PRIMALITY

MATH 195

Primality Testing

In cryptography, we need to generate large prime numbers. How can we test if a large number is prime?

If n is really prime, then by Fermat's little theorem, one has

$$\forall a \in (\mathbb{Z}/n\mathbb{Z})^*,\ a^{n-1} \equiv 1 \pmod{n}.$$

If this condition is not satisfied, then we can either be happy anyway or we stumble upon an $a \in (\mathbb{Z}/n\mathbb{Z})^*$ with $a^{n-1} \not\equiv 1 \pmod{n}$ and in that case we output "no". (If "no", we can prove that n cannot be prime.)

The resulting probabilistic primality test is called the *witness test* of Miller and Rabin [see also §7.4 in the text, the Miller-Rabin test].

Suppose that n is an odd prime, $a \in \mathbb{Z}$. Then $n \mid a^n - a$ (by Fermat's little theorem), so if we write $n-1 = 2^k u$ (where u is odd, $k \geq 1$), we have

$$\begin{aligned} n \mid a(a^{n-1}-1) &= a(a^{(n-1)/2}+1)(a^{(n-1)/2}-1) \\ &= a(a^{(n-1)/2}+1)(a^{(n-1)/4}+1)(a^{(n-1)/4}-1) \\ &= \cdots = a(a^u - 1)\prod_{\nu=0}^{k-1}(a^{2^i u}+1). \end{aligned}$$

So we have at least one of

$$\begin{aligned} a &\equiv 0 \pmod{n} \\ a^u &\equiv 1 \pmod{n} \\ a^{2^i u} &\equiv -1 \pmod{n} \end{aligned}$$

for some i with $0 \leq i < k$.

So now let n be any odd integer > 1 (not necessarily prime) and $n - 1 = 2^k u$ where u is odd. If a is an integer satisfying

$$\begin{aligned} a &\not\equiv 0 \pmod{n} \\ a^u &\not\equiv 1 \pmod{n} \\ a^{2^i u} &\not\equiv -1 \pmod{n} \end{aligned}$$

for any $0 \leq i < k$, then a is called a *witness to the compositeness of* n.

So, if a witness to the compositeness of n exists, n is really composite. Though you can be certain n is composite, you cannot extract a divisor (easily) from the proof or algorithm. We do have the following:

This is some of the material covered March 7, in Math 195: Cryptography, taught by Hendrik Lenstra, prepared by John Voight `jvoight@math.berkeley.edu`.

Theorem. *Let $n > 1$ be an odd integer. If n is prime, then no witnesses for n exist. If n is composite, then*

$$\frac{\#\{a : 1 \le a \le n-1, a \text{ a witness for } n\}}{n-1} \ge \frac{3}{4}.$$

Therefore, approximately 75% of congruence classes represent witnesses.

Example. Every one of the numbers $2, 3, 4, 5, 6, 7$ is a witness for $n = 9$, but neither 1 or 8 works. (Since $9 - 1 = 8 = 2^3$, $u = 1$, so the conditions are easily satisfied.)

We then have the following algorithm to probabilistically test for primality:

(1) Pick $a \in \{1, \ldots, n-1\}$ at random, and test whether a is a witness. If yes, output "yes".
(2) Otherwise, repeat. [Stop after a certain amount of time because probabilistically, n is likely tto be prime, but no mathematical proof.]

Large Primes

Now we can attend to the problem of finding a prime number with a given number of digits. For RSA, we need $n = pq$ with p and q both approximately 150-200 digits.

We have the following naive algorithm:

(1) Pick a random number with k digits.
(2) Test it for primality as above (using the witness test).
(3) Continue until the answer is "yes".

All algorithms you find will be a variation of this scheme.

Why does this algorithm work? In effect, how often are numbers of size 10^k prime? This question is answered by the prime number theorem (proved in 1896) by Hadamard (1865-1963) and de la Valle-Poussin (1866-1962).

Theorem (Prime number theorem)**.**

$$\frac{\#\{p \le x : p \text{ prime}\}}{x} \sim \frac{1}{\log x}$$

as $x \to \infty$.

This says that the limit of the left-hand side over the right-hand side tends to 1 as $x \to \infty$. "Roughly 1 out of every $\log x$ positive integers up to x is a prime number."

For example, with $k = 200$, $\log(10^{200}) \approx 460$, which means the probability that a 200 digit number is prime is $1/460$.

By restricting to odd numbers, the probability is twice as large, restricting to numbers not divisible by 3, it is $3/2$ times as large, and so on, so we can multiply the probability by

$$2 \cdot \frac{3}{2} \cdot \frac{5}{4} \cdot \cdots \cdot \frac{p}{p-1}$$

if we eliminate numbers divisible by primes up to p.

The prime number theorem is not easy to prove: D. Newman found an easier proof relying on complex analysis.