Resit Examination: Mastermath Elliptic Curves
Tuesday 26th January 2016

Answer all five questions. Attached you will find a copy of section 14 of Cassels' book, which you will find useful for question 5.

1. Compute the intersection number at $(0,0)$ of the affine curves

$$y^4 = x^5 \qquad \text{and} \qquad y = \alpha x$$

for all values of $\alpha \in \mathbb{C}$.

2. (i) Let C be a smooth, projective curve over a field k, and let $P \in C(k)$ be a point. Suppose that there exists a rational function $f \in k(C)$ satisfying $\mathrm{ord}_P(f) = -1$ and having no other poles. Show that $(f : 1)$ defines an isomorphism from C to $\mathbb{P}^1$. [Hint: consider the functions $f - \alpha$ for $\alpha \in \bar{k}$.]

(ii) Let E be a curve of genus 1 over k with a point $O \in E(k)$. Show that the function $E(k) \to \operatorname{Pic} E$ defined by $P \mapsto [P - O]$ is injective.

3. Let E be the elliptic curve over $\mathbb{C}$ defined by the Weierstrass equation

$$y^2 = x^3 + 4x^2 + 2x$$

and let $\phi\colon E \to E$ be the isogeny defined by

$$\phi(x,y) = \left(\alpha^{-2}\big(x + 4 + \frac{2}{x}\big), \alpha^{-3} y \big(1 - \frac{2}{x^2}\big)\right),$$

with $\alpha = i\sqrt{2}$.

(i) Compute the kernel of ϕ.

(ii) Compute the kernel of $\phi - [1]$, and conclude that $\phi - [1]$ has degree 3.

(iii) Prove that $\phi^2 = [-2]$.

4. Let E be the elliptic curve over $\mathbb{Q}$ defined by the Weierstrass equation

$$y^2 = x^3 - 4x + 3.$$

(i) Find the points of the elliptic curves obtained by reducing E modulo both 3 and 5.

(ii) Deduce that the torsion subgroup of $E(\mathbb{Q})$ has order 2.

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

$$E\colon y^2 = x^3 + 3x^2 + x, \qquad E'\colon y^2 = x^3 - 6x^2 + 5x.$$

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

(i) Show that the group $E'(\mathbb{Q})/\phi(E(\mathbb{Q}))$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

(ii) Assuming that $E(\mathbb{Q})/\hat{\phi}(E'(\mathbb{Q}))$ also has order 2, find the rank of $E(\mathbb{Q})$.

14

A 2-isogeny

An *isogeny* is a map

$$\mathcal{C} \to \mathcal{D}$$

of elliptic curves defined over the ground field and taking the specified rational point $o_{\mathcal{C}}$ on $\mathcal{C}$ into that on $\mathcal{D}$. Clearly the kernel of the isogeny, i.e. the set of points mapped into $o_{\mathcal{D}}$ is a finite group and is defined over the ground field as a whole.

In this section we consider the case when $\mathcal{C}$ has a rational point of order 2. It is convenient to modify our canonical form to

$$\mathcal{C}: \; Y^2 = X(X^2 + aX + b),$$

the point of order 2 being $(0,0)$. The function on the right hand side may not have a double root, so

$$b \neq 0, \qquad a^2 - 4b \neq 0.$$

We take $\mathbb{Q}$ to be the ground field. Let $\mathbf{x} = (x, y)$ be a *generic point* of $\mathcal{C}$; that is, x is transcendental and y is defined by

$$y^2 = x(x^2 + ax + b).$$

The field $\mathbb{Q}(x, y)$ is known as the *function field* of $\mathcal{C}$ over $\mathbb{Q}$.

Let

$$\mathbf{x}_1 = \mathbf{x} + (0, 0).$$

The transformation

$$\mathbf{x} \to \mathbf{x}_1$$

is an automorphism of $\mathbb{Q}(x, y)$ of order 2. We will find the fixed field.

