PRIMALITY TESTING

by

H.W. LENSTRA, Jr.

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 50-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 (a) and (b) 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, I may remark that, to my knowledge, no clairvoyants have ever been employed to identify Mersenne primes or to factorize large numbers. Such an attempt might lead to new insights, if not in mathematics then in parapsychology.

"Numerology" - this condescending denomination for the branch of science to which (a) and (b) belong was, until recently, fashionable among mathematicians of good taste, 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 the lecture of P.J. Hoogendoorn. 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 the lecture of M. Voorhoeve. The basic reference on primality testing is the beautiful paper by H.C. WILLIAMS [31]. It is not our purpose to copy it here, but some overlap is unavoidable. We encourage the reader to consult Williams' paper for many details and additional information.

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 may take $\sqrt{n}$ 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

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

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 A,B,...,Z. Such a polynomial, of degree 25, is explicitly given in [11]. A similar polynomial in 10 variables of degree 15905 is constructed in [15]. 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 [11, 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.M. Cole's proof that $2^{67}-1$ is composite consists of the single observation that

$$2^{67}-1 = 193707721.761838257287.$$

But it had taken him 'three years of Sundays' to find his proof, and the methods which he employed are far more interesting than the final proof itself [6,23].

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

$$n = f(A,B,\ldots,Z)$$

is completely constructive, see [11]. But for the polynomial from [11] 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]; cf. the lecture of P. van Emde Boas.) 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. The proof just consists of the remark that the usual algorithm to multiply two numbers less than n requires no more than $O((\log n)^2)$ bit operations.

Using the fast multiplication routine of SCHÖNHAGE and STRASSEN [25] we can replace $(\log n)^2$ in Theorem 2 by $(\log n)^{1+\varepsilon}$, for any $\varepsilon > 0$, or more precisely by $O((\log n) \cdot (\log\log n) \cdot (\log\log\log n))$ (for $n > e^e$).

THEOREM 3. (PRATT [23]). *If* n *is prime, this can be proved using only* $O((\log n)^4)$ *bit operations.*

Again, using [25], we can replace $(\log n)^4$ by $(\log n)^{3+\varepsilon}$, for any $\varepsilon > 0$.

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

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

of the ring $\mathbb{Z}/n\mathbb{Z}$ 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 $(\mathbb{Z}/n\mathbb{Z})^*$ is cyclic of order n-1. Conversely, if $(\mathbb{Z}/n\mathbb{Z})^*$ has order $\ge n-1$, then n is a prime number. Thus we see that n is prime if and only if there exists $(a \bmod n) \in (\mathbb{Z}/n\mathbb{Z})^*$ of order n-1. If we assume n to be odd and write

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

$$q_0 = 2$$

$$q_i \text{ prime} \qquad (1 \le i \le t) \tag{2}$$

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

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

$$a^{(n-1)/q_i} \not\equiv 1 \bmod n, \qquad \text{for } 1 \le i \le t. \tag{4}$$

Therefore, to prove that n is prime, we can write down integers a, $q_0 = 2$, $q_1,\ldots,q_t$, verify that (1), (3) and (4) hold, and prove (2) recursively. This proof requires t multiplications in (1), and t+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

$$f(n) \le t + t + 1 + \sum_{i=1}^{t} f(q_i)$$

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

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

as required.

We conclude that no more than $O(\log n)$ 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. This leads to the bound $O((\log n)\cdot(\log n)\cdot(\log n)^2) = O((\log n)^4)$ stated in the theorem.

Theorems 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* $\iff$ $3^{(n-1)/2} \equiv -1 \bmod n$.

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

$$(\tfrac{3}{n}) = (\tfrac{n}{3}) = (\tfrac{2}{3}) = -1.$$

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

It is known that $n = 2^m+1$ can only be prime if m is a power of 2; then n is one of the *Fermat numbers* $F_k = 2^{2^k}+1$. For $k = 0,1,2,3,4$ these numbers are actually prime, for $5 \le k \le 19$ and some other values (such as $k = 1945$) they are composite. It is reasonable to conjecture that they are, in fact, all composite for $k \ge 5$. 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 [31, Sec. 5] for more information on the Fermat numbers.

