Primality Testing Made Simple
IAP 2006 Mathematics Lecture Series
Kiran S. Kedlaya, January 27

The field of computational number theory has been active for decades, particularly because of the RSA algorithm in cryptography (more on which below). So it is somewhat surprising that the following result was only proved in 2002!

Theorem 1 (Agrawal-Kayal-Saxena)**.** *There is an explicit deterministic polynomial-time algorithm for determining whether or not an integer $N > 1$ is prime or composite.*

What this means in simple language: you give me $N > 1$, written down as a decimal expansion (or a binary expansion if you prefer, it's not crucial for this assertion). Note that I'm calling it capital N because I'm expecting it to be *really really large* (say, 100 digits). I claim that I can write down either a proof that N is prime or a proof that N is composite, and the amount of time that it will take me to do it is bounded by some power of the *logarithm* of N (i.e., by a power of the number of digits you had to write down to specify N in the first place).

That means that you can't get by doing something simple like trying to divide N by each integer i with $2 \leq i \leq \sqrt{N}$ and seeing if one of them goes into N evenly. That requires time about $\sqrt{N}$, which is much bigger than any polynomial in $\log(N)$.

Sidebar: at the time they proved this theorem, Neeraj Kayal and Nitin Saxena were undergraduates (!!) at the Indian Institute of Technology in Kanpur, and Manindra Agrawal was their advisor. What I'm presenting here is the "second generation" of their proof, from the published version of their paper [1]; this is somewhat simplified and streamlined from their original argument. There are lots of variants possible, to optimize for different aspects (e.g., if you want a faster algorithm which has a small probability of not succeeding); many of these have been catalogued by Dan Bernstein [2, 3].

Why one cares: RSA

The basic idea behind RSA is to give an "asymmetric" mechanism for concealing a secret. Underlying this is a little bit of elementary number theory due to Euler. For N a positive integer, let $\phi(N)$ be the number of integers from 1 to N, inclusive, which are coprime to N (i.e., have no common divisor with N other than 1). Then for any integer a coprime to N,

$$a^{\phi(N)} \equiv 1 \pmod{N}.$$

For instance, if $N = p$ is prime, then $\phi(N) = p - 1$, and in this case Euler's theorem reduces to Fermat's little theorem (more on which below). If $N = pq$ is the product of two distinct primes, then $\phi(N) = (p-1)(q-1)$.

Now suppose Alice wants to receive a secret message from Bob. She picks two large primes p, q and forms $N = pq$. She also picks a random integer d coprime to $\phi(N)$. She gives Bob the values of d and N, but not p or q. Now Bob can send her a message by breaking

it up into pieces which can be encoded as integers in $\{1, \ldots, N\}$ coprime to N, and for each such piece c, calculating and sending $m = c^d \pmod N$.

To decode the message, Alice has to find an integer e such that $de \equiv 1 \pmod{\phi(N)}$; she can then recover c as $m^e \pmod N$. The point is that this is easy provided that one knows $\phi(N)$! An observer trying to snoop on the transmission would have to recover the factorization of N in order to do likewise, and this is very very hard.

In particular, what we are doing here is *not* trying to factor an arbitrary integer. (If you could do that... well, watch the movie *Sneakers*[1] to find out what might happen.) Deciding primality is much much easier; it arises in RSA when Alice is trying to build her N at the beginning, because she wants to make sure that her p and q are really prime.

The easy part: proving compositeness

If a number N is composite, then there exists a simple proof of this: write down a nontrivial factorization and check the multiplication. The unsatisfactory aspect of this answer is that finding this simple proof is quite difficult to execute in practice!

On the other hand, there are somewhat more indirect ways to prove compositeness that are much easier to carry out without any prior knowledge. One way is to use the contrapositive of Fermat's little theorem. Pick a random small integer a (so presumably $a < N$). Use the Euclidean algorithm to figure out whether a and N have a common factor greater than 1 (i.e., replace the bigger of a, N by its remainder modulo the smaller one, and repeat until you get two equal numbers: that's the greatest common factor of a and N). If so, you just proved that N is composite. Much more likely, a and N are coprime, in which case you compute $a^{N-1} \pmod N$. If you don't get 1, then N must be composite!

This works extremely often; for instance, if $a = 2$, then the first odd composite N for which this fails is $N = 341$. However, there are infinitely many composite N for which this test fails unless a and N fail to be coprime; these are called *Carmichael numbers* (see exercises).

