Elliptic curve cryptography, winter 2009

MICHAEL NÜSKEN, DANIEL LOEBENBERGER

5. Exercise sheet
Hand in solutions until Monday, 30 November 2009, 23^{59}

Exercise 5.1 (Isomorphic elliptic curves). (7 points)

Let $E\colon y^2 = x^3 + ax + b$ over a field k and let $d \in k^\times$. The *twist* of E by d is the elliptic curve $E^{(d)}\colon y^2 = x^3 + ad^2x + bd^3$.

(i) Show that $j(E) = j(E^{(d)})$. [2]

(ii) Show that $E^{(d)}$ can be transformed into E over $k(\sqrt{d})$. [3]

(iii) Show that $E^{(d)}$ can be transformed over k to the form $dy^2 = x^3 + ax + b$. [2]

Exercise 5.2 (Half a point). (7 points)

Elliptic curve $y^2 = x^3 + ax + b$ over $\mathbb{F}_p$ with $p \geq 5$.

(i) Let Q be a point on E and $R = 2Q$. How can one *compute* Q from R? [3]

(ii) What are possible numbers of solutions? [1]

(iii) What can you say about $\#E(\mathbb{F}_p)$ or the group structure of $E(\mathbb{F}_p)$, respectively, if there is point R with 2 (or 4) solutions for $R = 2Q$? [3]

Exercise 5.3 (Endomorphisms). (11 points)

We now explore several constructions for morphisms from an elliptic curve $E\colon x^3 + ax + b$ over $\mathbb{F}_q$ to itself:

(i) Show that the map $-\colon \overline{\mathbb{F}}_q \to \overline{\mathbb{F}}_q,\ (x, y) \mapsto (x, -y)$ is a group homomorphism. Determine its degree and the size of its kernel. [0]

(ii) Show that for each $k \in \mathbb{Z}$ the map $[k]\colon \overline{\mathbb{F}}_q \to \overline{\mathbb{F}}_q,\ P \mapsto [k]P$ is a group homomorphism. [1]

(iii) Determine $r_1(x)$ for $[3]$. Determine the degree and check if it is separable. [6]

(iv) Show that the Frobenius map $\varphi_q\colon \overline{\mathbb{F}}_q \to \overline{\mathbb{F}}_q,\ (x, y) \mapsto (x^q, y^q)$ is a group homomorphism. Determine its degree and the size of its kernel. [2]

(v) Show that for each $k \in \mathbb{Z}$ we have $\varphi_q \circ [k] = [k] \circ \varphi_q$. Hint: Do not try to find explicit formulae for kP! [2]

Exercise 5.4 (Strange endomorphisms). (8+4 points)

In this exercise we will consider some curves which have more endomorphisms than usual:

Consider the elliptic curve $E\colon y^2 = x^3 - x$ over $\mathbb{F}_p$.

3 (i) Show that the map $i\colon \overline{\mathbb{F}}_p \to \overline{\mathbb{F}}_p,\ (x, y) \mapsto (-x, iy)$, where $i^2 = -1$, is an endomorphism of the curve $E(\overline{\mathbb{F}}_p)$.

(ii) Consider $p \equiv_4 -1$.

1 (a) Determine if i is separable.

3 (b) Show that we have $\varphi_p \circ i \neq i \circ \varphi_p$ and express $i \circ \varphi_p$ in terms of $\varphi_p \circ i$.

(iii) Consider $p \equiv_4 +1$.

1 (a) Show that we have $\varphi_p \circ i = i \circ \varphi_p$.

+4 (b) Show that $\varphi_p = -1 - 2i$ in case $p = 5$. [Notice that $(-1 - 2i)(-1 + 2i) = 5$.]