The line through $(0,0)$ and (x,y) is

$$X = tx, \qquad Y = ty,$$

which meets $\mathcal{C}$ in $(0,0)$, $\mathbf{x}$ and $-\mathbf{x}_1 = (x_1, -y_1)$. We get

$$x_1 = b/x$$

$$y_1 = -by/x^2.$$

One invariant under $\mathbf{x} \to \mathbf{x}_1$ is clearly t^2, which is

$$t^2 = (y/x)^2 = \frac{x^2 + ax + b}{x}$$

$$= \lambda \qquad \text{(say)} \quad [= x + x_1 + a].$$

Another is

$$y + y_1 = \mu \qquad \text{(say)}.$$

To find an algebraic relation between λ, μ we compute

$$\mu^2 = y^2(1 - b/x^2)^2$$

$$= \frac{x^2 + ax + b}{x}(x^2 - 2b + b^2/x^2).$$

Here the first factor is just λ. The second is

$$(x + b/x)^2 - 4b = (\lambda - a)^2 - 4b$$

$$= \lambda^2 - 2a\lambda + (a^2 - 4b).$$

Hence

$$\mu^2 = \lambda(\lambda^2 - 2a\lambda + (a^2 - 4b)).$$

Conversely, we can express x, y in terms of λ, μ and

$$\lambda^{1/2} = y/x,$$

since

$$\lambda^{-1/2}\mu = x - b/x$$

$$\lambda = x + (b/x) + a.$$

Hence

$$x = \frac{1}{2}(\lambda + \lambda^{-1/2}\mu - a), \qquad y = \lambda^{1/2}x. \qquad (*)$$

The field extension $\mathbb{Q}(x, y)/\mathbb{Q}(\lambda, \mu)$ is of degree 2 and so by Galois theory $\mathbb{Q}(\lambda, \mu)$ is the complete field of invariants.

The point (λ, μ) is a generic point of

$$\mathcal{D}: \; Y^2 = X(X^2 - 2aX + (a^2 - 4b)).$$

The map

$$\phi: \; \mathcal{C} \to \mathcal{D}$$

given by

$$\mathbf{x} = (x, y) \to \boldsymbol{\lambda} = (\lambda, \mu)$$

preserves the group law[12]. For let $\mathbf{a}$, $\mathbf{b}$ be points on $\mathcal{C}$ and let $f \in \mathbb{Q}(\mathbf{x})$ be a function with simple poles at $\mathbf{a}$, $\mathbf{b}$ and simple zeros at $\mathbf{o}$, $\mathbf{a}+\mathbf{b}$. Let f_1 be the conjugate under $\mathbf{x} \to \mathbf{x}_1$. Then $ff_1 \in \mathbb{Q}(\boldsymbol{\lambda})$: as a function of $\boldsymbol{\lambda}$ it clearly has simple poles at $\phi(\mathbf{a})$, $\phi(\mathbf{b})$ and simple zeros at $\phi(\mathbf{o}) = \mathbf{o}$ and $\phi(\mathbf{a}+\mathbf{b})$. Hence

$$\phi(\mathbf{a}+\mathbf{b}) = \phi(\mathbf{a}) + \phi(\mathbf{b}).$$

The equation for $\mathcal{D}$ has the same general shape as that for $\mathcal{C}$. On repeating the process with λ and $\mathcal{D}$, we get ρ, σ with

$$\sigma^2 = \rho(\rho^2 + 4a\rho + 16b);$$

and so

$$\xi = \rho/4, \qquad \eta = \sigma/8$$

is a generic point of $\mathcal{C}$ again.

The points mapping into $(\lambda, \mu) = (0,0)$ are just the 2-division points other than $(0,0)$. Hence the kernel of the map $(x,y) \to (\xi, \eta)$ is just the 2-division points and $\mathbf{o}$. So the map must be multiplication by ± 2.

