MATHEMATICS OF COMPUTATION
VOLUME 42, NUMBER 165
JANUARY 1984, PAGES 297-330

Primality Testing and Jacobi Sums

By H. Cohen and H. W. Lenstra, Jr.

Abstract. We present a theoretically and algorithmically simplified version of a primality testing algorithm that was recently invented by Adleman and Rumely. The new algorithm performs well in practice. It is the first primality test in existence that can routinely handle numbers of hundreds of decimal digits.

1. Introduction. Most modern methods to determine whether a given number n is prime are based on Fermat's theorem and its generalizations. This theorem asserts that

(1.1) if n is prime, then
$$a^n \equiv a \bmod n \quad \text{for all } a \in \mathbf{Z}.$$

Thus, to prove that a number is composite, it suffices to find a single integer a for which $a^n \not\equiv a \bmod n$; here $a^n \bmod n$ can be efficiently calculated by repeated squarings and multiplications modulo n.

To prove that n is prime, however, we need a converse to (1.1). Two problems present themselves in this connection.

The first problem is that the direct converse of (1.1) is false: the composite numbers

$$\begin{aligned} n &= 561 = 3 \cdot 11 \cdot 17, & n &= 1105 = 5 \cdot 13 \cdot 17, \\ n &= 1729 = 7 \cdot 13 \cdot 19, & n &= 2465 = 5 \cdot 17 \cdot 29 \end{aligned}$$

also have the property that $a^n \equiv a \bmod n$ for all $a \in \mathbf{Z}$. Such composite numbers are called *Carmichael numbers*, and there are probably infinitely many of them.

The second problem is that even if the converse of (1.1) were true, it would not help us much, since checking all integers a $(\bmod n)$ is not computationally feasible, even for moderately sized n.

To solve the first problem we replace (1.1) by a stronger assertion. We discuss two ways to do this.

The first depends on the *Jacobi symbol* $(\frac{a}{n})$, which is defined for a, $n \in \mathbf{Z}$, n positive, $\gcd(2a,n) = 1$; see [5, Section 9]. It can be calculated efficiently by means of the quadratic reciprocity law. From the definition of $(\frac{a}{n})$ it follows that

(1.2) if n is an odd prime, then
$$a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) = \pm 1 \bmod n \quad \text{for all } a \in \mathbf{Z} \text{ with } \gcd(a,n) = 1.$$

Received October 25, 1982; revised May 9, 1983. Reprint requests to the second author.
1980 *Mathematics Subject Classification*. Primary 10A25, 10-04, 12C20.
Key words and phrases. Primality testing, Jacobi sum.

The converse of (1.2) is also true [14], [23]. More precisely, if n is odd and composite, $n > 1$, then the congruence in (1.2) is valid for at most half of all $a \pmod{n}$ with $\gcd(a,n) = 1$.

Another strengthening of Fermat's theorem that admits a converse reads as follows:

(1.3) if n is prime, then for any commutative ring R we have

$$(a+b)^n \equiv a^n + b^n \bmod nR \quad \text{for all } a,b \in R.$$

Here nR denotes the ideal $\{x + x + \cdots + x \ (n \text{ terms}) \colon x \in R\}$ of R. To prove (1.3) one just observes that the binomial coefficients $\binom{n}{i}$, $0 < i < n$, are divisible by n if n is prime. For $R = \mathbf{Z}$, we obtain (1.1) from (1.3) by putting $b = 1$ and using induction on a.

It can be shown that the converse of (1.3) is also true: if $n > 1$, and the congruence in (1.3) is valid for all commutative rings R and all $a,b \in R$, then n is prime. It suffices, in fact, to take $R = \mathbf{Z}[X]$, $a = X$, $b = 1$.

The primality test that we shall describe in this paper combines (1.2) and (1.3): the congruences on which our test is based are obtained from (1.3), and they generalize (1.2).

We are still faced with the second problem: it is not computationally feasible to check the congruence in (1.2) for all $a \pmod{n}$ with $\gcd(a,n) = 1$, nor to check the congruence in (1.3) for all R, a, b.

Several methods have been proposed to get around this problem. The first is to sacrifice certainty: if n passes the test in (1.2) for 100 randomly chosen values $a \in \{1, 2, \ldots, n-1\}$, then it is overwhelmingly likely that n is prime. For an even better test of this nature, due to Miller and Rabin, we refer to [19], [21], [8, p. 379].

The second method relies on future developments in analytic number theory: if the generalized Riemann hypothesis is true, and n is an odd integer > 1 that passes the test in (1.2) for all primes a not dividing n with $a \leqslant 70 \cdot (\log n)^2$, then n is a prime number (cf. [19], [24]). But even if the generalized Riemann hypothesis were proved, the practical value of this method would be questionable. For a typical 100-digit number this method is approximately 500 times as slow as the algorithm described in this paper, although asymptotically it is faster.

The final method is presently the only one that leads to rigorous primality proofs. It consists of subjecting n to a series of tests, similar to those in (1.2) and (1.3), with the following two properties. First, if n is prime then it passes the tests. Secondly, if n passes the tests, then information is obtained about the possible divisors of n. This information should eventually lead to the conclusion that 1 and n are the only divisors of n, so that n is prime.

To describe the type of information that is obtained, we let H be a group, and ψ a map from the set of divisors of n to H with the property that $\psi(rr') = \psi(r)\psi(r')$ if rr' divides n. If n passes the tests, then it follows that for suitable choices of H and ψ we have

(1.4) $\psi(r)$ is a *power* of $\psi(n)$, for every divisor r of n.

Thus it appears that one is trying to prove n prime by means of the following trivial primality criterion:

(1.5) an integer $n > 1$ is prime if and only if all divisors of n are powers of n.

The above general description applies in particular to the tests of Lucas and Lehmer, improved by Brillhart, Lehmer and Selfridge [2] and generalized by Williams (see [26] for references). In these tests one takes $H = (\mathbf{Z}/s\mathbf{Z})^*$, the group of units of $\mathbf{Z}/s\mathbf{Z}$, where s is an integer that is built up from known prime divisors of $n^t - 1$ for $t = 1,2,3,4,6$, and one puts $\psi(r) = (r \bmod s)$ for r dividing n. If (1.4) is true for this choice of H and ψ, and s is sufficiently large, e.g. $s > n^{1/2}$, then it is easy to find all divisors of n and in particular to decide whether n is prime. In [16, Section 8] it is shown how larger values of t can be used. For a discussion of these tests from the point of view of algebraic number theory we refer to [17]; here H arises as the Galois group of a suitable extension of the field $\mathbf{Q}$ of rational numbers, and ψ is the Artin symbol.

The primality test that was recently invented by Adleman and Rumely [1, Section 4] also fits the above description, although this may not be clear from the way it is formulated in [1]. In this algorithm one tests a collection of congruences involving Jacobi sums in cyclotomic rings. Using the higher reciprocity laws from algebraic number theory, one shows that any n satisfying all these congruences also satisfies (1.4), with $H = (\mathbf{Z}/s\mathbf{Z})^*$, $\psi(r) = (r \bmod s)$ for an auxiliary number s that is coprime to n. This number s is a squarefree integer exceeding $n^{1/2}$, and it is selected in such a way that

$$a^t \equiv 1 \bmod s \quad \text{for all } a \in \mathbf{Z} \text{ with } \gcd(a,s) = 1,$$

where t is a relatively small squarefree positive integer.

In this paper we present a theoretically and algorithmically simplified version of the test of Adleman and Rumely. The theoretical simplification is achieved, as in [16], by considering Gauss sums instead of Jacobi sums. This allows us to bypass the higher reciprocity laws that were used in [1]. Our approach has the additional advantage of working for nonsquarefree values of t and s as well.

From an algorithmic point of view the Gauss sums appearing in our test are distinctly inferior to the Jacobi sums from [1], since the latter belong to much smaller rings. For this reason it is important to reformulate our test in terms of Jacobi sums. This is done with the help of techniques that are familiar from the theory of cyclotomic fields. The reformulation results in congruences involving Jacobi sums that are simpler to test than the congruences appearing in [1].

It will be seen that assertions of the form (1.4) play an important role in this paper. The choice $H = (\mathbf{Z}/s\mathbf{Z})^*$, $\psi(r) = (r \bmod s)$ was already mentioned. Further, we shall consider $H = \mathbf{C}^*$, the multiplicative group of nonzero complex numbers, and ψ equal to a character, as defined in Section 6. Finally, for several small primes p we shall take $H = \mathbf{Z}_p^*$, the group of p-adic units, discussed in Section 5; in this case ψ is defined by $\psi(r) = r^{p-1}$.

W. G. Dubuque programmed the test of Adleman and Rumely in Maclisp for a DEC KL-10 computer at the Massachusetts Institute of Technology. He used it to prove the primality of a 62-digit number in 6 hours. This does not compare favorably with the older tests discussed by Williams [26]. In fact, Williams never found a prime number of this size that took more than 20 minutes to prove prime on an Amdahl 470-V7 computer. On the other hand, these older tests are slower for sufficiently large n. It should also be taken into account that Dubuque's implementation uses the standard multiprecision routines provided in Maclisp, which is certainly not the most efficient means possible.

Our algorithm has been implemented on the CDC Cyber 170-750 computer system at the SARA computer center in Amsterdam. Two programs have been written, one in Pascal and the other in Fortran; both programs make use of multiprecision routines in Compass. The Pascal program is the first primality testing program in existence that can routinely handle numbers of up to 100 decimal digits, and it does so within approximately 45 seconds. The Fortran program can deal with numbers of up to 200 decimal digits, and it does so within approximately 10 minutes.

The algorithm in this paper has been designed for optimal efficiency in practice. It is, however, difficult to establish a rigorous upper bound for the running time. The running time of the algorithm in [1, Section 4] has been analyzed by Pomerance and Odlyzko [1, Theorems 1 and 3]. They proved that, for each $n > e^{c}$, the algorithm terminates within $O(k(\log n)^{c \log\log\log n})$ steps with probability at least $1 - 2^{-k}$, for every $k \geqslant 1$; here c is an absolute, effectively computable constant. The same upper bound can be shown to hold for a suitable version of our algorithm, cf. (11.6)(b). For another version an $O((\log n)^{c \log\log\log n})$ upper bound can be rigorously established if the truth of the generalized Riemann hypothesis is assumed. We do not go into the details of this analysis since there exists a different algorithm for which this upper bound can be proved without any unproved assumption. This algorithm, also due to Adleman and Rumely, is described in [1, Section 5], and a simplified version in [16, Section 5]. It is, however, not of practical importance.

The present paper draws upon a number of techniques from algebra and number theory that have not traditionally been used in primality testing. We have therefore attempted to keep the exposition as self-contained as possible. The contents of the paper are as follows.

A brief outline of our algorithm, in three stages, is given in Section 2. Section 3 is devoted to the last stage, and Section 4 to the first. The central stage occupies Sections 5 to 11. In Sections 5 and 6 we collect the properties of p-adic numbers and characters that we need. In Section 7 we show how Gauss sums can be used to generalize the test in (1.2). The reformulation in terms of Jacobi sums occupies Sections 8 and 9. In Section 10 we shall see how algorithms related to finite fields lead to additional improvements, under certain conditions. Section 11, finally, describes the central stage of the primality testing algorithm. A detailed description of the entire algorithm, from a computational point of view, is contained in Section 12. The actual implementation is discussed in Section 13.

By $\mathbf{Z}$, $\mathbf{Z}_p$, $\mathbf{Q}$, $\mathbf{C}$ we denote the ring of integers, the ring of p-adic integers (see Section 5), the field of rational numbers, and the field of complex numbers, respectively. The number of times that a prime number p appears in m is denoted by $v_p(m)$, for $m \in \mathbf{Z}$, $m \neq 0$ (cf. Section 5). By $r|m$ we mean that r is a divisor of m, i.e.

a *positive* integer dividing m. Rings are supposed to be commutative with 1, and subrings have the same 1. The group of units of a ring R is denoted by R^*. For ζ_m, U_m, σ_χ, G, see Section 7.

2. Outline of the Algorithm. We give a brief description of our primality testing algorithm in three stages. Let n be the integer to be tested for primality, and assume that $n > 1$.

Stage 1. Select two positive integers t and s with the following properties:

(2.1) t is "small" (see Section 4),

(2.2) $s > n^{1/2}$ (or $s > n^{1/3}$, see Section 3),

(2.3) $a^t \equiv 1 \bmod s$ for all $a \in \mathbf{Z}$ with $\gcd(a,s) = 1$,

(2.4) the complete prime factorizations of t and s are known.

See Section 4 for more details concerning the selection of t and s.

Continuing Stage 1, check that $\gcd(st,n) = 1$ using the Euclidean algorithm; if $\gcd(st,n) \neq 1$, then a prime factor of n is found, by (2.4), and the algorithm halts.

Stage 2. Subject n to a series of tests similar to the test in (1.2). If it fails to pass any of these tests, then n is composite and the algorithm halts. Otherwise, attempt to prove the following assertion, using the information obtained from the tests:

(2.5) for every divisor r of n there exists $i \in \{0,1,\ldots,t-1\}$ such that $r \equiv n^i \bmod s$.

The theoretical possibility exists that this attempt is unsuccessful within a reasonable time limit. In this case one may tell the algorithm to halt with the message that it has not been able to decide whether n is prime or not.

A more detailed description of Stage 2 is found in Section 11.

Stage 3. If (2.5) has been proved, use (2.5) and (2.2) to factor n completely, and hence to decide whether n is prime or not. In Section 3 we shall see how this can be done.

Remark. From the description of Stage 3 one should not get the impression that the algorithm is helpful in factoring n if n is composite, since practically all composite numbers will be eliminated in Stage 1 or Stage 2.

3. The Final Stage of the Algorithm. Suppose that (2.5) has been proved and that $s > n^{1/2}$. To factor n completely it suffices to find all divisors $r \leqslant n^{1/2}$ of n. Such a divisor satisfies $r < s$ and is, by (2.5), congruent to $n^i \bmod s$ for some $i \in \{0, 1,\ldots,t-1\}$. Hence, if we determine r_i by $r_i \equiv n^i \bmod s$ and $0 \leqslant r_i < s$, for $0 \leqslant i < t$, and check which of the r_i divide n, then we obtain the complete prime factorization of n.

Next suppose that, besides (2.5), one knows only the weaker version $s > n^{1/3}$ of (2.2). Then the prime factorization of n is found by applying the following result to $d = r_i$, for $i = 0,1,\ldots,t-1$; notice that $\gcd(r_i,s) = 1$ since in Stage 1 we checked that $\gcd(st,n) = 1$.

(3.1) THEOREM. *Let d, s, n be positive integers satisfying* $\gcd(d,s) = 1$ *and* $s > n^{1/3}$. *Then there exist at most* 11 *divisors of n that are congruent to d modulo s, and there is an efficient algorithm determining all these divisors.*

We refer to [15] for a proof of this theorem and for a description of the algorithm. The running time of this algorithm, measured in bit operations, is $O((\log n)^3)$, if $d < s < n$. Its practical value remains to be tested.

4. Selection of Auxiliary Numbers. For a positive integer t we define

$$\begin{aligned} e(t) &= 2 && \text{if } t \text{ is odd,} \\ e(t) &= 2 \cdot \prod_{q \text{ prime},\, q-1 \mid t} q^{v_q(t)+1} && \text{if } t \text{ is even,} \end{aligned}$$

with $v_q(t)$ as defined in the introduction. We recall the condition (2.3) to be satisfied by the auxiliary numbers t and s:

$$(2.3) \qquad a^t \equiv 1 \bmod s \quad \text{for all } a \in \mathbf{Z} \text{ with } \gcd(a,s) = 1.$$

(4.1) PROPOSITION. *Let t and s be positive integers. Then condition* (2.3) *holds if and only if s divides $e(t)$.*

Proof. For odd t this is proved by taking $a = -1$ in (2.3). Let now t be even. We may clearly assume that s is a prime power: $s = q^m$, with q prime and $m \geqslant 1$. In this case the proposition easily follows from the following well-known result [5, Section 5]. If q is odd or $m \leqslant 2$, then $(\mathbf{Z}/q^m\mathbf{Z})^*$ is a cyclic group of order $(q-1)q^{m-1}$; and if $m \geqslant 3$, then $(\mathbf{Z}/2^m\mathbf{Z})^*$ is the direct sum of a group of order two and a cyclic group of order 2^{m-2}. This proves (4.1).

