CWI Monograph 1

Mathematics and Computer Science

Proceedings of the CWI symposium
November 1983

edited by
J. W. de Bakker
M. Hazewinkel
J. K. Lenstra

1986

Primality Testing[1]

H.W. Lenstra, Jr.
University of Amsterdam
P.O. Box 19268, 1000 GG Amsterdam, The Netherlands

Two fundamental problems from elementary number theory are the following:

(*a*) *(primality)* given an integer $n>1$, how can one tell whether n is prime or composite?

(*b*) *(factorization)* if n is composite, how does one find $a, b>1$ such that $n=ab$?

Many mathematicians have been fascinated by these problems throughout history. Among these are Eratosthenes (~−284−~−204), Fibonacci (~1180−~1250), Fermat (1601-1665), Euler (1707-1783), Legendre (1752-1833) and Gauss (1777-1855). Some of the fascination of the subject derives from the fact that, roughly speaking, problem (*a*) is 'easy' and (*b*) is 'difficult'. Suppose, for example, that two 80-digit numbers p and q have been proved prime; this is easily within reach of the modern techniques for dealing with (*a*). Suppose further, that the cleaning lady gives p and q by mistake to the garbage collector, but that the product pq is saved. How to recover p and q? It must be felt as a defeat for mathematics that, in these circumstances, the most promising approaches are searching the garbage dump and applying mnemo-hypnotic techniques. The 'numerologists' occupying themselves with primality and factorization do not accept this defeat. They imagine all composite numbers to be created by multiplication on the zeroth day of Creation, and they make it their task to unravel the mysteries involved in this process. In this connection, it is remarkable that no clairvoyants have ever been employed to identify Mersenne primes or to factor large numbers. Such an attempt might lead to new insights, if not in numerology then in parapsychology.

[1] This paper is a revised version of one of the contributions to [19].

'Numerology' — this condescending term was, until recently, the fashionable one for the branch of science under discussion, in spite of the famous names listed above. Nowadays, a change in this attitude is noticeable. Partly, this change is due to an increased interest in general problems of feasibility of computations. The revival of the specific problems (a) and (b) has, in addition, been stimulated by their striking application in cryptography. For the details of this application we refer to [11]. Suffice it to say that, in this application, it is essential that (a) is 'easy' and that (b) is 'hard'. It is an ironic fact that the only existing evidence for the 'hardness' of (b) is the failure of generations of 'numerologists' to come up with an efficient factorization algorithm.

This lecture is devoted to a discussion of problem (a). For (b) we refer to [26] and [37], and the references given there.

In complexity theory, it is customary to call an algorithm *good* if its running time is bounded by a polynomial in the length of the input. For problems (a) and (b) the input is the number n, which can be specified by $[\log n/\log 2]+1$ binary digits. Thus the length of the input has the same order of magnitude as $\log n$.

A well known algorithm for solving (a) and (b) consists of trial divisions of n by the numbers less than or equal to $\sqrt{n}$. In the worst case, this takes $\sqrt{n}$ steps, which is exponential in the length of the input. We conclude that this algorithm is not 'good'.

Before one searches for a short proof that n is prime, or for a short proof that n is composite, it is a good question to ask whether such a proof exists. In this direction, we first have the following theorem; an *arithmetic operation* is the addition, subtraction or multiplication of two integers.

THEOREM 1. *If n is composite, this can be proved using only $O(1)$ arithmetic operations. Similarly if n is prime.*

PROOF. For composite n, the theorem is trivial; to prove that n is composite, it suffices to write down integers $a, b>1$ and to do the single multiplication necessary to verify that $ab=n$. Thus, in the composite case, the O-symbol is even superfluous. For prime n, the theorem is less obvious. It is an outgrowth of the negative solution of Hilbert's tenth problem [7], that there exists a polynomial in twenty-six variables

$$f\in\mathbf{Z}[\underline{A}, \underline{B}, \underline{C}, ..., \underline{X}, \underline{Y}, \underline{Z}]$$

with the property that the set of prime numbers coincides with the set of *positive* values assumed by f if non-negative integers are substituted for $\underline{A}, \underline{B}, ..., \underline{Z}$. Such a polynomial, of degree 25, is explicitly given in [12]. A similar polynomial in 10 variables of degree 11281 is constructed in [20; English translation]. To prove that a positive integer n is prime it now suffices to write down twenty-six non-negative integers $A, B, ..., Z$ and to do the bounded amount of arithmetic necessary to verify that $n=f(A, B, ..., Z)$. In fact, according to [12, Theorem 5] no more than 87 arithmetic operations are needed in this verification. This proves Theorem 1.

From a practical point of view Theorem 1 has two serious defects. The first is, that it tells us that certain proofs exist, but it does not tell us how to find them. Thus, F.N. Cole's proof that $2^{67}-1$ is composite consists of the single observation that

$$2^{67}-1 = 193707721\cdot 761838257287.$$

But it had taken him 'three years of Sundays' to find his proof, and the methods that he employed are far more interesting than the final proof itself [6], [28].

With primes, the situation is slightly different. The proof that, for prime n, there exist non-negative integers $A,\ B,\ ...,\ Z$ such that

$$n = f(A,B, ..., Z)$$

is completely constructive, see [12]. But for the polynomial from [12] it is not difficult to prove that the largest of $A,B, ..., Z$ necessarily exceeds

$$n^{n^{n^{n}}}$$

(For a much better polynomial in this respect, see [1, Theorem 3.5].) The second defect of Theorem 1 is, that it is clearly unrealistic to count an addition or multiplication of numbers of this size as a single operation. It is more realistic to count *bit* operations, which may be defined as arithmetic operations on numbers of one digit. Thus, we have:

THEOREM 2. *If n is composite, this can be proved using only $O((\log n)^2)$ bit operations.*

PROOF. It suffices to remark that the usual algorithm to multiply two numbers less than n requires no more than $O((\log n)^2)$ bit operations. This proves Theorem 2.

Using the fast multiplication routine of SCHÖNHAGE and STRASSEN [30], [35] we can replace $(\log n)^2$ in Theorem 2 by $(\log n)^{1+\epsilon}$, for any $\epsilon>0$, or more precisely by $O((\log n)\cdot(\log\log n)\cdot(\log\log\log n))$ (for $n>e^e$).

THEOREM 3 (PRATT [28]). *If n is prime, this can be proved using only $O((\log n)^4)$ bit operations.*

Again, using [30], we can replace $(\log n)^4$ by $(\log n)^{3+\epsilon}$, for any $\epsilon>0$.

