Final Honour School of Mathematics Part C

Course Title: B3.7. Elliptic Curves.
Lecturer: Prof Victor Flynn
Checked by: Alan Lauder

20/2/16

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

1. (a) [5 marks] Let K be a field, complete with respect to a non-Archimedean valuation $|\ |$, and let x_n be a sequence in K. Show that $x_n \to 0$ in K if and only if $\sum x_n$ is convergent in K. For any $x, y \in K$, show that $|x| \neq |y| \implies |x+y| = \max(|x|, |y|)$.

   (b) [2 marks] For what prime p does $-\frac{9}{8} = 1 + 2p + 2p^2 + 2p^3 + \ldots$ in $\mathbb{Q}_p$?

   (c) [5 marks] Find an $x \in \mathbb{Z}$ such that $|x^2 + 3|_7 < 7^{-1}$. Show that there does not exist $x \in \mathbb{Z}$ such that $|x^2 + 14|_7 < 7^{-1}$.

   (d) [6 marks] State Hensel's Lemma. Let $p \equiv 1 \pmod 3$ be prime. Show that -3 is a quadratic residue mod p [*Hint: consider separately the cases* $p \equiv 1$ *(mod* 4*) and* $p \equiv 3$ *(mod* 4*)*]. Show that -3 is a square in $\mathbb{Q}_p^*$.

   (e) [7 marks] Let $q \equiv 1 \pmod{27}$ be prime. Show that $(x^2 + 3)(x^3 - q) = 0$ has solutions in $\mathbb{R}$ and in $\mathbb{Q}_p$ for every prime p, but has no solutions in $\mathbb{Q}$.

2. (a) [5 marks] Find the torsion group over $\mathbb{Q}$ of the elliptic curve $y^2 = x^3 + 4x$.

   (b) [7 marks] Let $n \in \mathbb{Z}$ satisfy $n \equiv 2 \pmod 5$. Find the torsion group over $\mathbb{Q}$ of the elliptic curve $y^2 = x(x+1)(x+n^2)$.

   (c) [7 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* $\psi_2(X) = X^3 + AX + B$.]

   (d) [6 marks] Let $k \in \mathbb{Z}$, $k \neq 0$, let $\mathcal{E}$ be the elliptic curve $y^2 = x^3 - k^2x + k^3$, and let (x, y) be a torsion point in $\mathcal{E}(\mathbb{Q})$. Show that $|y| \leq 5|k|^3$ and $|x| \leq 3|k|^2$.

   [*In this part,* $|\ |$ *denotes the standard absolute value* $|\alpha| = max(\alpha, -\alpha)$ *for* $\alpha \in \mathbb{Q}$.]

3. (a) [11 marks] Find the rank of the elliptic curve $Y^2 = X(X^2 + X + 2)$.

   [*Standard results may be used without proof, provided they are accurately stated.*]

   (b) [9 marks] Let A be an Abelian group with group operation $+$, and let $h : A \longrightarrow \mathbb{R}$ satisfy:

   (1) For any $Q \in A$, there exists $C_1 = C_1(Q)$ such that $h(P + Q) \leq 2h(P) + C_1$ for all $P \in A$.

   (2) There exists C_2, independent of P, such that $h(2P) \geq 4h(P) - C_2$ for all $P \in A$.

   (3) For any C_3, the set $\{P \in A : h(P) \leq C_3\}$ is finite.

   Suppose also that $A/2A$ is finite. Prove that A is finitely generated.

   (c) [5 marks] Let A and h be as in (b). Suppose that P is a torsion element of A [that is: there exists an integer $N > 0$ such that NP is the identity element of A]. Show that $h(P) \leq \frac{1}{3}C_2$.