The hard part: proving primeness

The novelty in the AKS paper is to introduce a clever method for proving that a number $N > 1$ is prime. Here's the idea (proof left as an exercise): if $N > 1$ is an integer and y is an integer coprime to N, then N is prime if and only if

$$(x + y)^N \equiv x^N + y^N \pmod N \tag{1}$$

(If N is a power of a prime p, you get the congruence modulo p but not modulo N.)

You can't actually use this as an efficient proof of primality because $(x + y)^N$ is a polynomial of $N + 1$ terms, which is much too many. Instead, we look at this in a "quotient" situation.

[1] That's also where the name of my MIT Mystery Hunt team, Setec Astronomy, comes from.

Interlude: rings and fields

Before explaining more, it will be useful to introduce a bit of the language of abstract algebra. If you've taken 18.70x, feel free to doze off for a few minutes.

A *ring* is a set R equipped with two operations $+$ (addition) and $\cdot$ (multiplication), satisfying the following long but reasonable list of properties.

- Addition is commutative: $a + b = b + a$.
- Addition is associative: $a + (b + c) = (a + b) + c$.
- Addition has an identity element: there exists $0 \in R$ such that for any $a \in R$, $a+0 = a$.
- Addition has inverses: for any $a \in R$, there exists $-a \in R$ such that $a + (-a) = 0$.
- Multiplication is commutative: $ab = ba$.
- Multiplication is associative: $a(bc) = (ab)c$.
- Multiplication distributes over addition: $a(b + c) = ab + ac$.
- Multiplication has an identity element: there exists $1 \in R$ such that for any $a \in R$, $1a = a$.

The prototypical example is the integers $\mathbb{Z}$. Given any ring R, the polynomials in a variable x with coefficients in R form another ring, called $R[x]$.

If R is a ring and $r \in R$, then we say that two elements $a, b \in R$ are *congruent modulo* r, written $a \equiv b \pmod{r}$, if $a - b$ is a multiple of r. This gives an equivalence relation (it's reflexive, symmetric, and transitive), and you can add and multiply such equivalences, so the set of equivalence classes forms a ring, called the *quotient ring* and denoted R/rR (or $R/(r)$). For example, if $R = \mathbb{Z}$ and $r = N$ is a positive integer, then $\mathbb{Z}/N\mathbb{Z}$ is the "integers modulo N" from elementary number theory.

You can also talk about congruences modulo more than one element: if $r, s \in R$, then $a \equiv b \pmod{r, s}$ means that $a - b$ can be written as a multiple of r plus a multiple of s. Think of first quotienting by r, then quotienting by s (or vice versa); that quotient is called $R/(r, s)$. (The equivalence class of 0 is an example of what is called an *ideal*.)

A *unit* in a ring R is an element with a multiplicative inverse. The set of units in R is closed under multiplication, and so forms an abelian group, denoted R^*. For $R = \mathbb{Z}/N\mathbb{Z}$, we write $\phi(N)$ (Euler's phi function) to mean the order (number of elements) of $(\mathbb{Z}/N\mathbb{Z})^*$; note that the elements of R^* correspond to congruence classes of integers coprime to N. (Aside: by Lagrange's theorem, any subgroup of $(\mathbb{Z}/N\mathbb{Z})^*$ has order dividing $\phi(N)$.)

A *field* is a ring in which $1 \neq 0$, and every nonzero element is a unit. The integers do not form a field, but the rational numbers $\mathbb{Q}$ do, as do the real numbers $\mathbb{R}$ and the complex numbers $\mathbb{C}$. If N is a positive integer, then $\mathbb{Z}/N\mathbb{Z}$ is a field if and only if N is *prime*; if $N = p$, we usually write $\mathbb{F}_p$ when we mean to think of $\mathbb{Z}/p\mathbb{Z}$ as a field. Similarly, if F is a

field and $P(x) \in F[x]$ is an irreducible polynomial, then $F' = F[x]/(P(x))$ is also a field; the field F' is "designed" to have a root of the polynomial $P(y)$, namely the class of $x \in F'$.

Important fact about fields: over any field F, a polynomial of degree n can have at most n distinct roots. The reason is the one you already know: each root forces the polynomial to split off a linear factor. Here's the key consequence for us.

Lemma 2. *Let F be a field, and let t and u be nonnegative integers. Then the equation $x^t = x^u$ has at most $|t-u|+1$ solutions $x \in F$.*

Proof. One solution is $x = 0$. The other solutions are all roots of the polynomial $x^{|t-u|} - 1$, so there are at most $|t-u|$ of them. □

Also important: polynomials over a field satisfy unique factorization (like positive integers).

