ASSIGNMENT MAT4230

This is the mandatory assignment for MAT 4230. This assignment needs to be passed in order to take the exam. The assignment must be handed in to me or at the institute's reception on the 7th floor, room 714 in NHA, by Tuesday 30th of October.

• *We assume that K is an algebraically closed field, with* $\mathrm{char}(K) \neq 3$. *We will study an elliptic curve E/K with Weierstrass equation*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x.$$

Note that since $a_6 = 0$, the point $P_0 = (0, 0)$ belongs to E.

(1) Show that P_0 is a singular point if and only if both $a_3 = 0$ and $a_4 = 0$.
(2) Show that P_0 is non-singular *and* $[2]P_0 = O_E$ if and only if $a_3 = 0$ and $a_4 \neq 0$.

• *We assume from now on that P_0 is a non-singular point on E and that* $[2]P_0 \neq O_E$.

(3) Show that, possibly after changing variables by $x = x'$ and $y = y' + (a_4/a_3)x'$, we can assume that $a_4 = 0$ and that E has Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2.$$

(4) Show that

$$L \ : \ y = 0,$$

the tangent line to E at P_0, has triple intersection with E at P_0 if and only if $a_2 = 0$ and $a_3 \neq 0$. Conclude that in this case

$$[3]P_0 = O_E,$$

i.e., P_0 is a point of order 3 on E.

• *We assume from now on that $a_2 = 0$ and $a_3 \neq 0$ so that* $[3]P_0 = O_E$. *In particular, E has Weierstrass equation*

$$y^2 + a_1xy + a_3y = x^3.$$

(5) For $u \in K$, show that the line

$$y = x + u$$

has a triple intersection point $(v, v + u)$ with E if and only if the equation

$$(*) \ x^3 - (x + u)^2 - (a_1x + a_3)(x + u) = (x - v)^3$$

holds. Conclude that

$$[3](v, v + u) = O_E.$$

(6) Show that the equality

$$(v+u)^3 = u^3$$

holds. Hint: compare the coefficients of x^2, x^1 and x^0 in the equation $(*)$ above. This yields three equations involving u, v, a_1 and a_3. (So a_1 and a_3 depend on the choice of u and v.) Eliminate a_1 and a_3 to produce the cubic relation between u and v.

• *It can be seen from equation* $(*)$ *that* $v \neq 0$ *(we will use this fact below). So in particular,* $(v, v+u) \neq (0,0)$*. It follows that* $v+u = \rho u$*, where* $\rho \in K$ *is a primitive third root of unity.*

(7) Use the standard formulas

$$\rho^2 + \rho + 1 = 0$$

and

$$3 = (1-\rho)(1-\rho^2)$$

to find an expression for $P_1 = (v, u+v)$ depending only on v. Use this to find expressions for a_1 and a_3 in terms of v.

• *From this exercise we can conclude that each choice* $0 \neq v \in K$*, yields an elliptic curve*

$$E_v \;:\; y^2 + a_1(v)xy + a_3(v)y = x^3,$$

with two distinguished points $P_0 = (0,0)$ *and* $P_1(v)$ *both of order* 3 *(we discard the finitely many* v *such that* E_v *is singular). In fact, it is not hard to see that they form a basis of the group of* 3*-torsion points*

$$E_v[3] \cong (\mathbb{Z}/3\mathbb{Z})^2.$$

The 1*-parameter family* E_v *is sometimes called the "Hessian family", and is a very classical and much studied family of elliptic curves.*