Honors 1: Undergraduate Math Lab*

Peter Sarnak[†], Steven Miller[‡], Alex Barnett[§]

September 5, 2002

Courant Institute of Mathematics
New York University
New York, NY

Abstract

1 Primality Testing

Given n, is n prime or composite? How difficult is this? How long does it take? Brute force: try factors up to $\sqrt{n}$, so can do in $\sqrt{n}$ steps.

$P = NP$ problem. Deep central problem in theoretical Computer Science. P is problems solvable in polynomial number of steps (in terms of input); if equals NP, a lot of problems are solvable quickly.

Telling when n is prime: isn't supposed to be hard, but until two weeks ago, wasn't known to be a P problem.

Notation: $A(x) = O\Big(B(x)\Big)$ if there exists a $C > 0$ (which can be computed; if it cannot be computed, we say so) such that $|A(x)| \leq CB(x)$.

Example: One could show every sufficiently large odd number is the sum of three primes. However, we didn't know how large sufficiently large was! IE, we couldn't go through the calculation and make explicit a number N_0 such that if n is odd and greater than N_0, then n is the sum of three primes. (Note: this has been removed, and we know have another proof giving an explicit N_0).

Theorem 1.1 (Agrawal, Kayal, Saxena) *There is a procedure which runs in at most* $O\Big(\log^{12} n\Big)$ *steps determines whether* n *is prime. (Might be a little more than* $\log^{12} n$*, ie, might be something like* $\log^{12} n(\log\log n)^A$*).*

---

*Homepage: `http://www.math.nyu.edu/~millerj/`

[†]E-mail: `sarnak@math.princeton.edu`

[‡]E-mail: `millerj@cims.nyu.edu or sjmiller@math.princeton.edu`

[§]E-mail: `barnett@nmr.mgh.harvard.edu`

There were algorithms that were known and faster, but only known to work all the time assuming certain well believed hypotheses (Riemann Hypothesis, RH).

(Go to http://www.math.nyu.edu/~millerj/problemlist/problems.htm for a copy of their paper).

Need a feel for numbers. When n is big, $\log n$ (to any power) is much less than n. For practical applications, the size of the constant is important, as a constant of size 10^{100} would make an algorithm useless for our real world applications (ie, for the ranges we can reach). In AKS, the constants are tractable.

Technical Point: In AKS, they quote a theorem from number theory (they treat this as a black box: someone from this class will hopefully investigate this result further). *There are many primes p for which $p-1$ has a large prime factor q, $q > p^{\frac{2}{3}}$.* Related to Sophie Germain primes: primes p where $p - 1 = 2q$, q prime. (She showed that for primes like this, $x^p + y^p = z^p$, you can solve Fermat's Last Theorem for such primes. It is not known if there are infinitely many primes like this). AKS does not need to know there are infinitely many Sophie Germain primes; fortunately all they need is that there are sufficiently many primes p with $p - 1$ with large prime factors.

Similar to Twin Primes: primes p_1, p_2 with $p_1 - p_2 = 2$. We don't know if there are infinitely many twin primes, but we do have heuristics (Hardy-Littlewood) predicting how many twin primes there are (and we observe exactly that many). Sophie Germain primes are more subtle, but should be able to get heuristics. For twin primes and related quantities, see David Schmidt's report on Prime Investigations (Princeton Undergraduate Math Lab, 2000 – 2001). Anyway, this would be a good project.

2 Arithmetic Modulo p

Number Theory: the study of whole numbers. $\mathbb{Z}$ is the integers, look at $\mathbb{Z}/n\mathbb{Z}$ $= \{0, 1, 2, \dots, n-1\}$. This is a finite group (under addition); in fact, it is a finite ring (can also multiply, have inverses for the non-zero elements only if n is prime).

Notation: $x \equiv y \bmod n$ means $x - y$ is a multiple of n.

Try and solve in $\mathbb{Z}$ the equation $2x + 1 = 2y$. The left hand side is odd, the right hand side is even. Thus, there are no solutions. Really, just did arithmetic mod 2 or in $\mathbb{Z}/2\mathbb{Z}$. Harder: $x^2 + y^2 + z^2 = 8n + 7$. This never has a solution. Look modulo 8. The RHS is 7 modulo 8. What are the squares mod 8? $1^1 = 1, 2^2 = 4, 3^2 = 1$, $4^2 = 0$, repeats. See there is no way to add three squares and get 7.

Idea: First, try and solve the equation modulo different primes. If you cannot solve it for some prime, then you cannot solve it over the integers.

2.1 Algebra Review

$\mathbb{Z}/n\mathbb{Z}$: do arithmetic over this ring. $\left(\mathbb{Z}/n\mathbb{Z}\right)^*$ are the invertible (multiplicatively) elements in the ring $\mathbb{Z}/n\mathbb{Z}$, ie, x is in $\left(\mathbb{Z}/n\mathbb{Z}\right)^*$ if there is a y such that $xy \equiv 1 \bmod n$. Note: if $\gcd(x,n) > 1$ (ie, x and n have a common prime divisor p), then you cannot invert x (there is no y with $xy \equiv 1 \bmod n$). Why? $xy \equiv 1 \bmod n$ means $xy = 1 + \lambda n$ for some integer λ. But if $p|x$ and $p|n$, then $p|1$ which is absurd. Exercise: if $\gcd(x,n) = 1$, there is an inverse (Euclidean Algorithm).

