Math 168: Homework Assignment 1

William Stein

Due: Wednesday, Oct 5, 2005

The 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. Homework will typically be assigned on Mondays and due on the following **Wednesday**. Then you have plenty of time to ask me questions about it.

2. Grading: For undergrads it is exactly as on the syllabus. For graduate students, make some effort on the homework and do a final project and you will get an A. I will greatly appreciate if grad students help the undergraduates in the course.

2 Problems

1. Prove that there are infinitely pairs (x, y) of rational numbers such that $3x^2 + 4y^2 = 7$.

2. Find (by brute force) all pairs (x, y) of integers with $0 \leq x < 5$ and $0 \leq y < 5$ and
$$y^2 \equiv x^3 - x \pmod{5}.$$

3. Find an elliptic curve E over a finite field $\mathbb{F}_p$ such that the group $E(\mathbb{F}_p)$ is not cyclic.

4. I'm giving you an account on my "super-fast" dual-opteron server `modular.ucsd.edu`, where you'll be able to run SAGE and Magma. Please select a login name. See also `http://modular.ucsd.edu/calc/`.

5. Find 10 distinct solutions (x, y), with $x, y \in \mathbb{Q}$ to the equation
$$y^2 + y = x^3 - 7x + 6.$$