We now consider the effect of the isogeny

$$\phi: \ \mathcal{C} \to \mathcal{D}$$

on rational points. Denote the rational points on $\mathcal{C}$, $\mathcal{D}$ by $\mathfrak{G}$, $\mathfrak{H}$ respectively.

We denote the multiplicative group of nonzero elements of $\mathbb{Q}$ by $\mathbb{Q}^*$.

Lemma 1. *Let $(u,v) \in \mathfrak{H}$. Then $(u,v) \in \phi\mathfrak{G}$ precisely when either $u \in (\mathbb{Q}^*)^2$ or $u = 0$, $a^2 - 4b \in (\mathbb{Q}^*)^2$.*

Proof. For $u \neq 0$, this follows by specializing $\lambda \to u$, $\mu \to v$ in (*). The point $(\lambda, \mu) = (0,0)$ comes from the points $(\alpha, 0)$ where $\alpha^2 + a\alpha + b = 0$: and $a \in \mathbb{Q}$ if and only if $a^2 - 4b \in (\mathbb{Q}^*)^2$.

This suggests the map

$$q: \ \mathfrak{H} \to \mathbb{Q}^*/(\mathbb{Q}^*)^2$$

given by

$$\begin{aligned} q((u,v)) &= u(\mathbb{Q}^*)^2 \qquad (u \neq 0) \\ &= (a^2 - 4b)(\mathbb{Q}^*)^2 \qquad (u = 0) \\ q(\mathbf{o}) &= (\mathbb{Q}^*)^2. \end{aligned}$$

[12] The argument is quite general for isogenies of any degree. Note that ff_1 is the norm of f for the extension $\mathbb{Q}(\mathbf{x})/\mathbb{Q}(\boldsymbol{\lambda})$, cf. §24, Lemma 1.

We note that the equation

$$v^2 = u(u^2 - 2au + a^2 - 4b)$$

implies that

$$q((u,v)) = (u^2 - 2au + a^2 - 4b)(\mathbb{Q}^*)^2$$

whenever the right hand side is defined.

Lemma 2. *The map*

$$q: \mathfrak{H} \to \mathbb{Q}^*/(\mathbb{Q}^*)^2$$

is a group homomorphism.

Proof. Write the equation of $\mathcal{D}$ as

$$\mathcal{D}: \ V^2 = U(U^2 + a_1 U + b_1).$$

Let $\mathbf{u}_j = (u_j, v_j)$ $(j = 1,2,3) \in \mathfrak{H}$ with

$$\mathbf{u}_1 + \mathbf{u}_2 + \mathbf{u}_3 = \mathbf{o},$$

so they are the intersection of $\mathcal{D}$ with a line

$$V = lU + m.$$

Substituting in the equation for $\mathcal{D}$, we have

$$\begin{aligned} U(U^2 + a_1 U + b_1) &- (lU + m)^2 \\ &= (U - u_1)(U - u_2)(U - u_3). \end{aligned}$$

Hence

$$u_1 u_2 u_3 = m^2.$$

This implies that

$$q(\mathbf{u}_1) q(\mathbf{u}_2) q(\mathbf{u}_3) = (\mathbb{Q}^*)^2$$

except, possibly, when one of the $\mathbf{u}_j$ is $(0,0)$. The verification in this case is left to the reader.

Lemma 3. *The image of*

$$q: \ \mathfrak{H} \to \mathbb{Q}^*/(\mathbb{Q}^*)^2$$

is finite.

Proof. Without loss of generality

$$a_1 \in \mathbb{Z}, \qquad b_1 \in \mathbb{Z}.$$

An element of $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ may be written $r(\mathbb{Q}^*)^2$, where

$$r \in \mathbb{Z}, \qquad \text{square free.}$$

We show that $r(\mathbb{Q}^*)^2$ is in the image of q only when $r \mid b_1$.

