Primality testing:
variations on a theme of Lucas

Carl Pomerance, Dartmouth College
Hanover, New Hampshire, USA

In 1801, Carl Friedrich Gauss wrote:

"The problem of distinguishing prime numbers from composite numbers, and of resolving the latter into their prime factors, is known to be one of the most important and useful in arithmetic. It has engaged the industry and wisdom of ancient and modern geometers to such an extent that it would be superfluous to discuss the problem at length. Nevertheless we must confess that all methods that have been proposed thus far are either restricted to very special cases or are so laborious and difficult that even for numbers that do not exceed the limits of tables constructed by estimable men, they try the patience of even the practiced calculator. And these methods do not apply at all to larger numbers... Further, the dignity of science itself seems to require that every possible means be explored for the solution of a problem so elegant and so celebrated."

Two elementary theorems:

Wilson: *If p is prime, then* $(p-1)! \equiv -1 \pmod{p}$.

Fermat: *If p is prime and $p \nmid a$, then* $a^{p-1} \equiv 1 \pmod{p}$.

How efficient are these as primality criteria?
It would seem neither, since they both involve gigantic numbers when p is large.

For Fermat, the repeated squaring algorithm is quite efficient:

Use

$$a^k \bmod n = \begin{cases} \left(a^{k/2} \bmod n\right)^2 \bmod n, & \text{if } k \text{ is even,} \\ a\left(a^{(k-1)/2} \bmod n\right)^2 \bmod n, & \text{if } k \text{ is odd.} \end{cases}$$

Let's check out Fermat for $a = 2,\ p = 91$. We have

$$2^5 \equiv 32 \pmod{p},\ 2^{10} \equiv 23 \pmod{p},\ 2^{11} \equiv -45 \pmod{p}$$
$$2^{22} \equiv 23 \pmod{p},\ 2^{44} \equiv -17 \pmod{p},\ 2^{45} \equiv -34 \pmod{p}$$
$$2^{90} \equiv 64 \pmod{p}.$$

Huh?

So, we conclude that it is efficient to check Fermat, but the theorem is wrong!?

Actually, the theorem is correct, and the calculation *proves* that 91 is composite!

Not boring you with the calculation, but if we try it we find that

$$2^{340} \equiv 1 \pmod{341}.$$

What should be concluded?

Answer: 341 is prime

So, we conclude that it is efficient to check Fermat, but the theorem is wrong!?

Actually, the theorem is correct, and the calculation *proves* that 91 is composite!

Not boring you with the calculation, but if we try it we find that

$$2^{340} \equiv 1 \pmod{341}.$$

What should be concluded?

Answer: 341 is prime or composite.

In fact: $341 = 11 \times 31$.

So the converse of Fermat is false in general.
But note that the converse of Wilson is correct:
If $(n-1)! \equiv -1 \pmod{n}$, *then* n *is* 1 *or prime.*

Unfortunately, we know no fast way to check the Wilson congruence.

Returning to Fermat, it seems the converse is *almost* true.
Can we find some way to turn Fermat around and make it a primality-proving engine?

Lucas: *Suppose that* $n > 1$ *and* a *are integers with*

$$a^{n-1} \equiv 1 \pmod{n} \text{ and}$$
$$a^{(n-1)/q} \not\equiv 1 \pmod{n} \text{ for all primes } q \mid n-1.$$

Then n *is prime.*

Proof. Let h be the multiplicative order of a in the group $(\mathbb{Z}/n\mathbb{Z})^\times$. The first congruence implies that $h \mid n-1$. The second batch of congruences imply that h is not a proper divisor of $n-1$. Thus, $h = n-1$ and so $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times| \geq n-1$. We conclude that n is prime. □

This delightfully simple and elegant idea of Lucas has been the basis of essentially all of primality testing.

But first, why do we need to go further, isn't this the converse of Fermat that we were looking for?

Questions:

1. If n is prime, is there a number a satisfying the hypothesis?

2. If so, how do we find such a number a?

3. If we have a number a, how do we find the primes $q \mid n-1$ needed for the second batch of congruences?

1. If n is prime, is there a number a satisfying the hypothesis?

That is, must $(\mathbb{Z}/n\mathbb{Z})^\times$ be a cyclic group? Yes, by a theorem of Gauss.

