Is this number prime?
Berkeley Math Circle 2002–2003
Kiran Kedlaya

Given a positive integer, how do you check whether it is prime (has itself and 1 as its only two positive divisors) or composite (not prime)? The simplest answer is of course to try to divide it by every smaller integer. There are various ways to improve on this exhaustive method, but they are not very practical for very large candidate numbers. So for a long time (centuries!), mathematicians have been interested in more efficient ways both to test for primality and to find complete factorizations. Nowadays, these questions have practical interest as well: large primes are needed for the RSA encryption algorithm (which among other things protects secure Web transactions), while factorization methods would make it possible to break the RSA system.

While factorization is still a hard problem (to the best of my knowledge!), testing large numbers for primality has become much easier over the years. In this note, I explain three techniques for testing primality: the Fermat test, the Miller-Rabin test, and the new Agrawal-Kayal-Saxena test.

1 The Fermat test

Recall Fermat's little theorem: if p is a prime number and a is an integer relatively prime to p, then

$$a^{p-1} \equiv 1 \pmod{p}.$$

Some experimentation shows that this typically fails when p is composite. Thus the Fermat test for checking the primality of an integer n:

1. Pick an integer $a \in \{2, \ldots, n-1\}$.
2. Compute $\gcd(a, n)$; if it's greater than 1, then stop: n is composite.
3. Compute $a^{n-1} \pmod{n}$. If it's not 1, then stop: n is composite.
4. Um, that's it. You can repeat with a different a if you want.

This test is nice because it's pretty simple and it's efficient. In theoretical terms, this test is *polynomial time* in the length of the input–to compute the GCD and the modular exponentiation each require a number of steps which is polynomial in the number of *digits* of n, and not a polynomial in n or some power of n. (The exponentiation can be done by repeated squaring: compute $a^2 \pmod{n}$, $a^4 \pmod{n}$, and so on, then combine the powers of 2 you need at the end. Oh, and make sure you keep reducing modulo n at each step so the numbers don't get any bigger than n.) So it's practical even for numbers which are hundreds of digits long.

This test is not so nice because it has serious difficulty confirming with certainty that a number is prime. That's because there are some composite numbers that will always sneak past step 3! An integer n is said to be a *Carmichael number* if $a^{n-1} \equiv 1 \pmod{n}$ whenever a is coprime to n. There are in fact infinitely many Carmichael numbers, the smallest of which is $561 = 3 \times 11 \times 17$. The only way to establish the compositeness of a Carmichael number using the Fermat test is to stumble across an a which is divisible by one of the prime factors of the number, i.e., to factor the number.

2 Interlude: the structure of $(\mathbb{Z}/n\mathbb{Z})^*$

This stuff isn't needed for the primality tests, but it may be useful for the problems at the end.

Let $(\mathbb{Z}/n\mathbb{Z})^*$ be the set of numbers modulo n which have no common factor with n other than 1; this is a set of size $\phi(n)$, where ϕ is Euler's totient function: if $n = p_1^{e_1} \cdots p_k^{e_k}$, then

$$\phi(n) = p_1^{e_1-1}(p_1 - 1) \cdots p_k^{e_k-1}(p_k - 1).$$

(For example, if p and q are prime, then $\phi(p) = p - 1$, $\phi(p^2) = p(p - 1)$, and $\phi(pq) = (p - 1)(q - 1)$.) The numbers which represent elements of $(\mathbb{Z}/n\mathbb{Z})^*$ are precisely the ones that have reciprocals modulo n.

We recall in passing why Euler introduced this function: he proved that if a is relatively prime to n, then

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

The simplest proof of this (which also gives a proof of Fermat's theorem, which is the special case when n is prime) is: let $x_1, \ldots, x_{\phi(n)}$ be representatives of the elements of $(\mathbb{Z}/n\mathbb{Z})^*$. Then $ax_1, \ldots, ax_{\phi(n)}$ are also representatives of the elements of $(\mathbb{Z}/n\mathbb{Z})^*$, so

$$x_1 \cdots x_{\phi(n)} \equiv (ax_1) \cdots (ax_{\phi(n)}) \pmod{n},$$

and cancelling common factors on both sides gives $a^{\phi(n)} \equiv 1 \pmod{n}$.