Suppose that $q((u,v)) = r(\mathbb{Q}^*)^2$. Then there are $s,\, t \in \mathbb{Q}$ such that

$$u^2 + a_1 u + b_1 = rs^2$$
$$u = rt^2.$$

Put $t = l/m$, where

$$l, m \in \mathbb{Z}, \qquad \gcd(l,m) = 1.$$

Then, on eliminating u,

$$r^2 l^4 + a_1 r l^2 m^2 + b_1 m^4 = rn^2,$$

where $n = m^2 s \in \mathbb{Z}$.

Suppose that there is a prime p with $p \mid r$, $p \nmid b_1$. Then $p \mid m$, so $p^2 \mid rn^2$ and hence $p \mid n$ because r is square-free. Then $p^3 \mid r^2 l^4$, so $p \mid l$, contrary to $gcd(l,m) = 1$.

Putting the three lemmas together, we get the

Theorem 1. *$\mathfrak{H}/\phi\mathfrak{G}$ is finite.*

Corollary. *$\mathfrak{G}/2\mathfrak{G}$ is finite.*

Proof. Consider the exact triangle

$$\begin{tikzcd} \mathcal{C} \arrow[rr, "\times 2"] \arrow[dr, "\phi"'] & & \mathcal{C} \\ & \mathcal{D} \arrow[ur, "\psi"'] & \end{tikzcd}$$

where $\mathfrak{H}/\phi\mathfrak{G}$ and $\mathfrak{G}/\psi\mathfrak{H}$ are both finite.

By considering in detail the equations arising in the Lemma 3, we can get more information about $\mathfrak{G}/2\mathfrak{G}$; e.g. by looking at the equations locally. There is, however, no local-global theorem and indeed even today there is no algorithm for deciding whether or not there is a solution. We shall come back to these questions in a late section. So one should not conclude from the fact that we can determine $\mathfrak{G}/2\mathfrak{G}$ in the examples that one can always do so.

We first enunciate more precisely what was proved.

Lemma 4. *The group $\mathfrak{H}/\phi\mathfrak{G}$ is isomorphic to the group of $q(\mathbb{Q}^*)^2$ in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ where*

(i) *$q \in \mathbb{Z}$ is square-free and $q \mid b_1$*

(ii) *The equation*

$$ql^4 + a_1 l^2 m^2 + (b_1/q)m^4 = n^2$$

has a solution in l, m, $n \in \mathbb{Z}$ not all 0.

Further, the point $(0,0)$ of $\mathfrak{H}$ corresponds to $q =$ the square-free kernel of b_1.

Example 1.

$$\mathcal{C}:\ Y^2 = X(X^2 - X + 6)$$
$$\mathcal{D}:\ Y^2 = X(X^2 + 2X - 23)$$

For $\mathfrak{H}/\phi\mathfrak{G}$ we have $q \mid (-23)$. Since -23 corresponds to $(0,0)$, we need look at only one of $q = +23$, $q = -1$, say the latter. The equation of Lemma 4 is

$$-l^4 + 2l^2m^2 + 23m^4 = n^2$$

i.e.

$$-(l^2 - m^2)^2 + 24m^4 = n^2,$$

which is impossible in $\mathbb{Q}_3$. Hence $\mathfrak{H}/\phi\mathfrak{G}$ is generated by $(0,0)$.

For $\mathfrak{G}/\psi\mathfrak{H}$, we have $q \mid 6$, so $q = -1$ or $q = \pm 2, \pm 3, \pm 6$. Since the form $X^2 - X + 6$ is definite, we must have $q > 0$. Hence $q = 2, 3$ or 6; and 6 belongs to $(0,0)$. Thus it is enough to look at one of $2, 3$, say 2. The equation is

$$2l^4 - l^2m^2 + 3m^4 = n^2,$$

which is seen to have the solution $(l,m,n) = (1,1,2)$. This corresponds to $(x,y) = (2,4)$.