TABLE 1. *Values of $e(t)$*

t	$e(t)$
2	24
$12 = 2^2 \cdot 3$	65520
$60 = 2^2 \cdot 3 \cdot 5$	$6.814 \cdot 10^9$
$180 = 2^2 \cdot 3^2 \cdot 5$	$2.601 \cdot 10^{15}$
$840 = 2^3 \cdot 3 \cdot 5 \cdot 7$	$8.644 \cdot 10^{24}$
$1260 = 2^2 \cdot 3^2 \cdot 5 \cdot 7$	$1.147 \cdot 10^{31}$
$1680 = 2^4 \cdot 3 \cdot 5 \cdot 7$	$2.697 \cdot 10^{33}$
$2520 = 2^3 \cdot 3^2 \cdot 5 \cdot 7$	$4.866 \cdot 10^{40}$
$5040 = 2^4 \cdot 3^2 \cdot 5 \cdot 7$	$1.532 \cdot 10^{52}$
$15120 = 2^4 \cdot 3^3 \cdot 5 \cdot 7$	$2.254 \cdot 10^{79}$
$55440 = 2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$	$4.920 \cdot 10^{106}$
$110880 = 2^5 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$	$2.109 \cdot 10^{137}$
$720720 = 2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13$	$2.599 \cdot 10^{237}$
$1441440 = 2^5 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13$	$1.669 \cdot 10^{301}$
$4324320 = 2^5 \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$	$7.928 \cdot 10^{455}$
$24504480 = 2^5 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17$	$4.795 \cdot 10^{656}$
$73513440 = 2^5 \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17$	$7.082 \cdot 10^{966}$
$367567200 = 2^5 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 17$	$6.208 \cdot 10^{1501}$
$1396755360 = 2^5 \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19$	$4.016 \cdot 10^{1913}$
$6983776800 = 2^5 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19$	$7.471 \cdot 10^{3010}$

(4.2) We now describe the selection of t and s in Stage 1.

First one chooses a positive integer t for which $e(t) > n^{1/2}$ or $e(t) > n^{1/3}$, depending on which algorithm is used in Stage 3. In theory this can be done by trying $t = 1,2,3,\ldots$ in succession. In practice it is more convenient to use a table which is computed once and for all, and which gives the values of $e(t)$ for some well-chosen integers t. An example is provided by Table 1; the values of $e(t)$ are rounded off downwards in this table. From Table 1 we see that for $n < 10^{100}$ we can take $t = 5040$ if the naive algorithm in Stage 3 is used, while $t = 1680$ suffices if we employ the algorithm from (3.1).

For the value of t that is chosen we write down the complete prime factorization of $e(t)$. This is done by listing all primes q for which $q - 1$ divides t, together with the exponent $m(q)$ of q in $e(t)$; this exponent can be read from the definition of $e(t)$. It is also convenient to write down the prime factorizations of the numbers $q - 1$, since these are needed in Stage 2. For $t = 5040 = 2^4 \cdot 3^2 \cdot 5 \cdot 7$ all this has been done in Table 2. This table is, of course, a byproduct of the computations leading to Table 1.

TABLE 2. *The prime factorization of* $e(5040)$, $5040 = 2^4 \cdot 3^2 \cdot 5 \cdot 7$

$q^{m(q)}$	$q-1$	$q^{m(q)}$	$q-1$	$q^{m(q)}$	$q-1$
2^6	1	31	$2 \cdot 3 \cdot 5$	181	$2^2 \cdot 3^2 \cdot 5$
3^3	2	37	$2^2 \cdot 3^2$	211	$2 \cdot 3 \cdot 5 \cdot 7$
5^2	2^2	41	$2^3 \cdot 5$	241	$2^4 \cdot 3 \cdot 5$
7^2	$2 \cdot 3$	43	$2 \cdot 3 \cdot 7$	281	$2^3 \cdot 5 \cdot 7$
11	$2 \cdot 5$	61	$2^2 \cdot 3 \cdot 5$	337	$2^4 \cdot 3 \cdot 7$
13	$2^2 \cdot 3$	71	$2 \cdot 5 \cdot 7$	421	$2^2 \cdot 3 \cdot 5 \cdot 7$
17	2^4	73	$2^3 \cdot 3^2$	631	$2 \cdot 3^2 \cdot 5 \cdot 7$
19	$2 \cdot 3^2$	113	$2^4 \cdot 7$	1009	$2^4 \cdot 3^2 \cdot 7$
29	$2^2 \cdot 7$	127	$2 \cdot 3^2 \cdot 7$	2521	$2^3 \cdot 3^2 \cdot 5 \cdot 7$

Next we have to choose s. One way to do this is as follows. First put $s = e(t)$. If s has a prime power factor $q^{m(q)}$ for which $s/q^{m(q)}$ is still larger than $n^{1/2}$ (or $n^{1/3}$, depending on Stage 3), then we choose such a $q^{m(q)}$ with q as large as possible, and we replace s by $s/q^{m(q)}$. This is repeated until it is no longer possible.

We describe a better way of choosing s. Write $e(t) = \prod_{q \in E} q^{m(q)}$. We restrict to divisors s of $e(t)$ of the form $s = \prod_{q \in S} q^{m(q)}$ with $S \subset E$. As we shall see in Section 11, each $q \in S$ gives rise to a certain amount of work in Stage 2 of the algorithm. The running time needed by this amount of work is proportional to a number $w(q)$ depending on q. The numbers $w(q)$ depend on the implementation of Stage 2 and they are best determined empirically. For a certain naive implementation a good approximation to $w(q)$ is given by

$$\sum_{p \text{ prime},\, p|q-1} \varphi\left(p^{v_p(q-1)}\right)^2,$$

where φ denotes Euler's function [4, Section 5.5]. In order to minimize the running time we should now choose S such that $\sum_{q \in S} w(q)$ is as small as possible, subject to the condition that $s > n^{1/2}$ or $n^{1/3}$. Putting $S' = E - S$, we see that we have to maximize $\Sigma_{q \in S'} w(q)$ subject to the condition that $\Sigma_{q \in S'} \log(q^{m(q)}) < \log(e(t)) - (\frac{1}{2}$ or $\frac{1}{3})\log n$. This is an instance of the *knapsack problem*. A well-known approximate solution method for this problem leads to the following way of selecting s. First put $s = e(t)$. If s has a prime power factor $q^{m(q)}$ for which $s/q^{m(q)}$ is still larger than $n^{1/2}$ or $n^{1/3}$, then we choose such a $q^{m(q)}$ with $w(q)/\log(q^{m(q)})$ as large as possible, and we replace s by $s/q^{m(q)}$. This is repeated until it is no longer possible. For more subtle methods to solve the knapsack problem we refer to [18].

The final value for s is a divisor of $e(t)$, so by (4.1) condition (2.3) is satisfied. Conditions (2.2) and (2.4) are also satisfied, and below we shall see to which extent (2.1) holds. This finishes the description of algorithm (4.2).

We now discuss how small t can be chosen such that we have $e(t) > n^{1/2}$ or $n^{1/3}$. From

$$e(t) \leqslant 2t \cdot \prod_{d|t} (d + 1)$$

and elementary estimates for the divisor function [4, Theorem 317] we obtain the following lower bound:

$$t > (\log n)^{(1-\varepsilon)(\log\log\log n)/\log 2}$$

for all $\varepsilon > 0$ and all n exceeding a bound depending on ε. The following theorem shows that this result is best possible, apart from the value of the constant in the exponent.

(4.3) THEOREM. *There exists an effectively computable positive constant c such that for all $n > e^e$ there is a positive integer t satisfying*

$$t < (\log n)^{c \log\log\log n} \quad \text{and} \quad e(t) > n^{1/2}.$$

This is a sharpening of a result of Prachar [20] that is due to Pomerance and Odlyzko. For the proof we refer to [1, Section 6]. Pomerance and Odlyzko proved that t can even be chosen squarefree; this was necessary for the test of Adleman and Rumely [1].

5. p-adic Numbers. Let p be a prime number. In this section we recall, without proofs, a few basic properties of *p-adic numbers*. For a fuller treatment we refer to [22, Chapitre II] and [6].

A *p-adic integer* is a sequence $(a_i \bmod p^i)_{i=1}^{\infty}$, with $(a_i \bmod p^i) \in \mathbf{Z}/p^i\mathbf{Z}$, such that $a_{i+1} \equiv a_i \bmod p^i$ for all $i \geqslant 1$. The set of p-adic integers forms a ring, denoted by $\mathbf{Z}_p$, under coordinatewise addition and multiplication. We view $\mathbf{Z}$ as a subring of $\mathbf{Z}_p$, by identifying $a \in \mathbf{Z}$ with $(a \bmod p^i)_{i=1}^{\infty} \in \mathbf{Z}_p$.

Let $m \in \mathbf{Z}$, $m \geqslant 1$. The map $\mathbf{Z}_p \to \mathbf{Z}/p^m\mathbf{Z}$ that sends $(a_i \bmod p^i)_{i=1}^{\infty}$ to $(a_m \bmod p^m)$ is a surjective ring homomorphism with kernel equal to $p^m\mathbf{Z}_p$. This shows that $\mathbf{Z}_p/p^m\mathbf{Z}_p \simeq \mathbf{Z}/p^m\mathbf{Z}$, so p-adic integers, when taken modulo p^m, yield ordinary integers modulo p^m.

Let E be a finite abelian group of p-power order. For $a = (a_i \bmod p^i)_{i=1}^{\infty} \in \mathbf{Z}_p$ and $\zeta \in E$ the element ζ^{a_m} of E does not depend on m, for m sufficiently large, and we denote it by ζ^a. This operation of $\mathbf{Z}_p$ on E satisfies the familiar rules

$$(\zeta\eta)^a = \zeta^a\eta^a, \qquad \zeta^{a+b} = \zeta^a\zeta^b,$$
$$\zeta^{ab} = (\zeta^a)^b, \qquad \zeta^1 = \zeta,$$

for $\zeta,\eta \in E$, $a,b \in \mathbf{Z}_p$, so it makes E into a *module* over $\mathbf{Z}_p$; see [10, Chapter III, Section 1].

A p-adic integer a is a *unit* of $\mathbf{Z}_p$ if and only if $a \not\equiv 0 \bmod p$, so $\mathbf{Z}_p^* = \mathbf{Z}_p - p\mathbf{Z}_p$. Every nonzero p-adic integer a can be written in a unique way as $a = p^m u$ with $m \in \mathbf{Z}$, $m \geqslant 0$ and $u \in \mathbf{Z}_p^*$; we write in this case $v_p(a) = m$, and we put $v_p(0) = \infty$. This extends the function v_p that was defined on $\mathbf{Z} - \{0\}$ in the introduction.

The set $1 + p\mathbf{Z}_p = \{a \in \mathbf{Z}_p\colon a \equiv 1 \bmod p\}$ is a subgroup of $\mathbf{Z}_p^*$. Let $a = (a_i)_{i=1}^{\infty} \in 1 + p\mathbf{Z}_p$. Then each a_i has p-power order in $(\mathbf{Z}/p^i\mathbf{Z})^*$, so for $x \in \mathbf{Z}_p$ we can define $a^x = (a_i^x)_{i=1}^{\infty}$. This makes $1 + p\mathbf{Z}_p$ into a $\mathbf{Z}_p$-module. Writing $a^{\mathbf{Z}_p} = \{a^x\colon x \in \mathbf{Z}_p\}$, we have

$$a^{\mathbf{Z}_p} = 1 + p^m\mathbf{Z}_p \text{ for } m = v_p(a-1), \text{ provided that } m \geqslant 1, \text{ and } m \geqslant 2 \text{ in the case } p = 2. \tag{5.1}$$

There are group isomorphisms

$$\mathbf{Z}_p^* \simeq (\mathbf{Z}/(p-1)\mathbf{Z}) \times (1 + p\mathbf{Z}_p) \simeq (\mathbf{Z}/(p-1)\mathbf{Z}) \times \mathbf{Z}_p \quad \text{if } p \geqslant 3, \tag{5.2}$$

$$\mathbf{Z}_2^* = 1 + 2\mathbf{Z}_2 \simeq \{1,-1\} \times (1 + 4\mathbf{Z}_2) \simeq (\mathbf{Z}/2\mathbf{Z}) \times \mathbf{Z}_2; \tag{5.3}$$

see [22, Section II.3], [6, Chapter 15, Section 7].

6. Characters. Let q be a prime number. A *character* χ modulo q is a group homomorphism from $(\mathbf{Z}/q\mathbf{Z})^*$ to $\mathbf{C}^*$. We extend such a character to a map $\mathbf{Z}/q\mathbf{Z} \to \mathbf{C}$ by $\chi(0 \bmod q) = 0$, and we put $\chi(a) = \chi(a \bmod q)$ for $a \in \mathbf{Z}$. The set of all characters modulo q forms a group under multiplication. We denote this group by X_q.

It is well known that $(\mathbf{Z}/q\mathbf{Z})^*$ is cyclic of order $q - 1$. Let a generator g be chosen. Mapping χ to $\chi(g)$, we obtain an isomorphism between X_q and the group of $(q-1)$st roots of unity. This implies easily:

$$\text{if } x,y \in (\mathbf{Z}/q\mathbf{Z})^* \text{ are such that } \chi(x) = \chi(y) \text{ for all } \chi \in X_q, \text{ then } x = y. \tag{6.1}$$

Let $q - 1 = \prod_{p \text{ prime}} p^{k(p)}$ be the prime factorization of $q - 1$, with $k(p) = v_p(q-1)$. For each prime p with $k(p) \geqslant 1$ we choose a character $\chi_{p,q} \in X_q$ of order $p^{k(p)}$; such a character is obtained by putting $\chi_{p,q}(g) = \zeta_{p^{k(p)}}$, a primitive $p^{k(p)}$th root of unity. We write

$$Y_q = \{\chi_{p,q}\colon p \text{ prime}, p \mid q-1\}. \tag{6.2}$$

It is easy to see that Y_q generates the group X_q.

(6.3) THEOREM. *Let t and s be positive integers satisfying* (2.3), *and let n be an integer satisfying $n > 1$ and* $\gcd(n,st) = 1$. *Write*

$$Y_s = \bigcup_{q \mid s,\, q \text{ prime}} Y_q$$

with Y_q as in (6.2). *Assume that every prime $p | t$ satisfies the following condition*:

(6.4) *for every prime divisor r of n there exists $l_p(r) \in \mathbf{Z}_p$ such that $r^{p-1} = (n^{p-1})^{l_p(r)}$ in the group $1 + p\mathbf{Z}_p$.*

Assume moreover that every $\chi \in Y_s$ satisfies the following condition:

(6.5) *for every prime divisor r of n we have $\chi(r) = \chi(n)^{l_p(r)}$ with $l_p(r)$ as in* (6.4), *where p is such that the order of χ is a power of p.*

Then (2.5) *is satisfied, i.e. for every divisor r of n there exists $i \in \{0, 1, \ldots, t-1\}$ such that $r \equiv n^i \bmod s$.*

Remark. Notice that $l_p(r)$ in (6.4) is uniquely determined if it exists, by (5.2), (5.3). In fact, we have $l_p(r) = \log_p r / \log_p n$, where $\log_p$ denotes the p-adic logarithm [25, Section 5.1]. In (6.5) it is meaningful to speak about $l_p(r)$, since if $\chi = \chi_{p,q}$, then p divides t, by (4.1).