The cardinality (number of elements in the set) of $\left(\mathbb{Z}/n\mathbb{Z}\right)^*$ is the number of $x \in \{0, 1, 2, \ldots, n-1\}$ such that $\gcd(x,n) = 1$. We denote the number of such x by $\phi(x)$, the Euler totient function. (Good Reference: H. Davenport: The Higher Arithmetic). Note that if p is prime, $\phi(p) = p - 1$. This implies that $\left|\left(\mathbb{Z}/p\mathbb{Z}\right)^*\right| = p - 1 = \mathbb{Z}/p\mathbb{Z} - \{0\}$. IE, we have a field if n is a prime, as every non-zero element is invertible.

$\left(\mathbb{Z}/n\mathbb{Z}\right)^*$, for any n, is a finite Abelian group (we have inverses under multiplication, and order of multiplication doesn't matter). Finite Abelian Groups is a trivial subject: Structure Theorem for Finite Abelian Groups: product of cyclic groups.

For $n = p$ a prime, $\left(\mathbb{Z}/n\mathbb{Z}\right)^*$ is a cyclic group of order $p - 1$.

If G is a group (have identity, closed under some binary operation, have inverses with respect to the binary operation, operation is associative), we say the order of $x \in G$, $\mathrm{ord}(x)$, is the least positive power m such that $x^m = e$, where $e \in G$ is the identity of the group. In a finite group, every element has finite order (proof: use the pidgeonhole principle).

Theorem 2.1 (Lagrange) *ord(x) | ord(G).*

Corollary 2.2 (Fermat's Little Theorem) *For any prime p, if* $\gcd(a,p) = 1$*, then* $a^{p-1} \equiv 1$ *mod p.*

2.2 Using Fermat's Little Theorem

To check and see if a number n is prime, why not check if $a^{n-1} \equiv 1 \bmod n$ if $\gcd(a,n) = 1$. It is very easy to quickly compute $\gcd(a,n)$ (use Euclid's Algorithm). Sketch: without loss of generality, let $a < n$. Write $n = b_0 a + b_1$, and now the gcd of a and n is the same as that of a and b_1 (note $0 \le b_1 < a$).

How long does it take to raise a to the $n-1$ power? Use repeated squares and base 2 expansion. Example $100 = 64 + 32 + 4$, or $1 \cdot 2^6 + 1 \cdot 2^5 + 1 \cdot 2^2$. Thus, do a^2, $a^2 \cdot a^2$, $a^4 \cdot a^4$, $a^8 \cdot a^8$, $a^{16} \cdot a^{16}$, $a^{32} \cdot a^{32}$. Then $a^{100} = a^{64} \cdot a^{32} \cdot a^4$.

If, by choosing an a, you find $a^{n-1} \not\equiv 1 \bmod n$, you have a certificate for compositeness, but you have no idea what the factors of n are!

When a machine uses Fermat's Little Theorem, it randomly chooses a fixed number of a's between 1 and $n-1$. Problems: how many times should you run these tests to be very confident of the result; are there any numbers which always pass this test, yet are composite?

About eight years ago it was proved there are infinitely many Carmichael numbers (numbers n such that $a^{n-1} \equiv 1 \bmod n$ for all a, but n is composite).

2.3 Quadratic Reciprocity

p, q odd primes. We define $\left(\frac{a}{p}\right)$ to be 1 if a is a non-zero square mod p, 0 if $a = 0$, and -1 otherwise (ie, if a is not a square mod p). Note a is a square mod p if there exists an $x \in \{0, 1, \ldots, p-1\}$ such that $a \equiv x^2 \bmod p$. For p an odd prime, half the non-zero numbers are squares, half are not.

Exercise: $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \bmod p$ for odd p. Note the above squared is $a^{p-1} \equiv 1$.

Theorem 2.3 (Quadratic Reciprocity) *$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) \cdot (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$, p, q odd primes.*

Gauss gave at least four proofs of this deep result. If either p or q is equivalent to 1 mod 4, then one has $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$, ie, I'm a square root modulo you if you are a square root modulo me.

Carmichael numbers were behaving like primes. We want to get rid of them. Instead of testing $a^{n-1} \equiv 1 \bmod n$, test and see if $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \bmod n$. Similar to the Euclidean Algorithm, can computer $\left(\frac{a}{n}\right)$ in $logn$ steps by constant applications of Quadratic Reciprocity.

Key Test: Will test that $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \bmod n$ for $1 \leq a \leq C \log^2 n$. If fails for some a, the number is composite. If it passes, by the Riemann Hypothesis (RH), then it is true for all a. Will then show this is a valid test for primality (ie, unlike Carmichael numbers, if this is satisfied for all a up to $C \log^2 n$, then n is prime. This will take about $\log^4 n$ steps).

Algebra Books: Herstein (Topics in Algebra); Birkhoff-Mclean (Algebra), Lang (Undergraduate Algebra).

3 Lecture Next Week

Steve will talk about reciprocity, finite fields.

4 WWW Resources

http://mathworld.wolfram.com/ is a good place to look up unfamiliar terms.