Homework 9: Elliptic Curves

Due Wednesday, November 28

William Stein

Math 124 Harvard University **Fall 2001**

There are 5 problems. Choose 4 of the 5 problems and clearly *indicate which ones you will be graded on (as usual, your score will be a fraction between* 0 *and* 1*). As usual, you may use PARI for any of them, as long as you explain what you are doing. Work in groups.*

1. (10 points) Let Φ be the set of the 15 possible groups of the form $E(\mathbb{Q})_{\mathrm{tor}}$ for E an elliptic curve over $\mathbb{Q}$ (see Lecture 27). For each group $G \in \Phi$, if possible, find a finite field $k = \mathbb{Z}/p\mathbb{Z}$ and an elliptic curve E over k such that $E(k) \approx G$. (Hint: It is a fact that $|p+1-\#E(\mathbb{Z}/p\mathbb{Z}))| \leq 2\sqrt{p}$, so you only have to try finitely many p to show that a group G does not occur as the group of points on an elliptic curve over a finite field.)

2. (6 points) Many number theorists, such as myself one week ago, incorrectly think that Lutz-Nagell works well in practice. Describe the steps you *would* take if you were to use the Lutz-Nagell theorem (Lecture 27) to compute the torsion subgroup of the elliptic curve E defined by the equation

$$y^2 + xy = x^3 - 8369487776175x + 9319575518172005625,$$

then tell me why it would be *very* time consuming to actually carry these steps out. Find the torsion subgroup of E using the `elltors` command in PARI. Does `elltors` use the Lutz-Nagell algorithm by default?

3. (6 points) Let E be the elliptic curve defined by the equation $y^2 = x^3 + 1$.
   (i) For each prime p with $5 \leq p < 30$, describe the group of points on this curve having coordinates in the finite field $\mathbb{Z}/p\mathbb{Z}$. (You can just give the order of each group.)
   (ii) For each prime in (i), let N_p be the number of points in the group. (Don't forget the point infinity.) For the set of primes satisfying $p \equiv 2 \pmod{3}$, can you see a pattern for the values of N_p? Make a general conjecture for the value of N_p when $p \equiv 2 \pmod{3}$.
   (iii) Prove your conjecture.

4. (6 points) Let p be a prime and let E be the elliptic curve defined by the equation $y^2 = x^3 + px$. Use Lutz-Nagel to find all points of finite order in $E(\mathbb{Q})$.

5. (4 points)
   (i) Let E be an elliptic curve over the real numbers $\mathbb{R}$. Prove that $E(\mathbb{R})$ is not a finitely generated abelian group.
   (ii) Let E be an elliptic curve over a finite field $k = \mathbb{Z}/p\mathbb{Z}$. Prove that $E(k)$ is a finitely generated abelian group.