Elliptic curves: exercise sheet 3

Due: 1st October 2013

Mastermath / DIAMANT, Fall 2013

René Schoof and Peter Stevenhagen

Exercise 21. Let k be a field. Let C be the smooth curve in $\mathbf{A}^2$ given by $y^2 = x$. Let $P = (\alpha, \beta)$ be a point in $C(k)$.

(a) Show that the function $y - \beta$ is a uniformizing element of P.

(b) Suppose that $\mathrm{char}(k) \neq 2$. Show that $x - \alpha$ is a uniformizing element of P if and only if $P \neq (0, 0)$.

Exercise 22. Let k be a field and let C be the smooth projective curve given by the equation $Y^2 = XZ$ in $\mathbf{P}^2$. Let $P = (0 : 0 : 1)$ and $Q = (1 : 0 : 0)$.

(a) Show that the divisor of the function $f = Y/Z$ is equal to $P - Q$.

(b) Show that the divisor of the function $g = X/Z$ is equal to $2P - 2Q$.

(c) Exhibit a function whose divisor is $R - P$ where $R = (1 : 1 : 1)$.

Exercise 23. Let k be a field of characteristic not 2 or 3 and let E be an elliptic curve over k given by the equation $y^2 = x^3 + Ax + B$ with $4A^3 + 27B^2 \neq 0$ in k. Let P be a point on E that is defined over k.

(a) Show that if P is of the form (α, β) with $\beta \neq 0$, then the function $x - \alpha$ is a uniformizing element of P.

(b) Show that if P is of the form $(\alpha, 0)$, then the function y is a uniformizing element of P.

(c) Show that if P is the point at infinity, then the function x/y is a uniformizing element for P.

Exercise 24. Let k be a field of $\mathrm{char}(k) \neq 7$ and let K be the Klein curve: $X^3Y + Y^3Z + Z^3X = 0$ in $\mathbf{P}^2$.

(a) Show that K is smooth.

(b) Compute the divisors of the functions X/Y and X/Z.

Exercise 25. Let C be a smooth projective curve defined over a field k. The support of a divisor $D = \sum_P n_P P$ is the finite set of points for which $n_P \neq 0$. For any divisor

$D = \sum_P n_P P$ and any function $f \in k(C)^*$ for which the supports of D and (f) are disjoint, we put $f(D) = \prod_P f(P)^{n_P}$. *Weil reciprocity* is the statement that

$$f((g)) = g((f)).$$

Prove this for $C = \mathbf{P}^1$.

Exercise 26. Let C be a smooth projective curve defined over a field k and let D be a divisor defined over k.

(a) Show that $L(D) = \{f \in k(C)^* : (f) \geq -D\} \cup \{0\}$ is a k-vector space. Its dimension is denoted by $l(D)$.

(b) Suppose that D' is a divisor of C defined over k that is *equivalent* to D, i.e., the classes of D and D' in $\mathrm{Pic}(C)$ are equal. Show that $\deg(D) = \deg(D')$. Show that $l(D) = l(D')$.

(c) Suppose that $k = \mathbf{F}_q$ is a finite field with q elements. Show that the number of *effective* divisors of C that are defined over k and are equivalent to D is equal to

$$\frac{q^{l(D)} - 1}{q - 1}.$$

Exercise 27. Let k be a field. For convenience we assume that it is algebraically closed. Let C be a smooth projective curve defined over a field k and let D be a divisor of C.

(a) Show that $l(D) = 0$ when $\deg(D) < 0$.

(b) Suppose that $\deg(D) \geq 0$. Show that either $l(D) = 0$ or $l(D) = l(D')$ for some effective divisor D'.

(c) Suppose that D is effective and suppose P is a point on C for which $n = \mathrm{ord}_P(D)$ is positive. Let $\pi \in k(C)$ be a uniformizing element of P. In other words, we have $\mathrm{ord}_P(\pi) = 1$. Show that the map

$$L(D) \longrightarrow k$$

given by $f \mapsto (\pi^n f)(P)$ is a k-linear map with kernel $L(D - P)$.

(d) Deduce from (a), (b) and (c) that for every divisor D with $\deg(D) \geq 0$, we have $l(D) \leq \deg(D) + 1$.

Exercise 28. Let C be a smooth projective curve over a finite field $\mathbf{F}_q$.

(a) Let $d \geq 1$. Show that C has only finitely many points that are defined over $\mathbf{F}_{q^d}$.

(b) Show that there are only finitely many effective divisors of bounded degree that are defined over $\mathbf{F}_{q^d}$.

(c) Show that for $d \gg 0$ the set of divisor classes of divisors of degree d that are defined over $\mathbf{F}_q$, is finite.

(d) Show that the group $\mathrm{Pic}^0(C)$ is finite.

Exercise 29. Let C be a smooth curve over a finite field $\mathbf{F}_q$. The Zeta-function of C is the power series defined by

$$Z_C(T) \;=\; \sum_{D \geq 0} T^{\deg D} \;\in \mathbf{Z}[[T]].$$

Here D runs over the effective divisors of C that are defined over $\mathbf{F}_q$. It is related to the zeta-function of Exercise 8 via $\zeta_C(s) = Z_C(q^{-s})$.

(a) Show that $Z_C(T)$ is well defined.

(b) Show that

$$Z_C(T) \;=\; \sum_{[D]} \frac{q^{l[D]} - 1}{q - 1} T^{\deg [D]}.$$

This time $[D]$ runs over the *equivalence classes* of divisors D of C that are defined over $\mathbf{F}_q$ and $l[D]$ indicates $l(D)$.

(c) Prove that $Z_C(T)$ is a rational function. Hint: use the Riemann-Roch Theorem.

Exercise 30. Let C be a smooth curve over a finite field $\mathbf{F}_q$.

(a) Let $d \geq 1$. Show that the number N_d of points in $C(\overline{k})$ with residue field $\mathbf{F}_{q^d}$ is divisible by d. We put $N_d = da_d$.

(b) Show that

$$Z_C(T) \;=\; \prod_{d=1}^{\infty} \left(\frac{1}{1 - T^d} \right)^{a_d}.$$

(c) Show that

$$Z_{\mathbf{P}^1}(T) \;=\; \frac{1}{(1 - T)(1 - qT)}.$$