PROOF. The proof relies on the structure of the group of units

$$(\mathbf{Z}/n\mathbf{Z})^* = \{(a \bmod n) : a\in\mathbf{Z},\ 0\leqslant a<n,\ \gcd(a, n)=1\}$$

of the ring $\mathbf{Z}/n\mathbf{Z}$ of integers modulo n. This is a finite abelian group of order $\phi(n)$, where ϕ is the Euler function. If n is a prime number, then $(\mathbf{Z}/n\mathbf{Z})^*$ is cyclic of order $n-1$. Conversely, if $(\mathbf{Z}/n\mathbf{Z})^*$ has order $\geqslant n-1$, then n is a prime number. Thus we see that n is prime if and only if there exists $(a \bmod n)\in(\mathbf{Z}/n\mathbf{Z})^*$ of order $n-1$. If we assume n to be odd and write

$$n-1 = \prod_{i=0}^{k} q_i, \tag{1}$$

$$q_0 = 2$$

$$q_i \text{ prime } (1\leqslant i\leqslant k) \tag{2}$$

then $(a \bmod n)$ has order $n-1$ in $(\mathbf{Z}/n\mathbf{Z})^*$ if and only if

$$a^{(n-1)/2} \equiv -1 \bmod n, \tag{3}$$

$$a^{(n-1)/q_i} \not\equiv 1 \bmod n, \quad \text{for} \quad 1\leqslant i\leqslant k. \tag{4}$$

Therefore, to prove that n is prime, we can write down integers a, $q_0=2$, $q_1, \ldots, q_k$, verify that (1), (3) and (4) hold, and prove (2) recursively. This proof requires k multiplications in (1), and $k+1$ exponentiations (mod n) in (3) and (4), plus what is needed for (2). So if $f(n)$ denotes the total number of multiplications and exponentiations in the proof, then

$$f(n)\leqslant k+k+1+\sum_{i=1}^{k} f(q_i)$$

where we define $f(2)=1$. By induction we prove that $f(n)\leqslant 3\cdot(\log n/\log 2)-2$. This is true for $n=2$, and if it holds for the q_i then

$$\begin{aligned} f(n) &\leqslant 2k+1+\sum_{i=1}^{k}(3(\log q_i/\log 2)-2) \\ &= (\sum_{i=0}^{k} 3(\log q_i/\log 2))-2 \\ &= 3(\log(n-1)/\log 2)-2 < 3(\log n/\log 2)-2 \end{aligned}$$

as required.

We conclude that no more that $O(\log n)$ multiplications and exponentiations are needed. Each exponentiation in (3), (4) can be done by $O(\log n)$ squarings and multiplications mod n. Finally, each of these multiplications, squarings and multiplications mod n (or mod a number smaller than n) can be done with $O((\log n)^2)$ bit operations. The total number of bit operations is therefore $O((\log n)\cdot(\log n)\cdot(\log n)^2)=O((\log n)^4)$. This proves Theorem 3.

Theorem 2 and 3 still have the first defect of Theorem 1: one is not told how to *find* the short proof whose existence is asserted. Nevertheless, the proof we have given of Theorem 3 is not exclusively of theoretical interest, and the same ideas are actually used in computer-assisted primality proofs. To illustrate this, we begin with a particularly simple case, in which $n-1$ has no odd prime factors at all.

THEOREM 4 (PÉPIN, 1877). *Let $n=2^m+1$, with $m>1$. Then n is prime $\Leftrightarrow$ $3^{(n-1)/2} \equiv -1 \bmod n$.*

PROOF. The implication $\Leftarrow$ follows from the proof of Theorem 3, with $a=3$. Conversely, suppose that n is prime. Then n is not divisible by 3, since $n>3$, so m is even. Then $n\equiv 2 \bmod 3$ and $n\equiv 1 \bmod 4$, so quadratic reciprocity gives

$$\left(\frac{3}{n}\right) = \left(\frac{n}{3}\right) = \left(\frac{2}{3}\right) = -1.$$

By Euler's theorem, $\left(\frac{3}{n}\right) \equiv 3^{(n-1)/2} \bmod n$. This proves Theorem 4.

It is known that $n=2^m+1$ can only be prime if n is a power of 2; then n is one of the *Fermat numbers* $2^{2^k}+1$. For $k=0, 1, 2, 3, 4$ these numbers are actually prime, for $5\leqslant k\leqslant 19$ and some other values (such as $k=2089$) they are known to be composite. It is reasonable to conjecture that they are, in fact, all composite for $k\geqslant 5$. The number F_{14} has been proved composite by Pépin's test, but no factor is known. To the uninitiated reader it may seem surprising that it is possible to prove that a number is composite, without the proof yielding a factorization. This is surprising indeed; the phenomenon will be further discussed at the end of this lecture. See [39, Sec. 5] and [3] for more information on the Fermat numbers.

For general n, the main difficulty of the above test is to find the complete factorization (1) of $n-1$. In the following variant only a partial factorization of $n-1$ is needed.

THEOREM 5. *Let n and s be integers satisfying*

$$n>1, \quad s>n^{1/2}.$$

Suppose that for every prime q dividing s there exists an integer a (depending on q) satisfying

$$a^{q^{m(q)}} \equiv 1 \bmod n, \quad \gcd(a^{q^{m(q)-1}}-1, n)=1 \tag{5}$$

where $m(q)$ denotes the number of factors q in s. Then n is a prime number.

PROOF. Let r be any prime dividing n and q any prime dividing s. From (5) we see that the order of $(a \bmod r)$ in the group $(\mathbf{Z}/r\mathbf{Z})^*$ equals $q^{m(q)}$, so by Lagrange's theorem $q^{m(q)}$ divides $r-1$. Since q is arbitrary, this implies that s divides $r-1$, so $r>s$. The inequality $s>n^{1/2}$ shows that n has at most one such prime factor. Hence n is prime, as required. This proves Theorem 5.

From the proof of Theorem 5 we see that the hypotheses imply that s divides $n-1$. To obtain a primality test from Theorem 5, one chooses s to be the largest divisor of $n-1$ that one is able to factor completely. For each q, the number a is constructed as follows. Search for an integer b such that

$$b^{n-1} \equiv 1 \bmod n, \quad b^{(n-1)/q} \not\equiv 1 \bmod n,$$

and put

$$a \equiv b^{(n-1)/q^{m(q)}} \bmod n.$$

If it is difficult to find such a number b, it is unlikely that n is prime, and one should attempt to show that n is composite, using Miller's method described below. The gcd in (5) is now equal to $\gcd(b^{(n-1)/q}-1, n)$, and it can be calculated efficiently using Euclid's algorithm. In fact, only one gcd-computation is necessary if one considers the product of the numbers $b^{(n-1)/q}-1 \bmod n$, with q ranging over the primes dividing s.