2. If so, how do we find such a number a?

A sequential search starting with $a = 2$ is conjectured to succeed quickly, and this is provable assuming the GRH. The probabilistic algorithm of choosing random numbers a is very fast in practice and in theory. (The randomness involved is in finding the proof that n is prime; there should be no doubt in the conclusion.)

3. If we have a number a, how do we find the primes $q \mid n-1$ needed for the second batch of congruences?

3. If we have a number a, how do we find the primes $q \mid n-1$ needed for the second batch of congruences?

Aye, there's the rub.

3. If we have a number a, how do we find the primes $q \mid n-1$ needed for the second batch of congruences?

Aye, there's the rub.

Well, for some numbers n it is not so hard, say if $n = 2^{2^k}+1$.

Pepin: *If $k \geq 1$, then $n = 2^{2^k}+1$ is prime if and only if $3^{(n-1)/2} \equiv -1 \pmod{n}$.*

Proof. If the congruence holds, then Lucas implies n is prime. Say n is prime. Then $n \equiv 5 \pmod{12}$ so that Euler and Gauss imply that the congruence holds. □

The Lucas idea applied to elliptic curve groups:

For $p > 3$ prime and a, b integers with $4a^3 + 27b^2 \not\equiv 0 \pmod{p}$, consider the set of nonzero triples $(x : y : z)$ mod p with

$$y^2 z \equiv x^3 + axz^2 + bz^3 \pmod{p},$$

where the notation $(x : y : z)$ means that for $c \not\equiv 0 \pmod{p}$, we identify $(x : y : z)$ with $(cx : cy : cz)$. We can create a group structure on these triples, with the identity being $(0 : 1 : 0)$. (The group law involves some simple polynomial operations and comes from the geometric chord-tangent method for elliptic curves.)

Hasse, Schoof: *The order of the group is in the interval* $(p+1-2\sqrt{p}, p+1+2\sqrt{p})$*; it can be quickly computed.*

Say we have a number n that we think is prime, we choose a, b with $(4a^3 + 27b^2, n) = 1$, we compute the order h of the elliptic curve "group" (as if n were prime), we have the complete prime factorization of h, and we have a point P on the curve of order h, found as with Lucas. Then if $h \in (n+1-2\sqrt{n}, n+1+2\sqrt{n})$, then n is prime.

This is the basic idea behind ECPP (Elliptic Curve Primality Proving), due to Goldwasser & Kilian, Atkin, and Elkies, though you can see it is really just Lucas in another setting.

Note: The elliptic curve group need not be cyclic, but it often is, and almost always is nearly so. Many tweaks make this idea into a better algorithm.

Back to the original Fermat/Lucas setting:

Proth, Pocklington, Brillhart, Lehmer, & Selfridge: *Suppose* $n > 1$ *and* a *are integers,* $F \mid n-1$, $F > \sqrt{n}$,

$$a^F \equiv 1 \pmod{n} \text{ and}$$
$$(a^{F/q}-1,\, n) = 1 \text{ for all primes } q \mid F.$$

Then n *is prime.*

Proof. Let p denote the least prime factor of n. The hypotheses imply that a has order F in $(\mathbb{Z}/p\mathbb{Z})^\times$, so that $p > F$. But $F > \sqrt{n}$, so n has no prime factors below $\sqrt{n}$, which implies that n is prime. □

Note that if n is prime and g is a cyclic generator of $(\mathbb{Z}/n\mathbb{Z})^\times$, then $g^{(n-1)/F}$ has order F. So, finding an element a of order F as in the theorem is at least as easy as finding a cyclic generator of the group.

But now, we only have to factor part of $n-1$.

Lucas and later Lehmer also explored using the Fibonacci sequence, and more general Lucas sequences to test n for primality.

For example, if $p \equiv \pm 2 \pmod 5$, then $u_k \equiv 0 \pmod p$ whenever $p+1 \mid k$ (and u_k denotes the kth Fibonaccci number). This can be turned into a primality criterion for those numbers $n \equiv \pm 2 \pmod 5$ provided you have the prime factorization of $n+1$, or a large factored portion. For $n \not\equiv \pm 2 \pmod 5$ we can use other Lucas sequences.

The $620 problem

If n is an odd composite number and D is 1 mod 4, $|D|$ minimal with $(D/n) = -1$, must

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

or must the rank of appearance of n in the Lucas sequence with discriminant D not be a divisor of $n + 1$?

Prove this and earn $620 ($500 from me, $100 from Wagstaff, $20 from Selfridge).

