Final Honour School of Mathematics Part C

Course Title: C9.1b. Elliptic Curves
Lecturer: Prof Minhyong Kim

16/2/13

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

1. (a) State and prove Hensel's Lemma.

(b)

(i) Which numbers $a \in \mathbb{Q}_2$ have cube roots in $\mathbb{Q}_2$?

(ii) Which numbers $a \in \mathbb{Q}_3$ have cube roots in $\mathbb{Q}_3$?

(iii) How many solutions are there to

$$x^{37} - x = 37$$

in $\mathbb{Q}_{37}$?

(c) Consider the equation

$$y^2 = x^3 + 6.$$

Find all p for which the equation has a solution in $\mathbb{Z}_p$.

[*Warning: You are not allowed to use the point at 'infinity'.*]

[*You may use standard facts from the lectures as long as they are stated clearly.*]

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

(a) 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 $a \in R$.

(b) 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].

(c) Let $\mathcal{E}$ be an elliptic curve given by an equation

$$\mathcal{E} : y^2 = x^3 + (3m+1)x + 9n^2,$$

where $m, n \in \mathbb{Z}$ and the polynomial $x^3 + (3m+1)x + 9n^2$ has no rational root. Prove that $\mathcal{E}(\mathbb{Q})$ is infinite.

[*You may use standard facts from the lectures as long as they are stated clearly.*]

(d) Let $\mathcal{E}$ be an elliptic curve given by an equation

$$\mathcal{E} : y^2 = x^3 + ax,$$

where a is a non-zero square-free integer. Show that $\mathcal{E}(\mathbb{Q})$ has no element of order 4.

3. Let l be a prime and $\mathcal{E}_l$ be the elliptic curve

$$y^2 = x^3 - l^2 x.$$

(a) Find the torsion subgroup $\mathcal{E}_{l,\mathrm{tor}}(\mathbb{Q})$ of the Mordell-Weil group.

(b) Show that the rank of

$$\mathcal{E}_l : y^2 = x^3 - l^2 x$$

is at most two.

(c) Compute the rank of

$$\mathcal{E}_5 : y^2 = x^3 - 25x.$$

(d) For $l \equiv 3 \mod 8$, show that $\mathcal{E}_l$ has rank zero.