The critical condition of Theorem 5 is the inequality $s>n^{½}$ that must be satisfied by the completely factored part of $n-1$. There are several ways to replace this condition by a weaker one. Suppose, for example, that s only satisfies

$$s>n^{1/3}.$$

From the proof of Theorem 5 we see that every prime divisor of n is $1 \bmod s$, and the same is then true for *every* divisor. Hence, if n is composite, there exist integers x and y satisfying

$$n = (xs+1)(ys+1), \quad x>0, \quad y>0.$$

From $n<s^3$ it follows that $xy<s$, so $(x-1)(y-1)\geqslant 0$ implies that $0<x+y\leqslant s$. Since $x+y\equiv(n-1)/s \bmod s$ this means that we know the value of $x+y$. We also know that $n=(xs+1)(ys+1)$, so x and y can now be solved from a quadratic equation. Hence, if we add the hypothesis that the solution of this equation does not give rise to a non-trivial factorization of n, we still can conclude that n is a prime number.

A second method to relieve the condition $s>n^{½}$ makes use of lower bounds for the unknown prime factors of $n-1$. For a discussion of this technique, and references to the literature, see [39, Sections 10, 11].

Later in this lecture we shall consider a third type of generalization of Theorem 5, in which the role of $n-1$ is played by n^t-1, where t is some positive integer; see Theorem 11.

G.L. Miller [21] introduced a different way to exploit the multiplicative structure of the integers $\bmod n$ in primality tests. It leads to the following theorem, in which 'GRH' denotes the generalized Riemann hypothesis, formulated in the course of the proof.

Theorem 6 (Miller). *Assume the validity of GRH. Then there exists an algorithm, described below, that in $O((\log n)^5)$ steps decides whether or not n is prime.*

This theorem has none of the defects of Theorem 1, 2 and 3, but it has a new one: the assumption of an unproved hypothesis.

Assume that n is odd, and write $n-1=u\cdot 2^k$, where u is odd and $k\geqslant 1$. Employing Rabin's terminology [29], we call an integer a a *witness* to the compositeness of n, or simply a witness for n, if the following three conditions hold:

$$n \text{ does not divide } a, \tag{6}$$

$$a^u \not\equiv 1 \bmod n, \tag{7}$$

$$a^{u\cdot 2^i} \not\equiv -1 \bmod n \text{ for } i=0, \ldots, k-1. \tag{8}$$

(Others say in this situation, that n is 'not a strong base a pseudoprime' ... .)

Whether or not a is a witness for n depends only on $a \bmod n$; so we may restrict to $0\leqslant a<n$. For a given such a, it takes only $O((\log n)^3)$ steps to check whether or not a is a witness for n, by the last paragraph of the proof of Theorem 3.

We note that witnesses are reliable: if a is a witness to the compositeness of n, then n is composite. To see this, suppose that (6), (7), (8) hold and that n is prime. By (6) and Fermat's theorem, $a^{u\cdot 2^k}=a^{n-1}\equiv 1 \bmod n$. Hence the last term in the sequence

$$a^u, a^{u\cdot 2}, \ldots, a^{u\cdot 2^k}$$

is $1 \bmod n$, but by (7) the first term is not $1 \bmod n$. Let $b=a^{u\cdot 2^i}$ be the last term in the sequence that is not $1 \bmod n$. Then $0\leqslant i\leqslant k-1$, and $b^2\equiv 1 \bmod n$ while $b\not\equiv 1 \bmod n$. Hence n divides $b^2-1=(b-1)(b+1)$ but it does not divide $b-1$. Therefore n divides $b+1$, which contradicts (8).

The algorithm referred to in Theorem 6 now runs as follows. We may assume that n is odd, and $n>1$. Check whether there is a witness a for n satisfying $0<a<70(\log n)^2$. If there is one, n is composite. If there is none, declare n to be prime. This algorithm clearly runs in time $O((\log n)^5)$.

To prove the correctness of the algorithm, we have to show that any composite odd n has a positive witness $a<70(\log n)^2$, if GRH is assumed. We sketch this proof only, referring to the literature for details.

First we describe the GRH as we need it. Let n be an arbitrary positive integer, and let $\chi:(\mathbf{Z}/n\mathbf{Z})^*\to\mathbf{C}^*$ (the group of non-zero complex numbers) be a group homomorphism. We view χ as a function on $\mathbf{Z}$ by $\chi(a)=\chi(a \bmod n)$ if $\gcd(a, n)=1$, and $\chi(a)=0$ otherwise. Such a function on $\mathbf{Z}$ is called a *character* modulo n. The L-series associated to χ is defined by

$$L(s, \chi) = \sum_{a=1}^{\infty} \frac{\chi(a)}{a^s}.$$

If χ is non-trivial, i.e. $\chi(a)\notin\{0,1\}$ for some a, this series converges for all $s\in\mathbf{C}$ with $\mathrm{Re}(s)>0$. We say that $L(s,\chi)$ satisfies the generalized Riemann hypothesis if $L(s,\chi)\neq 0$ for all $s\in\mathbf{C}$ with $\mathrm{Re}(s)>½$. For trivial χ, this is only meaningful if $L(s,\chi)$ has been analytically continued; to avoid this, let us simply say that $L(s,\chi)$, for trivial χ, satisfies the generalized Riemann hypothesis if and only if the classical Riemann hypothesis is true, which is equivalent to

$$\sum_{a=1}^{\infty} \frac{(-1)^a}{a^s} \neq 0 \quad \text{for all} \quad s \in \mathbf{C} \quad \text{with} \quad \tfrac{1}{2} < \mathrm{Re}(s) < 1.$$

The GRH in Theorem 6 is the conjunction of all generalized Riemann hypotheses described above.

LEMMA (ANKENY-MONTGOMERY). *There is an absolute constant c with the following property. Let χ be a non-trivial character modulo n, and suppose that $L(s, \chi)$ satisfies the generalized Riemann hypothesis. Then there exists $a \in \mathbf{Z}$, $0 < a < c \cdot (\log n)^2$, such that $\chi(a) \neq 0$ and $\chi(a) \neq 1$.*

PROOF. See [23, Theorem 13.1], or [13, Corollary 1.3] for a version in which also the classical Riemann hypothesis is needed.

COROLLARY. *Assume GRH, and let $G \neq (\mathbf{Z}/n\mathbf{Z})^*$ be a subgroup of $(\mathbf{Z}/n\mathbf{Z})^*$. Then there exists $a \in \mathbf{Z}$ such that*

$$0 < a < c \cdot (\log n)^2, \quad \gcd(a, n) = 1, \quad (a \bmod n) \notin G,$$

with c as in the lemma.

