PRIMALITY TESTING: VARIATIONS ON A THEME OF LUCAS

Carl Pomerance*

This lecture concerns the issue of deciding if a given number n is prime or composite. There exist very fast, probabilistic tests that recognize composite numbers; that is, they are expected to quickly arrive at the declaration that an input is composite if in fact it is composite. For example, consider the "strong probable prime test" of M. M. Artjuhov and J. L. Selfridge (independently). (This test is often referred to as the Miller-Rabin test.) Say n is an odd prime, written as $n = 1 + 2^s t$ with t odd. If $1 \le a \le n-1$, then either

$$a^t \equiv 1 \pmod{n} \ \text{ or } \ a^{2^j t} \equiv -1 \pmod{n} \ \text{ for some } j = 0, 1, \dots, s-1. \tag{1}$$

This theorem is an immediate corollary of Fermat's little theorem and the fact that ± 1 are the only square roots of 1 modulo an odd prime n. It is cheap to check if a pair a, n satisfies (1), and if it does, where $1 \le a \le n-1$, we say n is a strong probable prime to the base a. It is a theorem of M. Rabin that if n is an odd composite, then n is *not* a strong probable prime to the base a for at least $3/4$ of the values of a in $[1, n-1]$. So, a probabilistic test for n is to randomly choose numbers a in $[1, n-1]$ and see if (1) holds. If n is composite, then we should quickly discover this fact. If this test is given a prime number n, the test will not declare n composite, and after a while, one may become convinced that n is indeed a prime. But this negative experience with the test does not constitute a primaility proof. So, what remains to be considered is a test that can quickly come up with a proof that a given input number is prime, if indeed that number is prime.

Part of the landscape is the following conditional result of G. Miller, as improved by J. Oesterlé and E. Bach.

Theorem A. *On the Riemann Hypothesis for Dirichlet L-functions for quadratic characters, an odd number $n > 1$ is prime if and only if n is a strong probable prime to the base a for each integer a with* $1 < a < \min\{n, 2(\log n)^2\}$.

(As an incorrigible number theorist, I use "log" for the natural logarithm. It is trusted that computer scientists can readily make the translation to binary logarithms.) If χ is a Dirichlet character, the L-function associated to χ is $L(s,\chi) = \sum_{n=1}^{\infty} \chi(n)/n^s$. When χ is non-principal, it is easily seen that this defining series converges to an analytic function in the half plane $\operatorname{Re} s > 0$. In fact, $L(s,\chi)$ may be analytically extended to an entire function. The Riemann Hypothesis for $L(s,\chi)$ is the assertion that the only zeros of $L(s,\chi)$ in the right half plane lie on the line $\operatorname{Re} s = 1/2$. The connection to primality testing comes from results in analytic number theory that tie the distribution of the zeros of $L(s,\chi)$ to the least positive integer m with $\chi(m) \ne 1$.

Since it can be tested if n is a strong probable prime to the base a in $O(\log n)$ arithmetic operations with integers the size of n (when $1 < a < n$), Theorem A is the basis of an

* John Voight's careful notes of my lecture helped a great deal in the preparation of this manuscript. I also gratefully acknowledge the efforts of an anonymous referee whose thoughtful comments improved the presentation.

algorithm to decide if n is prime or composite that runs in $O((\log n)^3)$ arithmetic steps with integers the size of n. (The algorithm: test to see if (1) holds for each integer a in the interval in Theorem A.) The catch of course is that if n is declared prime, we only have the theorem that if the Riemann Hypothesis for Dirichlet L-functions for quadratic characters is true, then n is prime. To remove this last shred of doubt about n we look elsewhere.

The Lucas test

In 1876, Édouard Lucas proved the following theorem.
Theorem 1. *Suppose a, n are integers with $n > 1$ and suppose*

$$a^{n-1} \equiv 1 \pmod{n}, \quad a^{(n-1)/q} \not\equiv 1 \pmod{n} \text{ for all primes } q|n-1. \tag{2}$$

Then n is prime.[1]
The proof is very easy. Think of what (2) means for the order of the residue class $a \pmod{n}$ in the multiplicative group $(\mathbf{Z}/(n))^*$. This order must divide $n-1$, but it does not divide any $(n-1)/q$, so the order is exactly $n-1$. But Euler's theorem asserts that the order divides $\varphi(n)$. This then forces $n-1$ to be a divisor of $\varphi(n)$. If n is composite, we clearly have $\varphi(n) < n-1$ and so $n-1$ cannot be a divisor of $\varphi(n)$. Thus, n is prime.

Well this is just a great theorem, since the congruences in (2) may be rapidly checked via repeated squaring. So perhaps this is the end of the story, and we have a very short lecture? No such luck. There are a couple of problems surrounding the use of Theorem 1 as a primality test: (i) How do we find the number a?, (ii) How do we find the complete list of prime factors of $n-1$?

Problem (i) is perhaps not so insurmountable. If the number n is prime, then, as is well-known, there are primitive roots for n; these are numbers a which satisfy (2). In fact, among the numbers in the interval $[1, n]$, there are exactly $\varphi(n-1)$ primitive roots. It is not so hard to show, via some estimates in analytic number theory (see Exercise 4.1 in the Crandall-Pomerance book mentioned at the end), that

$$\varphi(n-1) > \frac{n}{2\log\log n} \quad \text{for} \quad n > 200\,560\,490\,131.$$

Thus, for large n, choosing a random number a in the interval $[1, n]$ will hit upon one with (2) holding with probability at least $1/(2\log\log n)$, and so within an expected number of $2\log\log n$ random choices, a successful candidate will be found. This probabilistic method, when successful, leaves no doubt at all that the number n is prime. This is in contrast to so-called "probabilistic primality tests," which as discussed at the start of the lecture, really only can prove that composites are composite. If your taste is more to deterministic algorithms, one can determine in polynomial time if n is prime or composite, along the general lines of Theorem 1, if one has the complete prime factorization of $n-1$. This is a result of M. R. Fellows and N. Koblitz, and also of S. Konyagin and me.

So then, how does one overcome problem (ii), obtaining the complete prime factorization of $n-1$? There's the rub; we have "reduced" the problem of proving primality to

[1] Lucas stated a somewhat weaker version of Theorem 1 in which the numbers $(n-1)/q$ are replaced by all of the proper divisors of $n-1$.

that of factoring. This is hardly a reduction at all, since we appear to be very far from a fast general factoring algorithm.

Though factoring is apparently hard in general, it is not universally hard. Thus, Theorem 1 is sometimes a great primality test. One particular class of examples for which Theorem 1 is essentially the end of the story is the sequence of Fermat numbers $F_k = 2^{2^k}+1$. Obviously, finding the complete list of prime factors of $F_k - 1$ is not a difficult challenge! By quadratic reciprocity one can easily see that the Jacobi symbol $\left(\frac{3}{F_k}\right)$ is -1 for $k \geq 1$, so that if F_k is prime, then 3 is a primitive root for F_k. Theorem 1 can then be simplified for the case of Fermat numbers as follows:

Corollary 1. *For $k \geq 1$, $F_k = 2^{2^k}+1$ is prime if and only if $3^{(F_k-1)/2} \equiv -1 \pmod{F_k}$.*

This result often goes by the name of Pepin's test, though in the original version, the number 5 was used in place of 3 (and it was assumed that $k \geq 2$).