Proof. We have $n^t \equiv 1 \bmod s$, by (2.3), so it suffices to consider *prime* divisors r of n. Fix such an r, and let $l(r)$ be a nonnegative integer satisfying

$$l(r) \equiv l_p(r) \bmod p^{h(p)} \quad \text{for every prime } p | t;$$

here $h(p)$ denotes a positive integer that is chosen sufficiently large for the rest of the argument to be valid. In particular, we assume that the order of every $\chi_{p,q} \in Y_s$ divides $p^{h(p)}$. By (6.5) we then have

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

for every $\chi_{p,q} \in Y_s$. Let now $q | s$ be a fixed prime. Then the characters $\chi_{p,q}$ generate X_q, so it follows that $\chi(r) = \chi(n^{l(r)})$ for all $\chi \in X_q$. By (6.1) this implies that $r \equiv n^{l(r)} \bmod q$. Put $m(q) = v_q(s)$. We claim that

$$r \equiv n^{l(r)} \bmod q^{m(q)}. \tag{6.6}$$

If $m(q) = 1$, this has just been proved. Suppose therefore that $m(q) \geqslant 2$. Then q divides t, by (4.1) and the definition of $e(t)$, so (6.4) holds for $p = q$. This yields

$$r^{q-1} = (n^{q-1})^{l_q(r)} \equiv (n^{q-1})^{l(r)} \bmod q^{m(q)};$$

here $h(q)$ is assumed to be so large that $(n^{q-1})^{q^{h(q)}} \equiv 1 \bmod q^{m(q)}$. We now know that the q-adic integer $a = r \cdot n^{-l(r)}$ satisfies

$$a \equiv 1 \bmod q, \qquad a^{q-1} \equiv 1 \bmod q^{m(q)}.$$

The latter congruence implies that the multiplicative order of a modulo $q^{m(q)}$ divides $q - 1$, the former that it is a power of q. It follows that this order equals 1, so $a \equiv 1 \bmod q^{m(q)}$. This proves (6.6).

Since (6.6) holds for any prime q dividing s, we may conclude that $r \equiv n^{l(r)} \bmod s$. Here $l(r)$ may be reduced modulo t, since $n^t \equiv 1 \bmod s$ by (2.3). This proves (6.3).

(6.7) *Remark.* If (6.4) holds, then clearly for *every* divisor r of n there exists $l_p(r) \in \mathbf{Z}_p$ with $r^{p-1} = (n^{p-1})^{l_p(r)}$, and we have

$$l_p(r_1 r_2) = l_p(r_1) + l_p(r_2) \quad \text{for } r_1 r_2 \text{ dividing } n, \quad l_p(n) = 1.$$

7. Gauss Sums. For any positive integer m we denote by U_m the group of mth roots of unity in $\mathbf{C}$, and by ζ_m a primitive mth root of unity; so ζ_m generates U_m.

In this section we fix a prime number q, a prime number p, and a positive integer k such that p^k divides $q - 1$. Further n is an integer with $n > 1$ and $\gcd(n, pq) = 1$.

We put $A = \mathbf{Z}[\zeta_{p^k},\zeta_q]$, the ring generated by ζ_{p^k} and ζ_q, and $K = \mathbf{Q}(\zeta_{p^k},\zeta_q)$, the field of fractions of A. We let B be the subring $A[1/q]$ of K. Every element of K has a unique representation

$$\sum_{0\leqslant i<(p-1)p^{k-1},\, 0\leqslant j<q-1} a_{ij}\zeta_{p^k}^i\zeta_q^j$$

with $a_{ij} \in \mathbf{Q}$, cf. [10, Chapter VIII, Section 3]. To multiply two such expressions one uses the rules

$$\zeta_{p^k}^{(p-1)p^{k-1}} = -\sum_{i=0}^{p-2}\zeta_{p^k}^{ip^{k-1}}, \qquad \zeta_q^{q-1} = -\sum_{j=0}^{q-2}\zeta_q^j.$$

Restricting the coefficients a_{ij} to $\mathbf{Z}$ one obtains the ring A. An element of K belongs to B if and only if the denominators of all of its coefficients a_{ij} are powers of q; and it belongs to the principal ideal nB of B if and only if, in addition, the numerators of these coefficients are divisible by n.

For $x \in \mathbf{Z}$, $x \not\equiv 0 \bmod p$, let σ_x be the field automorphism of K for which $\sigma_x(\zeta_{p^k}) = \zeta_{p^k}^x$ and $\sigma_x(\zeta_q) = \zeta_q$, cf. [10, Chapter VIII, Section 3]. Let

$$G = \{\sigma_x\colon 1 \leqslant x \leqslant p^k, x \not\equiv 0 \bmod p\}.$$

This is the Galois group of K over $\mathbf{Q}(\zeta_q)$. It is isomorphic to $(\mathbf{Z}/p^k\mathbf{Z})^*$, under an isomorphism mapping σ_x to $(x \bmod p^k)$. Denote by $\mathbf{Z}[G]$ the group algebra of G over $\mathbf{Z}$, see [10, Chapter V, Section 1]. For $u \in B^*$ and $\alpha = \sum_{\sigma\in G} n_\sigma\sigma \in \mathbf{Z}[G]$ we define $u^\alpha \in B^*$ by

$$u^\alpha = \prod_{\sigma\in G}\sigma(u)^{n_\sigma}.$$

This operation of $\mathbf{Z}[G]$ on B^* satisfies the rules

$$(uv)^\alpha = u^\alpha v^\alpha, \qquad u^{\alpha+\beta} = u^\alpha\cdot u^\beta,$$
$$u^{\alpha\beta} = (u^\alpha)^\beta, \qquad u^1 = u,$$

for $u,v \in B^*$, $\alpha,\beta \in \mathbf{Z}[G]$, $1 = \sigma_1 \in \mathbf{Z}[G]$; so it makes B^* into a module over $\mathbf{Z}[G]$.

Let χ be a character modulo q of order p^k. The *Gauss sum* $\tau(\chi)$ associated to χ is the element of A defined by

$$\tau(\chi) = \sum_{x=1}^{q-1}\chi(x)\zeta_q^x. \tag{7.1}$$

We have

$$\tau(\chi)\tau(\chi^{-1}) = \chi(-1)\cdot q, \tag{7.2}$$

see [25, Lemma 6.1(b)], [7, Chapitre 5, Proposition 7], so $\tau(\chi)^{-1} = \chi(-1)\tau(\chi^{-1})/q \in B$. This implies that $\tau(\chi) \in B^*$, so the expression $\tau(\chi)^{n-\sigma_n}$ in the following lemma makes sense.

(7.3) LEMMA. *If n is prime, then*

$$\tau(\chi)^{n-\sigma_n} \equiv \chi(n)^{-n} \bmod nB.$$

Proof. From (1.3) we obtain

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

and the lemma follows upon division by the unit $\chi(n)^n\tau(\chi)^{\sigma_n}$. This proves (7.3).

(7.4) This lemma will lead to the tests that were mentioned in Section 2, Stage 2. To see the connection with (1.2), we consider the case that χ is *quadratic*, i.e. has order $p^k = 2$. Then q is an odd prime, and χ is the Legendre symbol: $\chi(x) = (\frac{x}{q})$. From (7.2) we see that $\tau(\chi)^2 = a$, where $a = (\frac{-1}{q}) \cdot q$. The automorphism σ_n is the identity, so the congruence of the lemma is equivalent to $a^{(n-1)/2} \equiv (\frac{n}{q}) \bmod n$. This is the same as (1.2), since $(\frac{n}{q}) = (\frac{n}{n})$ by the quadratic reciprocity law, which can, in fact, be proved in this way.

We return to the general situation. We shall investigate what can, conversely, be said about n if the congruence in (7.3) is known to hold. For practical purposes it is important to build in some extra degrees of freedom, as expressed in the following corollary.

(7.5) COROLLARY. *If n is prime, then*

$$\tau(\chi)^{(n-\sigma_n)\beta} \equiv \chi(n)^{-n\beta} \bmod \mathfrak{n}$$

for any $\beta \in \mathbf{Z}[G]$ and any ideal $\mathfrak{n}$ of B with $n \in \mathfrak{n}$.

Proof. Raise the congruence in (7.3) to the power β; this is allowed because $\sigma[nB] = nB$ for all $\sigma \in G$. Next use that $nB \subset \mathfrak{n}$. This proves (7.5).

We shall make the following assumptions on β and $\mathfrak{n}$:

(7.6) $$\zeta_p^\beta \neq 1,$$

(7.7) $$\mathfrak{n} \cap \mathbf{Z} = n\mathbf{Z}, \qquad \sigma_n[\mathfrak{n}] = \mathfrak{n}.$$

The reader may think of $\beta = 1$, $\mathfrak{n} = nB$. If $\beta = \sum_x n_x\sigma_x \in \mathbf{Z}[G]$, then (7.6) is equivalent to

$$\sum_x n_x x \not\equiv 0 \bmod p.$$

The map sending ζ to ζ^β is an *automorphism* of the group U_{p^k}, if (7.6) holds. Condition (7.7) will be investigated in Section 10.

(7.8) THEOREM. *Let χ be a character modulo q of order p^k, and assume that*

(7.9) $\tau(\chi)^{(n-\sigma_n)\beta} \equiv \zeta \bmod \mathfrak{n}$ *for some $\zeta \in U_{p^k}$, some $\beta \in \mathbf{Z}[G]$ satisfying* (7.6) *and some ideal $\mathfrak{n}$ of B satisfying* (7.7).

Assume further that condition (6.4) *is satisfied. Then χ satisfies* (6.5), *i.e.*

$$\chi(r) = \chi(n)^{l_p(r)}$$

for every divisor r of n, with $l_p(r)$ as in (6.4) *and* (6.7).

Remark. For given β and $\mathfrak{n}$, the congruence (7.9) is true for at most one $\zeta \in U_{p^k}$; this follows from (7.17).

Proof. By (7.6) and $\gcd(n,p) = 1$ we can write $\zeta = \eta^{-n\beta}$ for some $\eta \in U_{p^k}$. Let $i \in \mathbf{Z}$, $i \geqslant 0$. We raise both sides of the congruence

$$(7.10) \qquad \tau(\chi)^{(n-\sigma_n)\beta} \equiv \eta^{-n\beta} \bmod \mathfrak{n}$$

to the power $\sum_{j=0}^{i-1} n^{i-1-j}\sigma_n^j$; this is allowed because $\sigma_n[\mathfrak{n}] = \mathfrak{n}$. Using that

$$(n - \sigma_n) \cdot \sum_{j=0}^{i-1} n^{i-1-j}\sigma_n^j = n^i - \sigma_n^i, \qquad \eta^{\sigma_n} = \eta^n$$

and writing $u = \tau(\chi)^\beta$, we find that

$$(7.11) \qquad u^{n^i - \sigma_n^i} \equiv \eta^{-in^i\beta} \bmod \mathfrak{n}$$

for every $i \in \mathbf{Z}$, $i \geqslant 0$. With $i = (p-1)p^k$ it follows that

$$(7.12) \qquad u^{n^{(p-1)p^k} - 1} \equiv 1 \bmod \mathfrak{n}.$$

Let now r be a *prime* divisor of n. Then we know from (7.5) that (7.10), with n, η, $\mathfrak{n}$ replaced by r, $\chi(r)$, rB, is true, so the same holds for (7.11). Taking $i = p - 1$, we obtain

$$(7.13) \qquad u^{r^{p-1} - \sigma_r^{p-1}} \equiv \chi(r)^{-(p-1)r^{p-1}\beta} \bmod rB.$$

We shall combine (7.11) and (7.13) modulo the ideal

$$\mathfrak{r} = rB + \mathfrak{n},$$

which contains both rB and $\mathfrak{n}$.

By (6.4), we have $r^{p-1} = (n^{p-1})^{l_p(r)}$ for some $l_p(r) \in \mathbf{Z}_p$. Choose $m \in \mathbf{Z}$, $m \geqslant 0$, such that

$$(7.14) \qquad m \equiv l_p(r) \bmod p^k.$$

From

$$r^{p-1} - n^{(p-1)m} = \left((n^{p-1})^{l_p(r)-m} - 1\right) \cdot n^{(p-1)m}$$

it then follows that

$$(7.15) \qquad v_p\left(r^{p-1} - n^{(p-1)m}\right) \geqslant v_p\left((n^{p-1})^{p^k} - 1\right),$$

and in particular, since the right-hand side exceeds k:

$$(7.16) \qquad r^{p-1} \equiv n^{(p-1)m} \bmod p^k, \qquad \sigma_r^{p-1} = \sigma_n^{(p-1)m}.$$

We apply (7.11) to $i = (p-1)m$, and divide it by (7.13); this is allowed since both sides of (7.13) are units in B. Using (7.16), we then find that

$$u^{n^{(p-1)m} - r^{p-1}} \equiv \left(\chi(r)\eta^{-m}\right)^{(p-1)r^{p-1}\beta} \bmod \mathfrak{r}.$$

Let a be the largest divisor of $n^{(p-1)p^k} - 1$ that is not divisible by p. If we raise the congruence to the power a, then by (7.15) the exponent on the left becomes divisible by $n^{(p-1)p^k} - 1$, so by (7.12) we obtain

$$1 \equiv \left(\chi(r)\eta^{-m}\right)^{(p-1)r^{p-1}\beta a} \bmod \mathfrak{r}.$$

Assume, for the moment, the following lemma.

(7.17) LEMMA. *If* $\zeta \in U_{p^k}$ *satisfies* $\zeta \equiv 1 \bmod \mathfrak{r}$, *then* $\zeta = 1$.

Then we find

$$(\chi(r)\eta^{-m})^{(p-1)r^{p-1}\beta a} = 1.$$

From $(p-1)r^{p-1}a \not\equiv 0 \bmod p$ and (7.6) it now follows that $\chi(r) = \eta^m$, so

$$\chi(r) = \eta^{l_p(r)}$$

by (7.14). This we proved for *prime* divisors r of n. By multiplicativity (cf. (6.7)) it holds for *any* divisor r of n. In particular, since $l_p(n) = 1$, we obtain $\chi(n) = \eta$, so $\chi(r) = \chi(n)^{l_p(r)}$ for all r dividing n. This proves (7.8).

Proof of (7.17). We have an equality of polynomials

$$\prod_{\zeta \neq 1} (X - \zeta) = (X^{p^k} - 1)/(X - 1) = \sum_{i=0}^{p^k - 1} X^i,$$

the product ranging over all $\zeta \in U_{p^k}$, $\zeta \neq 1$. Substituting 1 for X we find that

$$\prod_{\zeta \neq 1} (1 - \zeta) = p^k.$$

Therefore, if the lemma is wrong, we have $p^k \in \mathfrak{r} = rB + \mathfrak{n}$, so $p^k = rx + y$ for certain $x \in B$, $y \in \mathfrak{n}$. Upon multiplication by n/r this would give $p^k n/r \in \mathfrak{n}$, so $p^k n/r \in n\mathbf{Z}$ by (7.7). But r is a prime dividing n, and p is a prime not dividing n, so this is impossible. This proves (7.17).

We shall now develop several methods that can be used to prove that condition (6.4), which occurs both in (6.3) and in (7.8), is satisfied. A different way to do this can be found in Section 10; see (10.7). Our first two methods require that $p \geqslant 3$.

(7.18) PROPOSITION. *If* $p \geqslant 3$ *and* $n^{p-1} \not\equiv 1 \bmod p^2$, *then condition* (6.4) *is satisfied.*

Proof. By (5.1), the hypotheses imply that $(n^{p-1})^{\mathbf{Z}_p} = 1 + p\mathbf{Z}_p$. Since $r^{p-1} \in 1 + p\mathbf{Z}_p$ for all divisors r of n, it follows that (6.4) is satisfied. This proves (7.18).

(7.19) THEOREM. *Let* χ *be a character modulo* q *of order* p^k, *and assume that* $p \geqslant 3$. *Suppose that* (7.9) *is satisfied with a* ***primitive*** p^k*th root of unity* ζ. *Then* p *satisfies condition* (6.4).