For general n, the main difficulty is to find the complete factorization (1) of n-1. Once this has been done, it is generally not difficult to decide whether or not n is prime. If the methods described below fail to show that n is composite, it is usually easy to find an integer a for which (3) and (4) hold. In fact, one may replace (4) by the weaker condition

(5) for each i, $1 \le i \le t$, there exists an integer a_i such that

$$a_i^{n-1} \equiv 1 \bmod n, \qquad a_i^{(n-1)/q_i} \not\equiv 1 \bmod n.$$

This can be verified with the arguments used in the proof of Theorem 5.

The following is a variant of the above test in which only a partial factorization of n-1 is needed. For further variants, and references to the literature, see [31, Sections 10,11] and [5].

THEOREM 5. *Let* $n > 1$ *be an integer, and let*

$$n-1 = m_1 \cdot \prod_{i=1}^{s} g_i^{k_i}$$

where m_1 *and the* k_i *are positive integers, and* $g_1, g_2, \ldots, g_s$ *are pairwise relatively prime integers* ≥ 2. *Let further* $b_1, b_2, \ldots, b_s$ *be positive integers such that the following conditions hold:*

(a_1) *every prime factor of* g_i *is* $\geq b_i$ *(e.g.,* $b_i = 2$, *or* $b_i = g_i$ *if* g_i *is prime), for* $1 \leq i \leq s$;

(b_1) *for each* i, $1 \leq i \leq s$, *there exists an integer* a_i *such that*

$$(6) \qquad a_i^{n-1} \equiv 1 \bmod n, \qquad \gcd(a_i^{(n-1)/g_i} - 1, n) = 1;$$

$$(c_1) \qquad n < (1 + \prod_{i=1}^{s} b_i^{k_i})^2 .$$

Then n *is prime.*

PROOF. Let p be any prime dividing n. From (6) we see that the order of $(a_i \bmod p)$ divides n-1, but not $(n-1)/g_i$. Hence this order is divisible by $q_i^{k_i}$, for some prime q_i dividing g_i. Also, the order divides p-1, so $q_i^{k_i}$ divides p-1. Since the g_i are coprime, it follows that $\prod_{i=1}^{s} q_i^{k_i}$ divides p-1, so $p \geq 1 + \prod_{i=1}^{s} q_i^{k_i} \geq 1 + \prod_{i=1}^{s} b_i^{k_i}$. From ($c_1$) it follows that n can have at most one such prime factor. Hence n is prime, as required.

The gcd's in (6) can be calculated efficiently using Euclid's algorithm. In fact, by a trick in [5, p.623], only one gcd computation is necessary. Notice further that any known set of factorizations of n-1 can be brought in the form needed in Theorem 5, even with $m_1 = 1$, by calculating finitely many gcd's.

G.L. MILLER [16] introduced a different way to exploit the multiplicative structure of the integers mod 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, which in* $O((\log n)^5)$ *steps decides whether or not* n *is prime.*

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

Assume that n is odd, and write $n-1 = u.2^t$, where u is odd and $t \geq 1$. Employing RABIN's terminology [24], we call an integer a a *witness* to the compositeness of n, or simply a witness for n, if the following three conditions hold:

(7) n does not divide a,

(8) $a^u \not\equiv 1 \bmod n,$

(9) $a^{u.2^i} \not\equiv -1 \bmod n \qquad \text{for } i = 0,1,\ldots,t-1.$

(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 mod n; so we may restrict to $0 \le a < n$. 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 (7), (8), (9) hold and that n is prime. By (7) and Fermat's theorem, $a^{u.2^t} = a^{n-1} \equiv 1 \bmod n$. Hence the last term in the sequence

$$a^u, a^{u.2}, \ldots, a^{u.2^t}$$

is 1 mod n, but by (8) the first term is not 1 mod n. Let $b = a^{u.2^i}$ be the last term in the sequence which is not 1 mod n. Then $0 \le i \le t-1$, and $b^2 \equiv 1 \bmod n$ while $b \not\equiv 1 \bmod n$. Since the integers mod n form a field, this implies that $b \equiv -1 \bmod n$, contradicting (9).

