Elliptic Functions and related topics

Problem sheet 8

Dr. L. Rolen, Dr. M. H. Mertens

Exercise 1. (4 points)
consider the elliptic curves E and $\overline{E}$ over $\mathbb{Q}$ defined by the equations

$$E:\ Y^2 = X^3 + aX + b \qquad \text{and} \qquad \overline{E}:\ Y^2 = X^3 + \overline{a}X + \overline{b}$$

where

$$\overline{a} = -2a \qquad \text{and} \qquad \overline{b} = a^2 - 4b.$$

Let $T = (0,0) \in E(\mathbb{Q})$ and $\overline{T} = (0,0) \in \overline{E}(\mathbb{Q})$ and define the two maps

$$\phi : E \to \overline{E},\ P \mapsto \begin{cases} \left(\frac{y^2}{x^2}, \frac{y(x^2-b)}{x^2}\right) & \text{if } P = (x,y) \neq \mathcal{O}, T, \\ \overline{\mathcal{O}} & \text{if } P = \mathcal{O} \text{ or } P = T, \end{cases}$$

and

$$\psi : \overline{E} \to E,\ \overline{P} \mapsto \begin{cases} \left(\frac{\overline{y}^2}{4\overline{x}^2}, \frac{\overline{y}(\overline{x}^2-\overline{b})}{8\overline{x}^2}\right) & \text{if } \overline{P} = (\overline{x},\overline{y}) \neq \overline{\mathcal{O}}, \overline{T}, \\ \mathcal{O} & \text{if } \overline{P} = \overline{\mathcal{O}} \text{ or } \overline{P} = \overline{T}. \end{cases}$$

Show that the composition $\psi \circ \phi$ (resp. $\phi \circ \psi$) is the multiplication-by-2 map on E (resp. $\overline{E}$).

Exercise 2. (4 points)
For $\kappa > 0$ let $R(\kappa) := \{x \in \mathbb{Q} \ : \ H(x) \leq \kappa\}$.

(a) Show that $\#R(\kappa) \leq 2\kappa^2 + 1$.

(b) Prove that

$$\lim_{\kappa\to\infty} \frac{\#R(\kappa)}{\kappa^2} = \frac{12}{\pi^2}.$$

Hint: You may (and should) use the following formula from Analytic Number Theory (a proof is not required),

$$\sum_{n\leq x} \frac{\varphi(n)}{n} = \frac{x}{\zeta(2)} + O(\log x),$$

where φ denotes Euler's totient function, i.e. $\varphi(n)$ is the number of integers $x \in \{1, ..., n-1\}$ with $\gcd(x,n) = 1$.

Exercise 3. (4 points)
Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be distinct points on an elliptic curve E over $\mathbb{Q}$ defined by the equation

$$Y^2 = X^3 + aX + b,$$

where a, b are integers which satisfy $P_1 \pm P_2 \neq \mathcal{O}$. Define $P_3 = (x_3, y_3) = P_1 + P_2$ and $P_4 = (x_4, y_4) = P_1 - P_2$.

(a) Express the quantities $x_3 + x_4$ and $x_3 x_4$ in terms of x_1 and x_2.

(b) Prove that there is a constant κ, depending only on a and b, such that it holds for all rational points P_1 and P_2 on E that

$$h(P_1 + P_2) + h(P_1 - P_2) \leq 2h(P_1) + 2h(P_2) + \kappa.$$

Hint: Replace P_1 and P_2 by $P_1 + P_2$ and $P_1 - P_2$ and use that known bound $h(2P) \geq 4h(P) - \kappa_0$.

Exercise 4. (4 points)
One can define a group law on a singular cubic curve as well using the same geometric procedure as in Exercise 1 of Problem sheet 7 and excluding the singular points. The group of non-singular points of a singular cubic curve C is denoted by C_{ns}. Let C be defined by the equation $Y^2 = X^3$ (whose only singularity is at $(0, 0)$). Prove that the map

$$\phi : C_{ns}(\mathbb{Q}) \to \mathbb{Q},\ P \mapsto \begin{cases} \frac{x}{y} & \text{if } P = (x, y) \neq \mathcal{O}, \\ 0 & \text{if } P = \mathcal{O} \end{cases}$$

is an isomorphism of abelian groups so that in particular the group $C_{ns}(\mathbb{Q})$ is *not* finitely generated.

Deadline: Tuesday, Dec. 2, 2014 at the beginning of the lecture.