PRIMALITY TESTING: VARIATIONS ON A THEME OF LUCAS

CARL POMERANCE

Abstract. This survey traces an idea of Édouard Lucas that is a common element in various primality tests. These tests include those based on Fermat's little theorem, elliptic curves, Lucas sequences, and polynomials over finite fields, including the recent test of Agrawal, Kayal, and Saxena. The Lucas idea may be summed up as follows: build up a group so large that n must be prime.

1. Introduction

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."

In this call to arms, Gauss separates the problem of prime factorization into two problems: recognizing primes and factoring composites. This article discusses the first of these, the problem known as *primality testing*. In the following we take a historical perspective, but not necessarily in a normal historical progression: the order of topics is chosen for mathematical, not historical reasons. For pointers to more scholarly works, see the comments at the end of the article.

Let us begin our investigation.

2. 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 is, since they both involve gigantic numbers when p is large.

Supported in part by NSF grant 0703850.

For Fermat though, the repeated squaring algorithm is quite efficient. Use the recursion

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

Let's check out Fermat for $a = 2,\ p = 91$. Backing down from exponent 90, we get $90, 45, 44, 22, 11, 10, 5, \ldots$; well perhaps "5" is low enough to get started:

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

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

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

What should be concluded?

Answer: 341 is prime or composite.

It is good we mathematicians do not routinely reason from the converse; indeed $341 = 11 \times 31$.

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

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

Returning to Fermat, it seems the converse is *almost* true. That is, numbers such as 341, known as (base 2) *pseudoprimes*, appear numerically to be fairly rare. Can we find some way to turn Fermat around and make it a primality-proving engine? An answer was supplied in 1876.

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. (Here, φ denotes Euler's function.) □

This delightfully simple and elegant idea of Lucas has been the basis of essentially all of primality testing. The Lucas idea can be summed up as follows: *Build up a group that is so large that* n *is forced to be prime.*

But first, why do we need to go further, isn't this the converse of Fermat that we were looking for? Perhaps, but we would need to resolve the following questions:

(1) If n is prime, is there a number a satisfying the Lucas hypothesis?
(2) If so, how do we find such a number a?

[1] It can be seen even more easily that $2^{340} \equiv 1 \pmod{341}$ as follows. Note that $3 \times 341 = 1023 = 2^{10} - 1$, so that $2^{10} \equiv 1 \pmod{341}$, which upon taking the 34th power of both sides, yields the stated congruence.

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

For question 1, we are asking: if n is prime, must $(\mathbb{Z}/n\mathbb{Z})^\times$ be a cyclic group? Yes, by a theorem of Gauss. This is known in elementary number theory as the theorem on the primitive root.

For question 2, we are asking for an algorithm to find a primitive root. A sequential search starting with $a = 2$ is conjectured to succeed quickly, and this is provable assuming the Generalized Riemann Hypothesis (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.)

For question 3, we are asking how to find the complete prime factorization of $n-1$. To quote Shakespeare's Hamlet, "Aye, there's the rub."

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

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 3 is a quadratic nonresidue mod n. The congruence is then just Euler's criterion. □

3. 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 arithmetic operations and comes from the geometric chord-tangent method for elliptic curves.)

Hasse, Schoof: *The order of the group is in the interval*

$$(p + 1 - 2\sqrt{p},\ p + 1 + 2\sqrt{p});$$

this group order can be quickly computed.

Say we have a number n that we think is prime, we choose a, b with $\gcd(4a^3 + 27b^2, n) = 1$, 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. (If the order of the group is not in this interval, then n must be composite and P need not be found.)

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. The advantage is that while $n-1$ may be hard to factor, the number h may be easily factored. And if it isn't, another elliptic curve can provide a fresh chance.

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. For example, the factorization of h may include a very large prime factor, but is it really

prime? So, the method is iterated. As it stands, ECPP is the fastest algorithm in practice for "general" numbers.

4. Back to the original Fermat/Lucas setting

What if one only has a portion of $n-1$ factored? The Lucas result can be extended if this portion is large enough.

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

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

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 $n-1$.

Here are two families of numbers for which this method works well. They appear in a recent article of Denomme and Savin [5], where the authors found primality tests involving elliptic curves.