PROOF. It suffices to apply the lemma to a non-trivial $\chi : (\mathbf{Z}/n\mathbf{Z})^* \to \mathbf{C}^*$ that is trivial on G.

Let now $n > 1$ be composite and odd. To finish the proof of Theorem 6, with an unspecified constant c instead of 70, it suffices, by the corollary, to exhibit a proper subgroup $G \subset (\mathbf{Z}/n\mathbf{Z})^*$ containing all non-witnesses a that are not divisible by n. For this we take (cf. [36])

$$G = \{(a \bmod n) \in (\mathbf{Z}/n\mathbf{Z})^* : a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \bmod n\}$$

where $\left(\frac{a}{n}\right)$ is the Jacobi symbol. It is a charming theorem of LEHMER [14, cf. 33] that $G \neq (\mathbf{Z}/n\mathbf{Z})^*$ for composite odd n. It is an equally charming result of SELFRIDGE [39, Theorem 17.2] that G contains all non-witnesses $(\bmod\, n)$ not divisible by n. This finishes the proof of Theorem 6.

Using additional arguments it can be proved that the generalized Riemann hypothesis is only needed for the L-series associated to characters χ of the form $\chi(a) = \left(\frac{a}{d}\right)$, where d runs over the positive integers that are $1 \bmod 4$ and either prime or the product of two distinct primes, see [16].

The value 70 for the constant is taken from [24, Théorème 4]; here again the classical Riemann hypothesis is needed, in addition to the generalized Riemann hypotheses just described. It is reported that WEINBERGER (unpublished) obtained sharper results.

The idea used in the proof of Theorem 6 has two other applications. The first is a fast primality test for small numbers:

THEOREM 7 (SELFRIDGE, WAGSTAFF). *Every odd composite n*

satisfying:	*has a witness among:*
$n < 2047$	2
$n < 1373653$	2,3
$n < 2 \cdot 10^9$, $n \neq 25326001, 161304001,$ 960946321, 1157839381	2,3,5
$n < 25 \cdot 10^9$, $n \neq 3215031751$	2,3,5,7

PROOF. By computer, see [27]. This proves Theorem 7.

The numbers in the left hand column are composite:

$2047 = 23 \cdot 89,$
$1373653 = 829 \cdot 1657,$
$25326001 = 2251 \cdot 11251,$
$161304001 = 7333 \cdot 21997,$
$960946321 = 11717 \cdot 82013,$
$1157839381 = 24061 \cdot 48121,$
$3215031751 = 151 \cdot 751 \cdot 28351.$

The test provided by Theorem 7 is easily implemented on a programmable pocket calculator. Thus, an HP-41C can decide the primality of an arbitrary $n < 2 \cdot 10^9$ within two minutes, using only 2, 3, 5 as possible witnesses.

The second application is based on the following theorem.

THEOREM 8 (RABIN). *Every odd composite n has at least $\frac{3}{4}(n-1)$ witnesses among $\{1, 2, ..., n-1\}$.*

The proof is an attractive exercise in elementary number theory, in which the Carmichael numbers play a role. See [29], [22]. This proves Theorem 8.

Rabin proposes the following primality test. Let m be a large integer, like 100, and choose randomly m integers $a_i \in \{1, 2, ..., n-1\}$, $1 \leq i \leq m$. If one of these a_i is a witness for n, then n is composite. If none of the a_i is a witness for n, then either n is prime or we have extremely bad luck. By Theorem 8, this bad luck occurs in at most one out of every 4^m cases. While this method is basically incapable of yielding rigorous primality proofs, it is in practical circumstances difficult to doubt that it yields correct answers. In any case, Rabin's method can be used to produce primes on a commercial basis: if found defective, they can easily be replaced.

If we try to remove the unproved assumption from Theorem 6 we are left with an algorithm that is no longer 'good':

THEOREM 9 (ADLEMAN, POMERANCE, RUMELY). *There is an algorithm that within $(\log n)^{c' \log\log\log n}$ steps decides whether or not n is prime, for $n > e^e$. Here c' denotes an effectively computable constant.*

A complete proof of this theorem can be found in [2] and [17]. A probabilistic version of the algorithm, which is somewhat easier to explain, will be described below. This version of the algorithm has been implemented by H. COHEN and A.K. LENSTRA on the CDC-Cyber 170-750 computer system of the SARA Computer Centre in Amsterdam, cf. [4], [5]. It is the only primality test in existence that can routinely handle numbers of up to 100 decimal digits, and it does so within approximately 45 seconds. Numbers of up to 200 decimal digits are dealt with within approximately 10 minutes.

The algorithm that we shall describe can be viewed as a special case of the following primality criterion.

THEOREM 10. *Let $n > 1$ be an integer. Then n is prime if and only if every divisor of n is a power of n.*

The proof is left to the reader.

To prove that n is prime using Theorem 10 we must check that any divisor of n is a power of n, and it clearly suffices to consider only *prime* divisors of n. Below we shall see how to do this without explicitly knowing the prime divisors of n. Actually, something weaker will be done: rather than showing that a prime r dividing n is a power of n, one attempts to show that this is true for the images of r and n in certain auxiliary groups, such as the group $(\mathbf{Z}/s\mathbf{Z})^*$ for an integer s that is coprime to n.

An example of this approach is provided by Theorem 5 and its proof: in that theorem we have $n \equiv 1 \bmod s$, and the proof proceeds by showing that any prime divisor r of n satisfies $r \equiv 1 \bmod s$, i.e. is congruent to a power of n modulo s. The following theorem provides a less trivial example.

THEOREM 11. *Let n and s be positive integers, and let A be a commutative ring with 1 containing $\mathbf{Z}/n\mathbf{Z}$ as a subring (with the same 1). Suppose that there exists $\alpha \in A$ satisfying the following conditions:*

(9) $\alpha^s = 1$,

(10) $\alpha^{s/q} - 1 \in A^*$ *(the group of units of A) for every prime q dividing s,*

(11) *the polynomial $\prod_{i=0}^{t-1}(X - \alpha^{n^i})$ has coefficients in $\mathbf{Z}/n\mathbf{Z}$ for some positive integer t.*

Then every divisor r of n is congruent to a power of n modulo s.