One highly interesting feature of Theorem 1 is that it shows that every prime number has a short proof of primality. You might argue that what Theorem 1 does is reduce the primality of n to the primality of the prime factors of $n-1$, and you would be right. V. Pratt has shown though that there is no "combinatorial explosion," and that the total number of smaller cases for a prime input n is always less than $\log_2 n$, the binary logarithm of n. Thus, iterating Lucas's theorem shows that every prime number has a proof of its primality using at most $O((\log n)^2)$ arithmetic steps with positive integers at most n. This existence proof allows at least a little optimism that someday we might find a deterministic primality test that runs in polynomial time.

The $n-1$ test

Given that factoring is hard in general, and given that Theorem 1 is such a nice idea, people have tried to stretch this idea so that it can be used even when we have only a partial factorization of $n-1$. The following theorem of J. Brillhart, D. H. Lehmer, and J. L. Selfridge (following work of F. Proth and H. C. Pocklington) often goes by the name "$n-1$ test."

Theorem 2. *Suppose n, a, F are integers with $n > 1$, $F > \sqrt{n}$, $F | n-1$ and*

$$a^{n-1} \equiv 1 \pmod{n}, \quad \gcd(a^{(n-1)/q} - 1, n) = 1 \ \text{ for each prime } \ q|F. \tag{3}$$

Then n is prime.

To see why this theorem holds, let p be a prime factor of n. We see that (3) implies that the order of $a \pmod{p}$ in $(\mathbf{Z}/(p))^*$ is a multiple of F, and so $p > F$. Thus, n has the property that each of its prime factors exceeds its square root, a property that marks n as prime.

Theorem 2 can be strengthened somewhat, and in fact, S. Konyagin and I have shown that if one has a fully factored divisor of $n-1$ that exceeds n^ϵ, then one can decide in deterministic polynomial time if n is prime or composite. Here, ϵ is any fixed positive number, and the degree of the polynomial in the polynomial time assertion is allowed to depend on the choice of ϵ.

The $n+1$ test

But we are more intent here in generalizing Theorems 1 or 2 in another direction. The essence of these theorems is that when we work in the group $(\mathbf{Z}/(n))^*$ we are implicitly working in the factor groups $(\mathbf{Z}/(p))^*$ as p runs over the prime factors of n. If it is shown that some element of $(\mathbf{Z}/(n))^*$ has large order in each of these factor groups, then clearly each of these factor groups is large. If "large" means "exceeding $\sqrt{n}$," we conclude that $n = p$ is prime. What allows us to compute these orders is knowledge of the prime factorization, or a partial prime factorization, of $n-1$, the putative order of $(\mathbf{Z}/(n))^*$ if n is prime. And lack of this knowledge is a stumbling block for many numbers n.

So in seeking a generalization, we look to other groups which have other putative orders if n is prime. An example of such a group, also with 19th-century roots in the work of Lucas, is the subgroup of $\mathbf{F}_{n^2}^*$ of order $n+1$ (where $\mathbf{F}_q^*$ is the multiplicative group of the finite field of q elements).[2]

Suppose n is an odd prime. We construct the finite field $\mathbf{F}_{n^2}$ via a polynomial $f(x) = x^2 - bx + c$ where b, c are integers and $b^2 - 4c$, the discriminant of f, is a nonsquare modulo n, that is, the Legendre symbol $\big((b^2-4c)/n\big)$ is -1. This discriminant condition ensures that f is irreducible modulo n so that we have $\mathbf{F}_{n^2}$ realized as the quotient structure $\mathbf{F}_n[x]/(f(x))$. Algorithmically, we are just looking at elements $u + vx$ where $u, v \in \mathbf{F}_n$, and where we add and multiply polynomials as we always do, except that higher degree polynomials are reduced modulo $f(x)$.

Consider now the "Lucas sequence" in $\mathbf{F}_{n^2}$:

$$u_j = u_j(b,c) := \frac{x^j - (b-x)^j}{x - (b-x)} \quad \text{for} \quad j = 0, 1, \ldots. \tag{4}$$

Note that this sequence actually lives in the subfield $\mathbf{F}_n$; it begins as $0, 1$ and thereafter satisfies the linear recurrence

$$u_j = bu_{j-1} - cu_{j-2}. \tag{5}$$

These facts are perhaps easiest to see using the automorphism σ of $\mathbf{F}_{n^2}$ which sends an element to its n-th power. Under this automorphism, x gets sent to $b-x$ and vice versa, since both x and $b-x$ satisfy the polynomial f. Thus, u_j gets sent to itself by σ, and so must be in the fixed field of σ, namely $\mathbf{F}_n$. The recurrence (5) is seen to hold since the separate sequences $x^j, (b-x)^j$ satisfy the same recurrence (as $x, b-x$ are roots of f), so the linear combination u_j of these two sequences also satisfies the same recurrence.

If n is an odd integer that is not necessarily prime, we can still consider the Lucas sequence u_j defined via the recurrence (5). In this case, we consider b, c, u_j as residues modulo n. We can also use the formula (4) for u_j, but we must view it as working in the algebraic structure $\mathbf{Z}[x]/(n, f(x))$, which indicates that polynomials are reduced modulo $f(x)$ and coefficients are reduced modulo n. The formula (4) also can be seen to allow a speedy computation of the numbers u_j modulo n, via repeated squaring. The formula (4) can be used as well to develop direct algorithms that avoid polynomials for

[2] For n prime, $\mathbf{F}_{n^2}^*$ is cyclic of order n^2-1, so it has a unique subgroup of order $n+1$.

the Lucas sequence defined via (5). The algorithmic point is that it is not much harder to compute $u_j \pmod n$ than $a^j \pmod n$ for some residue $a \pmod n$.

The following theorem of M. Morrison is often referred to as the "$n+1$ test."

Theorem 3. *Suppose n is an odd integer greater than 1, and that b, c are integers with $\gcd(c,n) = 1$ and the Jacobi symbol $\left(\frac{b^2-4c}{n}\right) = -1$. Suppose too that F is an integer with $F > \sqrt{n}+1$, $F|n+1$ and*

$$u_{n+1} \equiv 0 \pmod n, \quad u_{(n+1)/q} \in (\mathbf{Z}/(n))^* \text{ for each prime } q|F. \tag{6}$$

Then n is prime.

To see this theorem, suppose p is a prime factor of n. First suppose that $\left(\frac{b^2-4c}{p}\right) = -1$. Then $f(x) = x^2 - bx + c$ is irreducible modulo p, and so $\mathbf{Z}[x]/(p, f(x))$ is isomorphic to the finite field $\mathbf{F}_{p^2}$. Since $x(b-x) = c$ in this field and since p does not divide c, we have that $x, b-x$ are nonzero elements in the field. Then (4) and (6) imply that the order of $x/(b-x)$ in the multiplicative group of the field is a divisor of $n+1$ and is itself divisible by F. But $x/(b-x)$ has order dividing $p+1$, since $x^{p+1} = x^p x = (b-x)x = (b-x)^{p+1}$. We conclude that $F|p+1$, so that $p \ge F-1 > \sqrt{n}$. Thus, every prime $p|n$ with $\left(\frac{b^2-4c}{p}\right) = -1$ exceeds $\sqrt{n}$. Now suppose that $p|n$ and $\left(\frac{b^2-4c}{p}\right) = 1$. Then $\mathbf{Z}[x]/(p, f(x))$ is isomorphic to $\mathbf{F}_p \times \mathbf{F}_p$, so that every unit has order dividing $p-1$. Thus, the order of $x/(b-x)$ divides $p-1$, but again (6) implies that this order is a multiple of F. So $F \le p-1$ and we again conclude that $p > \sqrt{n}$. Now, since $\left(\frac{b^2-4c}{n}\right) = -1$, every prime factor p of n has $\left(\frac{b^2-4c}{p}\right) = \pm 1$, so every prime factor of n exceeds $\sqrt{n}$. This can only happen if n itself is prime.

