Math 168: Homework Assignment 2

William Stein

Due: Wednesday, Oct 12, 2005

The SIX problems have equal point value, and multi-part problems are of the same value. You are allowed to use a computer on any problem, as long as you include the exact code used to solve the problem with your solution. Any software systems (e.g., Magma, SAGE, Mathematica, C) are allowed.

1 Announcements

1. Office Hours: Tuesdays 3-5 in my office (AP&M 5111).
2. Section: Thursday 5-6 **in my office**

2 Problems

1. One rational solution to the equation $y^2 = x^3 - 2$ is $(3, 5)$. Find a rational solution with $x \neq 3$ by drawing the tangent line to $(3, 5)$ and computing the second point of intersection.
2. Write down an equation $y^2 = x^3 + ax + b$ over a field K such that $-16(4a^3 + 27b^2) = 0$ (yes equals 0). Precisely what goes wrong when trying to endow the set $E(K) = \{(x, y) \in K \times K : y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$ with a group structure (in an algebraic way)?
3. Let E be the elliptic curve over the finite field $K = \mathbb{F}_5$ defined by the equation
$$y^2 = x^3 + x + 1.$$
   (a) List all 9 elements of $E(K)$.
   (b) What is the structure of $E(K)$, as a product of cyclic groups?
4. Let E be the elliptic curve defined by the equation $y^2 = x^3 + 1$. For each prime $p \geq 5$, let N_p be the cardinality of the group $E(\mathbb{F}_p)$ of points on this curve having coordinates in $\mathbb{F}_p$. For example, we have that $N_5 = 6, N_7 = 12, N_{11} = 12, N_{13} = 12, N_{17} = 18, N_{19} = 12, , N_{23} = 24$, and $N_{29} = 30$ (you do not have to prove this).

(a) 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 $p \equiv 2 \pmod 3$.

(b) (*) Prove your conjecture.

5. Suppose $y^2 = x^3 + ax + b$ with $a, b \in \mathbb{Q}$ defines an elliptic curve. Show that there is another equation $Y^2 = X^3 + AX + B$ with $A, B \in \mathbb{Z}$ whose solutions are in bijection with the solutions to $y^2 = x^3 + ax + b$ (via a bijection defined by algebraic formulas).

6. Let E be an elliptic curve over the real numbers $\mathbb{R}$. Prove that $E(\mathbb{R})$ is not a finitely generated abelian group.