Lecture 37: A Look Back

William Stein

Math 124 Harvard University **Fall 2001**

As we look back over our number theory course, several topics stand out: integers and congruences, factorization, public-key cryptography, continued fractions, binary quadratic forms, and elliptic curves. The integers and congruences are at the heart of almost everything we studied. We learned that integers factor as products of primes and got a taste of how to find such factorizations in some cases using Pollard's $(p-1)$ method and Lenstra's elliptic curve method. We learned the basics of the beautiful theory of binary quadratic forms, their composition law, and finiteness of the group of equivalence classes of binary quadratic forms of given discriminant. We also learned that every positive real number α has a continued fraction, and that it is eventually periodic if and only if α satisfies an irreducible quadratic polynomial. We learned about three public-key cryptosystems: the Diffie-Hellman key exchange, the RSA cryptosystem, which uses arithmetic in $(\mathbb{Z}/pq\mathbb{Z})^*$, and the ElGamal elliptic curve cryptosystem which is used by Microsoft in their digital rights management scheme. We spent the last month learning about the group law on an elliptic curve, torsion points and a big theorem of Mazur, about how modularity of elliptic curves is used in the proof of Fermat's Last Theorem, and about the Birch and Swinnerton-Dyer conjecture.

1 Integers, Congruences, and Factorization

The integers are built out of prime numbers, in the sense that every positive integer has an essentially unique representation as a product of primes. If N is an integer, the Pollard $p-1$ method was one method we studied for picking off sufficiently power-smooth divisors of N; it involves computing

$$\gcd(a^{\mathrm{lcm}(2,3,\ldots,B)}, N)$$

for various choices of a and B. This motivated Lenstra's elliptic curve method, which does a better job; it involves *trying* to compute

$$\mathrm{lcm}(2,3,\ldots,B)\cdot P \in E(\mathbb{Z}/N\mathbb{Z})$$

for various B, and points P on *various* "elliptic curves" E over $\mathbb{Z}/N\mathbb{Z}$, and hoping that something goes wrong.

The ring

$$\mathbb{Z}/N\mathbb{Z} = \{0, 1, \ldots, N-1\} \quad \text{(arithmetic mod } N\text{)}$$

and its group of units

$$(\mathbb{Z}/N\mathbb{Z})^* = \{a : 1 \leq a \leq N \text{ and } \gcd(a, N) = 1\}$$

appeared repeatedly throughout the course. We learned how to efficiently compute a^n in $\mathbb{Z}/N\mathbb{Z}$ using a method that involved the binary expansion of n. Wilson's theorem asserts that

$$(p-1)! \equiv -1 \pmod{p} \text{ if and only if } p \text{ is prime}$$

Fermat's little theorem says that if $x \in (\mathbb{Z}/N\mathbb{Z})^*$, then $x^{\varphi(N)} = 1$, where $\varphi(N) = \#(\mathbb{Z}/N\mathbb{Z})^*$; this is just a special case of Lagrange's theorem from group theory.

A primitive root modulo N is a generator of $(\mathbb{Z}/N\mathbb{Z})^*$. We proved that primitive roots exist when N is prime and I remarked that they also exist when $N = p^r$ is an odd prime power. There is no primitive root in $(\mathbb{Z}/8\mathbb{Z})^*$.

If $N = mr$ with $\gcd(m, r) = 1$, then the Chinese remainder theorem allows us to view a congruence modulo N as a system of two congruences, one modulo m and one modulo r.

2 Public-key Cryptography

The Diffie-Hellman key exchange is generally regarded as the first public-key cryptosystem that was unleashed on the public. If Nikita and Michael wish to publically agree on a shared private key, together they choose a modulus p and an element $g \in (\mathbb{Z}/p\mathbb{Z})^*$. Nikita chooses a secret random number n and Michael chooses a secret random number m. Nikita then sends g^n to Michael and Michael sends g^m to Nikita. Both Nikita and Michael can easily compute the secret key g^{nm}, but an outsider would have great difficulty in computing g^{nm}.

The RSA cryptosystem also involes arithmetic in $(\mathbb{Z}/N\mathbb{Z})^*$. Here, Nikita secretly chooses two huge random primes p and q, and computes both $N = pq$ and $\varphi(N) = (p-1)(q-1)$. She then chooses a random encryption key e that is coprime to $\varphi(N)$, and she computes an integer d such that $ed \equiv 1 \pmod{\varphi(N)}$. To encrypt a message $M \in \mathbb{Z}/N\mathbb{Z}$ to Nikita, you compute $M^e \pmod{N}$. Then Nikita can easily recover $M = (M^e)^d$, but an eavesdropper would have great difficulty in finding M.

Since RSA doesn't make sense in the context of elliptic curves, we turn to the ElGamal system. Nikita publically chooses an elliptic curve E over $\mathbb{Z}/p\mathbb{Z}$ and a point $B \in E(\mathbb{Z}/p\mathbb{Z})$. She then secretly computes a random integer n and publishes nB. To send Nikita a message $P \in E(\mathbb{Z}/p\mathbb{Z})$, you choose a random number r and send Nikita the pair

$$(rB, P + r(nB)).$$

From this pair, Nikita can compute

$$P = P + r(nB) - n(rB),$$

but Nikita's adversary will probably have great difficulty because the elliptic curve discrete log problem appears to be so difficult.

