Fachbereich Mathematik und Statistik
Dr. Michele Serra
Prof. Dr. Salma Kuhlmann
SS 2023

Universität Konstanz

Introduction to Elliptic Curves

Exercise Sheet 4
Torsion points and elliptic curves over finite fields

Exercise 13 **(2+2 points)**
For the following elliptic curves, use the Lutz-Nagell theorem to determine the full set of torsion points, and the order of each point. Justify your answers.

(a) $E\colon Y^2 = X^3 + 2$

(b) $E\colon Y^2 = X^3 + 4X$

Exercise 14 **(2+2 points)**
Determine the full set of torsion points of the following elliptic curves, this time without appealing to Lutz-Nagell theorem but using reduction!

(a) $E\colon Y^2 = X^3 + 8$

(b) $E\colon Y^2 = X^3 + 18X + 72$

Exercise 15 *(The Frobenius endomorphism)* **(1+1+2 points)**
Let p be a prime number, let s be a positive natural number and let $q = p^s$. Let $\mathbb{F}_q$ be the field with q elements and let $\bar{\mathbb{F}}_q$ be its algebraic closure.
Now let E be an elliptic curve defined over $\mathbb{F}_q$ and define the *Frobenius endomorphism* as

$$\begin{array}{rccc} \varphi_q\colon & E(\bar{\mathbb{F}}_q) & \longrightarrow & E(\bar{\mathbb{F}}_q) \\ & (x,y) & \longmapsto & (x^q, y^q) \end{array}$$

(a) Show that we have $\mathbb{F}_q = \{x \in \bar{\mathbb{F}}_q : x^q = x\}$.

(b) Show that φ_q is well defined, i.e., $(x,y) \in E(\bar{\mathbb{F}}_q) \Rightarrow \varphi_q(x,y) \in E(\bar{\mathbb{F}}_q)$.

(c) Show that $|E(\mathbb{F}_q)| = \deg(\varphi_q - \mathrm{id}_{\mathrm{E}})$
where the difference $\varphi_q - \mathrm{id}_{\mathrm{E}}$ is to be understood in $\mathrm{End}(E)$.

Hint to (c): You may use, without proof, the fact that $\deg_i(\varphi_q) = q$ and $\deg_s(\varphi_q) = 1$ (i.e., φ_q is purely inseparable).

Exercise 16 (Hasse's inequality) **(4 points)**

Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$ of characteristic $\neq 2$. Show taht

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

Results you can use without proof

- For $\alpha, \beta \in \operatorname{End}(E)$ define
$$\langle \alpha, \beta \rangle := \frac{1}{2}(\deg(\alpha+\beta) - \deg(\alpha) - \deg(\beta))$$
- The map $\langle\ ,\ \rangle \colon \operatorname{End}(E) \times \operatorname{End}(E) \to \mathbb{Q},\ (\alpha, \beta) \mapsto \langle \alpha, \beta \rangle$ is a positive definite symmetric bilinear form.
- For $\alpha, \beta \in \operatorname{End}(E)$ and $m, n \in \mathbb{Z}$ we have
$$\deg(m\alpha + n\beta) = m^2 \deg(\alpha) + 2mn\langle \alpha, \beta \rangle + n^2 \deg(\beta)$$
- (Cauchy-Schwarz inequality)
$$\langle \alpha, \beta \rangle^2 \leq \deg(\alpha) \deg(\beta)$$

*Please hand in your solutions by **Wednesday, 14 June 2023, 13:30h** in the **"envelope-postbox" by F409** or per e-mail to your tutor.*