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 $a < 70(\log n)^2$. 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 $\chi: (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$ (the group of non-zero complex numbers) be a group homomorphism. We view χ as a function on $\mathbb{Z}$ by $\chi(a) = \chi(a \bmod n)$ if $\gcd(a,n) = 1$, and $\chi(a) = 0$ otherwise. Such a function on $\mathbb{Z}$ 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 $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 0$. We say that $L(s,\chi)$ satisfies the generalized Riemann hypothesis if $L(s,\chi) \neq 0$ for all $s \in \mathbb{C}$ with $\mathrm{Re}(s) > \frac{1}{2}$. 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

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

The GRH in Theorem 6 is the conjunction of all generalized Riemann hypothesis 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* $a \in \mathbb{Z}$, $0 < a < c\cdot(\log n)^2$, *such that* $\chi(a) \neq 0$ and $\chi(a) \neq 1$.

PROOF. See [19, Theorem 13.1], or [12, Corollary 1.3] for a version in which also the classical Riemann hypothesis is needed.

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

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

with c *as in the lemma.*

PROOF. It suffices to apply the lemma to a non-trivial $\chi\colon (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$ which 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 $G \subset (\mathbb{Z}/n\mathbb{Z})^*$ containing all non-witnesses a which are not divisible by n. For this we take (cf. [30])

$$G = \{(a \bmod n) \in (\mathbb{Z}/n\mathbb{Z})^* : a^{(n-1)/2} \equiv (\tfrac{a}{n}) \bmod n\}$$

where $(\frac{a}{n})$ is the Jacobi symbol. It is a charming theorem of LEHMER [13, cf. 29] that $G \neq (\mathbb{Z}/n\mathbb{Z})^*$ for composite odd n. It is an equally charming result of SELFRIDGE [31, Theorem 17.2] that G contains all non-witnesses (mod n) not divisible by n. This finishes the proof.

Using additional arguments it can be proved that the generalized Riemann hypothesis is only needed for characters χ of the form $\chi(a) = (\frac{a}{d})$, where d runs over the positive integers which are 1 mod 4 and either prime or the product of two distinct primes, see [14].

The value 70 for the constant is taken from [20, Theorem 4]; here again the classical Riemann hypothesis is needed. 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
$n < 10^9$, $n \neq 25326001, 161304001, 960946321$	2,3,5
$n < 25.10^9$, $n \neq 3215031751$	2,3,5,7

PROOF. By computer, see [22]. The numbers in the left hand column are composite:

$2047 = 23.89$, $161304001 = 7333.21997$,
$1373653 = 829.1657$, $960946321 = 11717.82013$,
$25326001 = 2251.11251$, $3215031751 = 151.751.28351$.

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 $n < 10^9$ within 100 seconds, 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* $\{1,2,\ldots,n-1\}$.

The proof is an attractive exercise in elementary number theory, in which the Carmichael numbers play a role. See [24,17].

Rabin proposes the following primality test. Let m be a large integer, like 100, and choose randomly m integers $a_i \in \{1,2,\ldots,n-1\}$, $1 \le i \le m$. 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 difficult to doubt the correctness of the 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 which is no longer 'good':

THEOREM 9. (POLLARD). *For any* $\varepsilon > 0$, *there exists an algorithm which in* $O(n^{(1/8)+\varepsilon})$ *steps decides whether or not* n *is prime.*

For the proof, and a description of the algorithm, we refer to [21, Theorem 2]. It is based on a converse to Fermat's theorem, and has mainly theoretical value.

The most successful methods described above make use of the multiplicative structure of the ring $\mathbb{Z}/n\mathbb{Z}$. In some of them information on the factors of n-1 is needed; the number n-1 appears because, for n prime, the group $(\mathbb{Z}/n\mathbb{Z})^*$ is cyclic of order n-1. We shall now describe some methods in which information about the factors of n+1 is needed. The usual way to describe these methods employs LUCAS functions, see e.g. [31]. In order to offer something different, we present an algebraic approach here.