The first counterexample found (with the prime factorization of n) also earns $620 ($500 from Selfridge, $100 from Wagstaff, and $20 from me).

Working with a Lucas sequence mod p, where the characteristic polynomial $f(x)$ is irreducible mod p, is akin to working in the finite field $\mathbb{F}_p[x]/(f(x))$ of order p^2.

And taking this view there is no reason to restrict f to degree 2.

Say we have a monic polynomial $f \in (\mathbb{Z}/n\mathbb{Z})[x]$ of degree k with

$$x^{n^k} \equiv x \pmod{f(x)}, \quad \gcd(x^{n^j} - x,\, f(x)) = 1 \quad \text{for} \quad 1 \le j \le k/2.$$

If n is prime, these conditions hold if and only if f is irreducible over $\mathbb{F}_n = \mathbb{Z}/n\mathbb{Z}$.

The finite fields test:

Lenstra: *Suppose* n, k, f *are as on the previous slide. Suppose too that* $F \mid n^k - 1$ *and* $F > \sqrt{n}$. *Say* $g \in (\mathbb{Z}/n\mathbb{Z})[x]$ *satisfies*

1. $g(x)^F \equiv 1 \pmod{f(x)}$,

2. $(g(x)^{F/q} - 1,\ f(x)) = 1$ *for each prime* $q \mid F$,

3. *each elementary symmetric polynomial in* $g(x)^{n^j}$ *for* $0 \le j \le k-1$ *is in* $\mathbb{Z}/n\mathbb{Z}$.

If none of the residues $n^j \bmod F$ *for* $0 \le j \le k-1$ *are proper factors of* n, *then* n *is prime.*

Proof. Let p be a prime factor of n. We'll write bars over objects to indicate they're taken mod p. Let $\bar{f}_1$ be an irreducible factor of $\bar{f}$ in $\mathbb{F}_p[x]$. The first two items in the theorem imply that $\alpha := \bar{g}$ has order F in the finite field $K = \mathbb{F}_p[x]/(\bar{f}_1(x))$. Consider the polynomial

$$h(t) = (t - \alpha)(t - \alpha^n) \dots (t - \alpha^{n^{k-1}})$$

in $K[t]$. The third item implies that $h(t) \in \mathbb{F}_p[t]$. Then $h(\alpha^p) = 0$, so that $\alpha^p = \alpha^{n^j}$ for some j, and so $p \equiv n^j \pmod{F}$. $\square$

Note that it is easier to find a large factored divisor of n^k-1 then it is of $n-1$. For example, if $k = 2$, then we automatically have $24 \mid n^2-1$ (assuming n is coprime to 6). If $k = 12$, we automatically have $2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13 \mid n^{12}-1$, and so on.

Adleman, P, & Rumely: *There is a value of* $k < (\log n)^{c \log\log\log n}$ *such that the least common multiple of the prime powers* q *with* $\varphi(q) \mid k$ *exceeds* $\sqrt{n}$.

In particular, the finite fields test of Lenstra can be made into a probabilistic algorithm with expected time of $(\log n)^{O(\log\log\log n)}$ to decide if n is prime.

The finite fields test contains essentially the Lucas–Lehmer test for Mersenne primes: *Suppose p is an odd prime and $n = 2^p - 1$. Then n is prime if and only if*

$$x^{(n+1)/2} \equiv -1 \pmod{x^2 - 4x + 1}$$

in $(\mathbb{Z}/n\mathbb{Z})[x]$.

Proof. We apply the finite fields test with $f(x) = x^2 - 4x + 1$, $g(x) = x$ and $F = n+1$. Suppose the congruence above holds. Then $g(x)^F \equiv 1 \pmod{f(x)}$ and $g(x)^{F/2} \equiv -1 \pmod{f(x)}$, so that $g(x)^{F/2} - 1$ is a unit mod $f(x)$. From $x^{n+1} \equiv 1 \pmod{f(x)}$ we have $g(x)g(x)^n \equiv 1 \pmod{f(x)}$, and from $x^{-1} \equiv 4 - x \pmod{f(x)}$, we have $g(x) + g(x)^n \equiv 4 \pmod{f(x)}$. Thus, the hypotheses hold and every prime factor of n is 1 or n mod n. Hence n is prime.