Example 1. Say $n_l = 2^{2^l} - 2^{2^{l-1}} + 1$, where l is a positive integer. For example, $n_1 = 3$, $n_2 = 13$, $n_3 = 241$, etc. Can we find a fully factored divisor F_l of $n_l - 1$ with $F_l > \sqrt{n_l}$? That's easy, take $F_l = 2^{2^{l-1}}$. Good, but can we easily find a candidate for the number a in the PPBLS result? Let us try $a_l = 7^{(n_l-1)/F_l} \bmod n_l$. Assume that $l \ge 2$, so that $n_l \equiv 1 \pmod 4$. Also note that $n_l \equiv 3 \pmod 7$ when l is odd and $n_l \equiv 6 \pmod 7$ when l is even. Thus, if $l \ge 2$ we have the Jacobi symbol $(\frac{7}{n_l}) = -1$. Let us prove: *for* $l \ge 2$, n_l *is prime if and only if*

$$7^{(n_l-1)/2} \equiv -1 \pmod{n_l}. \tag{1}$$

Indeed, if this congruence holds, then both

$$a_l^{F_l} \equiv 1 \pmod{n_l}, \quad \gcd(a_l^{F_l/2} - 1, n) = 1,$$

so that n_l is prime by PPBLS. Conversely, if n_l is prime, (1) holds by the Euler criterion for quadratic residues. □

Example 2. Let $m_l = 3^{2^l} - 3^{2^{l-1}} + 1$. Now we can take $F_l = 3^{2^{l-1}}$. And we have the following result of Gauss [6] from his collected works (thanks are due to Paul Pollack for the reference): *Let* p *be a prime that is* $1 \bmod 3$*, so that there are integers* L, M *unique up to sign with* $4p = L^2 + 27M^2$*. Then* 2 *is a cube* $\pmod p$ *if and only if* L *and* M *are both even.* Well,

$$4m_l = (3^{2^{l-1}} - 2)^2 + 27(3^{2^{l-1}-1})^2,$$

so that if m_l is a prime, then 2 is not a cube modm_l. Let $a = 2^{(m_l-1)/F_l} \bmod m_l$ in the PPBLS test, so that: *m_l is prime if and only if*

$$2^{m_l-1} \equiv 1 \pmod{m_l}, \quad \gcd(2^{(m_l-1)/3} - 1, m_l) = 1.$$

5. The Fibonacci numbers and the $620 problem

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 $u_{p+1} \equiv 0 \pmod p$, where u_k denotes the kth Fibonacci number. This can be turned into a primality criterion for 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.

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

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

or must the rank of appearance of n in the basic 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). In particular, you can earn $620 if you are the first to come up with a composite number n and its prime factorization such that $n \equiv \pm 2 \pmod 5$, the $(n+1)$st Fibonacci number is 0 $\pmod n$, and $2^{n-1} \equiv 1 \pmod n$.

6. Generalizing Lucas sequences: the finite fields test

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

$$x^{n^d} \equiv x \pmod{f(x)}, \quad \gcd(x^{n^{d/q}} - x,\, f(x)) = 1 \text{ for each prime } q \mid d. \tag{2}$$

If n is prime, these conditions hold if and only if f is irreducible over $\mathbb{F}_n = \mathbb{Z}/n\mathbb{Z}$. Thus, we have an easily checkable criterion that would allow us to create the finite field $\mathbb{F}_{n^d}$ if n were prime. This idea lies behind Lenstra's finite fields primality test.

Lenstra: *Suppose n, d are positive integers with $n > 1$ and $f \in (\mathbb{Z}/n\mathbb{Z})[x]$ monic of degree d. Suppose too that $F \mid n^d - 1$ and $F > \sqrt{n}$. Say $g \in (\mathbb{Z}/n\mathbb{Z})[x]$ satisfies*

1. *$g(x)^F \equiv 1 \pmod{f(x)}$,*
2. *$\gcd(g(x)^{F/q} - 1,\, f(x)) = 1$ for each prime $q \mid F$,*
3. *each elementary symmetric polynomial in $g(x)^{n^j}$ for $0 \le j \le d-1$ is in $\mathbb{Z}/n\mathbb{Z}$.*

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

Proof. Let p be the least 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 multiplicative order F in the finite field $K = \mathbb{F}_p[x]/(\bar{f}_1(x))$. Consider the polynomial

$$h(t) = (t-\alpha)(t-\alpha^n)\cdots(t-\alpha^{n^{d-1}})$$

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 $p \equiv n^j \pmod F$. If n is composite, then $p \le \sqrt{n} < F$, so $p = n^j \bmod F$. Thus, if no $n^j \bmod F$ is a proper factor of n, then n is prime. □

Suppose n is prime. If f satisfies (2) and g is an element in the finite field $(\mathbb{Z}/n\mathbb{Z})[x]/(f(x))$ of multiplicative order F, then all three items in the theorem hold.

Note that it can be easier to find a large factored divisor of n^d-1 then it is of $n-1$. For example, if $d = 2$, then we automatically have $24 \mid n^2-1$ (assuming n is coprime to 6). If $d = 12$, we automatically have $2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13$ dividing $n^{12}-1$, and so on. In fact, there is always a fairly small d yielding a large cheap factor.

