Elliptic curve cryptography, winter 2009

MICHAEL NÜSKEN, DANIEL LOEBENBERGER

3. Exercise sheet
Hand in solutions until Sunday, 15 November 2009, 23^{59}

Exercise 3.1 (Get your Weierstraß). (11 points)

You are given an elliptic curve E given by a general cubic polynomial $f = \sum_{i+j\leq 3} a_{i,j}x^i y^j \in k[x,y]$. Assume you have that the point $P = (0 : 1 : 0)$ is a flex point on the curve (that is a point P for which the tangent of the curve through P has no further intersection points, ie. the tangent through P intersects the curve three times at P). The line $\mathcal{L}$ is given by $Z = 0$.

(i) Compute the homogenization F of f. $\boxed{1}$

(ii) Parametrize $\mathcal{L}$ with a parameter $t \in k$ such that you obtain a linear parametrization $L(t)$ for the points of the line with $L(0) = P$. $\boxed{2}$

(iii) Compute the univariate polynomial $p = F \circ L$. $\boxed{2}$

(iv) By the definition of a flex point, the polynomial p has now a triple root at $t = 0$. Formulate the corresponding conditions on the coefficients of F. $\boxed{3}$

(v) We have almost arrived at the generalized Weierstraß form. Substitute $x = \frac{a_{0,2}}{a_{3,0}}u$ and $y = \frac{a_{0,2}}{a_{3,0}}v$ in F. Show that this leads to a cubic $G(u,v)$ in general Weierstraß form. $\boxed{3}$

Exercise 3.2 (A strange operation). (5 points)

Consider the elliptic curve $E\colon y^2 = x^3 - 7x + 6$ over $\mathbb{F}_{19}$. In the lecture we have introduced an operation $\boxplus$, by taking two points P, Q on the curve E and defining $P \boxplus Q$ to be the (unique) third intersection point of the line connecting P and Q with the curve. In this exercise we will show that this operation $\boxplus$ in not associative. The three points $P = (0,5)$, $Q = (1,0)$, $S = (2,0)$ lie on the curve E.

(i) Compute $P \boxplus Q$ and $(P \boxplus Q) \boxplus S$. $\boxed{2}$

(ii) Compute $Q \boxplus S$ and $P \boxplus (Q \boxplus S)$. $\boxed{2}$

(iii) Conclude that $\boxplus$ is not associative. $\boxed{1}$

Exercise 3.3 (The group law). (12+4 points)

Consider the elliptic curve $E\colon y^2 = x^3 - x + 1$ over $\mathbb{R}$. The three points $P = (-1, 1)$, $Q = (0, 1)$, $S = (3, -5)$ lie on the curve.

$\boxed{1}$ (i) Plot the real picture of the curve.

$\boxed{1}$ (ii) Compute $-P$.

$\boxed{1}$ (iii) Write down the line connecting P and $-P$.

$\boxed{1}$ (iv) Include it in your plot.

$\boxed{2}$ (v) Compute $P + Q$ and $Q + S$ together with the two lines connecting them.

$\boxed{2}$ (vi) Include also those two lines in your plot.

$\boxed{2}$ (vii) Compute $(P + Q) + S$ and $P + (Q + S)$. What do you observe?

$\boxed{1}$ (viii) Compute $((P + Q) + S) + Q$.

$\boxed{1}$ (ix) Compute $P + \mathcal{O}$ and $\mathcal{O} + \mathcal{O}$.

$\boxed{+4}$ (x) Do the same computations as in (i) – (ix) when considering the curve over $\mathbb{F}_{17}$.

Exercise 3.4 (Associativity). (0+7 points)

$\boxed{+7}$ Show, using a computer algebra system of your choice, that the group law on elliptic curves in Weierstraß form as defined in the lecture is associative. That is given point P, Q, S on the curve, we have $(P + Q) + S = P + (Q + S)$.

Hint: Do not consider any special cases, i.e. assume that in all occuring additions we add affine points with $S \neq \pm T$.

Exercise 3.5 (Smooth. Irreducible!). (0+4 points)

$\boxed{+4}$ Assume you are given curve E defined by a cubic bivariate polynomial $f \in k[x, y]$, where k is algebraically closed. Further assume that $f = g \cdot h$ for two non-constant polynomials $g, h \in k[x, y]$, ie. f is reducible. Show that in this case the curve E is not smooth.