let E be an elliptic curve over $\mathbb{Q}$. Show that $E(\mathbb{Q})^{\mathrm{tors}}$ is finite.

Optional additional exercises: 3.7, 4.1–4.3, 7.1, 7.2, 7.5, 7.6, 7.7, 8.12(c,e) of [Silverman].