To explain the appearance of the number n+1, we observe that $n+1 = (n^2-1)/(n-1)$. Here n^2-1 is, for n prime, the order of the cyclic multiplicative group $\mathbb{F}_{n^2}^*$ of the field $\mathbb{F}_{n^2}$ of n^2 elements, and n-1 is the order of the subgroup $\mathbb{F}_n^*$. Thus $\mathbb{F}_{n^2}^*/\mathbb{F}_n^*$ is cyclic of order n+1. Alternatively, the kernel of the norm map $\mathbb{F}_{n^2}^* \to \mathbb{F}_n^*$ is cyclic of order n+1.

Since we do not know beforehand that n is prime, we have to set up a theory of quadratic extensions of $\mathbb{Z}/n\mathbb{Z}$ for arbitrary $n > 1$, cf. [4, Ch.III, Section 2.3]. For simplicity we take n *odd*.

Let R be a ring with 1 which, as an abelian group, is isomorphic to $(\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$. Then $\mathbb{Z}/n\mathbb{Z}$ may be considered as a subring of R, and there exists $x \in R$ such that every $a \in R$ can be uniquely written as $a + bx$, with

$a,b \in \mathbb{Z}/n\mathbb{Z}$. Let $v,w \in \mathbb{Z}/n\mathbb{Z}$ be chosen such that $x^2 = -w + vx$. Then R is isomorphic to $(\mathbb{Z}/n\mathbb{Z})[X]/(X^2-vX+w)$, with x corresponding to the residue class of X. The *discriminant* $\Delta = v^2 - 4w$ of $X^2 - vX + w$ is called the discriminant of R; it is well defined up to multiplication by squares of units of $\mathbb{Z}/n\mathbb{Z}$. It is easy to check that two R's with the same discriminant are isomorphic. In the sequel we assume that Δ is a *unit* in $\mathbb{Z}/n\mathbb{Z}$.

Let $y = v - x$. Then $y^2 = -w + vy$, and the map σ sending $a + bx$ to $a + by$, for $a,b \in \mathbb{Z}/n\mathbb{Z}$, is a ring automorphism of R. The *norm* of $\alpha \in R$ is defined by $\mathrm{norm}(\alpha) = \alpha \cdot \sigma(\alpha)$; this belongs to $\mathbb{Z}/n\mathbb{Z}$, and the norm restricts to a group homomorphism $R^* \to (\mathbb{Z}/n\mathbb{Z})^*$. Without referring to x, we may describe $\mathrm{norm}(\alpha)$ as the determinant of the $\mathbb{Z}/n\mathbb{Z}$-linear map $R \to R$ mapping r to αr. We leave it to the reader to define σ similarly. The group we are interested in is defined by

$$H = \{\gamma \in R^* : \mathrm{norm}(\gamma) = 1\}.$$

If $\alpha \in R^*$, then clearly $\alpha/\sigma(\alpha) \in H$. In particular, $x/y \in H$ if w is a unit in $\mathbb{Z}/n\mathbb{Z}$. For us, the basic property of H is:

(10) if n is prime, then H is cyclic of order $n - (\frac{\Delta}{n})$.

Here $(\frac{\Delta}{n})$ is the Jacobi symbol. The proof of (10) distinguishes two cases. First let $(\frac{\Delta}{n}) = -1$. Then $X^2 - vX + w$ is irreducible over $\mathbb{F}_n$, so R is a field: $R = \mathbb{F}_{n^2}$, and R^* is cyclic of order n^2-1. By the theory of finite fields we know that R, besides the identity, has only the Frobenius automorphism, mapping every $\alpha \in R$ to α^n. So this must be σ, and $\mathrm{norm}(\alpha) = \alpha \cdot \sigma(\alpha) = \alpha^{n+1}$ for all $\alpha \in R$. It follows that $H = \{\alpha \in \mathbb{F}_{n^2}^* : \alpha^{n+1} = 1\}$, which is a cyclic group of order n+1, as required. Next let $(\frac{\Delta}{n}) = 1$. Then $X^2 - vX + w$ has two distinct zeros ξ, η in $\mathbb{F}_n$, and we may identify R with $\mathbb{F}_n \times \mathbb{F}_n$ (componentwise addition and multiplication) by mapping $a + bx$ to $(a+b\xi, a+b\eta)$, for $a,b \in \mathbb{F}_n$. We have $R^* \cong \mathbb{F}_n^* \times \mathbb{F}_n^*$. The map σ interchanges the two coordinates, so $H = \{(\alpha,\alpha^{-1}) \in \mathbb{F}_n^* \times \mathbb{F}_n^*\}$, which is isomorphic to $\mathbb{F}_n^*$ and therefore cyclic of order n-1. This proves (10).

