Elliptic curve cryptography, winter 2009

MICHAEL NÜSKEN, DANIEL LOEBENBERGER

9. Exercise sheet
Hand in solutions until Monday, 18 January 2010, 23^{59}

Exercise 9.1 (Subfield curves). (8+3 points)

Consider the elliptic curve $E\colon y^2 = x^3 + x - 1$ defined over $\mathbb{F}_5$.

(i) Show that we have for $x \in \mathbb{F}_q$ that $\left(\frac{x}{\mathbb{F}_q}\right) = x^{\frac{q-1}{2}}$. Hint: Use that $\mathbb{F}_q^\times$ is cyclic. [2]

(ii) Compute $t := q + 1 - \#E(\mathbb{F}_5)$ by using the formula from exercise 7.1 (iii) and 9.1 (i). [2]

(iii) Write $x^2 - tx + q = (x - \alpha)(x - \beta)$ for $\alpha, \beta \in \mathbb{C}$. Determine $\alpha^3 + \beta^3$. [3]

(iv) From this information determine $\#E(\mathbb{F}_{5^3})$. [1]

(v) Determine $\#E(\mathbb{F}_{5^{100}})$ [+3]

Exercise 9.2 (Group order and structure). (10 points)

Consider $q = 73$.

(i) Determine the Hasse interval of possible group sizes $\#E(\mathbb{F}_q)$. [1]

(ii) Consider the elliptic curve $E_1\colon y^2 = x^3 - 2x + 2$ defined over $\mathbb{F}_q$. The point $(-36, 24)$ on E_1 has order 23. Determine $\#E_1(\mathbb{F}_q)$ and the possible group structure of E_1. [1]

(iii) Consider the elliptic curve $E_2\colon y^2 = x^3 - 2x + 1$ defined over $\mathbb{F}_q$. The point $(20, 2)$ has order 5 and the point $(-23, -12)$ has order 8. Determine $\#E_2(\mathbb{F}_q)$and the possible group structure of E_2. [2]

(iv) Consider the elliptic curve $E_3\colon y^2 = x^3 - 3x + 5$ defined over $\mathbb{F}_q$. The point $(25, 15)$ has order 9 and the point $(17, -7)$ has order 15. Determine $\#E_3(\mathbb{F}_q)$ and the possible group structure of E_3. [2]

(v) Consider the elliptic curve $E_4\colon y^2 = x^3 + 16$ defined over $\mathbb{F}_q$. Both points $P := (-5, 16)$ and $Q := (-35, -24)$ have order 9. Determine $\#E_4(\mathbb{F}_q)$ and conclude the group structure. Hint: Show that there is no k such that $Q = kP$ or $3Q = kP$ and use Hasse. [4]

Exercise 9.3 (Distribution of sizes of elliptic curves). (8 points)

In this exercise we will explore how the sizes of elliptic curves over some particular small finite field are distributed.

4 (i) Write a small program that counts the number of points of all elliptic curves in Weierstraß form over $\mathbb{F}_{11}$. To do so, generate all possible equations of the form $y^2 = x^3+ax+b$ with $a, b \in \mathbb{F}_{11}$ and count for each choice of a and b using for example the formula from exercise 7.1 (iii) how many pairs $(x, y) \in \mathbb{F}_{11}^2$ exist that fullfill that equation. Do not forget to count the point at infinity!

2 (ii) Nicely plot the statistics and compare your results to Hasse's bound $|\#E(\mathbb{F}_q) - q - 1| \leq 2\sqrt{q}$.

2 (iii) Explain the symmetry of the plot.

Exercise 9.4. (4 points)

4 Assume you are given an elliptic curve E defined over $\mathbb{F}_q$ together with two points P and Q with $\operatorname{ord}(P) = m$ and $\operatorname{ord}(Q) = n$ with $\gcd(m, n) = 1$. Determine $\operatorname{ord}(P + Q)$.

Exercise 9.5 (Implementing Schoof). (0+10 points)

+10 Implement Schoof's algorithm in a programming language of your choice. It may be useful to use a computer algebra system to do so.