Annals of Mathematics, 117 (1983), 173–206

On distinguishing prime numbers from composite numbers

By Leonard M. Adleman,* Carl Pomerance,* and Robert S. Rumely*

1. Introduction

We present here an algorithm that on input n will decide whether n is prime or composite in "nearly" polynomial time. Specifically, for all large n it will terminate within

$$(\log n)^{c \log\log\log n} \tag{1.1}$$

steps, where c is a positive constant for which an upper bound could in principle be computed. The algorithm depends on arithmetic in cyclotomic fields, and is based on the discovery that for any n there is a collection of pseudo-primality tests such that if n passes all the tests, its divisors lie in a small, explicitly given set.

We give two versions of the algorithm, one probabilistic, the other deterministic, each of which has a running time bound of the above form.

The probabilistic version is computer practical. (By a probabilistic algorithm, we mean one in which guesses are made to expedite the processing of the algorithm.) If it terminates, it correctly decides whether n is prime or composite. Thus it differs from the algorithm of Solovay-Strassen [35] which can only assert with certainty that n is composite (but which runs in polynomial time, $(\log n)^c$). The fastest previous probabilistic algorithm for primality, that of Williams-Holte [39], was based on factoring and had expected running time $\exp(c\sqrt{\log n \log\log n})$ (see Dixon [11]).

The deterministic version is to be distinguished from Miller's polynomial time primality test in that if the new algorithm asserts that a number is prime then its primality is provable from Peano's axioms, whereas Miller's algorithm only guarantees a proof under the additional assumption of the Extended

*Research supported in part by grants from the National Science Foundation.

003-486X/83/0117-1/0173/034$03.40/1

Riemann Hypothesis. The fastest previous unconditional deterministic algorithms required exponential time (Pollard's $n^{1/8}$ in [23], and a recent $n^{1/10.89}$ by Adleman-Leighton [3]). Our algorithm is subexponential but not polynomial: the $\log\log\log n$ in the running time bound is sharp.

The history of primality testing is a long one. The Sieve of Eratosthenes belongs to the basic landscape of mathematics, as does Fibonacci's observation that a composite n has a prime divisor $p \leq \sqrt{n}$. Gauss computed large tables of primes, from which he conjectured the Prime Number Theorem. In his *Disquisitiones*, he further proclaimed primality testing and factoring to be "among the most important problems in arithmetic." Mathematicians interested in these problems, represented in this century by the school of D. H. Lehmer, invented many clever methods for dealing with large numbers, and their efforts found an unexpected commercial application in cryptography. Recently, in theoretical computer science, primality testing became not only a problem in its own right, but a building block for other algorithms. We refer the reader to the survey articles of Williams [38], Lenstra [18], and Pomerance [27] for further discussion.

Our algorithm lies at the confluence of several old ideas in primality testing, as well as some new ones. Most modern primality tests have arisen from the Fermat congruence

$$b^{n-1} \equiv 1 \bmod n \qquad (n \text{ prime}, (b, n) = 1). \tag{1.2}$$

There have been two basic approaches to using (1.2). One is to factor $n - 1$ and show that $(\mathbf{Z}/n)^{\times}$ has order $n - 1$. The other, followed here, is to use the congruence as a "pseudo-primality" test. The left side of (1.2) can be rapidly evaluated by a process involving repeated squarings, and it can be shown that for any given $b > 1$, most n which satisfy the congruence are prime. However, there are composite numbers which satisfy it (pseudoprimes to the base b) and even composite numbers which satisfy it for all relatively prime b (Carmichael numbers). (See [25] and [26] for distribution estimates.)

