Freshman Seminar 21n: Elliptic Curves

William Stein

March 4, 2003

1 Remarks

Your reading this week and next is about Mordell's theorem, which is the assertion that the Mordell-Weil group $E(\mathbb{Q})$ of an elliptic curve is finitely generated. In simpler terms, given any elliptic curve E over $\mathbb{Q}$ there are points $P_1, \ldots, P_r \in E(\mathbb{Q})$ such that

$$E(\mathbb{Q}) = \{n_1 P_1 + \cdots + n_r P_r : n_1, \ldots, n_r \in \mathbb{Z}\}.$$

Though it is an open problem to give a provably correct algorithm to compute a finite generating set $P_1, \ldots, P_r$, in practice we can usually do this, and we'll learn a little about how in the next two weeks.

This week's reading and problems are very theoretical; next week's reading is example oriented and more computational.

Where are we going? After finishing chapter III, we'll study chapter IV about elliptic curves over finite fields and the elliptic curve factorization method. After Spring Break, we'll use the foundations we've developed, guided by your interests, to investigate some of the following topics: modularity of elliptic curves; connection between elliptic curves and Fermat's Last theorem; the Birch and Swinnerton-Dyer conjecture; cryptographic applications of elliptic curves; historical emergence of elliptic curves.

2 Reading Assignment

Read pages **63–88** of Chapter III of [Silverman-Tate].

3 Problems

1. (Jenna) Prove that the set of rational numbers x with height $H(x)$ less than κ contains at most $2\kappa^2 + \kappa$ elements.

2. (Jeff) Let $\alpha : \Gamma \to \mathbb{Q}^*/\mathbb{Q}^{*2}$ be the map defined in Section 5 of Chapter III of

[Silverman-Tate] by the rule

$$\begin{aligned} \alpha(\mathcal{O}) &= 1 \pmod{\mathbb{Q}^{*2}}, \\ \alpha(T) &= b \pmod{\mathbb{Q}^{*2}} \\ \alpha(x,y) &= x \pmod{\mathbb{Q}^{*2}} \qquad \text{if } x \neq 0. \end{aligned}$$

Prove that if $P_1 + P_2 + T = \mathcal{O}$, then

$$\alpha(P_1)\alpha(P_2)\alpha(T) \equiv 1 \pmod{\mathbb{Q}^{*2}}.$$

3. (Jeff/Mauro) Let A and B be abelian groups and let $\phi : A \to B$ and $\psi : B \to A$ be homomorphisms. Suppose there is an integer $m \geq 2$ such that

$$\begin{aligned} \psi \circ \phi(a) &= ma \qquad \text{for all } a \in A, \\ \phi \circ \psi(b) &= mb \qquad \text{for all } b \in B \end{aligned}$$

Suppose further that $\phi(A)$ has finite index in B, and $\psi(B)$ has finite index in A.

   (a) (Jeff) Prove that mA has finite index in A, and that the index satisfies the inequality
   $$[A : mA] \leq [A : \psi(B)] \cdot [B : \phi(A)].$$

   (b) (Mauro) Give an example to show that it is possible for the inequality in (a) to be a strict inequality.

4. (Jennifer) Let $P \in E(\mathbb{Q})$ be a point on an elliptic curve. The *canonical height* of P is
$$\hat{h}(P) = \lim_{n\to\infty} \frac{\log_e(H(2^n P))}{4^n},$$
where H is as in Chapter III of [Silverman-Tate]. Define a function $d : \mathbb{Q} \to \mathbb{Z}$ by letting $d(a/b)$ be the maximum of the number of digits of a and b (where we assume $\gcd(a,b) = 1$), and extend d to points $P = (x,y)$ by letting $d((x,y)) = d(x)$. Prove that
$$\hat{h}(P) = \log_e(10) \cdot \lim_{n\to\infty} \frac{d(2^n P)}{4^n}.$$