Proof. As in the proof of (7.8) we write $\zeta = \eta^{-n\beta}$ with $\eta \in U_{p^k}$. Since ζ is a primitive p^kth root of unity, the same is true for η. Let $u = \tau(\chi)^\beta$. Applying (7.11) to $i = (p-1)p^{k-1}$, we find that

$$u^{n^{(p-1)p^{k-1}} - 1} \equiv \eta^{p^{k-1}\beta} \bmod \mathfrak{n}. \tag{7.20}$$

Let r be a prime dividing n. Replacing n, η, $\mathfrak{n}$ by r, $\chi(r)$, rB, as in the proof of (7.8), we obtain

$$u^{r^{(p-1)p^{k-1}} - 1} \equiv \chi(r)^{p^{k-1}\beta} \bmod rB. \tag{7.21}$$

We combine (7.20) and (7.21) modulo $\mathfrak{r} = rB + \mathfrak{n}$. Let ω denote the order of $(u \bmod \mathfrak{r})$ in the group $(B/\mathfrak{r})^*$. Since η is a primitive p^kth root of unity, it follows from (7.6) and (7.17) that $\eta^{p^{k-1}\beta} \not\equiv 1 \bmod \mathfrak{r}$. Therefore (7.20) implies that ω does not divide $n^{(p-1)p^{k-1}} - 1$, but that it does divide $p(n^{(p-1)p^{k-1}} - 1)$. Consequently we have

$$v_p(\omega) = 1 + v_p\left(n^{(p-1)p^{k-1}} - 1\right).$$

From (7.21) we see that ω divides $p(r^{(p-1)p^{k-1}} - 1)$, so

$$v_p(\omega) \leqslant 1 + v_p\left(r^{(p-1)p^{k-1}} - 1\right).$$

It follows that

$$(7.22) \qquad v_p\left(r^{(p-1)p^{k-1}} - 1\right) \geqslant v_p\left(n^{(p-1)p^{k-1}} - 1\right).$$

Notice that the equality sign holds if and only if $\chi(r)^{p^{k-1}} \neq 1$.

From (7.22), (5.1) and the fact that $p \geqslant 3$ we obtain

$$r^{(p-1)p^{k-1}} = \left(n^{(p-1)p^{k-1}}\right)^l$$

for some $l \in \mathbf{Z}_p$. Since $\mathbf{Z}_p^*$ contains no elements of order p, by (5.2), this immediately implies that $r^{p-1} = (n^{p-1})^l$. This proves (7.19).

In the rest of this section we take $p = 2$ and, consequently, n odd. In this case an important role is played by *quadratic* characters. For such characters it is convenient to replace condition (7.9), with ζ a primitive 2nd root of unity (so with $\zeta = -1$), by a condition of the form $a^{(n-1)/2} \equiv -1 \bmod n$; cf. (7.4).

(7.23) LEMMA. *Let $a \in \mathbf{Z}$, and suppose that $a^{(n-1)/2} \equiv -1 \bmod n$. Then for every divisor r of n we have $v_2(r-1) \geqslant v_2(n-1)$, the equality sign holding if and only if $(\frac{a}{r}) = -1$. In particular $(\frac{a}{n}) = -1$.*

Proof. It is not difficult to see that it suffices to consider *prime* divisors r of n. So let r be a prime dividing n, and let ω be the order of $(a \bmod r)$ in the group $(\mathbf{Z}/r\mathbf{Z})^*$. From $a^{(n-1)/2} \equiv -1 \bmod r$ it follows that $v_2(\omega) = v_2(n-1)$, and since ω divides $r-1$ this implies that $v_2(r-1) \geqslant v_2(n-1)$. The inequality is strict if and only if ω divides $(r-1)/2$, so if and only if $a^{(r-1)/2} \equiv 1 \bmod r$, and this is equivalent to $(\frac{a}{r}) = 1$. This proves (7.23).

(7.24) PROPOSITION. *Suppose that $n \equiv 1 \bmod 4$, and that there exists $a \in \mathbf{Z}$ for which $a^{(n-1)/2} \equiv -1 \bmod n$. Then condition (6.4) is satisfied for $p = 2$.*

Proof. Let $r|n$ be prime. By (7.23) we have $v_2(r-1) \geqslant v_2(n-1)$, and $v_2(n-1) \geqslant 2$ by hypothesis. From (5.1) it now follows that $r \in n^{\mathbf{Z}_2}$, as required. This proves (7.24).

(7.25) PROPOSITION. *Suppose that $n \equiv 3 \bmod 8$ and that $2^{(n-1)/2} \equiv -1 \bmod n$. Then condition (6.4) is satisfied for $p = 2$.*

Proof. Let $r|n$ be prime. By (7.23) we have either $r \equiv 1 \bmod 4$ and $(\frac{2}{r}) = 1$, or $r \equiv 3 \bmod 4$ and $(\frac{2}{r}) = -1$. Since $(\frac{2}{r}) = 1$ for $r \equiv \pm 1 \bmod 8$ and $(\frac{2}{r}) = -1$ for $r \equiv \pm 3 \bmod 8$, it follows that we have either $r \equiv 1 \bmod 8$ or $r \equiv 3 \equiv n \bmod 8$. Therefore one of $v_2(r-1)$ and $v_2(rn^{-1} - 1)$ is $\geqslant 3$. But $3 = v_2(n^2 - 1)$, so (5.1) now implies that r or rn^{-1} belongs to $(n^2)^{\mathbf{Z}_2}$. Hence r belongs to $n^{2\mathbf{Z}_2} \cup n^{1+2\mathbf{Z}_2} = n^{\mathbf{Z}_2}$, as required. This proves (7.25).

Remark. If $n \equiv 3 \bmod 8$ and $2^{(n-1)/2} \not\equiv -1 \bmod n$, then n is clearly not prime, by (1.2).

The case $n \equiv 7 \bmod 8$, which is not covered by (7.24) or (7.25), is most conveniently dealt with by means of Proposition (10.8). Alternatively one can use the following theorem, which is the analogue of (7.19). We use the notation introduced at the beginning of this section.

(7.26) THEOREM. *Let χ be a character modulo q of order p^k, with $p = 2$ and $k \geqslant 2$. Suppose that* (7.9) *is satisfied with a* ***primitive*** *2^kth root of unity ζ. Suppose also that $q^{(n-1)/2} \equiv -1 \bmod n$. Then condition* (6.4) *is satisfied for $p = 2$.*

Remark. Suppose that n is prime, and that (7.9) holds with a primitive 2^kth root of unity ζ. We claim that the extra condition $q^{(n-1)/2} \equiv -1 \bmod n$ is then satisfied. To prove this, we first note that $\zeta = \chi(n)^{-n\beta}$ by (7.5) and (7.17), so $\chi(n)$ is a primitive 2^kth root of unity, and $\chi(n)^{2^{k-1}} = -1$. Let ψ be the quadratic character $\chi^{2^{k-1}}$. Then $\psi(n) = -1$ and $\psi(-1) = \chi(-1)^{2^{k-1}} = 1$, so by (7.2) and (7.3) we have $q^{(n-1)/2} = \tau(\psi)^{n-1} \equiv \psi(n) = -1 \bmod n$, as required.

It follows that n is composite if it does not pass the extra test $q^{(n-1)/2} \equiv -1 \bmod n$.

Proof of (7.26). In the case that $n \equiv 1 \bmod 4$ the theorem immediately follows from (7.24). Assume therefore that $n \equiv 3 \bmod 4$. As in the remark above, let $\psi = \chi^{2^{k-1}}$. Let r be a prime divisor of n. Arguing as in the proof of (7.19), we find that

$$(7.27) \qquad v_2(r^{2^{k-1}} - 1) \geqslant v_2(n^{2^{k-1}} - 1)$$

(cf. (7.22)), the equality sign holding if and only if $\psi(r) = -1$. Since $k \geqslant 2$ we have $v_2(n^{2^{k-1}} - 1) \geqslant 3$, so by (5.1) we have $r^{2^{k-1}} = n^{2^{k-1}l}$ for some $l \in \mathbf{Z}_2$. By (5.3), the only roots of unity in $\mathbf{Z}_2$ are ± 1, so $r = \pm n^l$. The remark about the equality sign in (7.27) implies that l is odd if and only if $\psi(r) = -1$. This can also be formulated as $\psi(r) = (-1)^l$.

Notice that $\psi(r) = (\frac{q}{r})$, by applying (7.4) with ψ, r in the role of χ, n, and using that $\psi(-1) = 1$. Therefore the extra condition $q^{(n-1)/2} \equiv -1 \bmod n$ and Lemma (7.23) imply that

$$v_2(r-1) \geqslant v_2(n-1), \quad \text{with equality if and only if } \psi(r) = -1.$$

Since $n \equiv 3 \bmod 4$, this can also be formulated as $r \equiv \psi(r) \bmod 4$. From $r \equiv \psi(r) = (-1)^l \equiv n^l \bmod 4$ it now follows that the plus sign in $r = \pm n^l$ must be valid.

This proves (7.26).

(7.28) *Remark.* The complications that arise in the case $p = 2$ disappear if, for $p = 2$, we restrict to $k = 1$, i.e. to *quadratic* characters. In that case (6.4) can be replaced by the simpler condition $v_2(r-1) \geqslant v_2(n-1)$ for all $r|n$; cf. [16, Section 2]. The restriction to quadratic characters implies that the auxiliary number t chosen in Stage 1 of the algorithm (see Sections 2 and 4) should satisfy the extra condition $t \not\equiv 0 \bmod 4$.

8. Jacobi Sums for Odd p.

We let q, p, k, n, χ, B, G, $\tau(\chi)$ be as in the previous section, and we retain the notations ζ_m, U_m, σ_x.

It is our purpose to reformulate condition (7.9) in such a way that it only refers to elements of the subring $\mathbf{Z}[\zeta_{p^k}]$ of B.

Let a and b be two integers. The *Jacobi sum* $j(\chi^a, \chi^b)$ associated to the characters χ^a and χ^b is the element of $\mathbf{Z}[\zeta_{p^k}]$ defined by

$$(8.1) \qquad j(\chi^a, \chi^b) = \sum_{x=0}^{q-1} \chi^a(x)\chi^b(1-x).$$

In B, we have

$$(8.2) \qquad j(\chi^a,\chi^b) = \tau(\chi^a)\tau(\chi^b)/\tau(\chi^{a+b}) \quad \text{if } a + b \not\equiv 0 \bmod p^k,$$

with the Gauss sums defined as in (7.1). For the proof of (8.2), see [25, Lemma 6.2(d)] or [7, Chapitre 5, Proposition 9]. If $ab(a + b) \not\equiv 0 \bmod p$ then (8.2) can be written as

$$(8.3) \qquad j(\chi^a,\chi^b) = \tau(\chi)^{\sigma_a+\sigma_b-\sigma_{a+b}}.$$

Notice that the condition $ab(a + b) \not\equiv 0 \bmod p$ forces p to be odd.

In what follows we write $[y]$ for the greatest integer not exceeding y, for a real number y. For $p \geqslant 3$, we put

$$(8.4) \qquad M = \{x \in \mathbf{Z}\colon 1 \leqslant x \leqslant p^k, x \not\equiv 0 \bmod p\}.$$

(8.5) THEOREM. *Suppose that $p \geqslant 3$. Let a, b be integers satisfying*

$$(8.6) \qquad (a + b)^p \not\equiv a^p + b^p \bmod p^2, \qquad ab(a + b) \not\equiv 0 \bmod p,$$

and let $\mathfrak{m}$ *be an ideal of* $\mathbf{Z}[\zeta_{p^k}]$ *for which*

$$(8.7) \qquad \mathfrak{m} \cap \mathbf{Z} = n\mathbf{Z}, \qquad \sigma_n[\mathfrak{m}] = \mathfrak{m}.$$

Define $\alpha \in \mathbf{Z}[G]$ *by*

$$\alpha = \sum_{x\in M} \left[\frac{nx}{p^k}\right]\sigma_x^{-1}.$$

If, with this notation, we have

$$(8.8) \qquad j(\chi^a,\chi^b)^\alpha \equiv \zeta \bmod \mathfrak{m} \quad \textit{for some } \zeta \in U_{p^k},$$

then (7.9) *is satisfied. If* (8.8) *does not hold, then n is composite.*

(8.9) *Remarks.* (a) Notice that $j(\chi^a,\chi^b)^\alpha$ belongs to $\mathbf{Z}[\zeta_{p^k}]$, since the coefficients of α are nonnegative.

(b) In the proof we shall see that if (8.8) holds, then (7.9) is true with the same ζ. This is important for (7.19).

(c) If $3 \leqslant p < 6 \cdot 10^9$, $p \notin \{1093, 3511\}$, then condition (8.6) is satisfied for $a = b = 1$, by [13]. From $(p - 1)^p \not\equiv p - 1 \bmod p^2$ it follows that in any case (8.6) holds for some $a \leqslant p - 2$ with $b = 1$.

(d) An example of an ideal $\mathfrak{m}$ of $\mathbf{Z}[\zeta_{p^k}]$ satisfying (8.7) is given by $\mathfrak{m} = n\mathbf{Z}[\zeta_{p^k}]$. In Section 10 we shall discuss a different way of choosing $\mathfrak{m}$.

Proof of (8.5). Let $\mathfrak{n}$ be the ideal of B generated by $\mathfrak{m}$. From

$$\mathfrak{n} = \left\{\left(\sum_{j=0}^{q-2} a_j\zeta_q^j\right) \cdot q^d\colon a_j \in \mathfrak{m}\ (0 \leqslant j \leqslant q - 2), d \in \mathbf{Z}\right\}$$

and $\gcd(q,n) = 1$ it is not difficult to derive that

$$(8.10) \qquad \mathfrak{n} \cap \mathbf{Z}[\zeta_{p^k}] = \mathfrak{m}.$$

From (8.7) it now follows that $\mathfrak{n}$ satisfies (7.7).

Define $\beta \in \mathbf{Z}[G]$ by

$$(8.11) \qquad \beta = \sum_{x\in M}\left(\left[\frac{(a + b)x}{p^k}\right] - \left[\frac{ax}{p^k}\right] - \left[\frac{bx}{p^k}\right]\right)\sigma_x^{-1},$$

with M as in (8.4). The following lemma will be proved below.

(8.12) LEMMA. *Let $a, b \in \mathbf{Z}$ satisfy* (8.6), *and let $\alpha, \beta \in \mathbf{Z}[G]$ be as in* (8.5) *and* (8.11). *Then we have*

$$(n - \sigma_n)\beta = (\sigma_a + \sigma_b - \sigma_{a+b})\alpha$$

in $\mathbf{Z}[G]$, and β satisfies condition (7.6):

$$\zeta_p^\beta \neq 1.$$

Assuming this lemma, we see from (8.3) that

$$j(\chi^a, \chi^b)^\alpha = \tau(\chi)^{(\sigma_a + \sigma_b - \sigma_{a+b})\alpha} = \tau(\chi)^{(n-\sigma_n)\beta},$$

so by (8.10) the congruence (8.8) is equivalent to

$$\tau(\chi)^{(n-\sigma_n)\beta} \equiv \zeta \bmod \mathrm{n} \quad \text{for some } \zeta \in U_{p^k}.$$

Since β and n satisfy (7.6) and (7.7), it is now immediate that (8.8) implies (7.9). The second assertion of the theorem is clear from (7.5). This proves (8.5).

Proof of (8.12). Define $\theta \in \mathbf{Z}[G]$ by

$$\theta = \sum_{x \in M} x\sigma_x^{-1},$$

with M as in (8.4). Let $m \in \mathbf{Z}$, $m \not\equiv 0 \bmod p$. Writing $x \equiv my \bmod p^k$, we then see that

$$\sigma_m\theta = \sum_{y \in M} r(my)\sigma_y^{-1},$$

where $r(my)$ is the element of M that is congruent to my modulo p^k. From $r(my) = my - [my/p^k]p^k$ it now follows that

$$(8.13) \qquad (m - \sigma_m)\theta = p^k \cdot \sum_{y \in M} \left[\frac{my}{p^k}\right]\sigma_y^{-1}.$$

Applying this to $m = n, a, b, a + b$, we find that

$$(n - \sigma_n)\theta = p^k\alpha,$$

$$(8.14) \quad (\sigma_a + \sigma_b - \sigma_{a+b})\theta = ((a + b - \sigma_{a+b}) - (a - \sigma_a) - (b - \sigma_b))\theta = p^k\beta$$

and therefore

$$p^k(n - \sigma_n)\beta = (\sigma_a + \sigma_b - \sigma_{a+b})(n - \sigma_n)\theta = p^k(\sigma_a + \sigma_b - \sigma_{a+b})\alpha.$$

Dividing by p^k, we obtain the first assertion of (8.12).

