Elliptic curve cryptography, winter 2009
Michael Nüskén, 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 $a \in \mathbb{C}$. 2
(ii) Show that $u_\infty := 1/x$ is a uniformizer for $\infty$. 2
(iii) Compute the divisors of $u_a$ and $u_\infty$ over $\mathbb{C}$. 1
(iv) Compute the divisors of $u_a$ and $u_\infty$ over $\mathbb{P}^1\mathbb{C}$. 1
(v) Compute the divisor of $f := \frac{(x-1)(x-3)^5}{(x+7)^3}$ over $\mathbb{P}^1\mathbb{C}$. 2

Exercise 10.2 (Divisors on elliptic curves). (10 points)
Let $E : y^2 = x^3 + ax + b$ be an elliptic curve defined over a field $k$ with $\text{char}(k) \neq 2, 3$.

(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 $\text{div}(\ell)$, its degree, and its sum. 3
(ii) Write now $P_3 = (x_3, y_3)$ and consider the vertical line $v := x - x_3$. Compute $\text{div}(v)$, its degree, and its sum. 3
(iii) Conclude on the divisor of $f := \frac{x}{\ell}$, determine its degree and its sum. 1
(iv) Explain why this shows that finding functions on the curve $E$ with a predescribed divisor may be more difficult than over $\mathbb{P}^1\mathbb{C}$. 3

Exercise 10.3 (Some examples). (7 points)

(i) Consider the elliptic curve $E : y^2 = x^3 + x + 1$ over $\mathbb{C}$ with the point $P = (0, 1)$ on it. The function $f := x^2 + y^2 - 1$ vanishes at $P$. Compute $\text{ord}_P(f)$. 2
(ii) Consider the elliptic curve $E : y^2 = x^3 + 2$ over $\mathbb{F}_{101}$ with the point $P = (6, 4)$ on it. The function $f := x + y - 10$ vanishes at $P$. Compute $\text{ord}_P(f)$. 5
Exercise 10.4 (A part of a missing proof). (12 points)

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

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

We define the norm of \( f(x, y) := g(x) + yh(x) \) to be
\[
\text{norm} (f) := g^2 - h^2 (x^3 + ax + b) \in k[x]
\]
and the degree of \( f \) as \( \deg(f) := \deg(\text{norm}(f)). \)

\( \text{(ii) Compute the degree of } x \text{ and the degree of } y. \)

For a polynomial 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 polynomial 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 \( P = \mathcal{O} \)
\[
q(\mathcal{O}) := \begin{cases} 
0 & \text{if } \deg(q) < 0 \\
\infty & \text{if } \deg(q) > 0 \\
l\text{coeff}(f_1) / l\text{coeff}(f_2) & \text{otherwise}
\end{cases}
\]

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

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

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

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

\( \text{(vi) Compute ord}_\mathcal{O}(x) \text{ and ord}_\mathcal{O}(y). \)

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