PROOF. We may assume that r is *prime*. Since r is a zero divisor (or zero) in A, there exists a maximal ideal M of A with $r \in M$. Let $\bar{A}$ be the field A/M, and $\bar{\alpha} = (\alpha \bmod M) \in \bar{A}$. By (9) and (10), the order of $\bar{\alpha}$ in $\bar{A}^*$ equals s. The polynomial $\prod_{i=0}^{t-1}(X - \bar{\alpha}^{n^i})$, which has $\bar{\alpha}$ as a zero, has coefficients in the subfield $\mathbf{F}_r$ of $\bar{A}$ of cardinality r. Therefore $\bar{\alpha}^r$ is also a zero of this polynomial, so there exists $i \in \{0, 1, ..., t-1\}$ with $\bar{\alpha}^r = \bar{\alpha}^{n^i}$, i.e. $r \equiv n^i \bmod s$. This proves Theorem 11.

If we take $A = \mathbf{Z}/n\mathbf{Z}$ and $t = 1$, then condition (11) is trivially satisfied. It is easy to deduce Theorem 5 from Theorem 11, by choosing α equal to the product of the a's appearing in Theorem 5, taken modulo n.

The proof of Theorem 11 shows that the residue classes $1, n, n^2, ..., n^{t-1}$ modulo s are permuted upon multiplication by $(r \bmod s)$, for any prime r dividing n. Writing n as the product of its prime factors, we see that multiplication by $(n \bmod s)$ also permutes these residue classes, which just means that $n^t \equiv 1 \bmod s$. Hence s must be chosen to be a divisor of $n^t - 1$.

Let $t = 2$. In this case known prime factors of $n+1 = (n^2-1)/(n-1)$ can be used in addition to those of $n-1$ to build up the number s. Starting from Theorem 11 one can, for practically every primality test based on factors of $n-1$, devise a corresponding test based on factors of $n+1$. These tests are usually formulated in terms of Lucas functions [39, Sections 12, 13, 14]. In the simplest case, corresponding to Pépin's Theorem 4, the number $n+1$ is a power of 2:

THEOREM 12 (LUCAS-LEHMER). *Let $n = 2^m - 1$, with $m > 2$. Define $(e_k)_{k=1}^{\infty}$ by $e_1 = 4$, $e_{k+1} = e_k^2 - 2$. Then n is prime if and only if $e_{m-1} \equiv 0 \bmod n$.*

PROOF. First let m be *even*. Then n is divisible by 3, and not prime. Also $e_{m-1} \equiv -1 \bmod 3$ by induction, so $e_{m-1} \not\equiv 0 \bmod n$. This proves the theorem for even m. Assume now that m is *odd*, and define

$$A = (\mathbf{Z}/n\mathbf{Z})[T]/(T^2 - \sqrt{2}T - 1),$$

where $\sqrt{2}$ denotes any element of $\mathbf{Z}/n\mathbf{Z}$ with $(\sqrt{2})^2 = 2$; e.g., $\sqrt{2} = (2^{(m+1)/2} \bmod n)$. Denoting the image of T in A by α we have

$$A = \{a + b\alpha : a, b \in \mathbf{Z}/n\mathbf{Z}\}, \quad \alpha^2 = \sqrt{2}\alpha + 1.$$

Let $\beta = \sqrt{2} - \alpha = -\alpha^{-1}$ be 'the' other zero of $X^2 - \sqrt{2}X - 1$ in A. From $\alpha + \beta = \sqrt{2}$ and $\alpha\beta = -1$ it follows easily by induction on k that

$$\alpha^{2^k} + \beta^{2^k} = (e_k \bmod n) \in \mathbf{Z}/n\mathbf{Z}$$

for all $k \geq 1$. Now let first n be prime. The discriminant of $X^2 - \sqrt{2}X - 1$ equals 6, and from $n \equiv 1 \bmod 3$, $n \equiv -1 \bmod 8$ and quadratic reciprocity it follows that $\left(\frac{6}{n}\right) = -1$. Hence A is a quadratic field extension of $\mathbf{F}_n$, and α and β are conjugate over $\mathbf{F}_n$. By the theory of finite fields this implies that $\alpha^n = \beta$. Multiplying this by α we get $\alpha^{2^m} = -1$, so

$$(e_{m-1} \bmod n) = \alpha^{2^{m-1}} + \beta^{2^{m-1}} = \alpha^{2^{m-1}} + \alpha^{-2^{m-1}} = 0.$$

This proves the 'only if' part. Suppose, conversely, that $(e_{m-1} \bmod n) = 0$. Then

$$\alpha^{2^m} = -1, \quad \alpha^{2^{m+1}} = 1,$$

so (9) and (10) of Theorem 11 are satisfied with $s=2^{m+1}$. Also, $\alpha^n = \alpha^{2^m-1} = -\alpha^{-1} = \beta$, so the polynomial

$$(X-\alpha)(X-\alpha^n) = (X-\alpha)(X-\beta) = X^2 - \sqrt{2}\cdot X - 1$$

has coefficients in $\mathbf{Z}/n\mathbf{Z}$, which is condition (11) of Theorem 11 with $t=2$. From Theorem 11 and $n^2 \equiv 1 \bmod s$ it now follows that any divisor of n is congruent to 1 or n modulo s. But $s>n$, so this means that n is prime. This proves Theorem 12.

It is known that $n=2^m-1$ can only be prime if m is prime: then n is one of the *Mersenne numbers* $M_p=2^p-1$, p prime. These are known to be prime for 30 values of p:

2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279,
2203, 2281, 3217, 4253, 4423, 9689, 9941, 11213, 19937,
21701, 23209, 44497, 86243, 132049, 216091,

see [34]. It is reasonable to conjecture that $\#\{m<x\colon 2^m-1 \text{ is prime}\}/\log x$ tends to a finite non-zero limit for $x\to\infty$. GILLIES [9] gives a probabilistic argument leading to the value $2/\log 2$ for the limit, but his reasoning is clearly in error since the same argument leads to a contradiction with the prime number theorem, cf. [10, § 22.20]. The number $e^\gamma/\log 2$, where γ is Euler's constant, has been proposed as a more likely value for the limit [25]; see also [38], [31].

If the complete factorization of $n-1$ is known then in practice it is easy to test n for primality, e.g. using Theorem 5. The same statement is true with $n-1$ replaced by $n+1$, using Theorem 11 with $t=2$. A combination of both tests is employed in the discovery of large *twin primes*, in the following way. Let m be a large number whose complete prime factorization is known; such a number can be found by multiplying together small numbers. Then $(m+1)-1$ and $(m-1)+1$ are completely factored, so we can apply an $(n-1)$-primality test to $m+1$ and an $(n+1)$-primality test to $m-1$. If both numbers turn out to be prime we have found a pair of twin primes. The largest known pair is

$$256200945\cdot 2^{3426} \pm 1 = 2^{3426}\cdot 3\cdot 5\cdot 7\cdot 11\cdot 13\cdot 113\cdot 151 \pm 1,$$

which have 1040 decimal digits. This pair was discovered by ATKIN and RICKERT [8].