The structure of the group H can also be determined for composite n, but we shall not need it in the sequel. As an exercise, the reader may prove that the converse of (10) is also true; but that there may exist *composite* n for which H is *non*-cyclic of order $n - (\frac{\Delta}{n})$.

The theory can be extended to cover the case that n is even, or that

Δ is no unit in $\mathbb{Z}/n\mathbb{Z}$, but this has no applications to primality tests.

Starting from (10) one can, for practically every test based on factors of n-1, devise a corresponding test based on factors of n+1. In the simplest case, corresponding to Pépin's Theorem 4, the number n+1 is a power of 2:

THEOREM 10. (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* $\iff e_{m-1} \equiv 0 \bmod n$.

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*. We apply the above theory to the ring $R = (\mathbb{Z}/n\mathbb{Z})[X]/(X^2 - \sqrt{2}X - 1)$, where $\sqrt{2}$ denotes any element of $\mathbb{Z}/n\mathbb{Z}$ with $\sqrt{2}^2 = 2$; e.g., $\sqrt{2} = 2^{(m+1)/2}$. As before, the residue class of X is denoted by x, and $y = \sqrt{2} - x$. Then $x+y = \sqrt{2}$, $xy = -1$. From these two relations it follows easily by induction on k that

$$x^{2^k} + y^{2^k} = (e_k \bmod n) \in \mathbb{Z}/n\mathbb{Z}$$

for all $k \geq 1$. We have $\Delta = \sqrt{2}^2 + 4 = 6$, and from $n \equiv 1 \bmod 3$, $n \equiv -1 \bmod 8$ and quadratic reciprocity it follows that $(\frac{\Delta}{n}) = -1$.

Now let first n be prime. Then $\mathrm{norm}(x) = x^{n+1} = x^{2^m}$, as we have seen in the proof of (10), and also $\mathrm{norm}(x) = xy = -1$. So $x^{2^m} = -1$. Multiplying this by $y^{2^{m-1}}$ and using that $xy = -1$ we find $x^{2^{m-1}} = -y^{2^{m-1}}$, i.e. $(e_{m-1} \bmod n) = 0$. This proves $\Rightarrow$.

Next suppose that $(e_{m-1} \bmod n) = 0$. Then $x^{2^{m-1}} + y^{2^{m-1}} = 0$, so $(x/y)^{2^{m-1}} = -1$. Let p be any prime dividing n. Then the ring $R' = R/pR$ is of the type described above, with n replaced by p. The element $x'/y' = (x/y \bmod pR)$ of R' satisfies $(x'/y')^{2^{m-1}} = -1 \neq 1$, so its multiplicative order is 2^m. Also, x'/y' is in the group H' belonging to R'. Hence (10) implies that 2^m divides $p - (\frac{\Delta}{p}) = p \pm 1$. Therefore $p \geq 2^m - 1$, but p divides $n = 2^m-1$, so $p = n$. This proves that n is prime, as required.

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 27 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,

and composite for all other $p < 44497$, see [28]. It is reasonable to conjecture that there are infinitely many Mersenne primes, and that in fact $\#\{m < x: 2^m - 1 \text{ is prime}\}/\log x$ tends to a finite non-zero limit for $x \to \infty$. It is an interesting problem to determine what this limit should be. GILLIES [8] gives a probabilistic argument leading to the value $2/\log 2$, but it is clearly in error since the same argument leads to a contradiction with the prime number theorem, cf. [10, §22.20].

