Final Honour School of Mathematics Part C

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

16/2/14

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

1. (a) Let $\mathcal{E}$ be an elliptic curve over $\mathbb{Q}_p$ with affine equation $y^2 = x^3 + Ax + B$, where $A, B \in \mathbb{Z}_p$. Prove that (x, y) reduces to the origin modulo p if and only if $|x|_p > 1$ or $|y|_p > 1$.

(b) Prove or disprove: If $a \in \mathbb{Q}^*$ has a square root in $\mathbb{Q}_p$ for all primes p, then it has a square root in $\mathbb{Q}$.

[Warning: We are *not* assuming it has a square root in $\mathbb{R}$.]

(c) State Hensel's lemma.

(d) Let $a \in \mathbb{Q}_p^*$. If $p \neq 2$, show that a has a square root if and only if $a = p^n u$ where n is even and $u \in \mathbb{Z}_p^*$ is such that $u \mod p$ has a square root. State and prove the analogous criterion for $p = 2$.

(e) Prove that $(x^2 + 7)(x^2 - 11)(x^2 + 77)$ has a root in each $\mathbb{Q}_p$ and $\mathbb{R}$.

2. Let $\mathcal{E}$ be an elliptic curve with affine equation $y^2 = x^3 + Ax + B$ where $A, B \in \mathbb{Z}_p$.

(a) Give the definition of a *formal group* over a ring R. State precisely the theorem regarding the isomorphism

$$\Phi : (p\mathbb{Z}_p, F_{\mathcal{E}}) \simeq (\mathcal{E}_1(\mathbb{Q}_p), +_{\mathcal{E}}),$$

where $+_{\mathcal{E}}$ refers to the elliptic curve group law and $F_{\mathcal{E}}$ is a formal group law. (Along the way, you should define $\mathcal{E}_1(\mathbb{Q}_p)$.)

(b) Given a formal group law F over $\mathbb{Z}_p$, show that there is a unique normalized invariant differential form $\omega \in \mathbb{Z}_p[[T]]dT$.

(c) Given a formal group law F over $\mathbb{Z}_p$, for each $m \in \mathbb{Z}$, define the homomorphism $[m]$ from F to itself. Show that

$$[p](T) = pf(T) + g(T^p)$$

for $f, g \in T\mathbb{Z}_p[[T]]$, where $f(T) = T +$ terms of degree $\geqslant 2$.

[You may assume that the power series $[m]$ defined previously are all homomorphisms.]

(d) Prove that

$$\mathcal{E}_1(\mathbb{Q}_p)$$

is torsion-free.

(e) Let $\mathcal{E}$ be the elliptic curve

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

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

3. Let

$$\mathcal{E} : y^2 = x(x^2 + ax + b)$$

be an elliptic curve, with $a, b \in \mathbb{Z}$, and let $\mathcal{C} = \mathcal{E}(\mathbb{Q})$. Define the map $q : \mathcal{C} \to \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ by setting

$$q(x, y) = x(\mathbb{Q}^\times)^2$$

if $x \neq 0$ and

$$q(x, y) = b(\mathbb{Q}^\times)^2$$

otherwise.

(a) Show that the image of q is finite.

(b) Now let $\mathcal{E}'$ be the elliptic curve $y^2 = x(x^2+a_1x+b_1)$, with $a_1 = -2a$ and $b_1 = a^2-4b$, and let $\mathcal{D} = \mathcal{E}'(\mathbb{Q})$. Stating clearly any properties you may require concerning the 2-isogeny $\phi : \mathcal{E} \to \mathcal{E}'$ and its dual $\hat{\phi}$, show that $\mathcal{C}/2\mathcal{C}$ is finite.

[You may assume that the map q above is a homomorphism, with kernel $\hat{\phi}(\mathcal{D})$.]

(c) In the special case $\mathcal{E} : y^2 = x(x^2 - p^2)$, where p is an odd prime, show that the rank is at most 2.

[You may use without proof the fact that the order of $\mathcal{C}/2\mathcal{C}$ is 2^{R+s} where R is the rank of $\mathcal{C}$ and 2^s is the order of its rational 2-torsion subgroup.]

(d) Show that if $x^4 + p^2y^4 = 2z^2$ has a non-trivial integer solution, then $(\frac{2}{p}) = 1$.

(e) Deduce that, for $\mathcal{E} : y^2 = x(x^2-p^2)$ as before, the rank is at most 1 if $p \equiv 3$ or $5 \pmod 8$. [You may use the fact that $(\frac{2}{p}) = 1$ if and only if $p \equiv \pm 1 \pmod 8$.] For $p = 5$ display a non-integral point (x, y) on the curve. [It may help to consider points for which x is a square.] Deduce that for $p = 5$ the rank is exactly 1.