The second assertion is equivalent to

$$(8.15) \qquad \sum_{x \in M}\left(\left[\frac{(a+b)x}{p^k}\right] - \left[\frac{ax}{p^k}\right] - \left[\frac{bx}{p^k}\right]\right)x^{-1} \not\equiv 0 \bmod p.$$

Here we consider the expression on the left as an element of $\mathbf{Z}_p$, to make x^{-1} meaningful, and the same applies to similar expressions below. To prove (8.15) we first show that

$$(8.16) \qquad v_p\left(\sum_{x \in M} x^{1-p}\right) = k - 1.$$

The values assumed by $(x^{1-p} \bmod p^k)$, for $x \in M$, are precisely the elements of $H = \{y \in (\mathbf{Z}/p^k\mathbf{Z})^*: y \equiv 1 \bmod p\}$, each taken $p - 1$ times. This is because H is a subgroup of index $p - 1$ in the cyclic group $(\mathbf{Z}/p^k\mathbf{Z})^*$. Therefore we have

$$\sum_{x \in M} x^{1-p} \equiv (p-1) \sum_{y \in H} y \bmod p^k$$
$$\equiv (p-1)\left(p^{k-1} + \tfrac{1}{2}p^k\left(p^{k-1} - 1\right)\right) \bmod p^k,$$

and (8.16) follows.

If $x, y \in \mathbf{Z}$ are congruent modulo p^k, then $x^p \equiv y^p \bmod p^{k+1}$, by the binomial theorem. It follows that there is a ring homomorphism $\mathbf{Z}[G] \to \mathbf{Z}/p^{k+1}\mathbf{Z}$ mapping σ_x to $(x^p \bmod p^{k+1})$, for $x \in M$. Applying this ring homomorphism to (8.14), we obtain a congruence

$$\left(a^p + b^p - (a+b)^p\right) \cdot \sum_{x \in M} x^{1-p}$$
$$\equiv p^k \cdot \sum_{x \in M} \left(\left[\frac{(a+b)x}{p^k}\right] - \left[\frac{ax}{p^k}\right] - \left[\frac{bx}{p^k}\right]\right) x^{-p} \bmod p^{k+1}.$$

By (8.6) and (8.16) the exponent of p in the expression on the left is precisely k. Hence this is also true for the expression on the right, so

$$\sum_{x \in M} \left(\left[\frac{(a+b)x}{p^k}\right] - \left[\frac{ax}{p^k}\right] - \left[\frac{bx}{p^k}\right]\right) x^{-p} \not\equiv 0 \bmod p.$$

Since $x^{-p} \equiv x^{-1} \bmod p$ this is the same as (8.15). This completes the proof of (8.12).

An alternative proof of (8.15) starts from the congruence

$$\sum_{x \in M} \left[\frac{mx}{p^k}\right] x^{-1} \equiv m\left(m^{(p-1)p^{k-1}} - 1\right)/p^k \bmod p^k,$$

which is valid for any $m \in \mathbf{Z}$, $m \not\equiv 0 \bmod p$. This congruence is proved by calculating $\prod_{x \in M} mx$ in two different ways.

Remark. The elements $\theta, \beta \in \mathbf{Z}[G]$ that we used in this section are familiar operators from the theory of cyclotomic fields. See for example [11, Chapter IV, Section 4], [25, Section 6.2], where they occur in connection with Stickelberger's theorem on the factorization of Gauss sums and Jacobi sums.

9. Jacobi Sums for $p = 2$. In this section we do for $p = 2$ what we did in the previous section for $p \geqslant 3$. The notation is unchanged; in particular, our hypothesis $\gcd(n, pq) = 1$ implies that n is *odd* for $p = 2$. We distinguish the cases $k = 1$, $k = 2$ and $k \geqslant 3$.

(9.1) THEOREM. *Let $p = 2$ and $k = 1$. If, in this case, we have*

(9.2) $$q^{(n-1)/2} \equiv \zeta \bmod n \quad \textit{for some } \zeta \in \{1, -1\},$$

then (7.9) *is satisfied. If* (9.2) *does not hold, then n is composite.*

Proof. The first assertion follows from $\tau(\chi)^2 = \chi(-1)q$ (see (7.2)), with $\beta = 1$ and $\mathfrak{n} = nB$ in (7.9). The second assertion follows from (7.5). This proves (9.1).

(9.3) THEOREM. *Let $p = 2$, $k = 2$ and $n \equiv 1 \bmod 4$. Let $\mathfrak{m}$ be an ideal of $\mathbf{Z}[\zeta_4]$ for which*

$$\mathfrak{m} \cap \mathbf{Z} = n\mathbf{Z}.$$

If, in this situation, we have

(9.4) $$j(\chi,\chi)^{(n-1)/2}\cdot q^{(n-1)/4}\equiv\zeta \bmod \mathfrak{m}\quad \textit{for some } \zeta\in U_4,$$

then (7.9) *is satisfied. If* (9.4) *does not hold, then n is composite.*

Proof. Let $\mathfrak{n}$ be the ideal of B generated by $\mathfrak{m}$. As in the proof of (8.5) we have $\mathfrak{n}\cap\mathbf{Z}[\zeta_4]=\mathfrak{m}$. From $n\equiv 1 \bmod 4$ it follows that σ_n is the identity automorphism, so $\mathfrak{n}$ satisfies (7.7).

By (8.2) and (7.2) we have

$$j(\chi,\chi)=\tau(\chi)^2/\tau(\chi^2),\qquad \tau(\chi^2)^2=\chi^2(-1)q=q$$

and therefore

$$\tau(\chi)^{n-\sigma_n}=\tau(\chi)^{n-1}=j(\chi,\chi)^{(n-1)/2}q^{(n-1)/4}.$$

It follows that (9.4) is the same as (7.9) with $\beta=1$ and $\mathfrak{n}$ as above. The second assertion of the theorem again follows from (7.5). This proves (9.3).

(9.5) THEOREM. *Let* $p=2$, $k=2$ *and* $n\equiv 3 \bmod 4$. *If, in this case, we have*

(9.6) $$j(\chi,\chi)^{(n+1)/2}q^{(n-3)/4}\equiv\zeta \bmod n\mathbf{Z}[\zeta_4]\quad \textit{for some } \zeta\in U_4,$$

then (7.9) *is satisfied. If* (9.6) *does not hold, then n is composite.*

Remark. There is no need to allow arbitrary ideals $\mathfrak{m}$ of $\mathbf{Z}[\zeta_4]$ satisfying (8.7) in this theorem, since from (10.5) it follows that the only such $\mathfrak{m}$ is $n\mathbf{Z}[\zeta_4]$.

Proof of (9.5). By (7.2) we have

$$\tau(\chi)\tau(\chi^{-1})=\chi(-1)q,\qquad \tau(\chi^2)^2=q,$$

and therefore by (8.2) we have

$$\begin{aligned}\tau(\chi)^{n-\sigma_n}&=\tau(\chi)^{n+1}/(\tau(\chi)\tau(\chi^{-1}))\\&=j(\chi,\chi)^{(n+1)/2}q^{(n+1)/4}/(\chi(-1)q)\\&=\chi(-1)\,j(\chi,\chi)^{(n+1)/2}q^{(n-3)/4}.\end{aligned}$$

It follows that (9.6) is the same as (7.9) with $\beta=1$ and $\mathfrak{n}=nB$, and with ζ replaced by $\chi(-1)\zeta$. This implies (9.5).

In the rest of this section we assume that $p=2$ and $k\geqslant 3$. The *triple Jacobi sum* $j(\chi,\chi,\chi)$ is the element of $\mathbf{Z}[\zeta_{2^k}]$ defined by

(9.7) $$j(\chi,\chi,\chi)=j(\chi,\chi)j(\chi,\chi^2).$$

To explain the notation we remark that

$$j(\chi,\chi,\chi)=\sum_{x,y,z\in\mathbf{Z}/q\mathbf{Z},\ x+y+z=1}\chi(x)\chi(y)\chi(z)$$

(see [7, Chapitre 5, Section 4]) but this will not be needed in the sequel. From (9.7) and (8.2) we see that

(9.8) $$j(\chi,\chi,\chi)=\tau(\chi)^3/\tau(\chi^3)=\tau(\chi)^{3-\sigma_3}.$$

We put

(9.9) $$M=\{x\in\mathbf{Z}\colon 1\leqslant x\leqslant 2^k,\ x\equiv 1 \text{ or } 3 \bmod 8\}.$$

Notice that M, when taken modulo 2^k, is a subgroup of $(\mathbf{Z}/2^k\mathbf{Z})^*$. The integer brackets [ ] are as in Section 8.

(9.10) THEOREM. *Let $p = 2$, $k \geqslant 3$ and $n \equiv 1$ or $3 \bmod 8$. Let $\mathfrak{m}$ be an ideal of $\mathbf{Z}[\zeta_{2^k}]$ for which*

$$\mathfrak{m} \cap \mathbf{Z} = n\mathbf{Z}, \qquad \sigma_n[\mathfrak{m}] = \mathfrak{m}.$$

Define $\alpha \in \mathbf{Z}[G]$ by

$$\alpha = \sum_{x \in M} \left[\frac{nx}{2^k}\right] \sigma_x^{-1}.$$

If, with this notation, we have

$$j(\chi,\chi,\chi)^{\alpha} \equiv \zeta \bmod \mathfrak{m} \quad \textit{for some } \zeta \in U_{2^k}, \tag{9.11}$$

then (7.9) *is satisfied. If* (9.11) *does not hold, then n is composite.*

Proof. Define $\beta \in \mathbf{Z}[G]$ by

$$\beta = \sum_{x \in M} \left[\frac{3x}{2^k}\right] \sigma_x^{-1}, \tag{9.12}$$

with M as in (9.9). Below we shall prove that

$$(n - \sigma_n)\beta = (3 - \sigma_3)\alpha \tag{9.13}$$

for $n \equiv 1$ or $3 \bmod 8$, and that β satisfies condition (7.6):

$$(-1)^{\beta} \neq 1. \tag{9.14}$$

Assuming this, one proves the theorem in exactly the same way as (8.5) was deduced from (8.12). The only difference is that (8.3) is replaced by (9.8).

To prove (9.13) we define $\theta \in \mathbf{Z}[G]$ by

$$\theta = \sum_{x \in M} x\sigma_x^{-1}.$$

We have

$$(m - \sigma_m)\theta = 2^k \sum_{x \in M} \left[\frac{mx}{2^k}\right] \sigma_x^{-1} \quad \text{for } m \in \mathbf{Z},\ m \equiv 1 \text{ or } 3 \bmod 8 \tag{9.15}$$

by the same argument that was used to prove (8.13). Applying this to $m = n$ and $m = 3$ we find that

$$(n - \sigma_n)\theta = 2^k\alpha,$$
$$(3 - \sigma_3)\theta = 2^k\beta, \tag{9.16}$$

and this implies (9.13). To prove (9.14) we apply to (9.16) the ring homomorphism $\mathbf{Z}[G] \to \mathbf{Z}$ that maps every $\sigma_x \in G$ to 1. This leads to

$$2 \cdot \sum_{x \in M} x = 2^k \cdot \sum_{x \in M} \left[\frac{3x}{2^k}\right], \tag{9.17}$$

so

$$\sum_{x \in M} \left[\frac{3x}{2^k}\right] = 2^{k-2} - 1. \tag{9.18}$$

This is odd, and therefore $(-1)^{\beta} = -1$, as required. This completes the proof of (9.10).

(9.19) THEOREM. *Let $p = 2$, $k \geqslant 3$ and $n \equiv 5$ or $7 \bmod 8$. Let $\mathfrak{m}$ be an ideal of $\mathbf{Z}[\zeta_{2^k}]$ for which*

$$\mathfrak{m} \cap \mathbf{Z} = n\mathbf{Z}, \qquad \sigma_n[\mathfrak{m}] = \mathfrak{m}.$$

Define $\alpha \in \mathbf{Z}[G]$ by

$$\alpha = \sum_{x \in M} \left[\frac{nx}{2^k}\right] \sigma_x^{-1}$$

and put $\phi = \chi^{2^{k-3}}$. If, with this notation, we have

$$(9.20) \qquad j(\chi,\chi,\chi)^{\alpha} j(\phi,\phi^3)^2 \equiv \zeta \bmod \mathfrak{m} \quad \textit{for some } \zeta \in U_{2^k},$$

then (7.9) is satisfied. If (9.20) does not hold, then n is composite.

Proof. Let β be defined by (9.12). Below we shall prove that

$$(9.21) \qquad \tau(\chi)^{(n-\sigma_n)\beta} = \chi(-1) j(\chi,\chi,\chi)^{\alpha} j(\phi,\phi^3)^2.$$

From this the theorem follows by the argument used in the proof of (8.5). Notice that β satisfies condition (7.6), by (9.14).

To prove (9.21) we apply (9.15) to $m = -n$; this is allowed because $-n \equiv 1$ or $3 \bmod 8$. We find that

$$(-n - \sigma_{-n})\theta = 2^k \sum_{x \in M} \left[\frac{-nx}{2^k}\right] \sigma_x^{-1} = -2^k\left(\alpha + \sum_{x \in M} \sigma_x\right).$$

Combination with (9.16) leads to

$$(n + \sigma_{-n})\beta = (3 - \sigma_3)\left(\alpha + \sum_{x \in M} \sigma_x\right) = (3 - \sigma_3)\alpha + 2 \cdot \sum_{x \in M} \sigma_x,$$

so

$$\tau(\chi)^{(n+\sigma_{-n})\beta} = j(\chi,\chi,\chi)^{\alpha} \cdot \tau(\chi)^{2\sum_{x \in M}\sigma_x}.$$

By (7.2) and (9.18) we have

$$\tau(\chi)^{(\sigma_n+\sigma_{-n})\beta} = (\chi(-1)q)^{\beta} = \chi(-1)q^{2^{k-2}-1}.$$

Upon division we obtain

$$\tau(\chi)^{(n-\sigma_n)\beta} = \chi(-1) j(\chi,\chi,\chi)^{\alpha} \tau(\chi)^{2\sum_{x \in M}\sigma_x} / q^{2^{k-2}-1}.$$

To prove (9.21) it therefore suffices to show that

$$(9.22) \qquad \tau(\chi)^{2\sum_{x \in M}\sigma_x} = q^{2^{k-2}-1} j(\phi,\phi^3)^2.$$

This is easily seen to be a consequence of the Hasse-Davenport relations, see [12, Chapter 2, Theorem 10.1]. We give a direct argument, by applying induction on k. For $k = 3$ we have $\chi = \phi$, so by (8.2), (7.2) and $\phi^4(-1) = 1$ we find that

$$q \cdot j(\phi,\phi^3)^2 = q \cdot (\tau(\phi)\tau(\phi^3))^2/\tau(\phi^4)^2 = (\tau(\phi)\tau(\phi^3))^2,$$

which is the same as (9.22). Let now $k > 3$. Put $\psi = \phi^4 = \chi^{2^{k-1}}$; this is the quadratic character modulo q. From $8|2^{k-1}$ it follows that $\chi\psi = \chi^y$ for some $y \in M$. Therefore we have

$$\tau(\chi)^{2\Sigma_{x\in M}\sigma_x} = (\tau(\chi)\tau(\chi\psi))^{\Sigma_{x\in M}\sigma_x}.$$

Assume for the moment that

$$\tau(\chi)\tau(\chi\psi) = \chi(4)^{-1}\tau(\psi)\tau(\chi^2). \tag{9.23}$$

Applying $\Sigma_{x\in M}\sigma_x$ and using that $\psi = \psi^x$ for $x \in M$, we find that

$$\tau(\chi)^{2\Sigma_{x\in M}\sigma_x} = \chi(2)^{-2\Sigma_{x\in M}x} \cdot \tau(\psi)^{2^{k-2}} \cdot \tau(\chi^2)^{\Sigma_{x\in M}\sigma_x}.$$

By (9.17), the first factor on the right-hand side is 1. Since ψ is quadratic and $\psi(-1) = 1$, we see from (7.2) that the second factor equals $q^{2^{k-3}}$. The third factor can be written as

$$\tau(\chi^2)^{2\Sigma_{x\in M'}\sigma_x},$$

where $M' = \{x\colon 1 \leqslant x \leqslant 2^{k-1},\ x \equiv 1 \text{ or } 3 \bmod 8\}$, and by the induction hypothesis this is equal to $q^{2^{k-3}-1}j(\phi,\phi^3)^2$. This completes the induction step.