As with the $n-1$ test, if n is prime, it is not hard to come up with a polynomial $x^2 - bx + c$ that can prove n prime in the $n+1$ test. And, as with the $n-1$ test, the real constraint in the applicability of the $n+1$ test is the finding of a large fully factored divisor of $n+1$. One class of numbers n for which this is no problem at all is the Mersenne numbers $M_p = 2^p - 1$. A necessary condition for M_p to be prime is that p is prime, but this condition is not sufficient, as can be seen from the factorization $M_{11} = 2047 = 23 \times 89$, and from many other examples. The $n+1$ test especially adapted to Mersenne numbers is known as the Lucas-Lehmer test.

J. Brillhart, D. H. Lehmer, and J. L. Selfridge have shown how to combine Theorems 2 and 3 into one test, where all one needs to make it work is a large fully factored divisor F of $n^2 - 1$.

Theorem 4. *Suppose n is an odd integer greater than 1, and suppose that a, F_1 are integers with $F_1|n-1$ and (3) holds with F_1 in place of F. Suppose too that b, c, F_2 are integers with $F_2|n+1$, $\gcd(c,n) = 1$, the Jacobi symbol $\left(\frac{b^2-4c}{n}\right) = -1$, and (6) holds with F_2 in place of F. Let $F = \mathrm{lcm}[F_1, F_2]$. If $F > \sqrt{n}$ and the least positive residue of $n \pmod F$ is not a factor of n strictly between 1 and n, then n is prime.*

(Note that F is F_1F_2 or is 1/2 of this product.) To see the proof, let p be a prime factor of n. Note that the proof of Theorem 2 shows that $p \equiv 1 \pmod{F_1}$. Also, the proof of

Theorem 3 shows that $p \equiv \left(\frac{b^2-4c}{p}\right) \pmod{F_2}$. If $\left(\frac{b^2-4c}{p}\right) = 1$ then $p \equiv 1 \pmod F$, so that $p > \sqrt{n}$. If $\left(\frac{b^2-4c}{p}\right) = -1$, then we have $p \equiv n \pmod F$, since n satisfies the same two congruences we have derived for p. But the least positive residue of $n \pmod F$ is not a proper prime factor of n, so either $p = n$ or p is at least the next integer congruent to $n \pmod F$, that is $p > F$. Again $p > \sqrt{n}$. So n must be prime.

From work of H. C. Williams and collaborators, we can also prove primality rapidly with a large divisor of $n^4 - 1$. These combined tests lead us to think of possible generalizations.

The finite fields test

To prove n is prime, if we can make use of the finite fields $\mathbf{F}_n$ and $\mathbf{F}_{n^2}$, why not try for the general case $\mathbf{F}_{n^k}$? Assuming there is a way to do this, we should expect again some limitation of usefulness occurring because we do not have a large fully factored divisor of $n^k - 1$. However, note that if k is chosen judiciously, then we have "for free" certain prime factors of $n^k - 1$. For example, suppose that n has only prime factors above 61, and look at $n^{60} - 1$. Necessarily this huge number must be divisible by

$$2^4 \cdot 3^2 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 31 \cdot 61 = 6\,814\,407\,600,$$

and this is known even without looking for other prime factors, which can have an enhanced "chance" of working.[3] In fact, it was shown in connection with the Adleman-Pomerance-Rumely (APR) primality test that for each number n there is a number k with $k < (\log n)^{c \log\log\log n}$ (with c some computable and fairly reasonable constant) such that if

$$F = \prod_{p^j(p-1)|k} p, \quad \text{(where the product is over pairs } j, p \text{ with } j \geq 0 \text{ and } p \text{ prime)} \tag{7}$$

then $F > \sqrt{n}$. Note that if $\gcd(n, F) = 1$, then $F | n^k - 1$. Thus, if we can only do the algebra to make use of the finite field $\mathbf{F}_{n^k}$, we may end up with a fairly speedy primality test that works in general.

Shortly after the APR primality test came out, H. W. Lenstra, Jr. came up with just such a test. Suppose n is strongly suspected of being prime, with our goal to prove it prime if it is indeed so.

The first step is to find the smallest number k such that the number F defined in (7) exceeds $\sqrt{n}$. Since such a number k exists below $(\log n)^{c \log\log\log n}$, even a relatively stupid search for k will not take too long. Compute $\gcd(n, F)$. If $\gcd(n, F) > 1$, then we can easily find a prime factor of n, and the issue of the primality of n is settled. So assume $\gcd(n, F) = 1$. (If desired, it is possible to replace F with any of its divisors that exceeds $\sqrt{n}$.)

[3] For example, the prime 41 divides $n^{60} - 1$ for density $1/2$ of all primes n, and each of the primes $19, 37, 181$ divide for density $1/3$.

The next step is to find a monic, degree k polynomial $f(x)$ with coefficients modulo n that would be irreducible in $\mathbf{F}_n[x]$ if n were prime. A quick test for irreducibility is to compute

$$\gcd(f(x), x^{n^j} - x), \quad j = 1, 2, \ldots, \lfloor k/2 \rfloor; \tag{8}$$

if n is prime, then f is irreducible if and only if each of the gcd's in (8) is 1. Note that the Euclid gcd algorithm can readily break down if n is composite, since at some intermediate step we may be called on to divide by some polynomial with a non-invertible leading coefficient. However, this breakdown would not only prove that n is composite, but would factor n, which is not a bad outcome if our goal is to determine if n is prime or composite! Note too that the very first step in the Euclid chain to evaluate $\gcd(f(x), x^{n^j} - x)$ calls for dividing $f(x)$ into $x^{n^j} - x$ to get the remainder. This is a huge division problem, so instead one can use repeated squaring to compute $x^{n^j} \pmod{f(x)}$, and then subtract x. Also, this repeated squaring calculation may be saved to help with the next case of $j+1$. But where is $f(x)$ supposed to come from? In fact, if n is prime, about 1 out of every k polynomials of degree k will work, so a random search for f would be expected to succeed in about k trials.

