Fachbereich Mathematik
Elena Klimenko

WS 2017/18
Homework 9

NUMBER THEORY AND CRYPTOGRAPHY

Due in class on Friday, December 22nd, at 12:05 pm.

1. Let $C \geq 2$, let

$$E(\mathbb{Q}) = \mathcal{O} \cup \{(x,y) \in \mathbb{Q} \times \mathbb{Q} \mid y^2 = x^3 + bx + c \text{ with } b, c \in \mathbb{Z}\},$$

and let $h : E(\mathbb{Q}) \to [0,\infty)$, $\left(\frac{m}{M}, y\right) \mapsto \log(\max\{|m|, |M|\})$, be the (logarithmic) height function.

(a) Prove that the set

$$\{P \in E(\mathbb{Q}) \mid h(P) \leq C\}$$

contains at most $4(\lambda^2 - \lambda - 6)$ elements, where $\lambda = \lfloor e^C \rfloor$.
Here the symbol $\lfloor\ \rfloor$ denotes the greatest integer function (floor).

(b) Can you improve the upper bound given in (a)?

2. Prove that the only point with rational coordinates on the elliptic curve given by the equation

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

is the point $(0,0)$.

Hint: You can try to prove this by contradiction starting with the fact that the point with rational coordinates on the elliptic curve looks like $\left(\frac{m}{d^2}, \frac{n}{d^3}\right)$ in lowest terms. The fact that the equation

$$a^4 + b^4 = c^2$$

has no solutions in positive integers might also be helpful.

3. Let A and B be abelian groups written additively and let $\varphi : A \to B$ and $\psi : B \to A$ be homomorhisms. Suppose that there is an integer $m \geq 2$ so that

$$\psi \circ \varphi(a) = ma \quad \text{for all } a \in A.$$

Suppose further that the indices $[A : \psi(B)]$ and $[B : \varphi(A)]$ are finite. Prove that mA has finite index in A, moreover,

$$[A : mA] \leq [A : \psi(B)] \cdot [B : \varphi(A)]\,.$$

Problem 4 is on the back.

4. Let $\Gamma = E(\mathbb{Q})$ and $\widetilde{\Gamma} = \widetilde{E}(\mathbb{Q})$, where E, $\widetilde{E}$ are elliptic curves defined by the equations

$$y^2 = x^3 + \alpha x^2 + \beta x \quad (\alpha,\ \beta \in \mathbb{Z})$$

and

$$y^2 = x^3 + \widetilde{\alpha} x^2 + \widetilde{\beta} x \quad (\widetilde{\alpha} = -2\alpha,\ \widetilde{\beta} = \alpha^2 - 4\beta),$$

respectively.

Let $T = (0,0) \in E$ and $\widetilde{T} = (0,0) \in \widetilde{E}$. Suppose also that the homomorphisms $\varphi : \Gamma \to \widetilde{\Gamma}$ and $\psi : \widetilde{\Gamma} \to \Gamma$ are defined as follows.

$$\varphi(P) = \begin{cases} \left(\dfrac{y^2}{x^2}, \dfrac{y(x^2 - \beta)}{x^2} \right), & \text{if } P = (x,y) \neq \mathcal{O},\ T \\ \widetilde{\mathcal{O}}, & \text{if } P = \mathcal{O} \text{ or } P = T \end{cases}$$

and

$$\psi(\widetilde{P}) = \begin{cases} \left(\dfrac{\widetilde{y}^2}{4\widetilde{x}^2}, \dfrac{\widetilde{y}(\widetilde{x}^2 - \widetilde{\beta})}{8\widetilde{x}^2} \right), & \text{if } \widetilde{P} = (\widetilde{x},\widetilde{y}) \neq \widetilde{\mathcal{O}},\ \widetilde{T} \\ \mathcal{O}, & \text{if } \widetilde{P} = \widetilde{\mathcal{O}} \text{ or } \widetilde{P} = \widetilde{T} \end{cases}$$

Show that $\psi \circ \varphi(P) = 2P$.