Notice that the calculations required for the Lucas-Lehmer test can be done entirely within the ring $\mathbb{Z}/n\mathbb{Z}$, and that it is not necessary to calculate in R. Suppose, generally, that $\alpha \in R^*$, $\beta = \sigma(\alpha) \in R^*$, and that one is interested in the powers of the element α/β of H. Instead of calculating these directly in R, it is common to consider the *Lucas functions*

$$u_k(\alpha) = \sum_{j=0}^{k-1} \alpha^j \beta^{k-1-j}$$

$$= (\alpha^k - \beta^k)/(\alpha - \beta) \qquad (\text{if } \alpha - \beta \in R^*),$$

$$v_k(\alpha) = \alpha^k + \beta^k \qquad \text{for } k \geq 0.$$

These belong to $\mathbb{Z}/n\mathbb{Z}$, and usually provide the required information. They satisfy the recurrence relations

$$u_{k+2}(\alpha) = (\alpha+\beta)u_{k+1}(\alpha) - \alpha\beta \cdot u_k(\alpha),$$

$$v_{k+2}(\alpha) = (\alpha+\beta)v_{k+1}(\alpha) - \alpha\beta \cdot v_k(\alpha)$$

for $k \geq 0$, with coefficients $\alpha+\beta$, $\alpha\beta \in \mathbb{Z}/n\mathbb{Z}$. There exist several identities between the $u_k(\alpha)$ and $v_k(\alpha)$ which enable one to calculate $u_k(\alpha)$ and $v_k(\alpha)$ using $O(\log k)$ arithmetic operations modulo n, cf. [31, Section 12]. For example, in the situation of Theorem 10 we have $(e_i \bmod n) = v_{2^i}(x)$, and this is calculated using i-1 squarings and i-1 subtractions mod n.

The following theorem is the analogue of Theorem 5. As before, n denotes an odd integer > 1, and $R = (\mathbb{Z}/n\mathbb{Z})[X]/(X^2 - vX + w)$. We assume that $\Delta = v^2 - 4w$ is a unit in $\mathbb{Z}/n\mathbb{Z}$.

THEOREM 11. *Let*

$$n+1 = m_2 \cdot \prod_{j=1}^{t} h_j^{\ell_j}$$

where m_2 *and the* ℓ_j *are positive integers, and* $h_1, h_2, \ldots, h_t$ *are pairwise relatively prime integers* ≥ 2. *Let further* $c_1, c_2, \ldots, c_t$ *be positive integers such that the following conditions hold:*

(a_2) *every prime factor of* h_j *is* $\geq c_j$, *for* $1 \leq j \leq t$;

(b_2) *for each* j, $1 \leq j \leq t$, *there exists* $\alpha_j \in R^*$ *such that*

$$\alpha_j - \sigma(\alpha_j) \in R^*, \tag{11}$$

$$u_{n+1}(\alpha_j) = 0, \qquad \gcd(u_{(n+1)/h_j}(\alpha_j), n) = 1; \tag{12}$$

(c_2) $$n < (-1 + \prod_{j=1}^{t} c_j^{\ell_j})^2.$$

Then n *is prime.*

Notice that (11) is automatic if $\alpha_j = x+b$ for some $b \in \mathbb{Z}/n\mathbb{Z}$, since $(x-y)^2 = \Delta$ is a unit. The test of Theorem 11 is only useful for $(\frac{\Delta}{n}) = -1$, since for $(\frac{\Delta}{n}) = 1$ it is impossible to satisfy the conditions.

PROOF. The proof is completely analogous to the proof of Theorem 5. Let p be a prime dividing n, put $R' = R/pR$, and let H' belong to R' just as H belongs to R. By (11) and the definition of $u_k(\alpha_j)$, condition (12) means that the order of $(\alpha_j/\sigma(\alpha_j) \bmod pR) \in H'$ divides $n+1$, but not $(n+1)/h_j$. Hence this order is divisible by $r_j^{\ell_j}$ for some prime r_j dividing h_j. Using (10) and the coprimeness of the r_j one deduces that $p - (\frac{\Delta}{p})$ is divisible by $\prod_{j=1}^{t} r_j^{\ell_j}$, so $p \geq -1 + \prod_{j=1}^{t} c_j^{\ell_j}$ by (a_2). From (c_2) it now follows that n is prime.

