Primality testing: then and now

Trjitzinsky Memorial Lectures III,

University of Illinois Urbana–Champaign,

November 29, 2018

Carl Pomerance

Dartmouth College (emeritus)

University of Georgia (emeritus)

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

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

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

$$90 = 2 \cdot 45,\ 45 = 2 \cdot 22 + 1,\ 22 = 2 \cdot 11,\ 11 = 2 \cdot 5 + 1,$$

and $2^5 = 32$, so

$$2^{11} = 2^{2 \cdot 5 + 1} = 2 \cdot (2^5)^2 \equiv 46 \pmod{p},$$
$$2^{22} = (2^{11})^2 \equiv 23 \pmod{p},\ 2^{45} = 2 \cdot (2^{22})^2 \equiv 57 \pmod{p},$$
$$2^{90} = (2^{45})^2 \equiv 64 \pmod{p}.$$

Huh?

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

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

Actually, the theorem is correct, and the calculation that $2^{90} \not\equiv 1 \pmod{91}$ *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

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

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

Actually, the theorem is correct, and the calculation that $2^{90} \not\equiv 1 \pmod{91}$ *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 $|(\mathbb{Z}/n\mathbb{Z})^\times| \geq n-1$. 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?

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.*

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 $n = 2^m + 1$. Note: For this to be prime, a necessary condition is that $m = 2^k$ for some k.

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. Since $n \equiv 5 \pmod{12}$, Euler's criterion and Gauss's law of quadratic reciprocity imply that the congruence holds. □

What do we know about primes of the form $F_n := 2^{2^n} + 1$?

They are known as Fermat primes. Based on the fact that they are prime for $n = 0, 1, 2, 3, 4$, it seems he thought that they are always prime. However, **Euler** proved that $F_5 = 2^{2^5} + 1$ is composite, not by **Pepin**, but by finding a proper factor, namely 641.

Fermat probably could not have been more wrong about the numbers F_n being all prime, since for every $n > 4$ where we know the answer, it is composite! Most of these n's were determined by finding a factor.

The largest value of n where F_n has been tested for primality via **Pepin** is $n = 24$. But we know that every F_n is composite for $5 \leq n \leq 32$ and also for many larger values of n, see `http://www.prothsearch.com/fermat.html`.

Actually, the Fermat numbers F_n have played an important role in factoring. The continued fraction factoring algorithm cut its teeth on the case $n = 7$, the Pollard rho method on the case $n = 8$, the number field sieve on the case $n = 9$, and the elliptic curve method has been successfully used on many larger values of n. But this is a discussion for a different lecture!

A seminal paper on factoring dealt with the factorization of $2^{2^7}+1$:

M. Morrison & J. Brillhart, *A method of factoring and the factorization of* F_7, **Math. Comp.** **29** (1975), 183–205. Collection of articles dedicated to Derrick Henry Lehmer on the occasion of his seventieth birthday.

Before leaving the thin sequence of Fermat numbers, it is good to note their connection to a classical problem. **Gauss** proved in 1796 that if $n > 2$ is a power of 2 times a product of distinct Fermat primes, then there is a ruler and compass Euclidean construction of a regular n-gon. The numbers are:

$$3,\ 4,\ 5,\ 6,\ 8,\ 10,\ 12,\ 15,\ 16,\ 17,\ 20,\ 24,\ 30, \ldots .$$

He also claimed the converse holds, i.e., these are the only n where the regular n-gon is constructible, and **Wantzel** published a proof of this in 1837.

Another sequence of historical note are the Mersenne numbers $2^p - 1$, where p is prime. The only odd primes that are 1 more than a power of 2 are the Fermat primes, and the only primes that are 1 less than a power of 2 are the Mersenne primes.

But $2^p - 1$ with p prime is not always prime. It is for every prime p up to 20 except for $p = 11$. But then they drastically thin out. The largest Mersenne prime known is

$$2^{77,232,917} - 1,$$

a prime number with over 23 million decimal digits. It is the 50th and largest one found, but it might not be the 50th Mersenne prime since we have only searched exhaustively up to around exponent 50,000,000.

Just as the Lucas primality test works well for numbers n where we know the complete prime factorization of $n-1$, the Lucas–Lehmer test works well when we know the complete prime factorization of $n+1$.

The Lucas test builds up a subgroup in the unit group of the ring $R = \mathbb{Z}/n\mathbb{Z}$ that is so large that R is proved to be a field, and so n is prime.

The Lucas–Lehmer test builds up a large multiplicative subgroup of the unit group in the ring $R = (\mathbb{Z}/n\mathbb{Z})[x]/(f(x))$, where $f(x)$ is a quadratic polynomial in $(\mathbb{Z}/n\mathbb{Z})[x]$ that would be irreducible if n is prime. The test essentially shows that R is a finite field and n is prime.

In the case of Mersenne numbers, the test is particularly simple, the polynomial used is $f(x) = x^2 - 4x + 1$.

Some interesting papers on Mersenne primes:

D. B. Gillies, *Three new Mersenne primes and a statistical theory*, **Math. Comp.** **18** 1964 93–97.

C. Noll & L. Nickel, *The 25th and 26th Mersenne primes*, **Math. Comp.** **35** (1980), 1387–1390.

We have tried combining different tests. E.g., Carmichael numbers are composites for which the Fermat congruence holds for every coprime base, the first example being 561. After **Alford, Granville, & CP** we know there are infinitely many Carmichael numbers. There has been some controversy surrounding their distribution, see:

A. Granville & CP, *Two contradictory conjectures concerning Carmichael numbers*, **Math. Comp.** **71** (2002), 883–908.

