Examination: Mastermath Elliptic Curves

Tuesday 2nd June 2017

Answer all five questions. Calculators are **not** permitted. Justify your answers, and state the theorems that you use.

1. Let C be the affine plane curve over $\mathbb{C}$ given by the equation

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

R (a) For all values of $\alpha \in \mathbb{C}$, compute the intersection number at $(0,0)$ of C with the affine curve given by the equation $y = \alpha x$.

L (b) Determine the set of singular points in $\mathbb{P}^2(\mathbb{C})$ of the plane projective curve given by C.

2. This question concerns the following three lattices in $\mathbb{C}$:

$$\Lambda_1 = \langle 1, 2i \rangle, \quad \Lambda_2 = \langle 1, i/2 \rangle, \quad \Lambda_3 = \langle 1, i\sqrt{2} \rangle.$$

L (a) Compute the ring $\mathrm{End}(\mathbb{C}/\Lambda_1)$, that is, the ring of holomorphic functions $\phi\colon \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_1$ satisfying $\phi([0]) = [0]$.

L (b) Which (if any) of the three lattices are isogenous? Which (if any) are homothetic?

R **3.** Determine the torsion subgroup of $E(\mathbb{Q})$, where E is the elliptic curve given by the equation

$$y^2 = x^3 + 1.$$

In other words, give the structure of the group and give coordinates of generators.

4. Let E and E' be the elliptic curves over $\mathbb{Q}$ given by the equations

$$E : y^2 = x(x^2 + x - 7), \qquad E' : y^2 = x(x^2 - 2x + 29).$$

The curves E and E' are related by a 2-isogeny $\phi\colon E \to E'$, with dual $\hat{\phi}\colon E' \to E$.

L (a) Show that the groups $E'(\mathbb{Q})/\phi(E(\mathbb{Q}))$ and $E(\mathbb{Q})/\hat{\phi}(E'(\mathbb{Q}))$ are both isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

R (b) Calculate the rank of $E(\mathbb{Q})$.

5. Fix a field k of characteristic zero. Let C be a smooth projective plane curve over k. A point $P \in C(k)$ is called an *inflection point* if the tangent line at P meets C with multiplicity ≥ 3 at P, and an *ordinary inflection point* if the multiplicity is exactly 3.

L (a) Show that, on a smooth irreducible projective plane curve C over k of degree 3, every inflection point is ordinary.

L (b) If E is an elliptic curve over k defined by a Weierstrass equation, show that $P \in E(k)$ is an inflection point if and only if $3P = O$.

Let $F \in k[X, Y, Z]$ be an irreducible homogeneous polynomial, with $\deg F > 1$. The *Hessian* of F is the polynomial $H(F)$ that is the determinant of the 3×3 matrix of second partial derivatives of F:

$$H(F) = \det \begin{pmatrix} \frac{\partial^2 F}{\partial X^2} & \frac{\partial^2 F}{\partial X \partial Y} & \frac{\partial^2 F}{\partial X \partial Z} \\ \frac{\partial^2 F}{\partial Y \partial X} & \frac{\partial^2 F}{\partial Y^2} & \frac{\partial^2 F}{\partial Y \partial Z} \\ \frac{\partial^2 F}{\partial Z \partial X} & \frac{\partial^2 F}{\partial Z \partial Y} & \frac{\partial^2 F}{\partial Z^2} \end{pmatrix}.$$

Now let C be the plane projective curve defined by F, and assume that C is smooth. A standard result in geometry states that $H(F)$ is non-zero and defines a curve C_H having no components in common with F; that P is an inflection point of C if and only if $P \in (C \cap C_H)$; and that P is an ordinary inflection point if and only if $I_P(C, C_H) = 1$.

L (c) If k is algebraically closed of characteristic zero, prove that every elliptic curve over k has precisely nine distinct points P satisfying $3P = O$.

[Of course you may not use theorems from the course that say e.g. that $E[n]$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^2$.]

Formula sheet

Basic arithmetic Let $E : y^2 = x^3 + ax + b$ be a short Weierstrass equation.

(i) The discriminant of E (in the parts of Milne's book that we treated) is

$$\Delta = 4a^3 + 27b^2.$$

[In other sources, one uses the more standard -16 *times this quantity.]*

(ii) The j-invariant of E is

$$j = \frac{1728(4a^3)}{4a^3 + 27b^2}.$$

(iii) For $P = (x_1, y_1)$ a non-singular point of E, the x-coordinate of $2P$ is

$$\frac{(3x_1^2 + a)^2 - 8x_1 y_1^2}{4y_1^2}.$$

Descent by 2-isogeny Let E, E' be the two elliptic curves defined by

$$E : y^2 = x(x^2 + ax + b), \qquad E' : v^2 = u(u^2 + a'x + b')$$

with $a' = -2a$ and $b' = a^2 - 4b$, and let $\phi \colon E \to E'$ be the isogeny defined by

$$\phi(x, y) = (x + a + b/x, y - by/x^2) \text{ if } x \neq 0; \quad \phi((0,0)) = O.$$

Define a function $q \colon E'(\mathbb{Q}) \to \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ as follows:

$$q((u, v)) = [u] \text{ if } u \neq 0; \quad q((0,0)) = [a^2 - 4b]; \quad q(O) = [1].$$

Then q is a homomorphism of groups, and the sequence

$$E(\mathbb{Q}) \xrightarrow{\phi} E'(\mathbb{Q}) \xrightarrow{q} \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$$

is exact. Let r be a square-free integer. The class $[r] \in \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ lies in the image of q if and only if the equation

$$r^2\ell^4 + a'r\ell^2m^2 + b'm^4 = rn^2$$

has a non-zero solution (ℓ, m, n) with $\ell, m, n \in \mathbb{Z}$. Furthermore, this can only happen if r divides b'.