Adleman, Pomerance, & Rumely: *There is a value of d with*

$$d < (\log n)^{c \log\log\log n}$$

such that the least common multiple of the prime powers q with $\varphi(q) \mid d$ exceeds $\sqrt{n}$. Here c is an absolute constant.

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. To be polynomial time, the runtime estimate should be $(\log n)^{O(1)}$. The finite fields test just misses![2]

7. Mersenne primes

The finite fields test contains the Lucas–Lehmer test for Mersenne primes.

Lucas & Lehmer: *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 $g(x)^F \equiv 1 \pmod{f(x)}$ we have $g(x)g(x)^n \equiv 1 \pmod{f(x)}$, and from $x^{-1} \equiv 4-x \pmod{f(x)}$, we have $g(x)+g(x)^n \equiv x + x^{-1}x^{n+1} \equiv x + x^{-1} \equiv 4 \pmod{f(x)}$. Thus, the two elementary symmetric polynomials in $g(x), g(x)^n$ are in $\mathbb{Z}/n\mathbb{Z}$. Since $n^0 \bmod F = 1$ and $n^1 \bmod F = n$ are not proper factors of n, we conclude that 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 $(x-1)^2 = 2x$,

[2]The joke I like to tell is that though it has been proved that $\log\log\log n$ goes to infinity with n, it has never been observed doing so.

$2^{(n-1)/2} = 1$, and $x^n = 4 - x$,

$$(x-1)^{n+1} = \big((x-1)^2\big)^{(n+1)/2} = (2x)^{(n+1)/2} = 2x^{(n+1)/2} \quad \text{and}$$
$$(x-1)^{n+1} = (x-1)^n(x-1) = (x^n-1)(x-1) = (3-x)(x-1) = -2.$$

Equating these two expressions, we have the congruence in the theorem. □

This does not look like the familiar Lucas–Lehmer test, which is as follows: *For p an odd prime, let $n = 2^p - 1$, and consider the sequence (ℓ_j), where $\ell_0 = 4$ and $\ell_{j+1} = \ell_j^2 - 2 \bmod n$. Then n is prime if and only if $\ell_{p-2} = 0$.*

However, it is easy to prove the equivalence: Let $R = (\mathbb{Z}/n\mathbb{Z})[x]/(x^2 - 4x + 1)$. In the ring R, $x(4-x) = 1$. Thus, $x^{(n+1)/2} = -1$ if and only if $x^{(n+1)/2-k} = -x^{-k} = -(4-x)^k$ for any integer k. Use this when $k = (n+1)/4$, so that $x^{(n+1)/2} = -1$ if and only if $x^{(n+1)/4} + (4-x)^{(n+1)/4} = 0$. Let $\ell_j = x^{2^j} + (4-x)^{2^j}$. One easily checks that $\ell_0 = 4$ and $\ell_{j+1} = \ell_j^2 - 2$, so this is the same sequence ℓ_j as in the traditional Lucas–Lehmer test. □

The reader might have noticed that the sequence

$$v_j = x^j + (4-x)^j$$

in the ring R is the Lucas sequence $4, 14, 52, \ldots \bmod n$ obeying the recurrence $v_{j+1} = 4v_j - v_{j-1}$. We have $\ell_j = v_{2^j}$.

8. Drawbacks

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

The basic Lucas test or the PPBLS test needs a large factored divisor of $n-1$, and randomness is often used to find a number a.

The elliptic curve test uses randomness and it has not been rigorously proved to run in expected 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 deterministic, polynomial time algorithm. It is interesting that the basic idea of Lucas settles this immediately if one is prepared to assume the GRH. If p is an odd prime, we not only have the Fermat congruence $a^{p-1} \equiv 1 \pmod p$ when $p \nmid a$, but it is also true that the only square roots of $1 \pmod p$ are ± 1. Putting these two thoughts together and writing $p - 1 = 2^s t$, where t is odd, we have that either $a^t \equiv 1 \pmod p$ or $a^{2^i t} \equiv -1 \pmod p$ for some $0 \le i \le s-1$.

Given an odd number $n > 1$ where $n - 1 = 2^s t$ with t odd, let G_n be the subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$ generated by those residues a such that either

$$a^t \equiv 1 \pmod n \quad \text{or} \quad a^{2^i t} \equiv -1 \pmod n \text{ for some } 0 \le i \le s-1. \tag{3}$$

It follows from a result of E. Bach and predecessors that assuming the GRH, the group $(\mathbb{Z}/n\mathbb{Z})^\times$ is generated by its members smaller than $3(\log n)^2$. Further, it basically follows from a result of M. Rabin that, unconditionally, if n is an odd composite, the group G_n is a proper subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$ (and has index at least 4 when $n > 9$). Thus, assuming the GRH, if $n > 1$ is odd, then n is prime if and only if (3) holds for all integers $1 \le a \le \min\{n-1, 3(\log n)^2\}$. In fact, this last assertion is true with coefficient 3 replaced with 2. The first to give a GRH-conditional test like this was G. Miller.