The identity (9.23) is a special case of the Hasse-Davenport relations, and it can be proved directly as follows [5, Section 20.4]. We have

$$\begin{aligned} j(\chi,\chi) &= \sum_{x=0}^{q-1} \chi(x)\chi(1-x) = \sum_{x=0}^{q-1} \chi(x-x^2) \\ &= \sum_{y\in\mathbf{Z}/q\mathbf{Z}} \chi(y)m(y), \end{aligned}$$

where $m(y)$ is the number of $x \in \mathbf{Z}/q\mathbf{Z}$ for which $y = x - x^2$; this is 0, 1 or 2 according as the discriminant $1 - 4y$ of $X^2 - X + y$ is a nonsquare, zero, or a nonzero square in $\mathbf{Z}/q\mathbf{Z}$, so in all cases $m(y) = 1 + ((1-4y)/q) = 1 + \psi(1-4y)$. Therefore

$$\begin{aligned} j(\chi,\chi) &= \sum_{y\in\mathbf{Z}/q\mathbf{Z}} \chi(y)\cdot(1+\psi(1-4y)) \\ &= \sum_{y\in\mathbf{Z}/q\mathbf{Z}} \chi(y) + \sum_{z\in\mathbf{Z}/q\mathbf{Z}} \chi(z/4)\psi(1-z) \\ &= 0 + \chi(4)^{-1} \sum_{z\in\mathbf{Z}/q\mathbf{Z}} \chi(z)\psi(1-z) = \chi(4)^{-1}j(\chi,\psi). \end{aligned}$$

By (8.2) this is the same as

$$\tau(\chi)^2/\tau(\chi^2) = \chi(4)^{-1}\tau(\chi)\tau(\psi)/\tau(\chi\psi),$$

and this implies (9.23). This completes the proof of (9.19).

(9.24) *Remarks.* (a) From the proofs of the theorems in this section we see that if (9.2), (9.4), (9.6), (9.11) or (9.20) holds for some $\zeta \in U_{2^k}$, then (7.9) is true with ζ replaced by $\pm\zeta$. Notice that, for $k \geqslant 2$, the 2^kth root of unity $\pm\zeta$ is primitive if and only if ζ is primitive. This is important for (7.26).

(b) The number $\chi(-1) \in \{1, -1\}$ that appears in many formulae in this section is equal to -1 if and only if $k = v_2(q-1)$, which is often the case in the applications.

10. Choice of the Ideal. In this section p denotes a prime number, k a positive integer, ζ_{p^k} a primitive p^kth root of unity in $\mathbf{C}$ and n an integer for which $n > 1$ and $n \not\equiv 0 \bmod p$. By f we denote the order of $(n \bmod p^k)$ in the group $(\mathbf{Z}/p^k\mathbf{Z})^*$, and we let σ_n be the automorphism of the ring $\mathbf{Z}[\zeta_{p^k}]$ for which $\sigma_n(\zeta_{p^k}) = \zeta_{p^k}^n$.

In Section 11 we shall see that in our primality algorithm we have to test (8.8), (9.2), (9.4), (9.6), (9.11) and (9.20) for several choices of p, k, q. Each time this requires a calculation modulo an ideal $\mathfrak{m}$ of $\mathbf{Z}[\zeta_{p^k}]$ satisfying

$$(10.1) \qquad \mathfrak{m} \cap \mathbf{Z} = n\mathbf{Z}, \qquad \sigma_n[\mathfrak{m}] = \mathfrak{m}.$$

This calculation is easier to do if the ring $\mathbf{Z}[\zeta_{p^k}]/\mathfrak{m}$ is smaller, so if $\mathfrak{m}$ is larger. In this section we shall see how to choose $\mathfrak{m}$ as large as possible. The methods that we shall describe are usually successful if n is prime, even if we do not yet have a *proof* that n is prime. However, if n is composite, then the methods are not likely to work. It is therefore advisable to use them only if n is probably prime in the sense that it passed several tests as in (1.2).

(10.2) The first method is taken from [1, Section 4, A.5]. We apply Berlekamp's algorithm [8, Section 4.6.2] to find an fth degree polynomial $h \in \mathbf{Z}[T]$ with leading coefficient 1 such that $(h \bmod n)$ divides $\sum_{i=0}^{p-1} T^{ip^{k-1}}$ in $(\mathbf{Z}/n\mathbf{Z})[T]$. If n is prime, then such an h exists, and $(h \bmod n)$ is irreducible; cf. [25, Chapter 2]. We now let $\mathfrak{m}$ be the ideal of $\mathbf{Z}[\zeta_{p^k}]$ generated by n and $h(\zeta_{p^k})$. Then $\mathbf{Z}[\zeta_{p^k}]/\mathfrak{m}$ may be identified with the set of all expressions

$$\sum_{i=0}^{f-1} a_i \bar{\zeta}^i, \qquad a_i \in \mathbf{Z}/n\mathbf{Z} \ (0 \leqslant i < f),$$

where $\bar{\zeta} = (\zeta_{p^k} \bmod \mathfrak{m})$ is a zero of $(h \bmod n)$. This ring has n^f elements, and if n is prime, it is the field $\mathbf{F}_{n^f}$. We have $\mathfrak{m} \cap \mathbf{Z} = n\mathbf{Z}$, since this is the kernel of the natural map $\mathbf{Z} \to \mathbf{Z}[\zeta_{p^k}]/\mathfrak{m}$. The condition $\sigma_n[\mathfrak{m}] = \mathfrak{m}$ can be shown to be automatically satisfied if h has been obtained by means of Berlekamp's algorithm; but it can in any case easily be tested by checking if $\bar{\zeta}^n$ is a zero of $(h \bmod n)$. We remark that if n is prime, the condition $\sigma_n[\mathfrak{m}] = \mathfrak{m}$ is satisfied for all ideals $\mathfrak{m}$ of $\mathbf{Z}[\zeta_{p^k}]$ containing n. To see this, one uses (1.3) to show that $\sigma_n(\alpha) \equiv \alpha^n \bmod \mathfrak{m}$ for all $\alpha \in \mathbf{Z}[\zeta_{p^k}]$; then $\sigma_n[\mathfrak{m}] \subset \mathfrak{m}$, and equality holds because σ_n has finite order.

If $f = (p-1)p^{k-1}$, then the above method leads to $\mathfrak{m} = n\mathbf{Z}[\zeta_{p^k}]$, and from (10.5) it follows that this is in fact the only ideal of $\mathbf{Z}[\zeta_{p^k}]$ satisfying (10.1). The methods described in this section are therefore only useful if $f < (p-1)p^{k-1}$. This occurs for example if $p = 2$ and $k \geqslant 3$, since in that case $(\mathbf{Z}/p^k\mathbf{Z})^*$ is not cyclic.

If $f < (p-1)p^{k-1}$, then the coefficients of h are usually rather large. This makes Euclidean division by h into a complicated operation in practice, and the same thing is therefore true for multiplication in the ring $\mathbf{Z}[\zeta_{p^k}]/\mathfrak{m}$, at least for $f \neq 1$. The second method to construct $\mathfrak{m}$ does not have this disadvantage. It is as follows.

(10.3) First one constructs a ring F with n^f elements that contains $\mathbf{Z}/n\mathbf{Z}$ as a subring, such that F is a field if n is prime. For example, one can take $F = (\mathbf{Z}/n\mathbf{Z})[T]/g \cdot (\mathbf{Z}/n\mathbf{Z})[T]$, where g is an fth degree polynomial in $(\mathbf{Z}/n\mathbf{Z})[T]$ with leading coefficient 1 that is irreducible if n is prime; the latter property can be checked by an irreducibility test as described in [8, Exercise 4.6.2.16]. Writing ξ for the image of T in F we have $F = \{\sum_{i=0}^{f-1} a_i \xi^i \colon a_i \in \mathbf{Z}/n\mathbf{Z} \ (0 \leqslant i < f)\}$, with $g(\xi) = 0$.

To facilitate the multiplication in F one should choose g such that its coefficients are "small", and this can usually be done in practice.

It is important that F be constructed in such a way that we can recognize whether a given element of F belongs to the unit group F^*. In the example given we can do this by calculating the gcd with g in $(\mathbf{Z}/n\mathbf{Z})[T]$, using the Euclidean algorithm; this can only fail if at some stage a nontrivial common divisor of n and some leading coefficient is found, in which case n is factored [1, Section 5].

Once F has been made one constructs a ring homomorphism $\rho\colon F \to F$ such that if n is prime, we have $\rho(\alpha) = \alpha^n$ for all $\alpha \in F$. For F as above this is done by checking that $g(\xi^n) = 0$ and putting $\rho(\sum_{i=0}^{f-1} a_i \xi^i) = \sum_{i=0}^{f-1} a_i \xi^{in}$; if $g(\xi^n) \neq 0$, then n is composite.

Next one chooses an element $\beta \in F$, $\beta \neq 0$, such that $\beta^{(n^f-1)/p} \neq 1$. Such an element β should not be hard to find, since if n is prime, then a random $\beta \in F - \{0\}$ has this property with probability $(p-1)/p$.

If n is prime, then we must have

$$(10.4) \qquad \beta^{n^f-1} = 1, \qquad \beta^{(n^f-1)/p} - 1 \in F^*, \ \rho(\beta) = \beta^n.$$

One now checks that β does indeed have these properties, and one calculates $\bar{\zeta} = \beta^{(n^f-1)/p^k}$. Then $\bar{\zeta}$ is a zero of $\sum_{i=0}^{p-1} X^{ip^{k-1}} = (X^{p^k} - 1)/(X^{p^{k-1}} - 1)$, so we can define a ring homomorphism $\lambda\colon \mathbf{Z}[\zeta_{p^k}] \to F$ by $\lambda(\zeta_{p^k}) = \bar{\zeta}$. We have $\rho(\bar{\zeta}) = \bar{\zeta}^n$, and therefore $\lambda \circ \sigma_n = \rho \circ \lambda$.

Finally we let $\mathfrak{m}$ be the kernel of λ. Since $\mathbf{Z}/n\mathbf{Z} \subset F$, we have $\mathfrak{m} \cap \mathbf{Z} = n\mathbf{Z}$. We prove that $\sigma_n[\mathfrak{m}] = \mathfrak{m}$. For $\alpha \in \mathfrak{m}$ we have $\lambda(\sigma_n(\alpha)) = \rho(\lambda(\alpha)) = \rho(0) = 0$, so $\sigma_n(\alpha) \in \mathfrak{m}$. Hence $\sigma_n[\mathfrak{m}] \subset \mathfrak{m}$, and equality follows as before. We conclude that $\mathfrak{m}$ satisfies (10.1). From (10.5) below it follows that λ is surjective, so that $\mathbf{Z}[\zeta_{p^k}]/\mathfrak{m} \simeq F$.

This finishes the description of the second method to construct $\mathfrak{m}$. Some additional work would be needed to find explicit generators for $\mathfrak{m}$, but these are in fact not needed: to check a congruence modulo $\mathfrak{m}$ it suffices to apply λ and to check the corresponding equality in F.

If $f = 1$, then in the second method we can simply take $F = \mathbf{Z}/n\mathbf{Z}$ and ρ equal to the identity map. Notice that $f = 1$ if and only if $n \equiv 1 \bmod p^k$. This is not a rare event, since in practice p^k is small.

If one of our two methods successfully constructs an ideal $\mathfrak{m}$ satisfying (10.1), then $\mathfrak{m}$ is indeed largest possible, even if n is not prime. This is an immediate consequence of the following proposition.

(10.5) PROPOSITION. *Let $\mathfrak{m}$ be an ideal of $\mathbf{Z}[\zeta_{p^k}]$ satisfying* (10.1). *Then the number of elements of $\mathbf{Z}[\zeta_{p^k}]/\mathfrak{m}$ is at least n^f.*

Proof. From $\mathfrak{m} \cap \mathbf{Z} = n\mathbf{Z}$ it follows that $\mathbf{Z}/n\mathbf{Z} \subset \mathbf{Z}[\zeta_{p^k}]/\mathfrak{m}$. Write $\bar{\zeta} = (\zeta_{p^k} \bmod \mathfrak{m})$. It suffices to show that the map $(\mathbf{Z}/n\mathbf{Z})^f \to \mathbf{Z}[\zeta_{p^k}]/\mathfrak{m}$ sending $(a_i)_{i=0}^{f-1}$. to $\sum_{i=0}^{f-1} a_i \bar{\zeta}^i$ is injective. Suppose therefore that $\sum_{i=0}^{f-1} a_i \bar{\zeta}^i = 0$. From $\sigma_n[\mathfrak{m}] = \mathfrak{m}$ we see that σ_n induces an automorphism of $\mathbf{Z}[\zeta_{p^k}]/\mathfrak{m}$ that maps $\bar{\zeta}$ to $\bar{\zeta}^n$. Repeatedly applying this automorphism we find that

$$(10.6) \qquad \sum_{i=0}^{f-1} a_i \bar{\zeta}^{in^j} = 0 \quad \text{for } 0 \leqslant j < f.$$

From the identity $\prod_{x=1}^{p^k-1}(1-\zeta_{p^k}^x)=p^k$ in the proof of (7.17) and $\gcd(p,n)=1$ it follows that $1-\bar{\zeta}^x\in(\mathbf{Z}[\zeta_{p^k}]/\mathfrak{m})^*$ for all $x\in\mathbf{Z}$, $x\not\equiv 0 \bmod p^k$. Therefore the Vandermonde determinant $\det(\bar{\zeta}^{in^j})_{0\leqslant i,j<f}=\prod_{0\leqslant i<j<f}(\bar{\zeta}^{n^j}-\bar{\zeta}^{n^i})$ is a unit in $\mathbf{Z}[\zeta_{p^k}]/\mathfrak{m}$, and (10.6) implies that $a_i=0$ for $0\leqslant i<f$. This proves (10.5).

It is an attractive feature of our second method to construct $\mathfrak{m}$ that it gives us an easy way to check condition (6.4).

(10.7) PROPOSITION. *Let F be a ring with n^f elements that contains $\mathbf{Z}/n\mathbf{Z}$ as a subring. Suppose that F contains an element β satisfying* (10.4) *for some ring homomorphism ρ: $F\to F$. If $p=2$ and $n\equiv 3 \bmod 4$, suppose that $k\geqslant 2$. Then p satisfies condition* (6.4).

Proof. Put $\bar{\zeta}=\beta^{(n^f-1)/p^k}$. From the proof of (10.5) we see that $\det(\rho^j(\bar{\zeta}^i))_{0\leqslant i,j<f}\in F^*$ and hence that $1,\bar{\zeta},\bar{\zeta}^2,\dots,\bar{\zeta}^{f-1}$ is a basis of F over $\mathbf{Z}/n\mathbf{Z}$. Hence F is, in the terminology of [16, Section 8], a Galois extension of rank f of $\mathbf{Z}/n\mathbf{Z}$ with group $\langle\rho\rangle$. We can now apply [16, Theorem (8.4)] with s equal to the largest power of p dividing n^f-1, and $\alpha=\beta^{(n^f-1)/s}$. Then we find that for each $r|n$ there exists $i\in\mathbf{Z}$ such that $r\equiv n^i \bmod s$; then $rn^{-i}\in 1+s\mathbf{Z}_p=(n^f)^{\mathbf{Z}_p}$, by (5.1), and (6.4) follows immediately. This proves (10.7).