We next discuss how Theorem 11 can for general t be used for primality testing. For A one takes a ring that if n were prime would be the field $\mathbf{F}_{n^t}$ of n^t elements. If n behaves as if it were a prime number then such a ring is in practice not difficult to construct: as in the proof of Theorem 12 one can take $A=(\mathbf{Z}/n\mathbf{Z})[T]/(f)$, where $f\in(\mathbf{Z}/n\mathbf{Z})[T]$ is a polynomial of degree t that passes a suitable irreducibility test (see [15, Sec. 5]). For s one takes the largest divisor

of n^t-1 that one is able to factor completely, and for α one takes an element of A^* of order s. If n is actually prime then α is usually easy to construct, by manipulating with elements of the form $\beta^{(n^t-1)/s}$, $\beta\in A$. In this case conditions (9) and (10) are clearly satisfied, and the polynomial in (11) is a power of the irreducible polynomial of α over $\mathbf{F}_n$ so it has certainly coefficients in $\mathbf{F}_n$. Suppose, conversely, that (9), (10) and (11) are found to be true. Then we cannot immediately conclude that n is prime, but we know, by Theorem 11, that any r dividing n is congruent to a power of n modulo s. If s is sufficiently large then this information can be used to finish the primality proof, in the following manner. Suppose that

$$s>n^{1/2}$$

(as in Theorem 5), and let r_i be determined by

$$n^i \equiv r_i \bmod s, \quad 0\leqslant r_i<s$$

for $0\leqslant i<t$. If n is composite then it has a non-trivial divisor r with $r\leqslant n^{1/2}<s$, and since r is congruent to a power of n modulo s it must be equal to one of the r_i. Hence, if we verify that none of the r_i is a non-trivial divisor of n, we have proved that n is prime. A similar but somewhat more involved procedure can be followed if s satisfies the weaker inequality $s>n^{1/3}$, see [18].

We refer to [17, Theorem 8.4] for a more flexible version of Theorem 11, in which it is possible to vary α with q, as in Theorem 5.

For very small values of t, such as $t=2$, 3, 4, 6, it is again possible to employ lower bounds for the unknown prime divisors of n^t-1, cf. [39, Sections 13-16] and the references given there. It is doubtful whether such lower bounds are equally useful for the larger values of t considered below.

To analyze the above algorithm we must know how to choose t such that $s>n^{1/2}$. We need the following theorem.

THEOREM 13 (ODLYZKO-POMERANCE). *There exists an effectively computable constant c'' with the following property. For every integer $n>e^e$ there exists a positive integer t satisfying*

$$t<(\log n)^{c''\log\log\log n}$$

$$t \text{ is squarefree}$$

such that the number

$$s = \prod\nolimits_{q \text{ prime},\, q-1 \text{ divides } t} q$$

satisfies

$$s>n^{1/2}.$$

PROOF. See [2, Sec. 6]. This proves Theorem 13.

Let t be as in Theorem 13; the condition that t be squarefree is irrelevant for our present purpose. If q is a prime number for which $q-1$ divides t, then

$n^t \equiv 1 \bmod q$ by Fermat's theorem, unless q divides n. Hence, if s is as in the theorem, then s divides $n^t - 1$ provided that $\gcd(n, s) = 1$. Also, the complete factorization of s is known, and $s > n^{1/2}$. We conclude that these values for t and s can be used in the primality test described above. The resulting algorithm has, for prime n, an expected running time that is less than $(\log n)^{c' \log\log\log n}$ for some constant c'. This does not yet prove Theorem 9, since we have no such bound for the worst case running time. It appears that the size of t makes the test unsuitable for practical primality testing.

The test underlying Theorem 9 is closely related to the test just described. It depends on properties of *Gauss sums*, which we shall now consider. By ζ_m we denote a primitive m-th root of unity.

Let p and q be prime numbers not dividing n for which p divides $q-1$. We choose a character $\chi = \chi_{p,q}$ modulo q that has order p; i.e., $\chi: \mathbf{F}_q^* \to <\zeta_p>$ is a surjective group homomorphism, where $<\zeta_p>$ denotes the subgroup of $\mathbf{C}^*$ generated by ζ_p. Such a χ can be obtained by choosing a primitive root g modulo q and putting $\chi(g^i \bmod q) = \zeta_p^i$ for $i \in \mathbf{Z}$. We define the *Gauss sum* $\tau(\chi)$ by

$$\tau(\chi) = \sum_{x=1}^{q-1} \chi(x)\zeta_q^x.$$

This is an element of the cyclotomic ring $R = \mathbf{Z}[\zeta_p, \zeta_q]$. We have

$$\tau(\chi)^n \equiv \chi(n)^{-n} \cdot \tau(\chi^n) \bmod nR \quad \text{if } n \text{ is } \textit{prime}.$$

To prove this, notice that modulo nR we have

$$\begin{aligned} \tau(\chi)^n &\equiv \sum_{x=1}^{q-1} \chi(x)^n \cdot \zeta_q^{nx} \quad (\text{since } n \text{ is prime}) \\ &= \sum_{y=1}^{q-1} \chi(n)^{-n} \cdot \chi(y)^n \cdot \zeta_q^y \quad (\text{with } y \equiv nx \bmod q) \\ &= \chi(n)^{-n} \cdot \tau(\chi^n), \end{aligned}$$

as required. We investigate what can, conversely, be said about n if the following weaker condition is satisfied:

$$\tau(\chi)^n \equiv \eta(\chi)^{-n} \cdot \tau(\chi^n) \bmod nR \quad \text{for some } \eta(\chi) \in <\zeta_p>. \tag{12}$$

Let σ be the automorphism of R with $\sigma(\zeta_p) = \zeta_p^n$ and $\sigma(\zeta_q) = \zeta_q$. Then (12) can be written as

$$\tau(\chi)^{n-\sigma} \equiv \eta(\chi)^{-n} \bmod nR.$$

Raising both sides to the power $\sum_{i=0}^{p-2} n^{p-2-i}\sigma^i$ we obtain:

$$\tau(\chi)^{n^{p-1}-1} \equiv \eta(\chi) \bmod nR.$$

Now let r be any prime divisor of n. Then we know that (12), with n replaced by r and $\eta(\chi)$ by $\chi(r)$, is valid, so for the same reason we have

$$\tau(\chi)^{r^{p-1}-1} \equiv \chi(r) \bmod rR.$$

Combination of the last two congruences suggests that

$$\chi(r) = \eta(\chi)^{(r^{p-1}-1)/(n^{p-1}-1)} \tag{13}$$

for any prime r dividing n. To make this meaningful we have to explain how to interpret the fractional exponent. For this we need the following hypothesis on p:

$$v_p(r^{p-1}-1) \geqslant v_p(n^{p-1}-1) \quad \text{for every prime } r \text{ dividing } n, \tag{14}$$

where $v_p(m)$ denotes the number of factors p in m. If (14) is satisfied we can write $(r^{p-1}-1)/(n^{p-1}-1) = a/b$, with $a, b \in \mathbf{Z}$, $b \equiv 1 \bmod p$, and the residue class of $(r^{p-1}-1)/(n^{p-1}-1) \bmod p$ is then defined to be $(a \bmod p)$; this does not depend on the choice of a and b. Since $\eta(\chi)^p = 1$ it is now meaningful to define the right hand side of (13) as $\eta(\chi)^a$.