So if n is prime, we have now "constructed" the finite field $\mathbf{F}_{n^k}$ via the polynomial $f(x)$, and we have a large divisor F of the order of the multiplicative group of the field. But, since we are not absolutely sure that n is prime, we will instead refer to the algebraic structure that would be our field if n were prime, namely $K = \mathbf{Z}[x]/(n, f(x))$. Our next step is to find an element of multiplicative order F in K. This task can again be accomplished via a random search that is expected to either succeed, or fail, but in the latter case, n will be proven composite. Indeed, take a random nonzero element $\alpha \in K$. (That is, take random residues $a_0, \ldots, a_{k-1}$ modulo n, not all zero, and let $\alpha = \sum a_i x^i$.) And then, via repeated squaring, find $\beta = \alpha^{(n^k-1)/F}$. If n is prime, then with reasonable probability, β has order F, and this can be easily tested. In fact, we test for a stronger property:

$$\beta^F = 1 \;\text{ and for each prime }\; q|F, \text{ the element } \beta^{F/q} - 1 \;\text{ is a unit in } K. \tag{9}$$

The parallel with (3) and (6) should be clear. To test if some element of K is a unit, well this is just showing that the gcd with $f(x)$, working always modulo n, is 1. If a nonzero non-unit is detected, or if the gcd procedure breaks down, we again have a proof that n is composite. So the test (9) is repeated for various random choices of α, until it is either successful, or until some choice is found with either $\beta^F \neq 1$ or a nonzero non-unit is found. In the latter cases n is declared composite, and the test stops.

So assume now that we have successfully found an element β of K satisfying (9). Our next step is to form the polynomial

$$g(t) = (t - \beta)(t - \beta^n)(t - \beta^{n^2}) \ldots (t - \beta^{n^{k-1}}) \;\in K[t]. \tag{10}$$

Note that if n is prime then the coefficients of g are in the subfield $\mathbf{F}_n$ of K, since g is invariant under the Frobenius automorphism σ, which takes an element of K and raises it to the n-th power. However, we are still not sure that n is prime. But we can test if the coefficients of g are in the subring $\mathbf{Z}/(n)$ of K. If not, then n can be declared composite.

Suppose that, despite various short circuits we have described that should throw out composite numbers n, somehow n has remained in play, yet is indeed composite. Let p be a prime factor of n. What do our calculations show? Let $\overline{f}(x)$ be the polynomial $f(x)$ with its coefficients reduced modulo p. It may be that $\overline{f}$ is reducible in $\mathbf{F}_p[x]$, so let f_1 be some irreducible factor, with degree k_1. With $\overline{\beta}$ being the element β reduced modulo p and modulo f_1 (that is, $\overline{\beta}$ is the homomorphic image of β under the natural projection $K \to \mathbf{F}_p[x]/(f_1(x)) = \mathbf{F}_{p^{k_1}}$), we have from (9) that $\overline{\beta}$ has order F in the multiplicative group of $\mathbf{F}_{p^{k_1}}$. Let $\overline{g}$ be g where we have replaced each β with $\overline{\beta}$. Thus, the coefficients of $\overline{g}$ lie in the prime field $\mathbf{F}_p$. Since $\overline{\beta}$ is a root of $\overline{g}$, it follows that $\overline{\beta}^p$ is a root as well. But we evidently know all of the roots of $\overline{g}$ in $\mathbf{F}_{p^{k_1}}$, so we must have

$$\overline{\beta}^p = \overline{\beta}^{n^j},$$

for some $j = 0, 1, \ldots, k-1$. But $\overline{\beta}$ has multiplicative order F, so that

$$p \equiv n^j \pmod{F},$$

for some $j = 0, 1, \ldots, k-1$. This is just great, because we can test this last condition. Namely, for each $j = 0, 1, \ldots, k-1$, compute the least non-negative residue of $n^j \pmod{F}$. If none of these numbers are divisors of n strictly between 1 and n, then any prime factor p of n must be greater than F. But $F > \sqrt{n}$ and we are done; n has only prime factors greater than its square root, so it must be prime.

So the last step in the finite fields test is to search over the least non-negative residues of $n^j \pmod{F}$ for divisors of n strictly between 1 and n. If one is found, then n is factored. If none are found, then n has been proved prime.

In summary, we have algorithmically described the following theorem.

Theorem 5. *Suppose n, k, F are positive integers with $n > 1$, $F | n^k - 1$, $F > \sqrt{n}$.*

1. *Suppose $f \in \mathbf{Z}[x]$ is monic of degree k and $x^{n^j} - x$ is a unit in $\mathbf{Z}[x]/(n, f(x))$ for $j = 1, \ldots, \lfloor k/2 \rfloor$.*
2. *Suppose $\beta \in \mathbf{Z}[x]/(n, f(x))$ is such that $\beta^F = 1$ and $\beta^{F/q} - 1$ is a unit for each prime factor q of F.*
3. *Suppose the elementary symmetric polynomials in $\beta, \beta^n, \ldots, \beta^{n^{k-1}}$ are in the subring $\mathbf{Z}/(n)$ of $\mathbf{Z}[x]/(n, f(x))$.*
4. *Suppose that none of the least positive residues of $n^j \pmod{F}$ for $j = 1, \ldots, k-1$ are factors of n strictly between 1 and n.*

Then n is prime.

The expected number of arithmetic steps in the finite fields test is some fixed power of k, and since k may be chosen of magnitude $(\log n)^{c \log\log\log n}$, the overall complexity is of the same shape, with a larger value of c. This test is "almost" polynomial time since $\log\log\log n$ drifts to infinity so very slowly. A joke I like to tell: while it has been proved that $\log\log\log n$ tends to infinity with n, it has never been observed doing so.

The asymptotic complexity of the finite fields test is attractively small, but it is not a practical primality test. Indeed it is overshadowed by variants that are quite practical, variants that have succeeded in proving the primality of some extraordinarily large numbers of several thousand digits. These modern primality provers include W. Bosma, M.-P. van der Hulst, and P. Mihailescu. Their algorithms start from the H. Cohen and H. W. Lenstra, Jr. version of the APR test. It is worth remarking that the APR test has a deterministic variant, with the same rough complexity of $(\log n)^{c \log\log\log n}$, and this still stands as the fastest known deterministic primality test. For probabilistic tests, though, we can do better.

Elliptic curve primality proving

Suppose $p > 3$ is prime, a, b are integers with $4a^3 + 27b^2 \not\equiv 0 \pmod p$, and $E_{a,b}$ is an elliptic curve over $\mathbf{F}_p$, defined by an equation

$$Y^2 = X^3 + aX + b.$$

The $\mathbf{F}_p$-rational points on $E_{a,b}$ are those pairs $(x, y) \in \mathbf{F}_p^2$ which satisfy the equation, plus the point O, the "point at infinity," corresponding to the projective point $(0 : 1 : 0)$ on the homogenized equation $Y^2Z = X^3 + aXZ^2 + bZ^3$. (Each projective point $(x : y : z)$ which satisfies the homogenized equation, except for $(0 : 1 : 0)$, corresponds to an affine point $(x/z, y/z)$ which satisfies the original equation.) Denote the set of $\mathbf{F}_p$-rational points on $E_{a,b}$ by $E_{a,b}(p)$. This set of points forms an abelian group with identity element O and with the group addition law coming from the property that if a line cuts the curve in 3 points, counting multiplicities, then the sum of the 3 points is O (and that any vertical line intersects the curve at O). This geometric view is inherited from the theory of elliptic curves over the field of reals. Analytic geometry comes equipped with equations which can continue to be used when working over other fields such as $\mathbf{F}_p$. Thus, we can write down explicit formulas for the addition law. The addition law falls into three cases depending on whether one of the points being added is O, we are adding two different affine points, or doubling an affine point, and each of the latter two itself has two cases depending on whether or not the sum is O:

$$O + P = P + O = P \quad \text{for all} \quad P \in E_{a,b}(p),$$

$$(x, y) + (x, -y) = O \ \text{for} \ \ (x, y) \in E_{a,b}(p),$$

and

$$(x_1, y_1) + (x_2, y_2) = (x_3, y_3) \ \ \text{for} \ \ (x_1, y_1), (x_2, y_2) \in E_{a,b}(p), \ \ (x_2, y_2) \neq (x_1, -y_1),$$

where

$$x_3 = m^2 - x_1 - x_2, \ \ y_3 = m(x_1 - x_3) - y_1$$

and

$$m = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, & \text{if } x_2 \neq x_1 \\ \dfrac{3x_1^2 + a}{2y_1}, & \text{if } x_2 = x_1. \end{cases}$$