Now assume that $n = 2^p - 1$ is prime. Since $n \equiv 7 \pmod{24}$, we have $(\frac{2}{n}) = 1$, $(\frac{3}{n}) = -1$. In particular $f(x) = x^2 - 4x + 1$ is irreducible mod n. We compute $(x-1)^{n+1}$ in the finite field $K = \mathbb{F}_n[x]/(f(x))$ two ways. Using $(x-1)^2 = 2x$ and $x^n = 4 - x$,

$$(x-1)^{n+1} = \left((x-1)^2\right)^{(n+1)/2} = (2x)^{(n+1)/2} = 2x^{(n+1)/2},$$

$$(x-1)^{n+1} = (x-1)^n(x-1) = (x^n - 1)(x-1) = (3-x)(x-1) = -2.$$

Equating these two expressions we have the congruence in the theorem. $\square$

There are drawbacks with each of the tests considered so far:

The basic Lucas test needs a large factored divisor of $n-1$, and randomness is used to produce a proof.

The elliptic curve test uses randomness and it has not been rigorously proved to run in polynomial time.

The finite fields test uses randomness and it is not a polynomial time algorithm.

From a theoretical perspective what would be ideal is a determininistic, polynomial-time algorithm ...

Which brings us to the test of Agrawal, Kayal, & Saxena.

Agrawal, Kayal, & Saxena: *Suppose n, r are positive integers with $(n, r) = 1$ and the multiplicative order of $r \in \mathbb{Z}/n\mathbb{Z}$ exceeds $(\log_2 n)^2$. If, in $(\mathbb{Z}/n\mathbb{Z})[x]$,*

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

for each integer a in $[0, \sqrt{\varphi(r)} \log_2 n]$, then either n has a prime factor in this interval or n is a prime power.

Note: It is easy to show that a number r that has the requisite multiplicative order exists below $(\log_2 n)^5$. Using some fancy stuff, one can get r smaller.

Using Fast Fourier Transform techniques for integer arithmetic and polynomial arithmetic, it is possible to show that the running time of the AKS test is $O(r^{1.5}(\log n)^3)$ times some power of $\log\log n$.

Thus, since r can be bounded by a power of $\log n$, it follows that the test runs in polynomial time. And no randomness is needed.

Heuristically, there should be a value for r near $(\log n)^2$ leading to the complexity $(\log n)^6$, but the best that has been proved for r is a little lower than $(\log n)^3$, leading to $(\log n)^{7.5}$ for the complexity of the test.

Note that the AKS test uses the polynomial $x^r - 1$. Might we use other polynomials?

Lenstra & P: *Suppose* $f(x) \in (\mathbb{Z}/n\mathbb{Z})[x]$ *is a monic polynomial of degree* $d > (\log_2 n)^2$ *with*

$$f(x^n) \equiv 0 \pmod{f(x)},\ x^{n^d} \equiv x \pmod{f(x)},$$
$$(x^{n^{d/q}} - x, f(x)) = 1 \text{ for all primes } q \mid d.$$

If

$$(x+a)^n \equiv x^n + a \pmod{f(x)} \text{ for all } a \in [0, \sqrt{d}\log_2 n],$$

then either n *is divisible by a prime in this interval or* n *is a prime power.*

The proofs of this theorem and the AKS theorem both involve building up large groups using the given information. Sound familiar? Again it is the idea of Lucas.

One can show, with considerable effort, that there is a fast algorithm to produce a valid $f(x)$ for the theorem with degree $\leq 4(\log_2 n)^2$ (or prove n composite along the way). In fact, to be valid, it is sufficient that $f(x)$ is irreducible, but it is not an easy task to quickly, rigorously, and deterministically produce an irreducible polynomial over a finite field.

The proof uses the cyclotomic periods that Gauss used in his proof on the constructibility of regular n-gons. We have found it pleasing to use this signature result of Gauss to make progress on his call-to-arms of distinguishing prime numbers from composite numbers.

Further reading:

M. Agrawal, N. Kayal, and N. Saxena, *PRIMES is in P*, Ann. of Math. **160** (2004), 781–793.

R. Crandall and C. Pomerance, *Prime numbers: a computational perspective*, 2nd ed., Springer, New York, 2005.

A. Granville, *It is easy to determine if a given number is prime*, Bull. Amer. Math. Soc. **42** (2004), 3–38.

H. Williams, *Édouard Lucas and primality testing*, Canadian Math. Soc. Monographs **22**, Wiley, New York, 1998.