3 Continued Fractions

A continued fraction is a finite or infinite expression of the form

$$a_0 + \cfrac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \cdots}}},$$

where $a_0 \in \mathbb{R}$ and $a_1, a_2, \ldots$ are positive real numbers. Usually we considered only integral continued fractions, in which case the a_i are in $\mathbb{Z}$.

The partial convergents

$$\frac{p_n}{q_n} = [a_0, \ldots, a_n]$$

have many amazing properties, and the recurrence that defines p_n and q_n lies at the heart of almost everything we proved about continued fractions:

$$\begin{array}{llll} p_{-1} = 1, & p_0 = a_0, & p_1 = a_1 p_0 + p_{-1} = a_1 a_0 + 1, & p_n = a_n p_{n-1} + p_{n-2}, \\ q_{-1} = 0, & q_0 = 1, & q_1 = a_1 q_0 + q_{-1} = a_1, & q_n = a_n q_{n-1} + q_{n-2}. \end{array}$$

The nicest result that we proved was that $\alpha \in \mathbb{R}$ has an eventually-periodic continued fraction if and only if α is a root of an irreducible quadratic polynomial.

4 Binary Quadratic Forms

A binary quadratic form is a polynomial

$$q(x, y) = ax^2 + bxy + cy^2$$

with $a, b, c \in \mathbb{Z}$. For example $q(x, y) = x^2 + y^2$ is a binary quadratic form, and there is a simple criterion for whether or not an integer n is of the form $n = q(x, y)$ for $x, y \in \mathbb{Z}$.

The discriminant $b^2 - 4ac$ of q is congruent to either 0 or 1 modulo 4. Suppose D is a negative discrimant and consider the set of equivalence classes of binary quadratic forms of discriminant D, where two forms q_1 and q_2 are equivalent if and only if there exists $g \in \mathrm{SL}_2(\mathbb{Z})$ such that $q_{|g} = r$, where

$$q_{|g}(x, y) = q\left(g \begin{pmatrix} x \\ y \end{pmatrix}\right).$$

A reduced binary quadratic form is one for which $|b| \leq a \leq c$ and, in addition, when one of the two inequalities is an equality then $b \geq 0$. Every form is equivalent to exactly one reduced form, so it is possible to decide whether or not two forms are equivalent. Also, there are only finitely many equivalence classes of fixed discriminant $D < 0$. This finite set has a natural group structure.

5 Elliptic Curves

From the point of view of number theory, elliptic curves $y^2 = x^3 + ax + b$ are perhaps the most interesting of all curves. The points on E form a group if we declare that $P + Q + R = \mathcal{O}$ if and only if P, Q, and R are colinear.

The group

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

may be either finite or infinite, though Barry Mazur proved that the group $E(\mathbb{Q})_{\mathrm{tor}}$ of elements of finite order has size at most 16.

The Birch and Swinnerton-Dyer conjecture predicts that $E(\mathbb{Q})$ is infinite if and only if $L(E, 1) = 0$, where

$$L(E, s) = \sum_{n=1}^{\infty} a_n n^{-s}$$

and the a_n encode information about E over $\mathbb{Z}/p\mathbb{Z}$ for all primes p. More precisely, $\mathrm{ord}_{s=1} L(E, s)$ should equal the rank of $E(\mathbb{Q})$. It is an open problem to exhibit a curve such that $L(E, 1) = L'(E, 1) = L''(E, 1) = L'''(E, 1) = 0$.

Andrew Wiles proved Fermat's last theorem a few years ago by showing that if $a^\ell + b^\ell = c^\ell$ is a counterexample, then the elliptic curve

$$y^2 = x(x - a^\ell)(x + b^\ell)$$

is attached to a modular form, which, by work of Ken Ribet, can't possibly exist.

6 Remarks on the Final Examination

Due to popular demand, and so we can have a review session during reading week, I've decided to slightly modify the final exam dates: The take-home final exam will be available **Friday, January 11** and due on **Monday, January 21** at 5pm. It should not take you every waking moment during those days to do the exam. Choose a subset of the days that is good for you.

I will give a **review session** on *Wednesday, January 9 at 11am* in SC 216, i.e., the regular place and time that our course meets. I intend to answer your questions then and get you pointed in the right direction for the final, which I'll make available on Friday, January 11.

I posted "A. Student's" solutions to assignments 1, 4, 5, 6, 7, and 9 on the web page.[1] If you typed up good solutions to assignments 2, 3, 8, or 10, please email them to me. I'll post them under Anonymous Student (A. Student) or under your name, whichever you prefer. You will be doing the other students in our course a great favor.

For your convenience, I assembled all of the lecture notes and homework assignments (without solutions) together into a single book, which I've posted at

`http://modular.fas.harvard.edu/edu/Fall2001/124/lectures/lectures_all`

[1] I make no warranties as to the correctness of A. Student's solutions.