We use the notation MP to denote repeated addition of P to itself M times. By using a repeated doubling addition chain, MP can be computed in $O(\log M)$ calls to our elliptic addition rules. An important message to take from these simple rules is that if n were a suspected prime, you could perform the addition rules by working modulo n, except that you might get into "trouble" with the inversion called for in the calculation of the "slope" m. However, this trouble would only reveal that n is composite after all, and in fact, would factor n.

The order of the group $E_{a,b}(p)$ depends on all three variables a, b, p, but the key variable is p, with a, b providing "fine tuning." To be more precise, we have

Theorem B. (Hasse's Theorem) *For integers a, b and prime $p > 3$ with $4a^3 + 27b^2$ not divisible by p, we have*

$$(\sqrt{p} - 1)^2 < \#E_{a,b}(p) < (\sqrt{p} + 1)^2.$$

Thus, Hasse's Theorem can be used as a primality test:

Theorem 6. *Suppose n is an integer with $n > 1$ and $\gcd(n, 6) = 1$ and that a, b are integers with $\gcd(4a^3 + 27b^2, n) = 1$. Let $P = (x, y)$, where x, y are residues modulo n that satisfy the congruence $y^2 \equiv x^3 + ax + b \pmod{n}$ and suppose F is an integer with $F > (n^{1/4} + 1)^2$. Following the rules for elliptic curve addition as if n were prime, suppose there is no breakdown and we have computed that*

$$FP = O, \quad (F/q)P \neq O \ \text{ for each prime } \ q|F. \tag{11}$$

Then n is prime.

For suppose p is a prime factor of n. It follows from (11) that in the group $E_{a,b}(p)$, the point $\overline{P}$ (with coordinates reduced modulo p) has order F. But then, by Hasse's Theorem,

$$F < (\sqrt{p} + 1)^2.$$

By our assumption on F, we thus have $n^{1/4} < \sqrt{p}$, so that each prime factor of n exceeds $n^{1/2}$. We conclude that $n = p$ is prime.

Theorem 6, which is due to S. Goldwasser and J. Kilian, is the natural generalization of the Lucas idea to the family of elliptic curve groups. To make it useful as a primality test, we will need some algorithmic way of coming up with the parameters a, b, F. Suppose n is prime. For a given a, b, the order of $E_{a,b}(n)$ is in the Hasse interval $\left((\sqrt{n} - 1)^2, (\sqrt{n} + 1)^2\right)$. A valid number F to be used in Theorem 6 is a fully factored divisor of this order that is sufficiently large, that is, $F > (n^{1/4} + 1)^2$. As with the $n - 1$ and $n + 1$ tests, we might expect that most of the time it will be hard to find F. But we have an extra degree of freedom now: the parameters a, b are up for grabs.

So here is a possible plan. Choose a, b at random, with $\gcd(4a^3 + 27b^2, n) = 1$. Determine the order of $E_{a,b}(n)$ and try to find a fully factored divisor F of the order with $F > (n^{1/4} + 1)^2$. Since factoring is hard in general, do not try too long on the factorization of the order, but rather give up if success does not come quickly, and try again with a new pair a, b. If success is at hand and a suitable triple a, b, F have been located, one needs to find a point P on $E_{a,b}(n)$ satisfying the conditions of Theorem 6. If n is prime and F is squarefree, it is not so hard to find such a point P via a random search. Indeed, the probability that a random point will have order in the elliptic curve group being a multiple of F is not too small, so a random search should be expected to find one, and once such a point is found, it is simple to produce a multiple of it whose order is exactly F. (If F is not squarefree, it is not guaranteed that a point of order F will exist in the elliptic curve group, but it is guaranteed that a subgroup of order F exists, and one can fashion a version of Theorem 6 that deals with non-cyclic subgroups. Or one can hold out for cases where a point P of order F exists.) Choosing random points in $E_{a,b}(n)$, when n is prime, is also easy. One chooses an integer x at random. With approximate probability $1/2$, the integer $x^3 + ax + b$ is a quadratic residue modulo n, and if it is, one can rapidly find a square root y modulo n via several random algorithms. Then (x, y) is a point on the curve.

To make such a scheme plausible, we would need a subroutine that determines the order of the elliptic curve group $E_{a,b}(n)$, when n is prime. In fact, we have such a subroutine, a deterministic method of R. Schoof that runs in polynomial time. This beautiful algorithm finds the order modulo various small primes, using the so-called division polynomials for elliptic addition, and then glues using the Chinese remainder theorem. So, assuming that group-order-finding is no problem, the problem comes down to assessing the chance of success in finding a large and fully factored divisor F of the order.

What kinds of numbers are easy to factor? Surely smooth numbers have this property.[4] But if we wish to spend only a brief time with factoring, the number would have to be very smooth indeed to be quickly factored. And such very smooth numbers are so sparsely distributed that a random method, that would have us hit on one by chance, would be expected to take a fairly long time before success. Are there any other numbers other than smooths that can be factored quickly? Again, we are not looking for some very sparse set of numbers, but rather a fairly thick set of numbers so that it will not be too rare an event to hit on one.

Prime numbers seem to fit the bill. They are not too rare, they are easy to recognize, and when recognized they are fully factored. The reader might detect some circularity here. After all, we are supposed to be discussing how to prove primality, and here we are saying that primality is easy to discover, so let us use primality as a subroutine in our primality test!

We have actually faced this problem before in Theorems 1–4. In the tests based on these theorems, we indeed reduced the problem of n's primality to that of the prime factors of F. If any of these prime factors were so large that they could not be proved prime quickly by trial division, we might be forced to iterate the method to prove those primes are prime before we could complete the proof that n is prime. But, you might protest, in Theorems 1–4 the prime factors of F are clearly smaller than n, so this iteration has an end in sight. If one takes a prime group order in Theorem 6, one will be reducing the primality of n to that of another prime of the same magnitude, maybe even n itself, which is hardly progress. Very well, you have me there! So instead of looking for a prime group order, say we look for a group order that is 2 times a prime. Since the group order is of magnitude n, if it is 2 times a prime, then that prime will be about $n/2$, and we can see that with a

[4] See my lecture "Smooth numbers and the quadratic sieve."

logarithmic number of iterations, we should complete the proof.

