Freshman Seminar 21n: Elliptic Curves

William Stein

March 11, 2003

1 Remarks

The first part of this week's reading is about how to compute $E(\mathbb{Q})$ in some cases, and the second part is about elliptic curves over finite fields.

2 Reading Assignment

Read pages **89–98** and **107–111** of [Silverman-Tate]. Please carefully write up the solutions to your problems and give them to Grigor (use his box on the third floor near the main office). Grigor will look at your write up and give you helpful feedback.

3 Problems

1. (a) (Jenna) Prove that the additive group of rational number $(\mathbb{Q}, +)$ is not finitely generated.
   (b) (Jenna) Prove that the multiplicative group of nonzero rational numbers $(\mathbb{Q}^*, *)$ is not finitely generated.
   (c) (Jenna) Prove that the group of real points $E(\mathbb{R})$ on an elliptic curve is not finitely generated.
   (d) (Alex) Prove for any integer $n \geq 2$, that $\mathbb{Q}^*/\mathbb{Q}^{*n}$ is not finitely generated.
   (e) (Mauro) Prove that $(\mathbb{Z}, +)$ is a normal subgroup of $(\mathbb{Q}, +)$, and show that the quotient $\mathbb{Q}/\mathbb{Z}$ is not finitely generated.
2. (Jeff) Let p be a prime and let C_p be the curve $y^2 = x^3 + px$.
   (a) Prove that the rank of $C_p(\mathbb{Q})$ is either 0, 1, or 2.
   (b) If $p \equiv 7 \pmod{16}$, prove that C_p has rank 0.
   (c) If $p \equiv 3 \pmod{16}$, prove that C_p has rank either 0 or 1. (Can the rank ever be 0? Use a computer to decide.)
3. Using the method developed in Section III.6 of [Silverman-Tate], find the rank of each of the following curves. Check your answers with the output from MAGMA and/or mwrank.

(a) (Mauro) $y^2 = x^3 + 3x$
(b) (Alex) $y^2 = x^3 + 5x$
(c) (Jenna) $y^2 = x^3 + 73x$
(d) (Jennifer) $y^2 = x^3 + 7x$

4. (Jennifer) Let $p \geq 3$ be a prime, and let $m \geq 1$ be an integer which is relatively prime to $p - 1$.

   (a) Prove that the map $x \mapsto x^m$ is an isomorphism from $\mathbb{F}_p^*$ to itself.

   (b) Prove that the equation

   $$x^m + y^m + z^m = 0$$

   has exactly $p+1$ projective solutions (i.e., solutions modulo scalars) with $x, y, z \in \mathbb{F}_p$.