Elliptic curve cryptography, winter 2009

MICHAEL NÜSKEN, DANIEL LOEBENBERGER

2. Exercise sheet
Hand in solutions until Sunday, 8 November 2009, 23^{59}

Exercise 2.1 (Characteristic). (3 points)

Let k be a field. Recall that $\operatorname{char}(k) := \min\{m \mid m \cdot 1_k = 0_k\}$ where we define $\min\{\} := \infty$. Show that the *characteristic* $\operatorname{char}(k)$ *of* k is either prime or ∞. $\boxed{3}$

Exercise 2.2 (Smoothy). (14 points)

Let C be a cubic curve given by a polynomial $f \in k[x, y]$ and let $F \in k[X, Y, Z]$ be its homogenization, i.e. $F = Z^3 f(X/Z, Y/Z)$. In the course we saw that f is smooth if and only if it is smooth at infinity and there are no (affine) solutions to the system of equations $f = 0, f_x = 0, f_y = 0$. We will show that this is equivalent to the requirement that the system of equations $F = 0, F_X = 0, F_Y = 0, F_Z = 0$ has only the solution $X = Y = Z = 0$. To do so let $P = (x, y)$ be a point on $\{f = 0\}$, that is with $f(P) = 0$.

(i) Show that if all derivatives of f vanish at P then all derivatives of F vanish at $(X, Y, 1)$, where $X = x$ and $Y = y$. $\boxed{3}$

(ii) Show that for any homogeneous polynomial F all derivatives are homogeneous. $\boxed{2}$

(iii) Show that we always have $\boxed{1}$

$$F(0, 0, 0) = F_X(0, 0, 0) = F_Y(0, 0, 0) = F_Z(0, 0, 0) = 0.$$

(iv) Using (ii), show that if all derivatives of F vanish at $(X, Y, 1)$ then all derivatives of F vanish at $(\beta X, \beta Y, \beta)$ for some $\beta \in k^\times$. $\boxed{1}$

(v) Conclude that if all derivatives of F vanish at (X, Y, Z) then $\boxed{3}$

- all derivatives of $f(U, V) = F(U, V, 1)$ vanish at the point $\left(\frac{X}{Z}, \frac{Y}{Z}\right)$ provided $Z \neq 0$,
- all derivatives of $g(U, V) := F(U, 1, V)$ vanish at the point $\left(\frac{X}{Y}, \frac{Z}{Y}\right)$ provided $Y \neq 0$,
- all derivatives of $h(U, V) := F(1, U, V)$ vanish at the point $\left(\frac{Y}{X}, \frac{Z}{X}\right)$ provided $X \neq 0$.

(vi) We have now shown that for a single point $P = X : Y : Z$ with $XYZ \neq 0$ 4
we can either look at f and its derivatives or at g or at h. For a point where one of the coordinates vanishes, we look at those functions among $\{f, g, h\}$ which pose no division problem. Prove now that the curve is smooth at all its points iff the system of equations $F = 0, F_X = 0, F_Y = 0, F_Z = 0$ has only the solution $X = Y = Z = 0$.

Exercise 2.3 (Transformers). (8 points)

Consider the curve given by the polynomial $x^3 - 2xy^2 + y^3 - x$ over the reals.

2 (i) Show that this curve has three points at infinity.

2 (ii) Write down the transformation that maps the (projective point representing the) x-direction to $(0, 0)$, the y-direction to the x-direction, and the point $(0, 0)$ to the y-direction.

2 (iii) Compute the equation of the transformed curve.

2 (iv) Plot the curve and its transform.

Exercise 2.4 (Degree? Invariant.). (9+4 points)

In the lecture we have discussed projective linear transformations. Namely we consider a transformations $\tau\colon \mathbb{P}k^2 \to \mathbb{P}k^2,\ x \mapsto M \cdot x$, where $M \in k^{3\times 3}$ is invertible.

2 (i) Consider an affine point (x, y). We apply τ by first embedding (x, y) in the projective space, obtaining the point $(X : Y : 1)$. We now apply τ, obtaining $(U : V : W) := \tau(X : Y : Z)$. If W is non-zero we get the transformed point $(u, v) = (U/W, V/W)$. Combine all those steps and write down the resulting map $\sigma\colon k^2 \to k^2,\ (x, y) \mapsto (u, v)$, i.e. give the corresponding formulas for u and v.

3 (ii) Show that σ maps lines to lines.

4 (iii) Show that σ maps ellipses, hyperbolas and parabolas to ellipses, hyperbolas and parabolas.

+4 (iv) Generalize this to show that σ maps curves defined by a polynomial $g \in k[x, y]$ of degree k to another curve defined by a polynomial of the same degree.