Elliptic curve cryptography, winter 2009

MICHAEL NÜSKEN, DANIEL LOEBENBERGER

7. Exercise sheet
Hand in solutions until Monday, 14 December 2009, 23^{59}

Exercise 7.1 (Count it!). (10+10 points)

Let $E\colon y^2 = x^3 + ax + b$ be an elliptic curve defined over $\mathbb{F}_q$ with characteristic neither 2 nor 3. Denote by $E(\mathbb{F}_q)$ the set of F_q-rational points on the curve E and write $\#E(\mathbb{F}_q)$ for the number of $\mathbb{F}_q$-rational points on the curve.

(i) Show that $\#E(\mathbb{F}_q) \leq 2q + 1$. $\boxed{2}$

(ii) Show that we always have $\#E(\overline{\mathbb{F}}_q) = \infty$. $\boxed{2}$

(iii) Consider the (generalized) Legendre symbol $\boxed{3}$

$$\left(\frac{a}{\mathbb{F}_q}\right) := \begin{cases} 0 & \text{if } a = 0, \\ 1 & \text{if there is } b \in \mathbb{F}_q \text{ with } b^2 = a, \\ -1 & \text{if there is no } b \in \mathbb{F}_q \text{ with } b^2 = a. \end{cases}$$

Prove that $\#E(\mathbb{F}_q) = q + 1 + \sum_{x \in \mathbb{F}_q} \left(\frac{x^3+ax+b}{\mathbb{F}_q}\right)$.

(iv) Consider the curve $E\colon x^3 + x + 1$ over $\mathbb{F}_5$. Compute $\#E(\mathbb{F}_5)$ using the formula from (iii). $\boxed{3}$

(v) Consider the same situation over $\mathbb{F}_{5^2} = \mathbb{F}_5[x]/(x^2 + x + 1)$. Compute $\#E(\mathbb{F}_{5^2})$ using the formula from (iii). $\boxed{+5}$

(vi) Let E be now any curve in Weierstraß form defined over $\mathbb{F}_q$ and let $E^{(d)}$ be its twist by a nonsquare $d \in \mathbb{F}_q^\times$ as in Exercise 5.1. Write $\#E(\mathbb{F}_q) = q + 1 - t$. Show that $\#E^{(d)}(\mathbb{F}_q) = q + 1 + t$. *Hint*: Use the results from Exercise 5.1. Note that we always have $\left(\frac{ab}{\mathbb{F}_q}\right) = \left(\frac{a}{\mathbb{F}_q}\right) \cdot \left(\frac{b}{\mathbb{F}_q}\right)$. $\boxed{+5}$

Exercise 7.2 (Torsion). (11 points)

In class we considered the n-torsion of an elliptic curve E defined over $\mathbb{F}_q$ for $n = 2, 3$. In this exercise we will extend the results from the lecture:

(i) Prove by direct computations that in characteristic neither 2 nor 3 we have $E[4] \simeq \mathbb{Z}_4 \times \mathbb{Z}_4$. *Hint*: Consider points P with $2P = -2P$. $\boxed{5}$

(ii) Consider now E in characteristic 2. Show by direct computations that $E[3] \simeq \mathbb{Z}_3 \times \mathbb{Z}_3$. *Hint*: Write $P = (x_1, y_1)$ and $2P = (x_2, y_2)$. Then for $E\colon y^2 + xy = x^3 + a_2x^2 + a_6$ we have 6

$$x_2 = \frac{x_1^4 + a_6}{x_1^2} \text{ and } y_2 = x_2 + m(x_2 - x_1) + y_1, \text{ with } m = \frac{a_1 + x_1^2}{x_1}.$$

Otherwise if $E\colon y^2 + a_3y = x^3 + a_4x + a_6$ then

$$x_2 = m^2 \text{ and } y_2 = a_3 + m(m^2 - x_1) + y_1, \text{ with } m = \frac{x_1^2 + a_4}{a_3}.$$

Exercise 7.3 (Torsion of arbitrary abelian groups). (7 points)

7 Let G be any (finite) additively written abelian group and denote by $G[n]$ the set of all points of order dividing m. Prove that if $n = a \cdot b$ with $\gcd(a, b) = 1$ then $G[n] \simeq G[a] \times G[b]$. *Hint*: Extended Euclidean Algorithm!

Exercise 7.4 (Division polynomials). (0+20 points)

+20 The goal of this exercise is to prove the statement from the lecture that for $n \in \mathbb{Z}$ we have

$$nP = \left(\frac{\phi_n(x)}{\psi_n^2(x)}, \frac{\omega_n(x,y)}{\psi_n(x,y)^3}\right).$$

The goal of this exercise is to prove that. *Hint*: Start from the cases $n = 1$, $n = 2$. Do $n = 3$ and $n = 4$ with a computer algebra system of your choice. Try to prove the general statement by induction. *Warning*: This seems to be extremely tricky!