For the final result of this section we assume that $n\equiv 3 \bmod 4$. Let $u\in\mathbf{Z}/n\mathbf{Z}$ be chosen such that $u^2+4\in(\mathbf{Z}/n\mathbf{Z})^*$, and let F be the ring

$$(\mathbf{Z}/n\mathbf{Z})[T]/(T^2-uT-1).$$

Denote by ξ the residue class of T, and let ρ be the automorphism of F with $\rho(\xi)=u-\xi$. Notice that $\rho(\xi)=-\xi^{-1}$.

If n is prime and $((u^2+4)/n)=-1$, then F is a *field* in which ξ and $\rho(\xi)$ are conjugate, so $\rho(\xi)=\xi^n$ by the theory of finite fields, and $\xi^{n+1}=-1$. The following proposition tells us what can, conversely, be said if $\xi^{n+1}=-1$. The reader interested in Lucas functions [26] should notice that $\xi^{n+1}=-1$ is equivalent to $\xi^{(n+1)/2}+\rho(\xi)^{(n+1)/2}=0$, since $n\equiv 3 \bmod 4$.

(10.8) PROPOSITION. *Suppose that $n\equiv 3 \bmod 4$, and that, with the above notation, we have $\xi^{n+1}=-1$. Then $p=2$ satisfies condition* (6.4).

Proof. This is an immediate consequence of (10.7), with $k=2$, $f=2$ and $\beta=\xi$. This proves (10.8).

We leave it to the reader to deduce (10.8) directly from properties of the Lucas function, and to prove that the assumptions of (10.8) also imply that $((u^2+4)/n)=-1$.

11. The Central Stage of the Algorithm. In this section we give a more detailed description of the second stage of our primality test than was given in Section 2.

(11.1) Let n be the integer to be tested for primality, $n>1$, and let t and s be integers satisfying (2.1), (2.2), (2.3), (2.4) and $\gcd(st,n)=1$. We describe an algorithm that leads either to a proof that n is composite or to a proof that (2.5) holds.

(a) First one selects, for every prime power p^k dividing t, an ideal $\mathfrak{m}=\mathfrak{m}_{p,k}$ of $\mathbf{Z}[\zeta_{p^k}]$ satisfying (10.1). This is done either by taking $\mathfrak{m}=n\mathbf{Z}[\zeta_{p^k}]$ or by using one of the methods described in Section 10.

(b) Next one lets Y_s be as in (6.3), and checks that every $\chi=\chi_{p,q}\in Y_s$ satisfies (7.9). If p is odd, this is done by selecting a, b as in (8.6), calculating the Jacobi sum

$j(\chi^a, \chi^b)$, and checking that (8.8) is satisfied; if (8.8) is not satisfied for some pair p, q, then n is composite by (8.5), and the algorithm halts. If $p = 2$, then one proceeds in a similar way, replacing (8.8) by (9.2), (9.4), (9.6), (9.11) or (9.20), whichever is applicable.

(c) Finally one checks that every prime p dividing t satisfies condition (6.4). The procedure by which this is done is described in (11.2) for odd p and in (11.5) for $p = 2$. If this has been done then from (7.8) it follows that every $\chi \in Y_s$ satisfies (6.5). From Theorem (6.3) one can now draw the desired conclusion that (2.5) holds. This is the end of the second stage.

(11.2) Let n, t, s be as in (11.1), and let p be an odd prime dividing t. We describe a procedure that leads either to a proof that n is composite or to a proof that p satisfies condition (6.4). If in (11.1)(a) algorithm (10.3) has been used to construct m, it suffices to apply (10.7). Otherwise we can proceed as follows.

(a) First one tests whether $n^{p-1} \not\equiv 1 \bmod p^2$. If this holds, then (6.4) is satisfied. by (7.18), and the procedure halts.

(b) Secondly, one checks whether there exists a prime q dividing s, with $q - 1$ divisible by p, such that $\chi = \chi_{p,q}$ satisfies (7.9) with a *primitive* p^kth root of unity ζ; here $k = v_p(q - 1)$. The calculations that are needed to check this have already been carried out in stage (b) of algorithm (11.1), cf. Remark (8.9)(b). If such a prime q indeed exists, then (6.4) is satisfied by (7.19), and one stops.

(c) Suppose now that both (a) and (b) have failed to establish (6.4). Then one first tests whether n is the pth power of an integer. If this is the case, then clearly n is composite, and the procedure halts.

(d) Next one determines a prime number q (not necessarily dividing s) for which

$$(11.3) \qquad q \equiv 1 \bmod p, \qquad n^{(q-1)/p} \not\equiv 1 \bmod q.$$

Such a prime q can be found by trying all primes in succession; cf. Remark (11.4)(a) below.

(e) Now if q divides s, we claim that n is composite (see (11.4)(b)), and the procedure halts. Suppose finally that q does not divide s. Then one first checks that q does not divide n. Next one lets χ be a character modulo q of order p, and one tests, using (8.5), whether (7.9) is satisfied with $\zeta \in U_p$ *primitive*. If this is the case, then (6.4) is satisfied, by (7.19), and if this is not the case, then we claim that n is composite (see (11.4)(b)). In all cases the procedure halts.

(11.4) *Remarks.* (a) If n is not a pth power, then the density of the set of primes q satisfying (11.3) is $1/p$. To see this, note that for a prime q not dividing n condition (11.3) is equivalent to the condition that q splits completely in $\mathbf{Q}(\zeta_p)$, but not in $\mathbf{Q}(\zeta_p, n^{1/p})$; next one can apply the well-known theorem that the density of the set of primes splitting completely in a normal number field of degree d over $\mathbf{Q}$ equals $1/d$; see [11, Chapter VIII].

It follows that a prime $q \equiv 1 \bmod p$ satisfies (11.3) with probability $(p - 1)/p$. Therefore the desired q should not be hard to find. If the truth of the generalized Riemann hypothesis is assumed, then it can be proved that the least prime q satisfying (11.3) is $\leqslant c \cdot p^2 \cdot (\log p + \log n)^2$ for some absolute, effectively computable constant c, by [9, Corollary 1.3]. Without unproved hypotheses no satisfactory upper bound for q is known. Consequently we can give no satisfactory upper bound for the running time of part (d) of procedure (11.2).

(b) To justify the claims made in (11.2)(e), suppose that n is prime and that q is a prime satisfying (11.3) with q not dividing n. Let χ be as in (11.2)(e) if q does not divide s, and $\chi = \chi_{p,q}$ if q does divide s. Write order$(\chi) = p^k$. Then from (11.3) it follows that $\chi(n)$ is a primitive p^kth root of unity, so (7.5) implies that χ satisfies (7.9) with $\zeta \in U_{p^k}$ *primitive*.

Hence if one finds that (7.9) is not true with ζ primitive, one can conclude that n is composite. This applies in particular if q divides s, since in this case it was discovered in (11.2)(b) that $\chi = \chi_{p,q}$ does not satisfy (7.9) with ζ primitive. This proves the claims in (11.2)(e).

(c) Procedure (11.2) is quite efficient in practice, despite the theoretical difficulties mentioned in (11.4)(a). In fact, it only rarely happens that parts (c), (d) and (e) of the procedure are needed. This occurs, for example, if n is a prime number that is congruent to a pth power modulo $p^2 \cdot s$. If n is very likely to be prime the procedure can be speeded up by omitting part (c) and by restricting the search in (d) to the primes q not dividing s.

(11.5) Let n, t, s be as in (11.1), and assume that t is *even*. We describe a procedure that either proves that $p = 2$ satisfies (6.4) or proves that n is composite.

First suppose that $n \equiv 1 \bmod 4$. In this case one determines an integer a satisfying $(\frac{a}{n}) = -1$, by trying all primes 2,3,5,... in succession, and one tests whether $a^{(n-1)/2} \equiv -1 \bmod n$; if this is the case, then $p = 2$ satisfies (6.4), by (7.24), and otherwise n is composite, by (1.2). If it is difficult to find an integer a with $(\frac{a}{n}) = -1$, one tests whether n is a square.

Secondly, suppose that $n \equiv 3 \bmod 4$. In this case one determines an integer u satisfying $((u^2 + 4)/n) = -1$, by trying $u = 1,2,3,\ldots$; cf. (11.6)(a). Next, one lets $\xi = (T \bmod T^2 - uT - 1) \in (\mathbf{Z}/n\mathbf{Z})[T]/(T^2 - uT - 1)$ be as defined before (10.8), and one tests whether $\xi^{n+1} = -1$; if this is the case, then $p = 2$ satisfies (6.4), by (10.8), and otherwise n is composite, by the remark preceding (10.8).

This finishes the description of the procedure. Alternatively, one might make use of (7.25) or (7.26).

(11.6) *Remarks.* (a) The remarks made in (11.4)(a) about the existence and the size of q also apply to the number a that appears in the above procedure for $n \equiv 1 \bmod 4$.

Suppose that $n \equiv 3 \bmod 4$. We prove that there exists $u \in \mathbf{Z}$ with $((u^2 + 4)/n) = -1$. Let r be a prime divisor of n with $v_r(n)$ *odd*, and let a be the least positive integer for which $(\frac{a}{r}) = -1$. By the minimality of a there exists v with $v^2 \equiv a - 1 \bmod r$, and then $((v^2 + 1)/r) = -1$. Now let $u \in \mathbf{Z}$ be such that $u \equiv 2v \bmod r$, and such that u is divisible by all other primes that divide n. Then one easily checks that $((u^2 + 4)/n) = -1$, as required.

If the generalized Riemann hypothesis is true then there is an absolute effectively computable constant c with the following property: if n is a positive odd integer that is not a square, and n has no prime factor $\leqslant c^2(\log n)^4$, then the least positive integer u with $((u^2 + 4)/n) = -1$ satisfies $u \leqslant c(\log n)^2$. This is proved by combining [9, Corollary 1.3] with [3, Lemma 1]. We are indebted to A. M. Odlyzko for this observation.

(b) The search for q in (11.2)(d) and the search for a and u in (11.5) are the only points in our primality testing algorithm that prevent us from proving a worst case running time estimate of the form $(\log n)^{c \log\log\log n}$. From (11.4)(a) and (11.6)(a) it follows that the truth of the generalized Riemann hypothesis would imply such a bound for the algorithm; we should then choose $\mathfrak{m} = n\mathbf{Z}[\zeta_{p^k}]$ in (11.1)(a). If we wish the result of Pomerance and Odlyzko quoted in Section 1 to be valid for our algorithm, we should use algorithm (10.3) in (11.1)(a), and apply (10.7) to check (6.4). The condition $k \geqslant 2$ in (10.7), for $p = 2$ and $n \equiv 3 \bmod 4$, is not a serious restriction; cf. (7.28).

12. Detailed Description of the Algorithm.

(12.1) Let N be some large integer. We describe, from a computational point of view, an algorithm to determine whether an integer n, $1 < n \leqslant N$, is prime.

Step 1. *Preparation of Tables.* These tables depend only on N, and can be made once and for all.

(a) Select a positive integer t with $e(t) > N^{1/2}$ (cf. Section 4, Table 1).

(b) Perform steps (b1) and (b2) for each odd prime $q | e(t)$.

(b1) Find by trial and error a primitive root g modulo q, i.e. an integer $g \not\equiv 0 \bmod q$ such that $g^{(q-1)/p} \not\equiv 1 \bmod q$ for every prime $p | q - 1$. Make a table of the function $f\colon \{1,2,\ldots, q-2\} \to \{1,2,\ldots, q-2\}$ defined by $1 - g^x \equiv g^{f(x)} \bmod q$.

(b2) Perform steps (b2a), (b2b), (b2c), (b2d), (b2e), (b2f) for each prime $p | q - 1$.

(b2a) Put $k = v_p(q-1)$, the number of factors p in $q - 1$.

(b2b) If $p^k \neq 2$, compute

$$j_{p,q} = \sum_{x=1}^{q-2} \zeta_{p^k}^{x+f(x)} \in \mathbf{Z}\big[\zeta_{p^k}\big].$$

Here an element $\Sigma_{0 \leqslant i < (p-1)p^{k-1}} a_i \zeta_{p^k}^i$ of $\mathbf{Z}[\zeta_{p^k}]$, with $a_i \in \mathbf{Z}$, is to be represented as a vector $(a_i)_{0 \leqslant i < (p-1)p^{k-1}}$; cf. Section 7. (Notice that $j_{p,q} = j(\chi,\chi)$ for $\chi = \chi_{p,q}$; see (8.1).)

(b2c) If $p \neq 2$, do the following. Let

$$M = \{x \in \mathbf{Z}\colon 1 \leqslant x \leqslant p^k, x \not\equiv 0 \bmod p\},$$
$$\theta = \sum_{x \in M} x\sigma_x^{-1} \in \mathbf{Z}[G],$$
$$\alpha(v) = \sum_{x \in M} \left[\frac{vx}{p^k}\right]\sigma_x^{-1} \in \mathbf{Z}[G] \quad \text{for } v \in M,$$

where $[y]$ denotes the greatest integer $\leqslant y$ and σ_x and G are as in Section 7. Calculate

$$j_{0,p,q} = j_{p,q}^{\theta}, \qquad j_{v,p,q} = j_{p,q}^{\alpha(v)}$$

for each $v \in M$, as elements of $\mathbf{Z}[\zeta_{p^k}]$ (see Section 7 for the definition of the action of $\mathbf{Z}[G]$). The numbers $j_{v,p,q}$, for $v \in \{0\} \cup M$, should be tabulated.

(b2d) If $p = 2$, $k = 1$, let

$$j_{0,2,q} = q, \qquad j_{1,2,q} = 1,$$

and tabulate these values.

(b2e) If $p = 2$, $k = 2$, do the following. Calculate

$$j_{0,2,q} = j_{2,q}^2 \cdot q \in \mathbf{Z}[\zeta_4],$$

and let

$$j_{1,2,q} = 1, \qquad j_{3,2,q} = j_{2,q}.$$

The numbers $j_{v,2,q}$, for $v = 0, 1, 3$, should be tabulated.

(b2f) If $p = 2$, $k \geqslant 3$, do the following. Calculate

$$j^{*}_{2,q} = j_{2,q} \cdot \sum_{x=1}^{q-2} \zeta_{2^k}^{2x+f(x)}, \qquad j^{\#}_{2,q} = \left(\sum_{x=1}^{q-2} \zeta_8^{3x+f(x)} \right)^2$$

as elements of $\mathbf{Z}[\zeta_{2^k}]$, where $\zeta_8 = \zeta_{2^k}^{2^{k-3}}$. (Notice that $j^{*}_{2,q} = j(\chi, \chi, \chi)$ and $j^{\#}_{2,q} = j(\phi, \phi^3)^2$, with $\phi = \chi^{2^{k-3}}$, as in Section 9.) Put

$$\begin{aligned} L &= \{x \in \mathbf{Z}\colon 1 \leqslant x \leqslant 2^k, x \text{ is odd}\}, \\ M &= \{x \in L\colon x \equiv 1 \text{ or } 3 \bmod 8\}, \\ \theta &= \sum_{x \in M} x\sigma_x^{-1} \in \mathbf{Z}[G], \\ \alpha(v) &= \sum_{x \in M} \left[\frac{vx}{2^k} \right] \sigma_x^{-1} \in \mathbf{Z}[G] \quad \text{for } v \in L, \end{aligned}$$

and calculate

$$\begin{aligned} j_{0,2,q} &= \left(j^{*}_{2,q} \right)^{\theta}, \\ j_{v,2,q} &= \left(j^{*}_{2,q} \right)^{\alpha(v)} \quad \text{for } v \in M, \\ j_{v,2,q} &= \left(j^{*}_{2,q} \right)^{\alpha(v)} \cdot j^{\#}_{2,q} \quad \text{for } v \in L - M. \end{aligned}$$

The numbers $j_{v,2,q}$, for $v \in \{0\} \cup L$, should be tabulated.