A criterion for primality

Remember that we wanted to use the congruence

$$(x+y)^N \equiv x^N + y^N \pmod{N}$$

as a test for the primality of N. What we'll do instead is, for various small values of y, check this congruence modulo $(N, x^r - 1)$. If we make r big enough and check enough different values of y, we'll be able to prove that N must at least be a prime power, and from there it's easy to check whether N is actually prime. The following theorem makes the previous sentence precise. Note: for convenience, all logarithms are in base 2 unless otherwise specified.

Theorem 3. *Let $N > 1$ be a positive integer and put $c = \lfloor \log^2 N \rfloor$. Let r be a positive integer such that none of $N, N^2, \ldots, N^c$ is congruent to 1 modulo r. Put $s = \lfloor \sqrt{\phi(r)} \log N \rfloor$, and suppose that N has no prime factor $\leq \max\{r, s\}$. Suppose also that for $b = 1, \ldots, s$, we have a congruence of polynomials*

$$(x+b)^N \equiv x^N + b \pmod{N, x^r - 1}. \tag{2}$$

Then N is a power of a prime.

We'll come back to the choice of r in the next section; in the meantime, we need to prove Theorem 3. To do this, let p be a prime divisor of N, and assume that N is not a power of p; from this assumption we will ultimately deduce a contradiction. (Strictly speaking, we don't need to make this counterfactual hypothesis right away, but I think it clarifies the exposition slightly.)

Following [1], for a polynomial $f(x) \in \mathbb{F}_p[x]$ (or $f(x) \in \mathbb{Z}[x]$) and an integer m, we say that *m is introspective for $f(x)$* if

$$f(x)^m \equiv f(x^m) \pmod{p, x^r - 1}.$$

This property is clearly multiplicative in f: if m is introspective for both $f(x)$ and $g(x)$, then m is also introspective for $fg(x)$. It is also multiplicative in m, as we now see.

Lemma 4. *If the integers m and m' are both introspective for $f(x)$, then so is mm'.*

Proof. The introspection equation for m states:

$$f(x)^m \equiv f(x^m) \pmod{p, x^r - 1}.$$

Substitute $x^{m'}$ for x:

$$f(x^{m'})^m \equiv f(x^{mm'}) \pmod{p, x^{rm'} - 1}.$$

Since $x^{rm'} - 1$ is divisible by $x^r - 1$, we may read the previous congruence also modulo $(p, x^r - 1)$. The introspection equation for m', with both sides raised to the m-th power, reads:

$$f(x)^{mm'} \equiv f(x^{m'})^m \pmod{p, x^r - 1}.$$

Putting together the previous two equations yields the claim. □

The integer p is introspective for *every* polynomial (as in (1)). On the other hand, if we let P be the set of products

$$P = \left\{ \prod_{b=0}^{s} (x+b)^{e_b} : e_0, \ldots, e_s \geq 0 \right\};$$

then (2) states that N is introspective for each $f(x) \in P$, as is N/p. That means that if we let I be the set of products $(N/p)^i p^j$ for i, j nonnegative integers, then every integer in I is introspective for every polynomial in P.

Let G be the subgroup of $(\mathbb{Z}/r\mathbb{Z})^*$ generated by N and p, and let d be the order of G; then $d \leq |(\mathbb{Z}/r\mathbb{Z})^*| = \phi(r)$. On the other hand, already the subgroup generated by N has order $> c$, so $d > c$ and in particular $d > \log^2 N$.

Consider pairs of integers in the range $0, \ldots, \lfloor \sqrt{d} \rfloor$; the number of such pairs is $(\lfloor \sqrt{d} \rfloor + 1)^2 > d$, so there must be two different pairs (i, j) and (k, l) such that $t = (N/p)^i p^j$ and $u = (N/p)^k p^l$ are congruent modulo r. We cannot have $t = u$: otherwise some power of N would be a power of p, and then unique factorization would imply that N is a power of p, contrary to hypothesis. So $t \neq u$; since t and u are at least 1 and at most $N^{\lfloor \sqrt{d} \rfloor}$, we have $1 \leq |t - u| < N^{\lfloor \sqrt{d} \rfloor}$.

What this means is that the equation $f(x)^t = f(x)^u$ has "many" solutions in $\mathbb{F}_p[x]/(x^r - 1)$, namely all $f(x) \in P$. The way we'll get our contradiction is to quotient ourselves into a field and show that we still have "too many" solutions of $f^t(x) = f^u(x)$.