If n is prime, the set $(\mathbb{Z}/n\mathbb{Z})^*$ has a very nice multiplicative structure.

Theorem 2.1. *If n is a prime number, then there exists an integer g such that each element of $(\mathbb{Z}/n\mathbb{Z})^*$ is represented by a power of g.*

Such an element g is called a *primitive root* of n. There are a few additional cases where primitive roots exist: if n is a prime power, or twice a prime power.

3 The Miller-Rabin test

By using a bit more information about the structure of $(\mathbb{Z}/n\mathbb{Z})^*$, one can get a better test, called the Miller-Rabin test.

1. If n is even, stop: there is a much easier test available!
2. Choose an integer a from $\{2, \ldots, n-1\}$ uniformly at random.
3. Factor $n-1$ as $2^t m$, where m is odd.
4. Compute $b = a^m \pmod{n}$.
5. If $b \equiv \pm 1 \pmod{n}$, then stop: n is probably prime.
6. Otherwise, repeat the following $t-1$ times. Replace b by b^2. if $b \equiv -1 \pmod{n}$ then stop: n is probably prime. If $b \equiv 1 \pmod{n}$ then stop: n is composite. Otherwise, continue.
7. If we get this far, stop: n is composite.

This one has a similar defect to the Fermat test: it is unable to state with certainty that n is prime. But it's not as bad as the Fermat test, because no composite n can defeat the test "too often".

First of all, let's see why n is definitely composite if the algorithm says it is. The key point is that 1 has only two square roots modulo any odd prime p, namely 1 and -1. (If $a^2 \equiv 1 \pmod{p}$, then $(a+1)(a-1) \equiv 0 \pmod{p}$ so either $a+1$ or $a-1$ is divisible by p.) So if n were prime, b could never become 1 without having been 1 or -1 at the previous step, so it could never report as composite within the loop. And if n were prime, even if we got through the loop $t-2$ times, at the last step b would have to be ± 1 because its square would be $a^{m2^t} \pmod{n} = a^{n-1} \pmod{n} \equiv 1 \pmod{n}$. So n is definitely composite if the test says it is.

But what if n is composite and the test says it's prime? Pick a different a and try again! This time your efforts will not be in vain: if n is composite, it can be shown the probability that any one choice of a will fail to flag n as composite is at most $1/4$. (The idea: if n is not a prime or prime power, then there are at least four square roots of 1 modulo n, so if we happen to get to 1 by repeated squarings, there's a good chance we went through some other square root of 1 besides -1.)

For "industrial grade" applications, this is good enough; applying the test, say, 50 times guarantees that the probability of a composite sneaking past the test is imperceptibly small. It does not and cannot, however, actually prove that n is prime. It turns out that one can prove that it is enough to check all values of a in a small range (from 1 to $70(\log n)^2$) to ensure that n is prime, but only assuming a well-believed but currently intractable conjecture in number theory (the Extended Riemann Hypothesis, a special case of which is one of the "million dollar problems" of the Clay Mathematics Institute).

There are also some "almost polynomial time" algorithms for producing a proof that n is prime, but they use much more sophisticated mathematics than I can discuss right now (elliptic and hyperelliptic curves). So it was a bit of a surprise when in August 2002, Agrawal, Kayal and Saxena produced a polynomial-time algorithm that can determine whether or

not n is prime; the surprise is that their algorithm uses nothing fancier than the theory of polynomials over $(\mathbb{Z}/p\mathbb{Z})$! (Not to mention that Kayal and Saxena at the time were undergraduates doing a research project with Agrawal!)

4 Interlude: finite fields

Again, you can find this stuff in any good abstract algebra book. One of my favorites is *Algebra*, by Michael Artin.

