Number Theory B Homework 1

Xinyi Yuan

March 4, 2013

1. Prove that the chord-tangent construction defines a group law on (the smooth part of) a cubic curve without referring to the divisor class group. In particular, it works for singular cubic curves.

2. Consider the cubic curve $X^3 + Y^3 = aZ^3$ over a field k. It is non-singular if $a \neq 0$ and $\mathrm{char}(k) \neq 3$. The point $O = (1, -1, 0)$ makes the curve an elliptic curve.

- Prove that three points on the curve add to zero if and only if they are colinear. (Think: what do we need to prove?)
- Prove that the inverse of a point (X, Y, Z) is (Y, X, Z).
- Prove that

$$[2](X, Y, Z) = \big(-Y(X^3 + aZ^3),\ X(Y^3 + aZ^3),\ X^3Z - Y^3Z\big).$$

- Write down a Weierstrass equation of E.

3. Let E be an elliptic curve over $\mathbb{R}$. What can you say about the structure of $E(\mathbb{R})$ as a Lie group? (Hint: Over $\mathbb{C}$, we have $E(\mathbb{C}) = \mathbb{C}/\Lambda$.)

4. Let E_1, E_2 be elliptic curves over a field k. Let ℓ be a prime not equal to the characteristic of k. Prove that the natural map

$$\mathrm{Hom}_k(E_1, E_2) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \longrightarrow \mathrm{Hom}_{\mathbb{Z}_\ell}(T_\ell(E_1), T_\ell(E_2))$$

is injective.

5. Let E be an elliptic curves over a field k. Let ℓ be a prime not equal to the characteristic of k. Assume $\mathrm{End}_k(E) \neq \mathbb{Z}$. Prove that the image of the representation

$$\mathrm{Gal}(k^{\mathrm{sep}}/k) \longrightarrow \mathrm{GL}(T_\ell(E))$$

is an abelian group.

6. Let E_1, E_2 be elliptic curves over a finite field k. Prove that E_1 and E_2 are isogenous if and only if $\#E_1(k) = \#E_2(k)$. Can we conclude that $E_1(k)$ is isomorphic to $E_2(k)$ as finite groups in that case?

7. Let k be a field of characteristic $p > 0$.

- Prove that there are only finitely many supesingular elliptic curves over k (up to isomorphisms).
- For $p = 2, 3$, write down all supersingular elliptic curves over k.

8. Let E be an elliptic curves over a field k of characteristic $p > 0$. Assume that $j(E) \notin \overline{\mathbb{F}}_p$, or equivalently, $E_{\bar{k}}$ is not defined over $\overline{\mathbb{F}}_p$. Prove that $\mathrm{End}_k(E) = \mathbb{Z}$.

9. Consider the elliptic curve $E : y^2 = x^3 - x$ over $\mathbb{Q}$. Find all primes $p > 3$ so that the reduction of E modulo p is a supersingular elliptic curve over $\mathbb{F}_p$. Alternatively, do the same problem for $E' : y^2 = x^3 + 1$.