Again, the influence of Lucas is unmistakable: just build up a group that is too large for n to be composite.

But, we still have the drawback that this deterministic, polynomial time test requires the assumption of the GRH. This brings us to our final topic.

9. The AKS test

In 2002, for their senior thesis, N. Kayal and N. Saxena solved the problem with their advisor, M. Agrawal. Let $\log_2$ denote the base-2 logarithm.

Agrawal, Kayal, & Saxena: *Suppose n, r are coprime positive integers such that $n > 1$ and the multiplicative order of $r \pmod n \in (\mathbb{Z}/n\mathbb{Z})^\times$ 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.

It is not so hard to show via an elementary method that a number r that has the requisite multiplicative order exists below $(\log_2 n)^5$. Further, it is simple to check numerically if a number is a power of a smaller number or if a number has a small prime factor. Since the congruence in the theorem holds for all integers a when n is prime, the theorem can be turned into a deterministic, polynomial time algorithm to recognize primes. Finally, we have a resolution to the quest of Gauss!

Using Fast Fourier Transforms 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 constant power of $\log\log n$. Thus, with $r < (\log_2 n)^5$, the runtime is essentially bounded by $(\log n)^{10.5}$.

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.

The AKS test is based on the polynomials $x^r - 1$, where the condition on the multiplicative order of $r \pmod n$ guarantees when n is prime that $x^r - 1$ has an irreducible factor over $\mathbb{F}_n$ of large degree. Might we use other polynomials than $x^r - 1$? Indeed we can.

Lenstra & Pomerance: *Let $n > 1$ be an integer. Suppose $f(x) \in (\mathbb{Z}/n\mathbb{Z})[x]$ is a monic polynomial of degree $d > (\log_2 n)^2$ with $f(x^n) \equiv 0 \pmod{f(x)}$ and such that (2) holds. If*

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

for each integer $a \in [0, \sqrt{d}\log_2 n]$, 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 $\le 2(\log_2 n)^2$ (or prove n composite along the way). It thus follows that we have a deterministic algorithm to test n for primality that runs in about $(\log n)^6$ elementary operations.[3]

[3]As of yet, tests in the AKS family have not proven to be computer-practical. They are of interest as theorems in the field of algorithmic number theory.

Our difficulties with producing an $f(x)$ would be obviated if only one could quickly and deterministically produce an irreducible polynomial over a finite field of given degree. However, we know no such method, even for degree 2! Our 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.

10. The last word

This article leaves much unsaid—it would take a book to give a thorough synopsis of primality testing. For example, [2]. Further, the emphasis in this article has been on the simplicity and commonality of some of the basic ideas. For a more accurate historical treatment, see [3], [4] (thanks due to Hugh Williams for informing me of these), and [8]. For many more details on the AKS test, see not only the book [2], but the original paper of Agrawal, Kayal, and Saxena [1] and the survey paper of Granville [7]. Lenstra and I are still working on our improvement of the AKS test, though a proof of the theorem above can be found in [2] and [7]. Finally, [2] and the Internet have information about implementations and records.

References

[1] M. Agrawal, N. Kayal, and N. Saxena, PRIMES *is in* P, Ann. of Math. **160** (2004), 781–793.
[2] R. Crandall and C. Pomerance, *Prime numbers: a computational perspective*, 2nd ed., Springer, New York, 2005.
[3] A.-M. Decaillot, *L'arithméticien Édouard Lucas (1842–1891): théorie et instrumentation*, Rev. Histoire Math., **4** (1998), 191-236.
[4] A.-M. Decaillot, *Édouard Lucas (1842–1891); le parcours original d'un scientifique français dans the deuxième moitié du XIXe siècle*, Thèse de l'Université René Descartes–Paris V, Paris, 1999.
[5] R. Denomme and G. Savin, *Elliptic curve primality test for Fermat and related primes*, J. Number Theory **128** (2008), 2398–2412.
[6] C. F. Gauss, *Notizen über cubische und biquadratische Reste*, Werke. Band VII, Abt. I, Georg Olms Verlag, Hildensheim, 1973, Reprint of the 1906 original, pp. 5–14.
[7] A. Granville, *It is easy to determine if a given number is prime*, Bull. Amer. Math. Soc. **42** (2004), 3–38.
[8] H. C. Williams, *Édouard Lucas and primality testing*, Canadian Math. Soc. Monographs **22**, Wiley, New York, 1998.

AMS Classification Numbers: Primary 11-02, Secondary 11Y11

Dartmouth College, Hanover, NH 03755, USA
E-mail address: carl.pomerance@dartmouth.edu