Final Honour School of Mathematics Part C

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

23/11/17

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 K be a field, complete with respect to a non-Archimedean valuation $|\ |$, with valuation ring $R = \{x \in K : |x| \leqslant 1\}$. Prove Hensel's Lemma, that if $f(x) \in R[x]$ and $a_0 \in R$ satisfies $|f(a_0)| < |f'(a_0)|^2$, then there exists a unique $a \in R$ such that $f(a) = 0$ and $|a - a_0| \leqslant |f(a_0)|/|f'(a_0)|$.

   (b) [8 marks] Show that there does not exist $x \in \mathbb{Z}$ such that $|x^{10} - 2|_{11} \leqslant 11^{-3}$. For any prime p, show there does not exist $x \in \mathbb{Z}$ such that $|x^p - p|_p \leqslant p^{-2}$. Find $x \in \mathbb{Z}$ such that $|x^2 + 2|_3 \leqslant 3^{-5}$. Find $x \in \mathbb{Q}$ such that $|x^2 + 7|_2 \leqslant 2^{-8}$.

   (c) [7 marks] Let p_1, p_2, p_3 be distinct primes satisfying $p_1 \equiv p_2 \equiv p_3 \equiv 5 \pmod 8$, such that p_i is a quadratic residue modulo p_j for any $i \neq j$. Show that, for any prime p, there exist $x, y \in \mathbb{Q}_p$ such that $y^2 = p_1 x^4 - p_1 p_2^2 p_3^2$.

2. (a) [8 marks] State and prove the Nagell-Lutz Theorem for $\mathbb{Q}$-rational torsion points on the elliptic curve $y^2 = x^3 + Ax + B$, with $A, B \in \mathbb{Z}$. [You may assume the result that any $\mathbb{Q}$-rational torsion point (x, y) on such a curve satisfies $x, y \in \mathbb{Z}$. You may also use the polynomial identity: $\phi_1(X)\psi_1(X) + \phi_2(X)\psi_2(X) = 4A^3 + 27B^2$, where $\phi_1(X) = 3X^2 + 4A$, $\psi_1(X) = (3X^2 + A)^2$, $\phi_2(X) = -27(X^3 + AX - B)$ and $\psi_2(X) = X^3 + AX + B$.]

   (b) [7 marks] Show that the torsion group over $\mathbb{Q}$ of the elliptic curve $\mathcal{E} : Y^2 = X^3 - 3$ is the trivial group. Show that 3 divides $\#\widetilde{\mathcal{E}}(\mathbb{F}_p)$ for every prime $p > 3$. [*Hint: consider separately* $p \equiv 1$ *and* $p \equiv 2$ *(mod* 3*).*]

   (c) [6 marks] Find the torsion group over $\mathbb{Q}$ of the elliptic curve $Y^2 = X^3 + X^2 - X$.

   (d) [4 marks] Let (x, y) be a $\mathbb{Q}$-rational torsion point on the elliptic curve $Y^2 = X^3 + AX + B$, with $A, B \in \mathbb{Z}$, and let $\Delta = 4A^3 + 27B^2$. Show that $|x| \leqslant \max\big(2|A|, |\Delta| + |B|\big)$. [In this part, $|\ |$ denotes the standard absolute value $|\alpha| = \max(\alpha, -\alpha)$.]

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

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

   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) [9 marks] Show that the image of q is a subset of the finite set

$$\{r : r \text{ is a square free integer and } r | b_1\}.$$

   (b) [7 marks] Find the rank of the elliptic curve $Y^2 = X(X^2 - X - 1)$.

   (c) [9 marks] Let p be a prime satisfying $p \equiv 3 \pmod 4$. Show that the elliptic curve $y^2 = x^3 + px$ has rank at most 1. When $p \equiv 7 \pmod{16}$ show that the rank is 0.