Let $\Phi_r(x)$ be the *r-th cyclotomic polynomial*, i.e., the monic polynomial with coefficients in $\mathbb{C}$ whose roots are the primitive r-th roots of unity. Then $\Phi_r(x)$ has coefficients in $\mathbb{Z}$ and

$$x^r - 1 = \prod_{m|r} \Phi_m(x)$$

as polynomials over $\mathbb{Z}$; we can thus also view this as an equality of polynomials over $\mathbb{F}_p$. Let $h(x)$ be an irreducible factor of $\Phi_r(x)$ over $\mathbb{F}_p$, and let $\mathbb{F}$ be the finite field $\mathbb{F}_p[y]/(h(y))$.

Lemma 5. *Suppose that $g(x) \in \mathbb{F}_p[x]$ is a nonzero polynomial such that $g(y^{N^i}) = 0$ for all nonnegative integers i. Then $\deg(g(x)) \geq d$.*

Proof. Raising both sides of $g(y^{N^i}) = 0$ to the j-th power, for j a nonnegative integer, yields $g(y^{N^i p^j}) = 0$ (since the coefficients of g don't change when you take their p-th powers). Since $y^0, y^1, \ldots, y^{r-1} \in \mathbb{F}$ are all distinct, we get distinct roots of g corresponding to all of the elements of G, proving the claim. □

Let H be the set of products $\prod_{b=0}^{s}(x+b)^{e_b} \in \mathbb{F}_p[x]$ with each $e_b \geq 0$ and $\sum e_b < d$; they are all distinct because polynomials over a field satisfy unique factorization (remember, N has no prime factors $\leq s$). Then $H \subseteq P$, so that if $e(x) \in H$, then $e(x)^t = e(x)^u$. Suppose $e(x), f(x) \in H$ are congruent modulo $h(x)$; then $g(x) = e(x) - f(x)$ satisfies $g(y^{N^i}) = 0$ for each nonnegative integer i. By Lemma 5, either $g = 0$ or $\deg(g) \geq d$, but the latter is impossible. That is, the elements of H remain distinct when viewed modulo $(p, h(x))$.

That means that the number of solutions of the equation $z^t = z^u$ in $\mathbb{F}_p[x]/(h(x)) \cong \mathbb{F}$ is at least

$$|H| = \binom{d+s}{d-1}.$$

To conclude, all we have to do is confirm that this is indeed "too many" solutions, i.e., that

$$\binom{d+s}{d-1} > N^{\lfloor\sqrt{d}\rfloor}.$$

For this we argue that

$$\begin{aligned}
\binom{d+s}{d-1} &\geq \binom{s+1+\lfloor\sqrt{d}\log N\rfloor}{\lfloor\sqrt{d}\log N\rfloor} && \text{(since } d > \sqrt{d}\log N\text{)} \\
&\geq \binom{1+2\lfloor\sqrt{d}\log N\rfloor}{\lfloor\sqrt{d}\log N\rfloor} && \text{(since } s = \lfloor\sqrt{\phi(r)}\log N\rfloor \geq \lfloor\sqrt{d}\log N\rfloor\text{)} \\
&\geq 2^{\lfloor\sqrt{d}\log N\rfloor+1} && \text{(since } \lfloor\sqrt{d}\log N\rfloor > \lfloor\log^2 N\rfloor \geq 1\text{; see exercises)} \\
&> N^{\lfloor\sqrt{d}\rfloor},
\end{aligned}$$

yielding a contradiction and completing the proof of Theorem 3.

The AKS theorem

To prove Theorem 1 using Theorem 3, we follow the following algorithm.

1. For $i = 2, \ldots, \lfloor\log N\rfloor$ in succession, compute $\lfloor N^{1/i}\rfloor$ and check whether $\lfloor N^{1/i}\rfloor^i = N$. If so, return COMPOSITE.
2. Put $c = \lfloor\log^2 N\rfloor$.
3. Start with $r = 1$ and keep incrementing r until none of $N, N^2, \ldots, N^c$ is congruent to 1 modulo r.

4. Put $s = \lfloor \sqrt{\phi(r)} \log N \rfloor$. For $i = 2, \ldots, \max\{r, s\}$ in turn, check (using the Euclidean algorithm) whether N and i have a common factor. If so, return PRIME if the common factor equals N and COMPOSITE otherwise.

5. For $b = 0, \ldots, s$ in succession, check whether the congruence

$$(x + b)^N \equiv x^N + b \pmod{N, x^r - 1}$$

holds; if not, return COMPOSITE.