It follows that $\mathfrak{G}/\psi\mathfrak{H}$ is generated by $(0,0)$ and $(2,4)$. To find generators for $\mathfrak{G}/2\mathfrak{G}$ we need to look at the effect of ψ on the generators of $\mathfrak{H}/\phi\mathfrak{G}$. In this case $\phi(0,0) = \mathbf{o}$, so $\mathfrak{G}/2\mathfrak{G}$ is also generated by $(0,0)$ and $(2,4)$.

Second example. This is related to Fermat's equation

$$U^4 + V^4 = V^4.$$

Then

$$Y = V^2W^2/U^4, \qquad X = W^2/U^2$$

satisfy

$$\mathcal{C}: \; Y^2 = X(X^2-1),$$

so

$$\mathcal{D}: Y^2 = X(X^2+4).$$

For $\mathfrak{H}/\phi\mathfrak{G}$, we have $q \mid 4$, so $q = -1, \pm 2$. Since X^2+4 is definite, we need $q > 0$, so only $q = 2$ needs to be looked at. The relevant equation is

$$2l^4 + 2m^4 = n^2,$$

which has the solution $(l, m, n) = (1, 1, 2)$, giving $(X, Y) = (2, 4)$ as the generator of $\mathfrak{H}/\phi\mathfrak{G}$. The point $(0,0)$ is in $\phi\mathfrak{G}$.

For $\mathfrak{G}/\psi\mathfrak{H}$, we have $q \mid (-1)$. Since -1 belongs to $(0,0)$, there is nothing to do. Then $\mathfrak{G}/\psi\mathfrak{H}$ is generated by $(0,0)$ and $\mathfrak{G}/2\mathfrak{G}$ is generated by $(0,0)$ and $\psi(2,4) = (1,0)$.

§14. Exercises

1. Find

(i) a set of generators for $\mathfrak{G}/2\mathfrak{G}$, where $\mathfrak{G}$ is the group of rational points and

(ii) the 2-power torsion, for the following curves

$$Y^2 = X(X^2+3X+5)$$
$$Y^2 = X(X^2-4X+15)$$
$$Y^2 = X(X^2+4X-6)$$
$$Y^2 = X(X^2-X+6)$$
$$Y^2 = X(X^2+2X+9)$$
$$Y^2 = X(X^2-2X+9)$$

2. Invent similar questions to 1 and solve them. [*Note.* You cannot expect to determine $\mathfrak{G}/2\mathfrak{G}$ in every case, but you can majorize its order. It might be helpful to write a Mickey Mouse program to look for points with small co-ordinates.]

3. Let $\mathcal{C}: Y^2 = X(X^2+aX+b)$, $\mathcal{D}: Y^2 = X(X^2+a_1X+b_1)$ with $a_1 = -2a$, $b_1 = a^2-4b$.

(i) Show that the odd torsion groups are isomorphic

(ii) Assuming the finite basis theorem, show that the ranks [= number of generators of infinite order] are the same

(iii) give an example to show that the orders of the groups of 2-power torsion need not be the same. Determine what the possibilities are.

4. (i) Construct an elliptic curve with a torsion element of order 8.

(ii) Show that no torsion element can have order 16.

(iii) Determine all abstract groups of 2-power order which can isomorphic to the 2-power torsion of an elliptic curve. Give elliptic curves in the possible cases and give a proof of impossibility for the others.

5. (Another kind of isogeny). Let

$$\mathcal{C}: Y^2 = X^3 + B$$

be defined over $\mathbb{Q}$ and let $\beta^2 = B$, $\beta \in \overline{\mathbb{Q}}$.

(i) Show that $Y = \pm\beta$ are inflexions and that $2(0,\beta) = (0,-\beta)$.