The probability that a random number near n is the double of a prime is about $1/(2\log n)$ by the prime number theorem. Thus, in an expected $O(\log n)$ random trials we should hit on a choice for a, b where the order of $E_{a,b}(n)$ is $2p$ for some prime p, and we can take $F = p$ or $2p$. The primality of n is reduced to the primality of p, we repeat the whole method with p, and so on.

This is a great plan, but a problem still remains. Do we know that as a, b vary over random choices, that the order of $E_{a,b}(n)$ is just as likely to be the double of a prime as a random number of the same magnitude?

We can ask a weaker question. Do we know that in the interval $\left((\sqrt{n}-1)^2, (\sqrt{n}+1)^2\right)$ there is even one number of the form $2p$ with p prime? Presumably so, and it is natural to conjecture that there are of order $\sqrt{n}/\log n$ such numbers in the interval. But can we *prove* that this is so? Unfortunately not, the tools of analytic number theory are just not strong enough at present to prove that there is even one double of a prime in the Hasse interval, much less that there are many doubles of primes.

In some sense, this lacuna is not a hindrance to the primality test. If in reality there are many doubles of primes in the Hasse interval, a random search should find one relatively soon, and in practice we will be on our way to proving that n is prime. However, as mathematicians, we are not only interested in proving that n is prime, we would like to prove the theorem that our algorithm is as good as we think it is.

Analytic number theory does have some relevant information for us. It can be used to show that for most primes n, not only does the Hasse interval $\left((\sqrt{n}-1)^2, (\sqrt{n}+1)^2\right)$ contain many numbers $2p$ with p prime, but so do the Hasse intervals for the primes p, and so on. That is, for most inputs n, the scheme we have outlined for primality testing is expected to conclude in polynomial time.

There is a second problem which was mentioned above. As a, b vary we know that the numbers $\#E_{a,b}(n)$ vary in the Hasse interval, but do they vary with the uniform distribution in this interval? Well no, they don't. But as has been shown by H. W. Lenstra, Jr., in connection with the elliptic curve factoring method, the distribution of the numbers $\#E_{a,b}(n)$ for fixed prime n and varying a, b, is very roughly uniform, at least for the middle half of the Hasse interval. And this estimate is good enough.

I have described here, in rough terms, the Goldwasser-Kilian primality test. It is a random algorithm that conjecturally is expected in polynomial time to prove a prime input n is indeed prime. And rigorously, it runs in expected polynomial time for most inputs.

Further developments

There are two further developments concerning primality proving with elliptic curves. By using Jacobian varieties of hyperelliptic curves of genus 2, Adleman and Huang have removed the theoretical lacuna that we discussed. That is, they have a random, polynomial-time primality test, that can be analyzed rigorously. Their idea is to use these Jacobian varieties in place of elliptic curves, at least at first. These behave similarly as in our discussion, but instead of the orders being about n, they are about n^2. And they look for orders that are themselves primes. This would seem crazy because why would you want to reduce the primality of n to another prime near n^2? Well what you lose in size, you can make up for in randomness. It is not a particular prime near n^2 that you reduce to, but rather a random prime near n^2. And this going up can be repeated a few more times, all the time gaining randomness. At that point, it is highly likely that you will be faced with a prime which is not in the possible exceptional set for the Goldwasser-Kilian algorithm, and you can proceed to go down as discussed. The reason the Adleman-Huang algorithm has a chance at rigorous analysis is due to the analog of the Hasse interval for the Jacobian varieties: it is $\left((\sqrt{n}-1)^4, (\sqrt{n}+1)^4\right)$. This interval is quite a bit longer in terms of its location on the number line than is the case for elliptic curves, and this added length is enough to have at hand some strong theorems in analytic number theory to prove the heuristics.

The other major development with the Goldwasser-Kilian method are techniques that make it computer practical. While the Schoof subroutine for determining curve order is beautiful, and runs in deterministic, polynomial time, it is not so very practical to be doing it repeatedly with very large primes. By using the theory of complex multiplication on elliptic curves, A. O. L. Atkin and F. Morain have come up with a method that first gives curve orders, and if it is a good order for us (namely we can quickly find a fully factored F as in Theorem 6), it is not so hard to find a corresponding elliptic curve. The method is heuristic since our stable of choices for the order is not so robust, but it seems to work very well in practice, with the largest numbers proved prime by the method having thousands of digits.

There is an important advantage of using elliptic curves to prove primality over the methods similar to the finite fields test. With the latter, at the end of a huge calculation, you have the answer, yes, n is prime. Well good, that is the point of the test. But you sort of knew the answer before starting, you just wanted verification, you wanted a proof. With elliptic curve primality proving, you not only get an answer, you get an actual chain of specific elliptic curves and points that can be very quickly used to re-prove primality by you or someone else. Thus, the extensive work to come up with the chain of elliptic curves has the very nice property that you gain more than a one-bit answer, you gain a proof that is much quicker to re-verify than it was to find in the first place. This primality certificate is an added value for elliptic curve primality proving and is one of its chief advantages.

For further reading and references to original papers and other surveys, see

E. Bach and J. Shallit, *Algorithmic number theory*, Volume I, MIT Press, 1996.

H. Cohen, *A course in computational algebraic number theory*, vol. 138 of Graduate Texts in Mathematics, Springer-Verlag, 1996.

R. Crandall and C. Pomerance, *Prime numbers: a computational perspective*, Springer-Verlag, New York, 2001.

H. C. Williams, *Édouard Lucas and primality testing*, vol. 22 of Canadian Mathematics Society Series of Monographs and Advanced Texts, John Wiley and Sons, 1998.

Addendum: The cyclotomic ring test of Agrawal, Kayal, and Saxena

Though this article is based on a lecture given at MSRI in August 2000, an exciting new development in August 2002 is described below. M. Agrawal, N. Kayal, and N. Saxena [1] have come up with a deterministic, polynomial-time primality test. The new test bears some similarities with the tests described above, especially Lenstra's finite fields test, and also Miller's GRH test. Unlike the GRH test, the new test is fully proved and does not depend on any unproved hypotheses. And unlike the finite fields test, the new test is determinisitic and runs in polynomial time.

We now describe the new test. The philosophy is that if n is prime, then modulo n, the polynomial $(x+a)^n$ is congruent to x^n+a. Actually, as Agrawal, Kayal, and Saxena point out, if this polynomial congruence holds for $a=1$, then the converse is true, that is, n must be prime. (The proof: if n is composite and q^k is a prime power appearing in the unique prime power factorization of n, then the coefficient of x^q in the binomial expansion of $(x+1)^n$ is $\binom{n}{q}$ which is clearly not divisible by q^k and so is not 0 modulo n.) However verifying the polynomial congruence is not a very efficient primality test, since there are n coefficients that supposedly must be worked out. The idea of Agrawal, Kayal, and Saxena is to instead verify that the polynomial congruence holds modulo x^r-1 for some number r that is bounded by a fixed power of $\log n$. This then is computationally tractable, but the problem remains if this is enough to conclude that n is prime given that various of these congruences hold. The following theorem provides the framework for such a conclusion. A key, and elementary algebraic fact used: If r is a positive integer not divisible by the prime p, then the splitting field of x^r-1 over the finite field $\mathbf{F}_p$ has degree equal to the multiplicative order of p in $(\mathbf{Z}/r\mathbf{Z})^*$.