With this interpretation it is straightforward to verify that (12) implies (13), provided that (14) is assumed. By induction on the number of prime factors one can now prove that (13) holds for *any* divisor r of n, prime or not. In particular, with $r = n$ we obtain $\chi(n) = \eta(\chi)$, so (13) now yields

$$\chi(r) = \chi(n)^{(r^{p-1}-1)/(n^{p-1}-1)} \tag{15}$$

for any r dividing n. Again we see that every divisor of n is a power of n, if images under χ are taken.

It is a vital question how to verify hypothesis (14). Trivially, we have

$$\text{if } n^{p-1} \not\equiv 1 \bmod p^2, \quad \text{then (14) holds.} \tag{16}$$

In [17, Sec. 2] it is proved that

$$\text{if (12) holds with } \eta(\chi) \neq 1, \text{ then (14) is true.} \tag{17}$$

The primality test based on the preceding theory runs as follows. Let t be a positive integer having all properties listed in Theorem 13, and let s have the same meaning as in that theorem. Choose, for every pair of prime numbers p, q with q dividing s and p dividing $q-1$ (so p dividing t) a character $\chi = \chi_{p,q}$ as above, and check that $\chi = \chi_{p,q}$ satisfies (12); we know that this is necessary for n to be prime. Next, attempt to prove that every prime p dividing t satisfies hypothesis (14). Usually, for each p there is a q dividing s with $\eta(\chi_{p,q}) \neq 1$, and then (17) applies. If there is no such q, and (16) does not apply either, one should test (12) for characters $\chi_{p,q}$ with q a prime *not* dividing s for which p divides $q-1$, until an example of $\eta(\chi_{p,q}) \neq 1$ is found.

At this stage of the algorithm one knows that every $\chi_{p,q}$, with p dividing $q-1$ and q dividing s, satisfies (15) for each r dividing n. We claim that this implies that each r is congruent to a power of n modulo s, so that the test can be completed in the same way as the test described before Theorem 13.

To prove the claim, let r divide n, and let $(i \bmod t)$ be determined by

$$i \equiv (r^{p-1}-1)/(n^{p-1}-1) \bmod p$$

(in the sense explained before) for each prime p dividing t; notice that here we use that t is squarefree. Then (15) implies that

$$\chi_{p,q}(r) = \chi_{p,q}(n^i)$$

for each pair p, q as above. For fixed q, the product of the primes p dividing $q-1$ equals $q-1$, so the characters $\chi_{p,q}$ generate the group of all characters modulo q; therefore $r \equiv n^i \bmod q$. Since this holds for all q dividing s, we conclude that $r \equiv n^i \bmod s$, as required.

The only non-deterministic part of the test is the verification of hypothesis (14). If n is composite it is conceivable that (14) is not satisfied, so that the algorithm will get stuck at this point. We refer to [2, Sec. 5] and [17, Sec. 5] for a variant that avoids hypothesis (14). It constructs an auxiliary number ν such that from a set of conditions similar to (12) it can be deduced that any divisor r of n is congruent to a power of ν, rather than a power of n, modulo s. This test is completely deterministic, and it has running time less than $(\log n)^{c' \log\log\log n}$ for $n > e^e$, where c' denotes an effectively computable constant. This concludes our sketch of the proof of Theorem 9.

There are several ways to improve the practical performance of the test [5], [17]. In the first place, the Gauss sums can be replaced by Jacobi sums, which belong to $\mathbf{Z}[\zeta_p]$ rather than $\mathbf{Z}[\zeta_p, \zeta_q]$. Secondly, characters of prime power order rather than of prime order can be employed, so that the condition that t be squarefree can be dropped. Finally, it is possible to combine the test with the tests described earlier depending on variants of Theorem 11. However, none of these improvements reduces the running time in a theoretically significant way.

As we noted in connection with the Fermat numbers, it is surprising that we can prove that a number is composite without actually finding a factor. To analyze this situation, let us assume that we proved n composite by exhibiting an integer a for which

$$a^{n-1} \not\equiv 1 \bmod n, \quad \gcd(a, n) = 1, \tag{18}$$

and applying Fermat's theorem that (18) is impossible for prime n. To see why this gives no factorization of n we must investigate how Fermat's theorem is proved. One proof is based on the remark that the map sending i to $a \cdot i$ (mod n) is a permutation of $\{1, 2, ..., n-1\}$, so

$$a^{n-1} \cdot (n-1)! = \prod_{i=1}^{n-1} (a \cdot i) \equiv \prod_{i=1}^{n-1} i = (n-1)! \bmod n.$$

Hence (18) implies that $(n-1)!$ has a non-trivial gcd with n, which tells us nothing more than that n is composite. Other proofs of Fermat's theorem have similar shortcomings. The situation would be different if factorials or binomial coefficients were easy to compute modulo n. This is clear from the proof of the following charming but useless theorem, in which we also consider 'division with remainder' as an arithmetic operation.

THEOREM 14 (SHAMIR). *There is an algorithm that for every composite n yields a non-trivial divisor of n, using no more than $O(\log n)$ arithmetic operations.*

PROOF. We notice that n is composite if and only if $1 < \gcd(a_0!, n) < n$ for some positive integer a_0. Since $\gcd(a!, n)$ is a non-decreasing function of a, and is equal to 1, n for $a = 1$, n respectively, we can determine such an a_0 by $O(\log n)$ bisections, provided that we know how to calculate $\gcd(a!, n)$.

Once we know $a!$, we can determine the gcd by Euclid's algorithm in $O(\log n)$ arithmetic steps. To calculate $a!$, we apply the formulae

$$(2b+1)! = (2b+1) \cdot (2b)!,$$

$$(2b)! = (b!)^2 \cdot \left[\begin{matrix} 2b \\ b \end{matrix}\right]$$

$O(\log a)$ times. To calculate the binomial coefficient $\left[\begin{matrix} 2b \\ b \end{matrix}\right]$ needed here, we remark that $\left[\begin{matrix} 2b \\ b \end{matrix}\right]$ is the middle block of n binary digits in the binary expansion of $(2^n+1)^{2b}$, for $2b < n$; and the exponentiation can be done by $O(\log(2b))$ multiplications.

