**Mastermath Elliptic Curves, Homework 12**
Due: 8th December 2015, 10:15

Students are expected to (try to) solve all problems below. The ones marked as "hand in" are to be handed in and count towards your grade according to the rules on the web page.

**Problem 73** (hand in)**.** Let $k$ be any field, and let $C \subset \mathbb{P}^2$ be the cuspidal cubic curve over $k$ defined by the projective equation $Y^2Z = X^3$. Show that the chord-tangent construction gives a group operation on $C(k)\backslash\{(0,0)\}$, isomorphic to the additive group $k^+$. [Hint: you may find it easier to work on the affine piece $Y \neq 0$].

**Problem 74** (hand in)**.** Let $E$ be the elliptic curve over $\mathbb{Q}$ defined by the Weierstrass equation

$$y^2 = x^3 + 2x + 6.$$

(a) Show that $E$ has good reduction at both 3 and 5.

(b) Find the number of points of the reduction of $E$ over $\mathbb{F}_3$ and over $\mathbb{F}_5$.

(c) Deduce that $E(\mathbb{Q})$ is torsion-free.

**Problem 75.** Let $E$ be an elliptic curve over $\mathbb{Q}$ with good reduction at 3. Prove that $E$ cannot have a rational 9-torsion point.

**Problem 76** (hand in)**.** For each of the following elliptic curves $E$ over $\mathbb{Q}$, find the torsion subgroup $E(\mathbb{Q})$. (That is, describe both the torsion points and the group structure on them.)

(a) $y^2 = x^3 + 1$

(b) $y^2 = x^3 - 43x + 166$

(c) $y^2 = x^3 - 219x + 1654$

(d) $y^2 = x(x-1)(x+2)$

**Problem 77.** Let $G$ be a finitely generated Abelian group. Describe how the dimension of the $\mathbb{F}_2$-vector space $G/2G$ is related to the rank of $G$ and the structure of the 2-power torsion subgroup of $G$.

**Problem 78** (Silverman, exercise 8.13)**.** (a) Let $k$ be a field and let $E/k$ be an elliptic curve with $P \in E(k)$ a point of order $\geq 4$. Show that $E$ can be described by an equation of the form

$$y^2 + uxy + vy = x^3 + vx^2$$

with $u, v \in k$ and $P = (0,0)$.

(b) Show that there is a 1-dimensional family of elliptic curves over $k$ with a $k$-rational point of order 6. [Hint: Set $3P = -3P$, and see how $u$ and $v$ must be related.]