Theorem A1. *Suppose n is a positive integer that is not a proper power. Suppose too that r is a prime not dividing n, that q is a prime factor of $r-1$ that exceeds $\ell := \lceil 3\sqrt{r}\log n\rceil$, and that*

$$n^{(r-1)/q} \not\equiv 1 \pmod{r}. \tag{A1}$$

Assume that for each integer a with $0 \le a < \ell$, we have

$$(x+a)^n \equiv x^n + a \pmod{x^r-1, n}. \tag{A2}$$

If n has no prime factors in $[1,\ell]$, then n is prime.

Proof. If every prime factor p of n satisfies $p^{(r-1)/q} \equiv 1 \pmod{r}$, then (A1) cannot hold. Thus n has a prime factor p with $p^{(r-1)/q} \not\equiv 1 \pmod{r}$, so that q divides the order, call it d, of p in the multiplicative group modulo r. Since $q|d$, we have in particular that $d > \ell$.

Let R denote the cyclotomic ring $\mathbf{F}_p[x]/(x^r-1)$, with R^* denoting the group of units in R. Then R is a direct sum of fields, one copy of $\mathbf{F}_p$ and $(r-1)/d$ copies of $\mathbf{F}_{p^d}$, while R^* is the direct sum of the multiplicative groups of these fields. For a positive integer m consider the homomorphisms ϕ_m, σ_m of R^* to itself, where

$$\phi_m(f(x)) = f(x)^m, \quad \sigma_m(f(x)) = f(x^m).$$

It is clear that ϕ_m is well defined (that is, it does not depend on the coset representative $f(x)$) and that it is a group homomorphism on R^*. It is less clear for σ_m, but it is nevertheless the case. One need only verify that $(x^m)^r - 1$ is divisible by x^r-1 in $\mathbf{F}_p[x]$.

Consider now the subgroup G of R^* generated by the monomials $x + a$ for $0 \le a < \ell$. (Since n is not divisible by any prime in $[1, \ell]$ it follows that $p > \ell$ so these monomials are indeed units in R.) Let

$$I = \{m \in \mathbf{N} \,:\, \phi_m(g(x)) = \sigma_m(g(x)) \text{ for all } g(x) \in G\}.$$

Note first that $p \in I$, this is really just Fermat's little theorem. Next note that $n \in I$. Indeed, by (A2) and since R is a homomorphic image of $\mathbf{Z}[x]/(x^r - 1, n)$, we have that $\phi_n(x + a) = \sigma_n(x + a)$ for each integer a, $0 \le a < \ell$. Since the polynomials $x + a$ generate G it follows that $n \in I$ as claimed. We also have that I is closed under multiplication. Indeed, if $m_1, m_2 \in I$, then for each $g(x)$ in G we have

$$\phi_{m_1 m_2}(g(x)) = g(x)^{m_1 m_2} = g(x^{m_1})^{m_2}.$$

But $g(x^{m_1})$ is in G, since it is equal to $g(x)^{m_1}$, which is clearly in G. Thus

$$g(x^{m_1})^{m_2} = g(x^{m_1 m_2}) = \sigma_{m_1 m_2}(g(x)),$$

and we conclude that $m_1 m_2 \in I$.

Take one of the copies of $\mathbf{F}_{p^d}$ that is part of the direct sum for R, and consider the projection from R to this field. This is realized as follows. Let $h(x)$ be an irreducible factor of $(x^r - 1)/(x - 1)$ in $\mathbf{F}_p[x]$, so that $h(x)$ has degree d. Then $K := \mathbf{F}_p[x]/(h(x))$ is isomorphic to $\mathbf{F}_{p^d}$ and is clearly a homomorphic image of R. The image of G under this projection is a subgroup G_0 of K^*. We can realize G_0 directly as the subgroup generated by the projections of the monomials $x + a$ for $0 \le a < \ell$. Since $p > \ell$ the monomials represent distinct members of G_0. Further, since the degree of $h(x)$ is d and $d > \ell$, the subset products of the ℓ monomials are all distinct members of G_0. We conclude that

$$\#G_0 \ge 2^\ell \ge 2^{3\sqrt{r}\log n} > n^{2\sqrt{r}}, \tag{A3}$$

since $2^3 > e^2$.

We finally note that if $m_1, m_2 \in I$ and $m_1 \equiv m_2 \pmod r$, then

$$m_1 \equiv m_2 \pmod{\#G_0}.$$

Indeed, for every $g(x) \in G$ we have

$$g(x)^{m_1} = g(x^{m_1}) = g(x^{m_2}) = g(x)^{m_2}, \tag{A4}$$

where the middle equality in (A4) holds since $x^r = 1$ in R and $m_1 \equiv m_2 \pmod r$. Thus (A4) implies that $m_1 \equiv m_2 \pmod E$, where E is the exponent of the group G (the maximal order of an element in G). But E is divisible by the exponent of the homomorphic image G_0 of G. And as G_0 is a subgroup of the multiplicative group of a field, it is cyclic, so its exponent is its order. It follows that $m_1 \equiv m_2 \pmod{\#G_0}$ as claimed.

It remains to consider the positive integers $n^i p^j$ where $0 \le i, j < \sqrt{r}$. There are more than r pairs i, j, so for two distinct pairs i_1, j_1 and i_2, j_2, we must have

$$n^{i_1} p^{j_1} \equiv n^{i_2} p^{j_2} \pmod{r}.$$

By the above comments, the integers $n^{i_1} p^{j_1}, n^{i_2} p^{j_2}$ are in I, so they must be congruent modulo $\#G_0$. But $n^{i_1} p^{j_1}, n^{i_2} p^{j_2} < n^{2\sqrt{r}} < \#G_0$ by (A3), so that we must have equality:

$$n^{i_1} p^{j_1} = n^{i_2} p^{j_2}.$$

The fundamental theorem of arithmetic then implies that n is a power of p. But since n is not a proper power, it must equal p. This completes the proof of Theorem A1.

Theorem A2. *There is an absolute positive constant c such that for any integer $n \ge 2$ there is a prime $r < c(\log n)^6$ and a prime $q | r - 1$ with $q > \lceil 3\sqrt{r} \log n \rceil$ such that* (A1) *holds.*

Proof. By Fouvry [3], there is an absolute positive constant c_0 such that for all $x \ge 11$, the number of primes $r < x$ with $r - 1$ divisible by a prime $q > r^{2/3}$ is at least $c_0 \pi(x)$, where $\pi(x)$ denotes the number of primes in the interval $[1, x]$. (The reason for taking $x \ge 11$ here is that the first prime r with this property is 11.) We apply this result with $x = c(\log n)^6$, where $c > 1000$ will be specified later. So, the number $N(n)$ of primes r with $1000(\log n)^6 < r \le c(\log n)^6$ and $r - 1$ has a prime factor $q > r^{2/3}$ satisfies

$$N(n) \ \ge \ c_0 \, \pi\left(c(\log n)^6\right) - \pi\left(1000(\log n)^6\right). \tag{A5}$$

There are positive numbers c_1, c_2 such that

$$c_1 y / \log y \le \pi(y) \le c_2 y / \log y \tag{A6}$$

for all large numbers y. The first to prove such a result is Chebyshev decades before the prime number theorem was proved. A more modern estimate in Rosser and Schoenfeld [5] is that (A6) holds for all $y \ge 114$ with $c_1 = 1, c_2 = 5/4$. Using this in (A5) we have that

$$N(n) \ \ge \ \frac{c_0 c (\log n)^6}{6 \log\log n + \log c} - \frac{1250 (\log n)^6}{6 \log\log n + \log 1000}. \tag{A7}$$

Note that since each prime r counted by $N(n)$ exceeds $1000(\log n)^6$ it follows that the largest prime q that divides $r - 1$, which is $> r^{2/3}$, is thus greater than $3\sqrt{r}\log n + 1$.

