Elliptic curve cryptography, winter 2009

MICHAEL NÜSKEN, DANIEL LOEBENBERGER

10. Exercise sheet
Hand in solutions until Monday, 25 January 2010, 23^{59}

Exercise 10.1 (Divisors over $\mathbb{P}^1\mathbb{C}$). (8 points)

In this exercise we will explore further the relationship between functions and their divisors over $\mathbb{P}^1\mathbb{C}$.

(i) Prove that the function $u_a := x - a$ is a uniformizer for $a \in \mathbb{C}$. $\boxed{2}$

(ii) Show that $u_\infty := 1/x$ is a uniformizer for ∞. $\boxed{2}$

(iii) Compute the divisors of u_a and u_∞ over $\mathbb{C}$. $\boxed{1}$

(iv) Compute the divisors of u_a and u_∞ over $\mathbb{P}^1\mathbb{C}$. $\boxed{1}$

(v) Compute the divisor of $f := \frac{(x-1)(x-3)^5}{(x+7)^{11}}$ over $\mathbb{P}^1\mathbb{C}$. $\boxed{2}$

Exercise 10.2 (Divisors on elliptic curves). (10 points)

Let $E\colon y^2 = x^3+ax+b$ be an elliptic curve defined over a field k with $\mathrm{char}(k) \neq 2, 3$.

(i) Suppose P_1, P_2, P_3 are three points on the line $\ell := c_0 + c_1x + c_2y$ with $c_0, c_1, c_2 \in k$, $c_2 \neq 0$. Compute $\mathrm{div}(\ell)$, its degree, and its sum. $\boxed{3}$

(ii) Write now $P_3 = (x_3, y_3)$ and consider the vertical line $v := x - x_3$. Compute $\mathrm{div}(v)$, its degree, and its sum. $\boxed{3}$

(iii) Conclude on the divisor of $f := \frac{\ell}{v}$, determine its degree and its sum. $\boxed{1}$

(iv) Explain why this shows that finding functions on the curve E with a predescribed divisor may be more difficult than over $\mathbb{P}^1\mathbb{C}$. $\boxed{3}$

Exercise 10.3 (Some examples). (7 points)

(i) Consider the elliptic curve $E\colon y^2 = x^3 + x + 1$ over $\mathbb{C}$ with the point $P = (0, 1)$ on it. The function $f := x^2 + y^2 - 1$ vanishes at P. Compute $\mathrm{ord}_P(f)$. $\boxed{2}$

(ii) Consider the elliptic curve $E\colon y^2 = x^3 + 2$ over $\mathbb{F}_{101}$ with the point $P = (6, 4)$ on it. The function $f := x+y-10$ vanishes at P. Compute $\mathrm{ord}_P(f)$. $\boxed{5}$

Exercise 10.4 (A part of a missing proof). (12 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 first part of the constructive way to compute the order of a *polynomial* function f at some point P. To do so we will construct a uniformization parameter u_P at P. Now we will only explore the case $P = \mathcal{O}$. A good part of the case $P \neq \mathcal{O}$ will be covered on the next exercise sheet. For the proof, we need some basic facts and several definitions for polynomial functions on the curve.

$\boxed{1}$ (i) Prove that we can write any polynomial function $f(x, y)$ on the curve as $f(x, y) = g(x) + yh(x)$.

We define the norm of $f(x, y) := g(x) + yh(x)$ to be

$$\operatorname{norm}(f) := g^2 - h^2(x^3 + ax + b) \in k[x]$$

and the degree of f as $\deg(f) := \deg(\operatorname{norm}(f))$.

$\boxed{1}$ (ii) Compute the degree of x and the degree of y.

For a quoynomial function $q(x, y) = \frac{f_1(x,y)}{f_2(x,y)}$ define $\deg(q) := \deg(f_1) - \deg(f_2)$. We also need a notion for the *value* of a quolynomial function $q(x, y)$ at $P \neq \mathcal{O}$. The following makes that precise:

$$q(P) := \begin{cases} \frac{f_1(P)}{f_2(P)} & \text{if there are } f_1, f_2 \in k[x, y] \text{ with } q = \frac{f_1}{f_2} \text{ and } f_2(P) \neq 0 \\ \infty & \text{otherwise} \end{cases}$$

One can show that this is indeed well defined. Writing now $q(x, y) = \frac{f_1(x,y)}{f_2(x,y)}$ we define for $P = \mathcal{O}$

$$q(\mathcal{O}) := \begin{cases} 0 & \text{if } \deg(q) < 0 \\ \infty & \text{if } \deg(q) > 0 \\ \operatorname{lcoeff}(f_1)/\operatorname{lcoeff}(f_2) & \text{otherwise} \end{cases}$$

We will show in the following that $u_{\mathcal{O}} := x/y$ is a uniformization parameter at $\mathcal{O}$.

$\boxed{2}$ (iii) Show that $u_{\mathcal{O}} := x/y$ vanishes at $\mathcal{O}$.

$\boxed{3}$ (iv) Write $f = \left(\frac{x}{y}\right)^{-\deg(f)} s$ with $s := \left(\frac{y}{x}\right)^{-\deg(f)} f$. Show that $s(P) \neq 0, \infty$.

$\boxed{1}$ (v) Conclude that $u_{\mathcal{O}}$ is a uniformization parameter at $\mathcal{O}$.

$\boxed{2}$ (vi) Compute $\operatorname{ord}_{\mathcal{O}}(x)$ and $\operatorname{ord}_{\mathcal{O}}(y)$.

$\boxed{2}$ (vii) Compute $\operatorname{ord}_{\mathcal{O}}(x^2 + y(x + 1))$.