There have also been thoughts about combining the Fermat test with the Lucas–Lehmer test. The following paper has a problem in this vein now worth \$620, though only \$30 was offered in the paper:

CP, J.L. Selfridge, & S.S. Wagstaff, Jr., *The pseudoprimes to* 25×10^9, **Math. Comp.** **35** (1980), 1003–1026.

Generalizing we could use the unit group in $(\mathbb{Z}/n\mathbb{Z})[x]/(f(x))$ where f has higher degree than 2, or we could use other families of groups.

For example, 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.*

R. Schoof, *Elliptic curves over finite fields and the computation of square roots mod* p, **Math. Comp.** **44** (1985), 483–494.

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), h is in the interval $(n+1-2\sqrt{n}, n+1+2\sqrt{n})$, we have the complete prime factorization of h, and we have a point P on the curve of order h, verified as with **Lucas**. Then n is prime.

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

Notes: If the order h is hard to factor, then we can switch out to a new elliptic curve group, a huge advantage. The elliptic curve group need not be cyclic, but it often is, and almost always is nearly so. Many tweaks make this into a better algorithm.

Every prime has an elliptic curve "certificate" that is about as speedy to verify as **Pepin** is for Fermat primes:

CP, *Very short primality proofs*, **Math. Comp.** **48** (1987), 315–322.

A seminal paper on practical elliptic curve primality proving:

A. O. L. Atkin & F. Morain, *Elliptic curves and primality proving*, **Math. Comp.** **61** (1993), 29–68.

Can this be made deterministic?

A. Abatzoglou, A. Silverberg, A. V. Sutherland, & A. A. Wong, *A framework for deterministic primality proving using elliptic curves with complex multiplication*, **Math. Comp.** **85** (2016), 1461–1483.

Before mentioning some modern developments on the theoretical side of proving primality, suppose you just wanted a quick and dirty "gut check" on whether some large number is prime.

The very simple Fermat congruence:

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

is a snap to check and usually doesn't lie. When the congruence fails for a pair a, p with $1 < a < p$, then p is definitely composite. And most pairs a, p where the congruence holds have p prime.

P. Erdős & CP, *On the number of false witnesses for a composite number*, **Math. Comp.** **46** (1986), 259–279.

S. H. Kim & CP, *The probability that a random probable prime is composite*, **Math. Comp.** **53** (1989), 721–741.

J. D. Lichtman & CP, *Improved error bounds for the Fermat primality test on random inputs*, **Math. Comp.** **87** (2018), 2871–2890.

In the latter paper it's shown, for example, that a random odd number of 200 bits that passes just one random Fermat test is composite with probability $< 10^{-4}$.

The "strong" Fermat test: If p is an odd prime with $p-1 = 2^j h$, with h odd, then for any a not divisible by p, either $a^h \equiv 1 \pmod{p}$ or $a^{2^i h} \equiv -1 \pmod{p}$ for some $i < j$.

After **Miller**, **Rabin**, **Damgård–Landrock–CP**, and **Burthe**, we now know that the probability of compositeness for a random odd p that passes k random applications of the strong test is $< 4^{-k}$. In fact, if the random number has 300 bits, the probability of just 1 random strong test lying is $< 1/4{,}000{,}000$, and with 600 bits, it's $< 1/(3 \times 10^{22})$.

I. Damgård, P. Landrock, & CP, *Average case error estimates for the strong probable prime test*, **Math. Comp.** **61** (1993), 177–194.

R. Burthe, *Further investigations with the strong probable prime test*, **Math. Comp.** **65** (1996), 373–381.

Let us return now to the idea where we build up a large subgroup of the unit group in the ring $(\mathbb{Z}/n\mathbb{Z})[x]/(f(x))$, where $f(x)$ is a polynomial.

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

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

If n is prime, these conditions hold if and only if f is irreducible over $\mathbb{F}_n = \mathbb{Z}/n\mathbb{Z}$. But the conditions can be easily checked for any n.

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*

- $g(x)^F \equiv 1 \pmod{f(x)}$,
- $(g(x)^{F/q} - 1,\ f(x)) = 1$ *for each prime* $q \mid F$,
- *the elementary symmetric polynomials of* $\{g(x), g(x)^n, \ldots, g(x)^{n^{k-1}}\}$ *are all in* $\mathbb{Z}/n\mathbb{Z}$.

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

Note that it can be much easier to find a large factored divisor of n^k-1 than of $n-1$, since factors can show up "for free". 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 $65{,}520 = 2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13 \mid n^{12}-1$, and so on.

Adleman, CP, & 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 run time of $(\log n)^{O(\log\log\log n)}$ to decide if n is prime.

The finite fields test, with expected run time $(\log n)^{c \log\log\log n}$, is a simplified version of a *deterministic* test with the same running time. This is the Jacobi sums test of **Adleman, CP, & Rumely**, which is actually computer practical. An early paper on its implementation:

H. Cohen & A. K. Lenstra, *Implementation of a new primality test*, **Math. Comp.** **48** (1987), 103–121, S1–S4.

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 and the Jacobi sums test do not run in polynomial time.

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.

Using Fast Fourier Transform techniques for integer 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.

THANK YOU