(ii) Let $\mathbf{x} = (x, y)$ be generic and put

$$\mathbf{x}_1 = \mathbf{x} + (0,\beta), \qquad \mathbf{x}_2 = \mathbf{x} + (0,-\beta).$$

Show that

$$\xi = x + x_1 + x_2, \qquad \eta = y + y_1 + y_2$$

are functions of (x, y) defined over $\mathbb{Q}$ and that

$$\mathcal{D}: \; \eta^2 = \xi^3 - 27B.$$

(iii) Show that the repetition of the above map is (essentially) multiplication by 3.

(iv) Denote by $\mathfrak{G}$, $\mathfrak{H}$ the groups of rational points on $\mathcal{C}$, $\mathcal{D}$ respectively. Denote by $\mathbb{Q}(\beta)^*$ the multiplicative group of non zero elements of $\mathbb{Q}(\beta)$. If $(x, y) \in \mathfrak{G}$ and

$$y + \beta \in \{\mathbb{Q}(\beta)^*\}^3$$

show that $\mathbf{x}$ is in the image of $\mathfrak{H}$ under $\mathcal{D} \to \mathcal{C}$.
[*Hint.* Put $y + \beta = (u + v\beta)^3$ and equate the coefficients of β.]

(v) Show that

$$(x, y) \to (y + \beta)\{\mathbb{Q}(\beta)^*\}^3$$

is a homomorphism

$$\mu: \; \mathfrak{G} \to \mathbb{Q}^*(\beta)/\{\mathbb{Q}(\beta)^*\}^3$$

whose kernel is the image of $\mathfrak{H}$.

(vi) (Requires algebraic number theory). Show that the image of μ is finite [*Hint.* cf. §16].

(vii) Deduce that $\mathfrak{G}/3\mathfrak{G}$ is finite.

Examination: Mastermath Elliptic Curves
Tuesday 6nd 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

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

(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 $y = \alpha x$.

(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 $\mathbb{C}$:

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

(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 $\phi([0]) = [0]$.

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

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 $\hat{\phi}\colon E' \to E$.

(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 $\mathbb{Z}/2\mathbb{Z}$.

(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.

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

(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 $I_P(C, C_H) = 1$.

(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'.

Resit examination: Mastermath Elliptic Curves
Tuesday 27th June 2017

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

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

$$y^2 = x^3 - 15x + 22.$$

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

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

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

(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 $\phi([0]) = [0]$.

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

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

$$E : y^2 = x(x^2 + 4x + 1), \qquad E' : y^2 = x(x^2 - 8x + 12).$$

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

(a) Show that the group $E'(\mathbb{Q})/\phi(E(\mathbb{Q}))$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$.

(b) Assuming that the group $E(\mathbb{Q})/\hat{\phi}(E(\mathbb{Q}))$ is trivial, calculate the rank of $E(\mathbb{Q})$.

4. Let C be the projective plane curve over $\mathbb{C}$ defined by the affine equation

$$6y^3 = x(x^3 - x^2 - 7x + 1).$$

(a) Show that C has a unique point O at infinity.

(b) Find the divisor of the rational function $y + 1 \in \mathbb{C}(C)$.

(c) Let P be the point with affine coordinates $(0, 0)$. Show that the divisor $P - O$ has order 3 in $\operatorname{Pic} C$.

5. Let E_1, E_2, E_3, E_4 be the four elliptic curves over $\mathbb{F}_5$ defined by the following affine Weierstrass equations:

$$E_1\colon y^2 = x^3 + x, \qquad E_2\colon y^2 = x^3 + x + 2,$$
$$E_3\colon y^2 = x^3 + x + 3, \qquad E_4\colon y^2 = x^3 + 4x + 1.$$

Which, if any, of the elliptic curves E_1, E_2, E_3, E_4 are isomorphic?

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

$$\frac{(3x_1^2 + a)^2 - 8x_1y_1^2}{4y_1^2}.$$

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'.

Examination: Mastermath Elliptic Curves
Tuesday 5th June 2018

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

All questions are worth the same number of points. Not all sub-questions are worth the same number of points.