Let n be a prime number and $h(x) = c_n x^n + \cdots + c_0$ a polynomial over $\mathbb{Z}/n\mathbb{Z}$. Then it makes sense to say $a \equiv b \pmod{n, h(x)}$ for polynomials a, b with integer coefficients (or coefficients in $\mathbb{Z}/n\mathbb{Z}$); it means that $a - b$ can be written as a multiple of $h(x)$ plus a multiple of n.

In case n is prime, and h is monic ($c_n = 1$) and irreducible mod n, then nicer things happen. In this case, the set R of equivalence classes of polynomials modulo n and $h(x)$ is what is called a *field* in abstract alebra. This means that not only can you add, subtract and multiply modulo n and $h(x)$, but you can also divide: for every polynomial P which is not congruent to zero modulo n and $h(x)$, there exists a polynomial Q such that $PQ \equiv 1 \pmod{n, h(x)}$.

For example, say $n = 3$ and $h(x) = x^2 + 1$. Then each element of R can be represented as $a + bx$, where a, b are elements of $\mathbb{Z}/3\mathbb{Z}$ and we multiply using the rule $x^2 = -1$. So what we have is a "mod 3" version of the complex numbers!

One nice property about fields is that polynomial equations over fields behave the way you expect. Namely, let $Q(y)$ be a monic polynomial whose coefficients are in R. (That is, the coefficients of Q are themselves polynomials in x.) Then the number of roots of $Q(y)$ in R is at most the degree of Q, just like over the real or complex numbers! And in fact, the same proof works: if r_1 is a root of Q, then Q factors as $(y - r_1)Q_1(y)$, where Q_1 has degree one less than that of Q. And so on: once we write down $d = \deg(Q)$ roots, then we must have

$$Q(y) = (y - r_1) \cdots (y - r_d).$$

We saw an example of this once before: if p is prime, then $\mathbb{Z}/p\mathbb{Z}$ is itself a field, obtained by taking $h(x) = x$, and there are at most two square roots of 1 in $\mathbb{Z}/p\mathbb{Z}$.

5 The Agrawal-Kayal-Saxena test

The basic idea of the AKS test is this: while it is possible to have a composite number n for which $a^{n-1} \equiv 1 \pmod{n}$ for most *integers* n, it is quite hard to have the relation

$$(x + 1)^n \equiv x^n + 1 \pmod{n}$$

between *polynomials*.

Theorem 5.1. *If the polynomial $(x+1)^n - x^n - 1$ has all coefficients divisible by n, then n is a prime power.*

As given, this is not a good primality test, because the polynomial $(x+1)^n - x^n - 1$ has n different coefficients to check, which is too many. Instead, we can check a consequence of this, which we write in the parlance of the previous section as

$$(x+1)^n \equiv x^n + 1 \pmod{n, x^r - 1}.$$

For $r = 1$, this is the Fermat test again, but for $r > 1$ this is a new criterion.

With that idea in mind, here is the AKS primality test.

1. Check whether $n^{1/k}$ is an integer for any of $k = 2, \ldots, \lfloor \log_2 n \rfloor$. If so, stop: n is composite.

2. Find the smallest prime r such that, for q the largest prime dividing $r-1$, we have

$$n^{(r-1)/q} \not\equiv 1 \pmod{r} \qquad \text{and} \qquad \binom{2q-1}{q} \geq n^{2\lfloor \sqrt{r} \rfloor}.$$

3. Check that n has no prime divisors less than or equal to r. If it does, stop; n is composite.

4. Check that $(x+b)^n \equiv x^n + b \pmod{n, x^r - 1}$ for $b = 1, \ldots, q$. If not, stop: n is composite.

5. Stop: n is prime.

I'm going to gloss over the subtlety of why r is not too large. A hard theorem in analytic number theory (due to Fouvry) shows we can take $r \leq c(\log n)^6$ for some constant c; in practice, it appears one can take $r \leq c(\log n)^2$.

Instead, I'll focus on why the test actually works; i.e., why it is that if we get to the end that we know for sure that n is prime. Note that there must be a prime divisor p of n such that $p^{(r-1)/q} \not\equiv 0, 1 \pmod{r}$, or else $n^{(r-1)/q}$ would be congruent to 0 or 1 mod r.