Now let $M(n)$ denote the number of distinct primes r such that for some integer j, $1 \le j < x^{1/3}$, we have $r | n^j - 1$. The number of primes r that divide a positive integer k is obviously at most $\log_2 k$ (since the worst case is when k is a power of 2 and then the total number of primes in the factorization of k is the base-two logarithm of k.) So using this result with k equal to $n^j - 1$, the number of primes that can divide $n^j - 1$ is at most $j \log_2 n$. Summing for $j < x^{1/3}$, we get that

$$M(n) \ \le \ x^{2/3} \log_2 n \ < \ 2 c^{2/3} (\log n)^5.$$

Hence by (A7), for c sufficiently large we have $N(n) > M(n)$ for all integers $n \geq 2$. Suppose r is counted by $N(n)$ and not by $M(n)$. Then we have $r-1 = bq$ where q is a prime larger than $r^{2/3}$, and so $b < x^{1/3}$. But since r is not counted by $M(n)$, the order of n in $(\mathbf{Z}/r\mathbf{Z})^*$ is at least $x^{1/3}$ and so cannot be a divisor of b. That is, (A1) holds. This completes the proof of Theorem A2.

It remains now to construct a primality test using Theorems A1 and A2. Note that if n is prime, then (A2) holds for any positive integer r and any integer a. The test then proceeds as follows. First one checks that n is not a proper power by using real arithmetic to compute approximations for $n^{1/2}, n^{1/3}$, etc. and checking if integers near to these approximations, when raised to the corresponding power give n. This need only be checked down to $n^{1/k}$ where $k = \lfloor \log_2 n \rfloor$. One next finds a prime r as guaranteed to exist in Theorem A2. If r is a factor of n, then n is declared composite, while if $r = n$, then n is declared prime (admittedly both of these possibilities are slim). One then checks if n has a prime factor in $[1, \ell]$ by trial division (where ℓ is as in Theorem A1), of course declaring n composite if a nontrivial factor is found. Finally one checks the congruence in (A2) for each value of a in $[0, \ell)$. (Of course we get $a = 0$ for free.) If any of these congruences should fail, n is declared composite. And if they all hold, then n is declared prime. By Theorem A1 such a final declaration of primality is valid.

As for the complexity of the new primality test, it is clear that the proper power testing and the trial division are negligible steps. The search for primes $r = O((\log n)^6)$ with $r-1$ divisible by a prime $q > 3\sqrt{r}\log n + 1$ can be achieved through a sieve taking $O((\log n)^{7+\epsilon})$ elementary operations. The verification of (A1) can be achieved in $O((\log n)^{1+\epsilon})$ elementary operations for any particular choice of r, so an upper bound on the work until a successful r is found is $O((\log n)^{7+\epsilon})$. The chief time bottleneck in the algorithm is the verification of the congruences in (A2). Here using Fast Fourier Transform methods for polynomial and integer arithmetic, one of the congruences in (A2) can be accomplished in $O(r(\log n)^{2+\epsilon})$ elementary operations, so the verification of all of them takes $O(r^{3/2}(\log n)^{3+\epsilon})$ elementary operations. Putting in the upper bound for r of $O((\log n)^6)$ we arrive at an upper bound of $O((\log n)^{12+\epsilon})$ elementary operations for the algorithm.

It is clear that we would have a more efficient algorithm with a smaller choice for r. It is conjectured that there are of order $y/(\log y)^2$ primes $r \leq y$ with $q = (r-1)/2$ prime. (Such a prime q is called a Sophie Germain prime.) Assuming this conjecture, the argument for Theorem A2 says that a successful r in the theorem will be found with $r = O((\log n)^2)$, leading to an overall complexity of $O((\log n)^{6+\epsilon})$. This estimate likely stands as the implementation complexity for the algorithm, but of course proof would depend on the stated conjecture concerning Sophie Germain primes. (And this assumes too that one is in a range where it is practical to use the Fast Fourier Transform methods.)

Towards the end of lowering the upper bound for r, there has been an improvement on the Fouvry theorem, by Baker and Harman [2]. They showed that a positive proportion of the primes r have a prime factor q in $r-1$ with $q > r^{0.676}$. Using this in the proof of Theorem 2, a successful prime r is guaranteed to be found satisfying $r = O((\log n)^{125/22})$, and using this estimate in the above complexity analysis leads to an upper bound of $O((\log n)^{507/44+\epsilon})$ for the algorithm. Note that $507/44 < 11.523$.

It is interesting that as it stands now, the constant c in Theorem A2 is not effectively computable, whether the Fouvry result or the Baker–Harman result is used. Indeed, the tools used to obtain these results include the Bombieri–Vinogradov prime number theorem (a rigorous estimate that can be thought of as achieving on average what can be achieved for individual terms assuming the Generalized Riemann Hypothesis). In turn, the Bombieri-Vinogradov theorem depends on Siegel's theorem which is unalterably ineffective (unless the Generalized Riemann Hypothesis is proved). However, there may be strategies around this minor lacuna.

One might think that there is an asymmetry in such an elegant and relatively simple algorithm using as a tool for its analysis a very hard theorem in analytic number theory. Perhaps, but it should be also pointed out that an earlier result of Goldfeld [4] is much simpler than that of Fouvry or Baker and Harman (though it also uses the Bombieri–Vinogradov theorem), and it achieves a positive proportion of primes r with $r-1$ divisible by a prime $q > r^{1/2+\delta}$, where $\delta > 0$ is fixed and small. This simpler result could be used to obtain a polynomial-time deterministic primality test, but with a worse time bound. Erdős often postulated that God has a book that contains the most elegant and tidy proofs of all interesting theorems which have such proofs. So we may actually be nearing a "book proof" that primality is in the complexity class P.

Acknowledgement. I would like to thank Hendrik Lenstra for helping me to overcome some difficulties in the above discussion.

References for the Addendum

[1] M. Agrawal, N. Kayal, and N. Saxena, *PRIMES is in P*, preprint, 2002, see `http://www.cse.iitk.ac.in/primality.pdf`.

[2] R. C. Baker and G. Harman, *The Brun-Titchmarsh theorem on average*, in Analytic number theory, Vol. 1 (Allerton Park, IL, 1995), 39–103, Progr. Math., 138, Birkhäuser Boston, Boston, MA, 1996.

[3] E. Fouvry, *Théorème de Brun–Titchmarsh; application au théorème de Fermat*, Invent. Math. **79** (1985), 383–407.

[4] M. Goldfeld, *On the number of primes p for which $p + a$ has a large prime factor*, Mathematika **16** (1969), 23–27.

[5] J. B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. **6** (1962), 64–94.