Step 2. *Preliminary Tests.* Let now an integer n be given, $1 < n \leqslant N$, to be tested for primality.

(c) Depending on the information that one may already have about n, it may be wise to test n for small divisors, or to subject n to the test of Miller and Rabin [8, p. 379].

(d) Test whether $\gcd(te(t), n) = 1$, using Euclid's algorithm. If not, then a prime divisor of n is obtained, since $te(t)$ is completely factored, and we stop.

(e) Select a divisor s of $e(t)$ with $s > n^{1/2}$ (cf. Section 4). Replace t by the smallest t' for which s divides $e(t')$. (Note that the new t is the exponent of the group $(\mathbf{Z}/s\mathbf{Z})^*$ and therefore divides the old t.)

Step 3. *Pseudoprime Tests with Jacobi Sums.* Perform steps (f), (g), (h) for each prime p dividing t.

(f) Declare a boolean variable λ_p (telling us whether (6.4) has been checked). Put $\lambda_p =$ "true" if p is odd and $n^{p-1} \not\equiv 1 \bmod p^2$, and $\lambda_p =$ "false" otherwise.

(g) For each integer $k \geqslant 1$ with $p^k | t$, determine integers u_k, v_k such that $n = u_k p^k + v_k$ and $0 \leqslant v_k < p^k$.

(h) Perform steps (h1), (h2), (h3) for each prime $q | s$ with $p | q - 1$.

(h1) Put $k = v_p(q - 1)$, and $u = u_k$, $v = v_k$ as in (g). Calculate

$$j^{u}_{0,p,q} \cdot j_{v,p,q} \bmod n\mathbf{Z}\left[\zeta_{p^k}\right]$$

by means of repeated squarings and multiplications modulo $n\mathbf{Z}[\zeta_{p^k}]$; here a residue class $(\sum_{0 \leqslant i < (p-1)p^{k-1}} a_i \zeta_{p^k}^i \bmod n\mathbf{Z}[\zeta_{p^k}])$, with $a_i \in \mathbf{Z}$, is to be represented as a vector

$(b_i)_{0 \leqslant i < (p-1)p^{k-1}}$, where $b_i \in \{0, 1, \ldots, n-1\}$, $b_i \equiv a_i \bmod n$. If there does not exist $h \in \{0, 1, \ldots, p^k - 1\}$ with

$$j_{0,p,q}^{u} \cdot j_{v,p,q} \equiv \zeta_{p^k}^{h} \bmod n\mathbf{Z}\left[\zeta_{p^k}\right],$$

then n is composite and the algorithm halts. (This is test (8.8) with $a = b = 1$ if p is odd; test (9.2) if $p^k = 2$; test (9.4) or (9.6) if $p^k = 4$; and test (9.11) or (9.20) if $p = 2$, $k \geqslant 3$.) Suppose now that h exists.

(h2) If $h \not\equiv 0 \bmod p$, and either $p^k = 2$, $n \equiv 1 \bmod 4$ or p is odd, put $\lambda_p =$ "true". (This combines (7.24) and (7.19).)

(h3) If $h \not\equiv 0 \bmod 2$, $p = 2$, $k \geqslant 2$ and $\lambda_2 =$ "false", do the following. Test whether $q^{(n-1)/2} \equiv -1 \bmod n$. If this does not hold, n is composite, and the algorithm halts. If it does hold, put $\lambda_2 =$ "true". (This is (7.26).)

Step 4. *Additional Tests.* Perform steps (i) and (j) for every prime p dividing t for which $\lambda_p =$ "false".

(i) Select a small prime number q not dividing s such that

$$\begin{aligned} &q \equiv 1 \bmod p, \\ &q \equiv 1 \bmod 4 \quad \text{if } p = 2 \text{ and } n \equiv 3 \bmod 4, \\ &n^{(q-1)/p} \not\equiv 1 \bmod q. \end{aligned}$$

If such a prime q cannot be found below a reasonable limit, do the following. Test whether n is a pth power. If so, declare n composite and halt. Otherwise, halt with the message that the algorithm is unable to prove that n is prime. Suppose now that q has been found. Halt if $n \equiv 0 \bmod q$.

(j) Put $k = 2$ if $p = 2$ and $n \equiv 3 \bmod 4$, and $k = 1$ else. Determine integers u_k, v_k as in (g). Calculate $j_{v,p,q}$ as in (b1), (b2b), (b2c), (b2d), (b2e), but only for $v \in \{0, v_k\}$. Test whether $j_{0,p,q}^{u_k} \cdot j_{v_k,p,q} \equiv \zeta_{p^k}^{h} \bmod n\mathbf{Z}[\zeta_{p^k}]$ for some $h \in \mathbf{Z}$, $0 \leqslant h < p^k$, $h \not\equiv 0 \bmod p$. If this is not the case, n is composite, and the algorithm halts. (To justify this, cf. (11.4)(b).) Otherwise, perform steps (h2) and (h3).

Step 5. *Final Trial Divisions.* (It is not likely that in this step it will be found that n is composite, cf. the remark at the end of Section 2.)

(k) Put $r_0 = 1$.

(l) Perform steps (l1), (l2), (l3) for $i = 1, 2, \ldots, t$.

(l1) Determine r_i by $r_i \equiv n r_{i-1} \bmod s$, $0 \leqslant r_i < s$.

(l2) If $r_i = 1$, declare that n is prime and halt.

(l3) If $r_i | n$, and $r_i < n$, declare that n is composite and halt.

(Notice that one of (l2) and (l3) applies for some $i \leqslant t$, since $n^t \equiv 1 \bmod s$.)

This finishes the description of the algorithm.

(12.2) *Remarks.* (a) Since we used $a = b = 1$ in (8.8) (see step (h1)), the correctness of the test is only guaranteed if $2^p \not\equiv 2 \bmod p^2$ for all primes $p | t$, cf. (8.6). This condition is satisfied for all $p < 1093$, see (8.9)(c). In practice we usually have $p < 20$, see Section 4, Table 1.

(b) Several improvements have not been incorporated in the above description. First of all, the results of Section 10 have not been used. Secondly, the algorithm of (3.1) has not been included. Finally, the possibility to combine the test with the older tests described in [26] has been neglected; see [16, Section 8].

13. The Implementation. The algorithm described in Section 12 has been implemented by H. Cohen and A. K. Lenstra on the CDC Cyber computer system at the SARA computer center in Amsterdam. In this section we discuss the main features of this implementation, referring to a forthcoming publication by H. Cohen and A. K. Lenstra for more details.

Two programs have been written, one in Pascal and the other in Fortran. Both programs make use of multiprecision routines that were written in the assembly language Compass by D. T. Winter and made available by the Mathematisch Centrum in Amsterdam.

The auxiliary number t was chosen to be 5040 for the Pascal program, and 55440 for the Fortran program. We have $e(5040) > 1.5 \cdot 10^{52}$ and $e(55440) > 4.9 \cdot 10^{106}$, so the Pascal program can deal with numbers of up to 104 decimal digits and the Fortran program with numbers of up to 213 decimal digits.

The programs incorporate the following improvements that are not included in the algorithm in Section 12. Use has been made of the results of Section 10, but only in those cases where the integer f defined at the beginning of that section equals 1. We also construct a ring F of n^2 elements that is a field if n is prime. This ring enabled us to combine our algorithm with the test that is based on known prime factors of $n^2 - 1$; see [16, Section 8].

The Fortran program does not make use of prepared tables as described in Step 1 of the algorithm in Section 12, since such tables would have required too much memory space. Instead, the entries of the tables that are needed are recomputed for every n.

For each prime power p^k dividing t special routines were written to do multiplications in $\mathbf{Z}[\zeta_{p^k}]/n\mathbf{Z}[\zeta_{p^k}]$; or, equivalently, to multiply polynomials of degree less than $m = (p-1)p^{k-1}$, with coefficients in $\mathbf{Z}/n\mathbf{Z}$, modulo the p^kth cyclotomic polynomial $\sum_{i=0}^{p-1} X^{ip^{k-1}}$. In addition to the necessary m reductions modulo n, the straightforward way to do one such multiplication takes m^2 integer multiplications. It is important to reduce this number. Theoretically, $2m - 1$ integer multiplications suffice, by a theorem of Winograd [8, p. 495]; but Winograd's method is completely impractical because it involves a great number of additions and multiplications by small constants. We made use of special formulae for each p^k. For example, for $p^k = 16$ we use 27 instead of 64 integer multiplications to do one multiplication in $\mathbf{Z}[\zeta_{16}]/n\mathbf{Z}[\zeta_{16}]$, and only 18 to do one squaring. It may be that along these lines further improvements are possible.

Tables 3 and 4 contain data on the running time of the Pascal program and the Fortran program, respectively. For each number d in the first column we tested 20 prime numbers of d decimal digits. Each prime was selected by drawing a random number of d digits and using the program to determine the least prime exceeding the number drawn. The second column gives the average running time $\bar{t} = (\sum_{i=1}^{20} t_i)/20$, the third one the sample standard deviation $((\sum_{i=1}^{20}(t_i - \bar{t})^2)/19)^{1/2}$, the fourth the maximal running time, and the fifth the minimal running time. All times are in seconds. The time spent on the composite numbers is not counted.

The two programs tested the same set of 20 primes of 100 digits. The tables show that for these numbers the Fortran program is slower than the Pascal program. This is mainly caused by the fact that each program works in a fixed precision, which is twice as large for the Fortran program as it is for the Pascal program. Only a minor part of the difference is due to the use of prepared tables in the Pascal program.

We indicate the speed of the multiprecision routines that are used. Denote by a_m, b_m numbers consisting of m words, each word containing 47 bits. Then the calculation of $a_8 \cdot b_8$, $a_{16} \cdot b_{16}$, $(a_{16} \bmod b_8) = a_{16} - [a_{16}/b_8]b_8$ and $(a_{32} \bmod b_{16}) = a_{32} - [a_{32}/b_{16}]b_{16}$ takes on the average less than $7 \cdot 10^{-5}$, $2.1 \cdot 10^{-4}$, $2 \cdot 10^{-4}$ and $4.7 \cdot 10^{-4}$ seconds, respectively.

TABLE 3. *Running times of the Pascal program in seconds (see text)*

number of digits	average	standard deviation	maximum	minimum
50	6.437	1.687	10.030	4.525
60	8.634	2.554	15.168	5.009
70	12.074	2.289	15.214	7.032
80	16.224	3.897	23.800	8.006
90	25.572	5.870	35.752	15.810
100	32.349	9.103	47.689	17.891

TABLE 4. *Running times of the Fortran program in seconds (see text)*

number of digits	average	standard deviation	maximum	minimum
100	50.442	15.203	75.416	26.031
120	97.797	28.274	147.259	51.077
140	156.429	43.122	210.756	77.316
160	246.204	44.144	298.144	111.888
180	359.728	55.833	436.039	259.021
200	495.748	80.025	614.254	258.859

Acknowledgements are due to D. T. Winter for writing the Compass multiprecision routines, and to A. K. Lenstra for his great help in implementing the algorithm and for performing all tests reported in this section.

Mathématiques et Informatique
LA au CNRS no 226
Université de Bordeaux I
351, cours de la Libération
33405 Talence, France

Mathematisch Instituut
Universiteit van Amsterdam
Roetersstraat 15
1018 WB Amsterdam, The Netherlands

→ L. M. ADLEMAN, C. POMERANCE & R. S. RUMELY, "On distinguishing prime numbers from composite numbers," *Ann. of Math.*, v. 117, 1983, pp. 173–206.

2. J. BRILLHART, D. H. LEHMER & J. L. SELFRIDGE, "New primality criteria and factorizations of $2^m \pm 1$," *Math. Comp.*, v. 29, 1975, pp. 620–647.

3. D. A. Burgess, "On the quadratic character of a polynomial," *J. London Math. Soc.*, v. 42, 1967, pp. 73–80.

4. G. H. Hardy & E. M. Wright, *An Introduction to the Theory of Numbers*, 5th ed., Oxford Univ. Press, Oxford, 1979.

5. H. Hasse, *Vorlesungen über Zahlentheorie*, 2nd ed., Springer-Verlag, Berlin, 1964.

6. H. Hasse, *Zahlentheorie*, 3rd ed., Akademie-Verlag, Berlin, 1969; English transl.: *Number Theory*, Springer-Verlag, Berlin, 1980.

7. J. R. Joly, "Equations et variétés algébriques sur un corps fini," *Enseign. Math.*, v. 19, 1973, pp. 1–117.

8. D. E. Knuth, *The Art of Computer Programming*, Vol. 2, *Seminumerical Algorithms*, 2nd ed., Addison-Wesley, Reading, Mass., 1981.

9. J. C. Lagarias, H. L. Montgomery & A. M. Odlyzko, "A bound for the least prime ideal in the Chebotarev density theorem," *Invent. Math.*, v. 54, 1979, pp. 271–296.

10. S. Lang, *Algebra*, Addison-Wesley, Reading, Mass., 1965.

11. S. Lang, *Algebraic Number Theory*, Addison-Wesley, Reading, Mass., 1970.

12. S. Lang, *Cyclotomic Fields*, Springer-Verlag, New York, 1978.

13. D. H. Lehmer, "On Fermat's quotient, base two," *Math. Comp.*, v. 36, 1981, pp. 289–290.

14. D. H. Lehmer, "Strong Carmichael numbers," *J. Austral. Math. Soc. Ser. A*, v. 21, 1976, pp. 508–510.

15. H. W. Lenstra, Jr., "Divisors in residue classes," *Math. Comp.*, v. 42, 1984, pp. 331–340.

16. H. W. Lenstra, Jr., *Primality Testing Algorithms* (*after Adleman, Rumely and Williams*), Sém. Bourbaki, Vol. 33, 1980/1981, Exposé 576, pp. 243–257 in: Lecture Notes in Math., Vol. 901, Springer-Verlag, Berlin, 1981.

17. H. W. Lenstra, Jr., "Primality testing with Artin symbols," pp. 341–347 in: N. Koblitz (ed.), *Number Theory Related to Fermat's Last Theorem*, Progress in Mathematics, Vol. 26, Birkhäuser, Boston, 1982.

18. S. Martello & P. Toth, "The 0-1 knapsack problem," Ch. 9, pp. 237–279 in: N. Christofides, A. Mingozzi, P. Toth and C. Sandi (eds.), *Combinatorial Optimization*, Wiley, New York, 1979.

19. G. L. Miller, "Riemann's hypothesis and tests for primality," *J. Comput. System Sci.*, v. 13, 1976, pp. 300–317.

20. K. Prachar, "Über die Anzahl der Teiler einer natürlichen Zahl, welche die Form $p - 1$ haben," *Monatsh. Math.*, v. 59, 1955, pp. 91–97.

→ M. O. Rabin, "Probabilistic algorithms for testing primality," *J. Number Theory*, v. 12, 1980, pp. 128–138.

22. J.-P. Serre, *Cours d'Arithmétique*, Presses Universitaires de France, Paris, 1970; English transl.: *A Course in Arithmetic*, Springer-Verlag, New York, 1973.

→ R. Solovay & V. Strassen, "A fast Monte-Carlo test for primality," *SIAM J. Comput.*, v. 6, 1977, pp. 84–85; erratum, ibid., v. 7, 1978, p. 118.

24. J. Vélu, "Tests for primality under the Riemann hypothesis," *SIGACT News*, v. 10, 1978, pp. 58–59.

25. L. C. Washington, *Introduction to Cyclotomic Fields*, Springer-Verlag, New York, 1982.

26. H. C. Williams, "Primality testing on a computer," *Ars Combin.*, v. 5, 1978, pp. 127–185.