We first parlay the fact that $(x+b)^n \equiv x^n + b \pmod{p, x^r - 1}$ for $b = 1, \ldots, q$ into something slightly stronger. First replace x by x^{n^i}; we then get

$$(x^{n^i} + b)^n \equiv x^{n^{i+1}} + b \pmod{p, x^{n^i r} - 1}.$$

Since $x^{n^i r} - 1$ is divisible by $x^r - 1$, we also have this modulo p and $x^r - 1$. By induction, we then have

$$(x+b)^{n^i} \equiv x^{n^i} + b \pmod{p, x^r - 1}.$$

Since $P^p + Q^p \equiv (P+Q)^p \pmod{p}$ for any polynomials P, Q, we also have (using $b^{p^j} \equiv b \pmod{p}$ by Fermat's theorem)

$$(x+b)^{n^i p^j} \equiv x^{n^i p^j} + b \pmod{p, x^r - 1}.$$

If we run i, j from 0 to $\lfloor \sqrt{r} \rfloor$, we get $(1 + \lfloor r \rfloor)^2 > r$ products $n^i p^j$; by the pigeonhole principle, two of them are congruent modulo r. Call those $t = n^i p^j$ and $u = n^k p^l$, with $t \geq u$. Suppose that $t \neq u$. Then we know that

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

for $b = 1, \ldots, q$.

Now I need a fact from abstract algebra (or any sufficiently good number theory book): the polynomial $x^r - 1$ factors over $\mathbb{Z}/p\mathbb{Z}$ into irreducible polynomials, each of whose degree is the smallest integer d such that $p^d \equiv 1 \pmod{r}$. Let $h(x)$ be one such factor. In our case, since d must divide $r - 1$ (by Fermat's theorem), and $p^{(r-1)/q} \not\equiv 1 \pmod{r}$, d must be a multiple of q. All that I really need is $d \geq q$.

Define the field R as the set of equivalence classes modulo p and $h(x)$. Then the equation $y^{t-u} - 1$ has at most $t - u \leq n^{2\lfloor \sqrt{r} \rfloor}$ solutions. However, we can produce more solutions than that: for any nonnegative integers $e_1, \ldots, e_q$ with $\sum e_i \leq q - 1$, we can take

$$y = (x + 1)^{e_1} \cdots (x + q)^{e_q},$$

and these give $\binom{2q}{q-1}$ distinct elments of R, e.g. by "stars-and-bars" counting. (Why are these all distinct in R? The difference between two such products is a polynomial of degree $q - 1 < d$, so cannot be a multiple of h modulo p.) That contradicts the third fact above, so our assumption $t \neq u$ is incorrect.

So we now have $t = u$. Writing $t = n^i p^j$ and $u = n^k p^l$, we must then have $n^{i-k} = p^{l-j}$, so n is a power of p. We ruled out n being a perfect power in the first step, so n must be prime!

Slight downer: this is not (yet) practical, because even though it is a polynomial-time algorithm, the computations are still a bit on the largish side. Recent improvements by several experts in computational number theory have improved the situation, so a practical version may be coming soon.

6 Problems

1. Prove that 561 is a Carmichael number. (Hint: you can do better than Euler's theorem in this case. Consider the powers of a modulo each prime factor of 561 separately.)

2. Find another Carmichael number besides 561. (Hint: you might want to try numbers of the form $3pq$, with p and q prime.)

3. Prove Theorem 5.1. (Hint: look at the coefficient of x^{p^k} for p a prime factor of n such that p^k divides n but p^{k+1} does not.)

4. (Unsolved problem!) Is it true that if $(x + 1)^n \equiv x^n + 1 \pmod{n, x^r - 1}$ for r an odd prime, then either n is a prime power or $n^2 \equiv 1 \pmod{r}$? If so, then one can give a much more efficient version of the AKS test; large computer searches have failed to yield any counterexamples. Even the case $r = 3$ would be of interest.