This algorithm, as we described it, takes $O((\log n)^3)$ arithmetic operations. For the modifications to bring it down to $O(\log n)$ we refer to Shamir's paper [32]. This concludes the proof of Theorem 14.

We notice that the best known deterministic factorization algorithm, which is due to Pollard, also depends on the calculation of factorials modulo n. This algorithm and several more practical ones are described in the papers of POMERANCE [26] and VOORHOEVE [37].

REFERENCES

1. L. ADLEMAN, K. MANDERS (1976). Diophantine complexity. *17th Annual IEEE Symp. on Foundations of Computer Science*, 81-88.
2. L.M. ADLEMAN, C. POMERANCE, R.S. RUMELY (1983). On distinguishing prime numbers from composite numbers. *Ann. of Math. 117*, 173-206.
3. R.P. BRENT, J.M. POLLARD (1981). Factorization of the eighth Fermat number. *Math. Comp. 36*, 627-630.
4. H. COHEN, A.K. LENSTRA (1985). *Implementation of a New Primality Test*, Report CS-R8505, CWI, Amsterdam; *Math. Comp.*, to appear.
5. H. COHEN, H.W. LENSTRA, JR. (1984). Primality testing and Jacobi sums. *Math. Comp. 42*, 297-330.
6. F.N. COLE (1903/4). On the factoring of large numbers. *Bull. Amer. Math. Soc. 10*, 134-137.
7. M. DAVIS (1973). Hilbert's tenth problem is unsolvable. *Amer. Math. Monthly 80*, 233-269.

8. M. GARDNER (1981). Mathematical games. *Scientific American 244* (2), 14-19.

9. D.B. GILLIES (1964). Three new Mersenne primes and a statistical theory. *Math. Comp. 18,* 93-97.

10. G.H. HARDY, E.M. WRIGHT (1979). *An Introduction to the Theory of Numbers,* 5th ed., Oxford University Press.

11. P.J. HOOGENDOORN. On a secure public-key cryptosystem, pp. 159-168 in [19].

12. J.P. JONES, D. SATO, H. WADA, D. WIENS (1976). Diophantine representation of the set of prime numbers. *Amer. Math. Monthly 83,* 449-464.

13. J.C. LAGARIAS, H.L. MONTGOMERY, A.M. ODLYZKO (1979). A bound for the least prime ideal in the Chebotarev density theorem. *Invent. Math. 54,* 271-296.

14. D.H. LEHMER (1976). Strong Carmichael numbers. *J. Austral. Math. Soc. Ser. A 21,* 508-510.

15. A.K. LENSTRA. Factorization of polynomials, pp. 169-198 in [19].

16. H.W. LENSTRA, JR. (1979). Miller's primality test. *Inform. Process. Lett. 8,* 86-88.

17. H.W. LENSTRA, JR. (1981). Primality testing algorithms (after ADLEMAN, RUMELY and WILLIAMS), Séminaire Bourbaki *33,* (1980/1981). no. 576, pp. 243-257 in: *Lecture Notes in Mathematics 901,* Springer, Berlin.

18. H.W. LENSTRA, JR. (1984). Divisors in residue classes. *Math. Comp. 42,* 331-340.

19. H.W. LENSTRA, JR., R. TIJDEMAN (eds.) (1982). *Computational Methods in Number Theory,* Mathematical Centre Tracts 154/155, Mathematisch Centrum, Amsterdam.

20. YU.V. MATIJASEVIČ (1981). Primes are nonnegative values of a polynomial in 10 variables. *Zap. Naučn. Sem. Leningrad. Otdel. Mat. Inst. Steklov (LOMI) 68* (1977), 62-82 (Russian; English translation: *J. Soviet Math. 15,* 33-44).

21. G.L. MILLER (1976). Riemann's hypothesis and tests for primality. *J. Comput. System. Sci. 13,* 300-317.

22. L. MONIER (1980). Evaluation and comparison of two efficient probabilistic primality testing algorithms. *Theoret. Comput. Sci. 12,* 97-108.

23. H.L. MONTGOMERY (1971). Topics in multiplicative number theory. *Lecture Notes in Mathematics 227,* Springer, Berlin.

24. J. OESTERLÉ (1979). Versions effectives du théorème de Chebotarev sous l'hypothèse de Riemann généralisée. Journées Arithmétiques de Luminy, *Astérisque 61,* 165-167.

25. C. POMERANCE. (1981). Recent developments in primality testing. *Math. Intell. 3,* 97-105.

26. C. POMERANCE. Analysis and comparison of some integer factoring algorithms, pp. 89-139 in [19].

27. C. POMERANCE, J.L. SELFRIDGE, S.S. WAGSTAFF, JR. (1980). The pseudoprimes to $25 \cdot 10^9$. *Math. Comp. 35,* 1003-1026.

28. V.R. PRATT (1975). Every prime has a succinct certificate. *SIAM J. Comput. 4,* 214-220.

29. M.O. RABIN (1980). Probabilistic algorithm for testing primality. *J. Number Theory 12,* 128-138.

30. A. SCHÖNHAGE, V. STRASSEN (1971). Schnelle Multiplikation grosser Zahlen. *Computing 7,* 281-292.

31. M.R SCHROEDER (1983). Where is the next Mersenne prime hiding? *Math. Intell. 5,* 31-33.

32. A. SHAMIR (1979). Factoring numbers in $O(\log n)$ arithmetic steps. *Inform. Process. Lett. 8,* 28-31.

33. R. SOLOVAY, V. STRASSEN (1978). A fast Monte-Carlo test for primality. *SIAM J. Computing 6* (1977), 84-85; erratum: *7,* 118.

34. H.J.J. TE RIELE. Perfect numbers and aliquot sequences, pp. 141-157 in [19].

35. J.W.M. TURK. Fast arithmetic operations on numbers and polynomials, pp. 43-54 in [19].

36. J. VÉLU (1978). Tests for primality under the Riemann hypothesis. *SIGACT News 10,* 58-59.

37. M. VOORHOEVE. Factorization algorithms of exponential order, pp. 79-87 in [19].

38. S.S. WAGSTAFF, JR. (1983). Divisors of Mersenne numbers. *Math. Comp. 40,* 385-397.

39. H.C. WILLIAMS (1978). Primality testing on a computer. *Ars Combin. 5,* 127-185.