1. Let $E/\mathbb{Q}$ be the elliptic curve given by

$$E : y^2 = x^3 + 22x^2 - 7x.$$

[Warning: read the exponents of x carefully.]

(a) Show that the equation of E defines an elliptic curve $\widetilde{E}$ over $\mathbb{F}_3$ and give the order of $\widetilde{E}(\mathbb{F}_3)$.

(b) Show that the equation of E defines an elliptic curve $\widetilde{E}$ over $\mathbb{F}_5$ and show $\widetilde{E}(\mathbb{F}_5) < 12$.

(c) Compute $E(\mathbb{Q})^{\mathrm{tors}}$. (That is, find the coordinates of generators and their order in the group and find the structure of the group.)

2. Let $i \in \mathbb{C}$ be a square root of -1, and let

$$\begin{aligned} \Lambda_1 &= i\mathbb{Z} + \mathbb{Z} \subset \mathbb{C}, \\ \Lambda_2 &= (1+i)\mathbb{Z} + (1-i)\mathbb{Z} \subset \mathbb{C}, \\ \Lambda_3 &= i\mathbb{Z} + 2\mathbb{Z} \subset \mathbb{C}. \end{aligned}$$

For $i = 1, 2, 3$, let $E_i = E_{\Lambda_i}$, and further define

$$E_4 : y^2 = x^3 + 2x \qquad \text{and} \qquad E_5 : y^2 = x^3 + 1.$$

(a) In each of the following cases, determine whether the two elliptic curves are isomorphic over $\mathbb{C}$.

   i. E_1 and E_2,

   ii. E_1 and E_3,

   iii. E_3 and E_4,
   [Hint: $E_4 \to E_4 : (x, y) \mapsto (-x, iy)$]

   iv. E_4 and E_5.

(b) Compute the structure of the ring $\mathrm{End}(E_3)$.

There are two more questions on the back of this sheet

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

$$E : y^2 = x(x^2 - 11), \qquad E' : y^2 = x(x^2 + 44).$$

The curves E and E' are related by a 2-isogeny $\phi\colon E \to E'$, with dual $\widehat{\phi}\colon E' \to E$, as described on the formula sheet.

(a) Show that the groups $E'(\mathbb{Q})/\phi(E(\mathbb{Q}))$ and $E(\mathbb{Q})/\widehat{\phi}(E'(\mathbb{Q}))$ both have order 2. *[Hint: the squares in* $\mathbb{F}_{11}^{\times}$ *are* $1, 3, 4, 5, 9$.*]*

(b) Assuming that $E(\mathbb{Q})$ contains no torsion points other than the obvious $(0, 0)$, describe the group $E(\mathbb{Q})$ completely.

4. Let C be the plane projective curve over $\mathbb{Q}$ given by

$$y^5 = x(x-1)(x-2)(x-3)$$

and let $Q_i = (i, 0) \in C(\mathbb{Q})$ for $i = 0, 1, 2, 3$.

(a) Show that C has a unique point O at infinity.

(b) Show that C is smooth.

(c) Find all points P in the affine part of $C(\overline{\mathbb{Q}})$ such that the tangent line of C at P is vertical.

(d) Find the divisor of the rational function y on C.

(e) Show that the divisor of the differential dx is

$$4Q_0 + 4Q_1 + 4Q_2 + 4Q_3 - 6O.$$

[Full credit for a proof that disregards the order at O*; bonus credit for a complete proof.]*

(f) Give a regular differential (that is, a differential without poles) on C.

(g) Show that the class of $Q_0 - Q_1$ in $\mathrm{Pic}^0(C)$ has order 5.

Formula sheet

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

(i) The discriminant of E is

$$\Delta = -16(4A^3 + 27B^2).$$

(ii) The j-invariant of E is

$$j = -1728\frac{(4A)^3}{\Delta}.$$

Let $E : y^2 = x^3+ax^2+bx+c$ be a slightly more general Weierstrass equation and $P = (x_1, y_1)$ a non-singular point of E. The x-coordinate of $2P$ is

$$\lambda^2 - a - 2x_1, \qquad \text{where} \qquad \lambda = \frac{3x_1^2 + 2ax_1 + b}{2y_1}.$$

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'.

