Freshman Seminar 21n: Elliptic Curves

William Stein

February 25, 2003

1 Remarks

Your reading for this week is about the Nagell-Lutz theorem about the subgroup of rational points of finite order on an elliptic curve, and how to use certain computer programs to compute with elliptic curves.

Helpful hint: To input the elliptic curve

$$y^2 + a_1xy + a_3y = x^3 + a_2x^3 + a_4x + a_6$$

to the computer programs we will use, enter $[a_1, a_2, a_3, a_4, a_6]$.

2 Reading Assignment

Read pages **49–58** of Chapter II of [Silverman-Tate]. For a much more clever (and more terse!) account of the same theorem, you might also want to look at Cassels, Sections 9–12, which I will hand out to you (reading Cassels is optional). Also, try out MAGMA, PARI, and MWRANK using the commands `magma`, `gp`, and `mwrank` on meccah, respectively, and browse some of the big documentation handout.

3 Problems

Try all the problems but definitely do the ones with your name in front of them.

1. (Mauro) Look at Figure 2.6 in Silverman-Tate. It is the graph of an elliptic curve with one real component along with the corresponding graph in the s-t plane. Choose an elliptic curve with two real components and draw its graph in the s-t plane.

2. (Alex) The third paragraph on page 52 of Silverman-Tate begins: "Let $P_1 = (t_1, s_1)$ and $P_2 = (t_2, s_2)$ be distinct points. If $t_1 = t_2$, then $P_1 = -P_2$, so $P_1 + P_2$ is certainly in $C(p^\nu)$" (i.e., the t-coordinate of the sum is divisible by p^ν). I think this is a *mistake* in the proof, because $P_1 = -P_2$ if and only if $t_1 = -t_2$ and $s_1 = -s_2$, as discussed at the bottom of page 53. Repair the mistake; that is, give a proof that if $t_1 = t_2$ then $P_1 + P_2$ is in $C(p^\nu)$.

3. (Jeff) Let $p \geq 2$ be a prime and let E be the elliptic curve

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

Find all points of finite order in $E(\mathbb{Q})$.

4. (Jenna) Let p be a prime and let $S = S_p = \mathbb{Z}[\frac{1}{p}]$ be the set of rational numbers of the form a/p^r for $a \in \mathbb{Z}$ and $r \geq 0$.

   (a) Prove that S is a subring of $\mathbb{Q}$.

   (b) Prove that the group of units in S is $\{\pm p^\nu : \nu \in \mathbb{Z}\}$.

   (c) Let $q \neq p$ be a prime. Prove that q generates a maximal ideal of S and describe the quotient field $S/(q)$. Prove that every maximal ideal of S is of this form.

5. (Jennifer) For each of the following elliptic curves E, determine the torsion subgroup of $E(\mathbb{Q})$. You may use the stronger form of Nagell-Lutz (i.e., $2P = 0$ or $y^2 \mid D$) and you may use a computer to automate use of Nagell-Lutz (but don't just write `TorsionSubgroup(EllipticCurve(...))` in MAGMA). By Mazur's theorem, the groups you get will represent all possibilities for $E(\mathbb{Q})_{\mathrm{tor}}$ for any elliptic curve E over $\mathbb{Q}$.

   (a) $y^2 = x^3 - 2$

   (b) $y^2 = x^3 + 8$

   (c) $y^2 = x^3 + 4$

   (d) $y^2 = x^3 + 4x$

   (e) $y^2 - y = x^3 - x^2$

   (f) $y^2 = x^3 + 1$

   (g) $y^2 = x^3 - 43x + 166$

   (h) $y^2 + 7xy = x^3 + 16x$

   (i) $y^2 + xy + y = x^3 - x^2 - 14x + 29$

   (j) $y^2 + xy = x^3 - 45x + 81$

   (k) $y^2 + 43xy - 210y = x^3 - 210x^2$

   (l) $y^2 = x^3 - 4x$

   (m) $y^2 + xy - 5y = x^3 - 5x^2$

   (n) $y^2 + 5xy - 6y = x^3 - 3x^2$

   (o) $y^2 + 17xy - 120y = x^3 - 60x^2$

6. (Mauro) Use **mwrank** to find generators for a subgroup of finite index of the group of rational points on the following elliptic curves:

   (a) $y^2 + y = x^3 - x^2 - 10x - 20$

(b) $y^2 + y = x^3 - x$

(c) $y^2 + y = x^3 + x^2 - 2x$

(d) $y^2 + y = x^3 - 7x + 6$

(e) $y^2 + xy = x^3 - x^2 - 79x + 289$

(f) $y^2 + y = x^3 - 79x + 342$

7. (Jenna) Use `gp` (PARI) to do the following elliptic curve arithmetic. Let $P = (1, 0)$ and $Q = (-1, 1)$ on $y^2 + y = x^3 + x^2 - 2x$.

   (a) Compute $4P + 5Q$.

   (b) Find the smallest multiple nP of P such that the x and y-coordinates of nP are not both integers, and hence prove that P has infinite order. Do the same for Q.

   (c) Find five distinct right triangles with rational side lengths and area 5 using arithmetic on an elliptic curve and Proposition 4.2 and Example 4.4 from the notes for 02/11/03. Use Nagell-Lutz to prove that there are infinitely many right triangles with rational side lengths and area 5 (assuming the truth of Proposition 4.2).

8. (Alex) Use `magma` to do the same arithmetic as in Exercise 7.

9. (Jennifer) Part (c) of the proposition on page 55 asserts that the map

$$\frac{C(p^\nu)}{C(p^{3\nu})} \to \frac{p^\nu R}{p^{3\nu} R}, \qquad P = (x, y) \mapsto t(P) = \frac{x}{y}$$

   is a one-to-one homomorphism. Let $p = 3$ and $\nu = 1$. Determine the size of the image of this map for the first 3 curves in Problem 6 (assume that the subgroup of finite index output by mwrank is actually of index 1).

10. (Jeff) Prove that for every rational number $t \neq 0, \frac{1}{4}$, the point (t, t) on the elliptic curve defined by

$$y^2 = x^3 - (2t - 1)x^2 + t^2 x$$

   is a point of order four. (See the discussion on page 57 of [Silverman-Tate], and feel free to use a computer to simplify the algebra.)