The following theorem is a combination of Theorems 5 and 11, in which conditions (c_1), (c_2) are replaced by a much weaker one.

THEOREM 12. *Let the notations and the hypotheses be as in Theorems* 5 *and* 11, *but let* (c_1) *and* (c_2) *be replaced by*

$$n < (1 + \tfrac{1}{2} d_1 d_2) \cdot \max(1 + d_1, -1 + d_2) \tag{c}$$

where

$$d_1 = \prod_{i=1}^{s} b_i^{k_i}, \qquad d_2 = \prod_{j=1}^{t} c_j^{\ell_j}.$$

Assume moreover that $(\frac{\Delta}{n}) = -1$. *Then* n *is prime.*

PROOF. Suppose, to the contrary, that $n = p \cdot m$, with p prime and $m > 1$. By the proofs of Theorems 5 and 11, we have

$$p \equiv 1 \bmod \prod_{i=1}^{s} q_i^{k_i}, \qquad p \equiv \left(\frac{\Delta}{p}\right) \bmod \prod_{j=1}^{t} r_j^{\ell_j}$$

for certain primes $q_i \geq b_i$, $r_j \geq c_j$, and these congruences are also true with p replaced by n, since $\left(\frac{\Delta}{n}\right) = -1$. By $n = p \cdot m$, $\left(\frac{\Delta}{n}\right) = \left(\frac{\Delta}{p}\right) \cdot \left(\frac{\Delta}{m}\right)$, they remain valid with p replaced by m. One of $\left(\frac{\Delta}{p}\right)$, $\left(\frac{\Delta}{m}\right)$ equals 1, so one of p-1, m-1 is divisible by

$$\operatorname{lcm}\left(\prod_{i=1}^{s} q_i^{k_i}, \prod_{j=1}^{t} r_j^{\ell_j}\right)$$

which by $\gcd(n-1,n+1) = 2$ is at least

$$\frac{1}{2} \cdot \prod_{i=1}^{s} q_i^{k_i} \cdot \prod_{j=1}^{t} r_j^{\ell_j} \geq \frac{1}{2} \cdot d_1 \cdot d_2 .$$

The other one of p, m is at least

$$\max\left(1 + \prod_{i=1}^{s} q_i^{k_i}, -1 + \prod_{j=1}^{t} r_j^{\ell_j}\right) \geq \max(1 + d_1, -1 + d_2).$$

This gives a contradiction with (c), and proves the theorem.

See [26] for a primality testing algorithm based on variants of Theorems 5, 11 and 12. For 'quadratic' analogues to the Miller-Rabin test we refer to [3].

There is a different way to combine the n±1-tests, namely in the discovery of large *twin primes*. Let m be a large number whose complete 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 two largest known pairs are

$$694503810 \cdot 2^{2304} \pm 1 = 2^{2305} \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13^2 \cdot 593 \pm 1,$$

$$1159142985 \cdot 2^{2304} \pm 1 = 2^{2304} \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 25733 \pm 1,$$

which have 703 decimal digits, see [2].

It is also possible to use higher degree extensions of $\mathbb{Z}/n\mathbb{Z}$ in primality proofs. For these methods one needs information about the factorization of $\Phi_k(n)$, where Φ_k is the k-th cyclotomic polynomial:

$$\Phi_1(n) = n-1, \qquad \Phi_2(n) = n+1, \qquad \Phi_3(n) = n^2+n+1,$$

$$\Phi_4(n) = n^2+1, \qquad \Phi_6(n) = n^2-n+1.$$

The appearance of these numbers can be explained as before. If n is prime, then the multiplicative group $\mathbb{F}_{n^k}^*$ modulo the subgroup generated by the multiplicative groups of all proper subfields is cyclic of order $\Phi_k(n)$; alternatively, the subgroup H of $\mathbb{F}_{n^k}^*$ consisting of all elements of relative norm 1 to every proper subfield is cyclic of this order. These methods can also be combined with the n±1-methods discussed before, see [31, Sections 15&16] for references.