6. Return PRIME.

Theorem 3 implies that the algorithm returns PRIME if N is prime and COMPOSITE if N is composite. The remaining content of Theorem 1 is that each step of this algorithm takes time polynomial in $\log N$. This is routine to check except for one point: one must check that the test in the third step will succeed for some r bounded by a polynomial in $\log N$. To see this, notice that

$$(N - 1) \cdots (N^c - 1) < N^{(c(c+1)/2)}$$

whereas $\mathrm{lcm}(1, \ldots, 2m) \geq 2^m$ (see exercises). So we will definitely find some $r < c(c + 1) \log N$.

References

[1] M. Agrawal, N. Kayal, and N. Saxena, PRIMES is in P, *Annals of Math.* **160** (2004), 781–793 (available online).

[2] D.J. Bernstein, Proving primality after Agrawal-Kayal-Saxena, available at `http://cr.yp.to/papers.html`.

[3] D.J. Bernstein, Proving primality in essentially quartic random time, available at `http://cr.yp.to/papers.html`.

Exercises

1. Verify that for p, q distinct primes and $N = pq$, $\phi(N) = (p-1)(q-1)$. Then show that (given that N is the product of two distinct primes) one can recover the factorization of N if one is given $\phi(N)$.

2. Let $N > 1$ be an integer. Prove that N is prime if and only if

$$(x+y)^N \equiv x^N + y^N \pmod{N}.$$

(Hint: if N is prime, check that $\binom{N}{i}$ is divisible by N for $i = 1, \ldots, N-1$. Otherwise, let p be the smallest prime factor of N, and look at $\binom{N}{p}$.)

3. Suppose I give you integers a, m, N with 100 decimal digits each, and I ask you to compute $a^N \pmod{m}$. How do you do this in less time than the age of the universe? (The point is that computing with 100-digit numbers isn't so bad on a typical computer, but a^N is too big to be written down. Hint: first suppose N is a power of 2.)

4. A *Carmichael number* is a composite positive integer N such that for any integer a coprime to N, $a^N \equiv 1 \pmod{N}$. Prove that 561 is a Carmichael number (easy), the prove that 561 is the *smallest* Carmichael number (not so easy). Optional: find the second smallest Carmichael number. (Google will tell you which number it is, but it won't provide proof!)

5. During the course of proving the AKS theorem, we constructed some finite fields other than the $\mathbb{F}_p$, by forming quotients $\mathbb{F}_p[x]/(h(x))$. For example, you can make a finite field of 9 elements by taking $p = 3$ and $h(x) = x^2 + 1$, but you can't make a finite field of 25 elements by taking $p = 5$ and $h(x) = x^2 + 1$. Explicitly construct finite fields with 4, 8, 25, 27 elements. (These turn out to be *unique* up to isomorphism, but don't worry about this for now.)

6. Let N be a integer congruent to 5 modulo 8, and let b be any integer. Prove that if none of

$$b, b^{(N-1)/2} + 1, b^{(N-1)/4} + 1, b^{(N-1)/4} - 1$$

is divisible by N, then N must be composite. Optional: find variants of this for $N \equiv 2^i + 1 \pmod{2^{i+1}}$. (Bernstein attributes this as "Artjuhov, 1966, et al.")

7. Prove that for each integer $s \geq 2$,

$$\binom{2s+1}{s} \geq 2^{s+1}.$$

(Hint: induct on s.) Optional: prove a stronger lower bound, like

$$\binom{2s+1}{s} \geq 2^{2s+1}/(2s+2).$$

(Hint: look at the binomial expansion of $(1+1)^{2s+1}$.)

8. (a) Prove that for p a prime, the number of times p divides $n!$ is

$$\sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor .$$

(That sum is not really infinite; the terms become zero as soon as $i > \log_p N$.)

(b) Use (a) to prove that for each positive integer s, $\binom{2s}{s}$ divides $\mathrm{lcm}(1, 2, \ldots, 2s)$. (Hint: use the fact that $\lfloor 2x \rfloor \leq 2\lfloor x \rfloor + 1$, which you may have seen on this year's Putnam competition.)

(c) Deduce that $\mathrm{lcm}(1, 2, \ldots, 2s) \geq 2^s$. (Hint: use the previous exercise and the fact that $\binom{2s}{s} = 2\binom{2s-1}{s-1}$.)

9. This isn't really apropos to this talk, but it looks a lot like Fermat's little theorem and yet is different in an extremely amusing way. Prove that for any integer $n > 1$,

$$2^{n-1} \not\equiv -1 \pmod{n}.$$

(Hint: first note that any counterexample n would have to be odd. Then prove that every prime factor of n would have to be congruent to 3 mod 4. Then...)