Elliptic Functions and related topics

Problem sheet 7

Dr. L. Rolen, Dr. M. H. Mertens

Exercise 1. (4 points)
Let E be an elliptic curve over some field K, $\mathrm{char}(K) \nmid 6$, defined by the equation $Y^2 = 4X^3 - c_2X - c_3$.

(a) Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be distinct points on $E \setminus \{\mathcal{O}\}$, such that $x_1 \neq x_2$. Show that there exists a unique third intersection point $P \bullet Q = (x_3, y_3)$ of E and the line passing through P and Q by giving explicit formulas for x_3 and y_3 in terms of $x_1, x_2, y_1, y_2, c_2, c_3$.

(b) Define the point $P \oplus Q := (x_3, -y_3)$. For $K = \mathbb{C}$, show that the group law on E obtained from the parametrization

$$\Phi : \mathbb{C}/L \to E,\ \Phi(z + L) = \begin{cases} (\wp(z), \wp'(z)) & \text{for } z \notin L \\ \mathcal{O} & \text{for } z \in L \end{cases}$$

and the addition theorem of the Weierstraß $\wp$-function with respect to the lattice L with $g_2(L) = c_2$ and $g_3(L) = c_3$ is the same as the geometric one ($(P, Q) \mapsto P \oplus Q$ as defined above).

Exercise 2. (4 points)
Let $n \in \mathbb{N}$ be a squarefree number and let E_n be the congruent number curve with equation $Y^2 = X^3 - n^2X$.

(a) Prove that the map

$$\begin{aligned} \mathcal{T}_n : \{(a, b, c) \in \mathbb{Q}^3 : a^2 + b^2 = c^2, ab = 2n\} &\to \{(x, y) \in E_n(\mathbb{Q}) \setminus \{\mathcal{O}\} : y \neq 0\}, \\ (a, b, c) &\mapsto \left(\frac{-nb}{c + a}, \frac{2n^2}{c + a}\right) \end{aligned}$$

is a well-defined bijection with inverse map

$$\begin{aligned} \mathcal{U}_n : \{(x, y) \in E_n(\mathbb{Q}) \setminus \{\mathcal{O}\} : y \neq 0\} &\to \{(a, b, c) \in \mathbb{Q}^3 : a^2 + b^2 = c^2, ab = 2n\}, \\ (x, y) &\mapsto \left(\frac{n^2 - x^2}{y}, -\frac{2nx}{y}, \frac{x^2 + n^2}{y}\right). \end{aligned}$$

(b) Find at least 3 non-congruent right triangles with rational side lengths and area 6.

Hint: You may use without proof the duplication formula for a generic point $P = (x, y)$ on an elliptic curve E defined by the equation $Y^2 = 4X^3 - c_2X - c_3$,

$$2P = (x_3, y_3), \quad x_3 = \frac{1}{4}a^2 - 2x,\ y_3 = -ax_3 - y + ax,\ a = \frac{12x^2 - c_2}{2y}.$$

Exercise 3. (4 points)
Prove Fermat's Last Theorem for $n = 4$, i.e. that there are no integers a, b, c with $abc \neq 0$ such that

$$a^4 + b^4 = c^4.$$

Exercise 4. (4 points)
We have a look at a *Fermat curve* E with equation $Y^2 = 4X^3 - 1728$. Show that $E(\mathbb{Q}) = \langle (12, 72) \rangle \cong \mathbb{Z}/3\mathbb{Z}$ by proving that the sets $E' := \{(x, y) \in E \setminus \{\mathcal{O}\} : x \neq 0\}$ and $F := \{(u, v) \in \mathbb{Q}^2 : u^3 + v^3 = 1\}$ are in bijection via $u = \frac{72+y}{12x}$ and $v = \frac{72-y}{12x}$.
Hint: Remember Fermat's Last Theorem for $n = 3$.

Deadline: Tuesday, Nov. 25, 2014 at the beginning of the lecture.