Final Honour School of Mathematics Part C

Course Title: C3.7. Elliptic Curves
Lecturer: Prof Minhyong Kim

16/2/15

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

1. (a) [10 marks] State and prove Hensel's lemma.

(b) [5 marks] Which of the following numbers has a cube root in $\mathbb{Q}_3$? Be sure to justify your answer.

$$(i) \quad 35 \qquad (ii) \quad 132 \qquad (iii) \quad 10/459.$$

(c) [10 marks] Prove that $2y^2 = x^4 - 17$ has a solution in $\mathbb{R}$ and in $\mathbb{Q}_p$ for all primes p.

[*You may use any of the theorems stated during lectures.*]

2. (a) [10 marks] For the elliptic curve $\mathcal{E}$ with equation $y^2 = x^3 + 1$ compute the groups

(i) $\mathcal{E}(\mathbb{F}_5)$
(ii) $\mathcal{E}(\mathbb{F}_7)$

For case (i) describe directly the group law on the points of the curve.

(b) [10 marks] Compute the torsion subgroups of the rational points of the elliptic curves over $\mathbb{Q}$ given by the equations

$$D_1 : \quad y^2 = x^3 + x^2 + 2x + 1; \qquad D_2 : y^2 = x^3 + 64.$$

[*You may use any of the theorems stated during lectures.*]

(c) [5 marks] Let $\mathcal{E}$ be the elliptic curve over $\mathbb{Q}$ given by the equation

$$y^2 = x^3 + 8.$$

Prove or disprove: $\mathcal{E}$ has infinitely many rational points.

[*You may use any of the theorems stated during lectures.*]

3. (a) [15 marks] Find the structure of the Mordell-Weil group of

$$\mathcal{C}: \quad y^2 = x^3 - 10x.$$

(b) [7 marks] Let p be a prime such that $p \equiv 5 \mod 8$. Show that

$$\mathcal{E}_p: \quad y^2 = x^3 + px$$

has rank at most 1.

(c) [3 marks] What is the rank of $\mathcal{E}_p$ for $p = 5$, $p = 13$, and $p = 29$?

End of Last Page