Elliptic curve cryptography, winter 2009

MICHAEL NÜSKEN, DANIEL LOEBENBERGER

11. Exercise sheet
Hand in solutions until Monday, 01 February 2010, 23^{59}

Exercise 11.1 (Constructing functions with a given divisor). (5 points)

Consider the elliptic curve $E\colon y^2 = x^3 + x - 1$ defined over $\mathbb{F}_{17}$. Let $D := [1,-1] + [0,4] + [8,-3] + [2,-3] - 4[\mathcal{O}] \in \mathrm{Div}^0(E)$. Compute a function f on E with $\mathrm{div}(f) = D$ by following the proof characterizing principal divisors. [5]

Exercise 11.2 (Properties of the order at some point). (7 points)

Assume you are given two quolynomial functions f, g on an elliptic curve E with a point P on it. Goal of this exercise is to compute and $\mathrm{ord}_P(f+g)$.

(i) Show that $\mathrm{ord}_P(fg) = \mathrm{ord}_P(f) + \mathrm{ord}_P(g)$. [2]

(ii) Now assume $f = -g$. Compute $\mathrm{ord}_P(f+g)$. [1]

(iii) Show that if $\mathrm{ord}_P(f) \neq \mathrm{ord}_P(g)$ we have [2]

$$\mathrm{ord}_P(f+g) = \min(\mathrm{ord}_P(f), \mathrm{ord}_P(g)).$$

(iv) Finish by proving that if $f \neq -g$ we have [2]

$$\mathrm{ord}_P(f+g) \geq \min(\mathrm{ord}_P(f), \mathrm{ord}_P(g)).$$

Exercise 11.3 (Divisors). (10 points)

Let E be an elliptic curve and $D = \sum_{P \in E} n_P[P] \in \mathrm{Div}(E)$ a divisor. Write $D \geq 0$ if and only if for all $P \in E$ we have $n_P \geq 0$.

(i) Characterize all functions on E with $\mathrm{div}(f) \geq 0$. [1]

(ii) Characterize all functions on E with $\mathrm{div}(f) + [P] - [Q] \geq 0$, where P and Q are different points on E. [2]

(iii) Characterize all functions on E with $\mathrm{div}(f) + [\mathcal{O}] \geq 0$. [3]

(iv) Characterize all functions on E with $\mathrm{div}(f) + 2[\mathcal{O}] \geq 0$. [4]

Exercise 11.4 (The second part of a missing proof). (13 points)

Let $E\colon y^2 = x^3 + ax + b$ be an elliptic curve defined over a field k with char $k \neq 2, 3$. In this exercise we will describe the second part of the constructive way to compute the order of a *polynomial* function $f = g(x) + yh(x)$ at some point P. We will here explore the case $P = (x_P, y_P)$ with $y_P \neq 0$ and show in the following that $u_P := x - x_P$ is a uniformization parameter at P.

[1] (i) Show that u_P vanishes at P.

Now write $f = (x - x_P)^r f_0$ with $f_0 := g_0(x) + yh_0(x)$ where $(x - x_P)^r$ is the highest power of $(x - x_P)$ that divides both: $g(x)$ and $h(x)$.

[1] (ii) Show that $g_0(x_P) \neq 0$ or $h_0(x_P) \neq 0$.

[2] (iii) Let $\bar{f}_0 := g_0(x) - yh_0(x)$. Show that if $f_0(P) = 0$ and $y_P \neq 0$ then $\bar{f}_0(P) \neq 0$.

[3] (iv) Conclude that we can write $f_0 = (x - x_P)^s f_1$ for some polynomial function f_1 on E where $(x - x_P)^s$ is the highest power of $x - x_P$ that divides $\operatorname{norm}(f_0)$. Hint: Note that $\operatorname{norm}(f_0) = f_0 \cdot \bar{f}_0$.

[3] (v) Finally prove that u_P is indeed a uniformization parameter for the point P and give a formula for the order of f at P.

[3] (vi) Consider the elliptic curve $E\colon y^2 = x^3 + 2x - 3$ with the point $P = (6, -15)$ on it. Let $f = y^2x^3 + xy + x - 36$ be a function on E. Compute $\operatorname{ord}_P(f)$.