Final Honour School of Mathematics Part C

C3.7 Elliptic Curves
Victor Flynn
Checked by: Alan Lauder

20/1/17

Examinations are 1.5 hours in duration. Students may answer as many questions as they wish; the best two answers count for the total mark.

Do not turn this page until you are told that you may do so

1. (a) [10 marks] Let $\mathcal{C}$ be a non-singular cubic curve, defined over a field K, with a K-rational point $\mathbf{o}$. Describe the standard law for adding two points on $\mathcal{C}$, and prove that it is associative.

   (b) [7 marks] State Hensel's lemma. For which primes p do there exist $x, y \in \mathbb{Z}_p$ such that $x^2 - 2y^2 = 3$? [*Hint: For $p > 3$, you may find it helpful to consider the sizes of the sets $\{x^2 : x \in \mathbb{F}_p\}$ and $\{3 + 2y^2 : y \in \mathbb{F}_p\}$.*]

   (c) [8 marks] Let $a, b \in \mathbb{Z}$ satisfy $a \equiv b \equiv 4 \pmod{27}$ and $b \equiv a + 3 \pmod{7}$. Show that, for any prime p, there exist $x, y, z \in \mathbb{Z}_p$ which satisfy $(x^3 - y^3 + a)(x^3 - z^3 + b)(y^3 - z^3 + b - a) = 0$. Show that there are no solutions in $\mathbb{Z}$.

2. (a) Let R be any ring (commutative, with 1), and let F, G be formal groups over R.

   (i) [7 marks] Show that there exists a unique normalised invariant differential for F, which is given by $\omega = F_X(0, T)^{-1} \mathrm{d}T \in R[[T]]\mathrm{d}T$, and that every invariant differential for F is of the form $a\omega$ for some $a \in R$.

   (ii) [6 marks] Let f be a homomorphism over R from F to G. Let ω_F, ω_G be the normalised invariant differentials on F, G, respectively. Show that $\omega_G \circ f = f'(0)\ \omega_F$. Deduce that, for any prime p, there exist $f, g \in R[[T]]$ such that $[p](T) = pf(T) + g(T^p)$ [where $[p]$ represents the multiplication-by-p map on F].

   (b) Let $\mathcal{C} : Y^2 = X(X + \alpha)(X + \beta)$, where $\alpha, \beta \in \mathbb{Q}$, satisfying $\alpha \neq 0$, $\beta \neq 0$ and $\alpha \neq \beta$.

   (i) [6 marks] Show that $2(x, y)$ has x-coordinate:

$$\frac{(x^2 - \alpha\beta)^2}{4x(x + \alpha)(x + \beta)}.$$

   Show that $\mathcal{C}(\mathbb{Q})$ has a point of order 4 if and only if:

$$\begin{aligned} &\Big(\alpha \in (\mathbb{Q}^*)^2 \text{ and } \beta \in (\mathbb{Q}^*)^2\Big) \\ \text{or } &\Big(-\alpha \in (\mathbb{Q}^*)^2 \text{ and } \beta - \alpha \in (\mathbb{Q}^*)^2\Big) \\ \text{or } &\Big(-\beta \in (\mathbb{Q}^*)^2 \text{ and } \alpha - \beta \in (\mathbb{Q}^*)^2\Big). \end{aligned}$$

   (ii) [6 marks] Now assume that $\alpha \in (\mathbb{Q}^*)^4$ and $\beta \in (\mathbb{Q}^*)^4$, so that $\alpha = c^4, \beta = d^4$, for some $c, d \in \mathbb{Q}^*$, and further assume that $c^2 + d^2 \in (\mathbb{Q}^*)^2$. Show that $\mathcal{C}(\mathbb{Q})$ has a point of order 8. [*Hint: You may find it helpful to define a curve $\mathcal{D}$ such that there are 2-isogenies $\phi : \mathcal{C} \longrightarrow \mathcal{D}$ and $\hat{\phi} : \mathcal{D} \longrightarrow \mathcal{C}$, with $\hat{\phi} \circ \phi = [2]$, the multiplication by 2 map on $\mathcal{C}$.*]
   Find an example of such an elliptic curve $\mathcal{C}$ for which $\mathcal{C}(\mathbb{Q})$ has a point of order 8.

3. Let $\mathcal{C} : Y^2 = X(X^2+aX+b)$ and $\mathcal{D} : Y^2 = X(X^2+a_1X+b_1)$, where $a, b \in \mathbb{Z}$ with $b(a^2-4b) \neq 0$ and $a_1 = -2a$, $b_1 = a^2 - 4b$. Let the map ϕ [which you may assume to be a homomorphism] be defined as usual by

$$\phi : \mathcal{C}(\mathbb{Q}) \to \mathcal{D}(\mathbb{Q}) : (x, y) \mapsto \Big(\frac{y^2}{x^2},\ y - \frac{by}{x^2}\Big) = \Big(\frac{x^2 + ax + b}{x},\ y - \frac{by}{x^2}\Big).$$

Let q be defined as usual by

$$q : \mathcal{D}(\mathbb{Q}) \to \mathbb{Q}^*/(\mathbb{Q}^*)^2 : (u, v) \mapsto u \text{ when } u \neq 0,$$

$$q : (0, 0) \mapsto b_1,\ \ q : \mathbf{o} \mapsto 1.$$

(a) [5 marks] Show that q is a homomorphism.
[You are only required to show that $q(P + Q) = q(P)q(Q)$ in the typical case when none of $P, Q, P + Q$ are $(0, 0)$ or $\mathbf{o}$.]

(b) [10 marks] Let p be prime, satisfying $p \equiv 2 \pmod 3$ and $p \equiv 5 \pmod 8$. Show that the elliptic curve $Y^2 = X(X^2 - pX + p^2)$ has rank 0.

(c) [10 marks] Let p_1, p_2 be primes, satisfying $p_1 \equiv 3 \pmod 8$, $p_2 \equiv 1 \pmod 8$, such that p_1 is not a quadratic residue modulo p_2. Show that the elliptic curve $Y^2 = X(X^2 - p_1p_2)$ has rank 0.