Elliptic curve cryptography, winter 2009  
MICHAEL NUŠKEN, DANIEL LOEBENBERGER

4. Exercise sheet  
Hand in solutions until Monday, 23 November 2009, 2359

Exercise 4.1 ($j$-invariant). (11 points)
Consider the elliptic curve $E: y^2 = x(x - 1)(x - \lambda)$ over any field $k$ whose characteristic is neither 2 nor 3.

(i) Put the curve $E$ in Weierstraß form and show that its $j$ invariant is

$$j(E) = 2^8 \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2}$$

(ii) Show that if $j \neq 0, 1728$ then there are six distinct values of $\lambda$ giving this $j$ and that if $\lambda$ is one such value then the six are

$$\{\lambda, \frac{1}{\lambda}, \frac{\lambda - 1}{\lambda}, \frac{\lambda}{\lambda - 1}, \frac{1}{1 - \lambda}, 1 - \lambda\}.$$  

(iii) Show that if $j = 1728$ then $\lambda \in \{-1, \frac{1}{2}, 2\}$ and if $j = 0$ then $\lambda^2 - \lambda - 1 = 0$.

Exercise 4.2 (Get your Legendre). (8 points)
Consider the elliptic curve $E: y^2 = x^3 - 7x + 6$ over the field $\mathbb{F}_{17}$.

(i) Factor the polynomial $x^3 - 7x + 6$ over $\mathbb{F}_{17}$. 

(ii) Take the three roots $e_0, e_1$ and $e_2$, apply the transformation $u = \frac{x - e_0}{e_1 - e_0}$ and $v = (e_1 - e_0)^{-3} y$ and write down the resulting equation. You should obtain a curve in Legendre form.

(iii) Of course, we have selected one particular ordering of the three roots. Compute the corresponding $\lambda$ for each of the other permutations of the roots.
Exercise 4.3 (A special case of Fermat’s last theorem). (17 points)

Fermat’s last theorem states, that the equation \( x^n + y^n + z^n = 0 \) has no non-trivial integer solutions for \( n \geq 3 \). In this exercise we consider the special case \( n = 3 \). Thus consider the cubic \( x^3 + y^3 + z^3 = 0 \) with \( xyz \neq 0 \).

(i) Check that \( 0 : -1 : 1, -1 : 0 : 1 \) and \( 1 : -1 : 0 \) are flex points and the tangent at \( 1 : -1 : 0 \) goes through \( 0 : 0 : 1 \).

(ii) Check that for the map
\[
\tau: \mathbb{P}^2_k \to \mathbb{P}^2_k,
\]
\[
(x : y : z) \mapsto (u : v : w)
\]
with \( (u, v, w) := (z, -3x + 3y, -\frac{1}{12}x - \frac{1}{12}y) \) we have
\[
\tau(0 : -1 : 1) = 12 : -36 : 1
\]
\[
\tau(-1 : 0 : 1) = 12 : 36 : 1
\]
\[
\tau(1 : -1 : 0) = 0 : 1 : 0
\]
\[
\tau(0 : 0 : 1) = 1 : 0 : 0
\]

(iii) Determine the transformed equation.

(iv) It can be proven that this curve has only three rational solutions, namely \( 12 : \pm 36 : 1 \) and \( 0 : 1 : 0 \). Show that the point \( 12 : 36 : 1 \) implies for the point \( x : y : z \) that \( y = 0 \), the point \( 12 : -36 : 1 \) implies \( x = 0 \) and that the point \( 0 : 1 : 0 \) implies \( z = 0 \).

(v) Conclude that Fermat’s theorem for \( n = 3 \) is indeed true.

Exercise 4.4 (Elliptic curves in characteristic 2). (5 points)

In the lecture we usually excluded the case that the base field has characteristic 2 or 3. In this exercise we explore elliptic curves over fields of characteristic 2. Determine the addition formula for two points \( P \neq \pm Q \) on the curve
\[
y^2 + xy = x^3 + a_2x^2 + a_6.
\]

Note (and prove) that negation here is given by \(- (x, y) = (x, x + y)\).