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

$$a^{n-1} \not\equiv 1 \bmod n, \qquad \gcd(a,n) = 1, \tag{13}$$

and applying Fermat's theorem that (13) 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 $a \cdot i \pmod n$ is a permutation of $\{1,2,\ldots,n-1\}$, 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 (13) tells us 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 defects. But it is worth mentioning that faster ways to calculate factorials or binomial coefficients modulo n can be helpful for factorization. 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 13. (SHAMIR). *There is an algorithm which 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

$$(2b+1)! = (2b+1)\cdot(2b)!,$$
$$(2b)! = (b!)^2\cdot\binom{2b}{b}$$

$O(\log a)$ times. To calculate the binomial coefficient $\binom{2b}{b}$ needed here, we remark that $\binom{2b}{b}$ 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 and tricks needed to bring it down to $O(\log n)$ we refer to SHAMIR's paper [27]. More practical factorization algorithms are discussed in the lecture of M. Voorhoeve, the thesis of L. MONIER [18], and the beautiful paper of R.K. GUY [9].

REFERENCES

[1] ADLEMAN, L. & K. MANDERS, *Diophantine complexity,* 17th Annual IEEE Symp. on Foundations of Computer Science (1976), 81-88.

[2] ATKIN, A.O.L. & N.W. RICKERT, *On a larger pair of twin primes,* Notices Amer. Math. Soc. 26 (1979), A-373 (#79T - A132).

[3] BAILLIE, R. & S.S. WAGSTAFF, JR., *Lucas pseudoprimes,* Math. Comp., to appear.

[4] BOURBAKI, N., *Algèbre,* Chapitres 1 à 3, Hermann, Paris 1970.

[5] BRILLHART, J., D.H. LEHMER & J.L. SELFRIDGE, *New primality criteria and factorizations of* $2^m \pm 1$, Math. Comp. 29 (1975), 620-647.

[6] COLE, F.N., *On the factoring of large numbers,* Bull. Amer. Math. Soc. 10 (1903/4), 134-137.

[7] DAVIS, M., *Hilbert's tenth problem is unsolvable,* Amer. Math. Monthly 80 (1973), 233-269.

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

[9] GUY, R.K., *How to factor a number,* Proc. Fifth Manitoba Conf. Numer. Math., Utilitas, Winnipeg (1975), 49-89.

[10] HARDY, G.H. & E.M. WRIGHT, *An introduction to the theory of numbers,* 4th ed., Oxford University Press, (1960).

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

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

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

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

[15] MATIJASEVIČ, YU.V., *Primes are non-negative values of a polynomial in 10 variables,* Zap. Naučn. Sem. Leningrad. Otdel. Mat. Inst. Steklov (LOMI) 68 (1977), 62-82 (Russian).

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

[17] MONIER, L., *Evaluation and comparison of two efficient probabilistic primality testing algorithms,* Theoret. Comput. Sci., to appear.

[18] MONIER, L., *Algorithmes de factorisation d'entiers,* Thèse de 3^{me} cycle, Orsay (1980).

[19] MONTGOMERY, H.L., *Topics in multiplicative number theory,* Lecture Notes in Mathematics 227, Springer-Verlag, Berlin (1971).

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

[21] POLLARD, J.M., *Theorems on factorization and primality testing,* Proc. Cambridge Philos. Soc. 76 (1974), 521-528.

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

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

[24] RABIN, M.O., *Probabilistic algorithm for testing primality,* unpublished, (1978). J. Number Theory 12 (1980), 128-138

[25] SCHÖNHAGE, A. & V. STRASSEN, *Schnelle Multiplikation grosser Zahlen,* Computing 7 (1971), 281-292.

[26] SELFRIDGE, J.L. & M.C. WUNDERLICH, *An efficient algorithm for testing large numbers for primality,* Proc. Fourth Manitoba Conf. Numer. Math., Utilitas, Winnipeg (1974), 109-120.

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

[28] SLOWINSKI, D., *Searching for the 27th Mersenne prime,* J. Recreational Math. 11 (1978/9), 258-261.

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

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

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