Examination: Mastermath Elliptic Curves (resit)
Tuesday 26th June 2018

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

All questions are worth the same number of points. Not all sub-questions are worth the same number of points.

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

$$E : y^2 = x(x^2 - 5), \qquad E' : y^2 = x(x^2 + 20).$$

The curves E and E' are related by a 2-isogeny $\phi\colon E \to E'$, with dual $\widehat{\phi}\colon E' \to E$, as described on the formula sheet.

(a) Show that the group $E'(\mathbb{Q})/\phi(E(\mathbb{Q}))$ has order 2.

(b) Compute the group $E(\mathbb{Q})/\widehat{\phi}(E'(\mathbb{Q}))$, and hence calculate the rank of $E(\mathbb{Q})$.

2. Recall that the Riemann–Roch theorem states that, for any divisor D on a smooth, projective curve of genus g over a field k, we have

$$\dim \mathcal{L}(D) - \dim \mathcal{L}(K - D) = 1 - g + \deg(D)$$

where K is a canonical divisor on the curve.

(a) Prove the equalities $\deg(K) = 2g - 2$ and $\dim \mathcal{L}(K) = g$.

(b) Let C be a smooth, projective curve of genus 2 over an algebraically closed field k. Show that there is a non-constant rational function $f \in k(C)$ having divisor of the form

$$(f) = P_1 + P_2 - P_3 - P_4$$

for points $P_1, P_2, P_3, P_4 \in C(k)$. [Hint: consider two rational functions $f_1, f_2 \in \mathcal{L}(K)$.]

There are two more questions on the back of this sheet

3. For each of the following pairs of elliptic curves, decide whether or not they are isomorphic over the given field.

(a) $\mathbb{C}/\langle 1, 1+i\rangle$ and $\mathbb{C}/\langle 1-i, 1+i\rangle$ over $\mathbb{C}$;

(b) $E_1\colon y^2 = x^3 + x$ and $E_2\colon y^2 = x^3 + 3x$ over $\mathbb{Q}$;

(c) $E_1\colon y^2 = x^3 + x$ and $E_2\colon y^2 = x^3 + 3x$ over $\mathbb{F}_5$;

(d) $E_1\colon y^2 = x^3 + 1$ and $E_2\colon y^2 = x^3 + t$ over $\mathbb{Q}(t)$.

4. Let k be a field of characteristic different from 2. Suppose that k contains i, a square root of -1. Let E be the elliptic curve over k given by

$$Y^2 = X^3 - X.$$

(a) Show that $[i](x,y) = (-x, iy)$ defines an endomorphism $[i] : E \to E$ and that $[i]$ satisfies $[i]^2 + 1 = 0$ in $\mathrm{End}(E)$.

(b) Show that the dual of $[i]$ is $-[i]$.

(c) For $a, b \in \mathbf{Z}$, show that the degree of the endomorphism $a + b[i]$ of E is equal to $a^2 + b^2$.

(d) Compute the points in $\ker(\phi)$ for $\phi = [1] + [i]$.

Formula sheet

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

(i) The discriminant of E is

$$\Delta = -16(4A^3 + 27B^2).$$

(ii) The j-invariant of E is

$$j = -1728\frac{(4A)^3}{\Delta}.$$

Let $E : y^2 = x^3 + ax^2 + bx + c$ be a slightly more general Weierstrass equation and $P = (x_1, y_1)$ a non-singular point of E. The x-coordinate of $2P$ is

$$\lambda^2 - a - 2x_1, \qquad \text{where} \qquad \lambda = \frac{3x_1^2 + 2ax_1 + b}{2y_1}.$$

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'.