Number Theory B Final Exam

Xinyi Yuan

May 2, 2013

1. (10 points) Let n be a positive integer. Prove that n is the area of a right-angle triangle with rational sides if and only if the elliptic curve

$$E : ny^2 = x^3 - x$$

over $\mathbb{Q}$ contains a rational point of infinite order.

2. (10 points) For the elliptic curve $E : ny^2 = x^3 - x$ over $\mathbb{Q}$, prove that $E(\mathbb{Q})$ is infinite if and only if $E(\mathbb{Q}(i))$ is infinite. (Hint: For any $P \in E(\mathbb{Q}(i))$, consider $P + \bar{P}$ and $P - \bar{P}$. Here $\bar{P}$ denotes the complex conjugate of P.)

3. (30 points) Let E be an elliptic curve over $\mathbb{R}$.

(1) Describe the structure of $E(\mathbb{R})/2E(\mathbb{R})$ in terms of the structure of $E(\mathbb{R})[2]$.

(2) Prove that $H^1(\mathbb{R}, E)$ is killed by multiplication by 2.

(3) Compute $H^1(\mathbb{R}, E)$ using the Kummer sequence

$$0 \longrightarrow E(\mathbb{R})/2E(\mathbb{R}) \longrightarrow H^1(\mathbb{R}, E[2]) \longrightarrow H^1(\mathbb{R}, E)[2] \longrightarrow 0.$$

4. (50 points) Let $k = \mathbb{F}_q$ be a finite field, and E be an elliptic curve over k.

(1) Denote by $\sigma \in \mathrm{Gal}(\bar{k}/k)$ the q-th power map. Show that for any $P \in E(\bar{k})$, there exists $Q \in E(\bar{k})$ such that $P = Q - Q^\sigma$.

(2) Prove that $H^1(k, E) = 0$.

(3) Prove that any smooth and projective curve of genus one over k has a rational point over k. (Thus it is an elliptic curve.)

(4) Prove that any smooth and projective curve of genus one over a *non-archimedean local field* K with *good reduction* has a rational point over K. (Hint: Hensel's lemma)

(5) Prove that the curve $C : 3x^3 + 4y^3 + 5z^3 = 0$ defined over $\mathbb{Q}$ is solvable over $\mathbb{Q}_v$ for any place v of $\mathbb{Q}$.