Lecture 1: What is Math 124?

William Stein

Math 124 Harvard University **Fall 2001**

1 Who is Teaching this Course?

I am *William Stein*. Come see me during my office hours, which are Wednesdays and Fridays, 2:00–3:00.

Quick Bio: I received a Ph.D. from Berkeley just over a year ago, where I worked with Hendrik Lenstra, Ken Ribet, and Robert Coleman. After graduating, I visited math institutes in Europe, Australia, and Asia and was a postdoctoral fellow here at Harvard. Now I am a Benjamin Peirce Assistant Professor. Lucky for you, my research specialty is number theory, with a focus on computing with "elliptic curves and modular forms".

2 Evaluation

- In-class midterm on October 17 (20% of grade)
- Homework every Wednesday (40% of grade)
- Take-home final (40% of grade)

3 What is this Course About?

See the lecture plan. The main ideas include:

3.1 Factorization

Do you remember writing whole numbers as products of primes? For example,

$$12 = 2 \times 2 \times 3.$$

Can this sort of thing always be done? Is it really hard or really easy? For example, is factoring social security numbers "trivial" or hopeless? In fact, it's trivial; even my wristwatch can do it!! (Mine might be the only wristwatch in the world that can factor social security numbers, but that's another story.) What about bigger numbers?

These questions are important to your everyday life. If somebody out there secretly knows how to factor 200-digit numbers quickly, then that person could easily read you credit card number and expiration date when you send it to `amazon.com`.

3.2 Congruences and Public-key Cryptography

Two numbers a and b are *congruent modulo another number* n if $a = b + nk$ for some integer k. That a and b are congruent just means you can "get from a to b on the number line" by adding or subtracting lots of copies of n. For example, $14 \equiv 2 \pmod{12}$ since $14 = 2 + 12 \cdot 1$.

$$\mathbf{Z}/n\mathbf{Z} = \{ \text{ equivalence classes of numbers modulo } n \ \}.$$

Your web browser's "secret code language" uses arithmetic in $\mathbf{Z}/pq\mathbf{Z}$ to send messages in broad weblight to `amazon.com`. How can this possibly be safe!? You will find out exactly what is going on.

3.3 Computers

Computers make the study of properties of whole numbers vastly more interesting. A computer is to a number theorist, like a telescope is to an astronomer. It would be a shame to teach an astronomy class without touching a telescope; likewise, it would be shame to teach this class without telling you how to look at the integers "through the lens of a computer".

3.4 Sums of Two Squares

I will tell you how to decide whether or not your order number is a sum of two squares. For example, an odd prime number is a sum of two squares if and only if when divided by 4 it leaves a remainder of 1. For example, 7 is not a sum of two squares, but 29 is.

3.5 Elliptic Curves

My experience is that elliptic curves are extraordinarily fun to study. Every such curve is like a whole galaxy in itself, just like the rational numbers are. An elliptic curve over $\mathbf{Q}$ is a curve that can be put in the form

$$y^2 = x^3 + ax + b,$$

where the cubic has distinct roots and $a, b \in \mathbf{Q}$. The amazing thing is that the set of pairs

$$E(\mathbf{Q}) = \{(x, y) \in \mathbf{Q} \times \mathbf{Q} : y^2 = x^3 + ax + b\} \cup \{\infty\}$$

has a natural structure of "group". In particular, this means that given two points on E, there is a way to "add" the two solutions together to get another solution.

Many exciting problems in number theory can be translated into questions about elliptic curves. For example, Fermat's Last Theorem, which asserts that $x^n + y^n = z^n$ has no positive integer solutions when $n > 2$ was proved using elliptic curves. Giving a method to decide which numbers are the area of a right triangle with rational side lengths has *almost*, but not quite, been solved using elliptic curves.

The central question about elliptic curves is *The Birch and Swinnerton-Dyer Conjecture* which gives a simple conjectural criterion to decide whether or not $E(\mathbf{Q})$ is infinite (and more). Proving the BSD conjecture is one of the Clay Math Institute's million dollar prize problems. I'll tell you what this conjecture is.