Hence there have been efforts to find more discriminating pseudo-primality tests. One such test is the defining congruence for the quadratic residue symbol

$$\pm 1 = \left(\frac{b}{n}\right) \equiv b^{(n-1)/2} \bmod n \qquad (n \text{ prime}, (b, n) = 1). \tag{1.3}$$

If n is composite, (1.3) fails for at least half the $b < n$ (Lehmer [15], Solovay-Strassen [35]). Solovay-Strassen made this test the basis for their Monte-Carlo algorithm: they observed that after checking (1.3) for k random b's one could declare n prime with probability of error less than $1/2^k$. Our algorithm proceeds from a different observation: in addition to pass-or-fail, (1.3) places limits on the structure of possible divisors of n. The basis for this is our "Extraction Lemma", explained in Section 4.

To obtain pseudo-primality tests which place additional constraints on possible divisors, we take the congruences defining p^{th} power residue symbols in the cyclotomic fields $\mathbf{Q}(\zeta_p)$. Our use of higher power residue pseudo-primality tests is new, though the idea of performing tests in number fields is not: the tests of Williams, Judd and Holte [39], [40] are examples, as is the classical Lucas-Lehmer test for primality of Mersenne numbers. However, the authors of such tests have generally used the language of recurring sequences and worked in fields of low degree, while we use the conceptual framework of algebraic number theory.

The classic difficulty in using pseudo-primality tests to prove primality has been how to link information from several different tests together. In tests based on factoring, an advance by Brillhart, Lehmer and Selfridge [7] was combining congruences arising from factors of both $n + 1$ and $n - 1$. One of the main features of our algorithm is a new way of linking information from different tests, using the power reciprocity laws and auxiliary moduli ("Euclidean primes") to carry information between fields.

The running time of our algorithm also deserves comment. In primality algorithms based on factoring, the running time is limited by the speed of factoring, and the current best factoring methods all have expected running time $\exp(c\sqrt{\log n \log\log n})$ (for example Morrison-Brillhart [22], cf. Pomerance [28]). On the other hand, algorithms based on pseudo-primality tests like (1.3) face the difficulty of finding a witness to the compositeness of n, if n is composite. Solovay-Strassen and Miller-Rabin [30] trade certainty for speed, expecting one will come upon a witness quickly by random guessing. Miller's celebrated algorithm [20] is based on a systematic search; if n is composite, Miller shows that on the ERH a witness will be found in the range $1 \leq b \leq c(\log n)^2$. Our algorithm, too, involves a systematic search, and it is over a set of size (1.1). This size estimate can be obtained using the ERH. However, unlike Miller's case, the estimate depends only loosely on n in that if it is true for n_0, then it is true for all nearby n. Thus it is possible to substitute sieve methods and averaging arguments for the ERH.

Finally, we note that Hendrik Lenstra [19] and Henri Cohen [9] have recently extended and recast the results of this paper, obtaining both theoretical simplifications and practical improvements for computer implementation. These promise to make routine the testing of primality for numbers some hundreds of digits long.

Future directions. The question of whether there is a primality testing algorithm which runs in polynomial time is still open. In fact, it is not even known if there is an infinite set S of primes and an algorithm that on input n

decides in polynomial time whether $n \in S$. A notorious open problem, whose solution would have important practical consequences, is to determine the complexity of factoring integers (see Rivest, Shamir, and Adleman [33]). For an analysis of current factoring methods, see Pomerance [28] and the references therein. The related questions of testing irreducibility and factoring polynomials with rational coefficients have very recently been settled by Lenstra, Lenstra, and Lovász [17], who gave a deterministic polynomial time algorithm for factoring polynomials in one variable over **Q**. For other computational complexity problems of a number-theoretic flavor we refer the reader to Adleman's announcement of the present algorithm [2], and to his thesis [1].

Acknowledgements. In our original proof of Theorem 3 (see § 6) we had followed the paper of Prachar [29] which made use of Tatuzawa's prime number theorem [36], and obtained the bound

$$(\log n)^{c(\log\log\log n)^2}$$

for the running time of the algorithm. On reading some of our notes, Andrew Odlyzko realized that a mean-value zero-density estimate of Gallagher [12] could be substituted for Tatuzawa's result, eliminating the exponent "2" in the bound. Odlyzko's improvement is especially significant because it gives a best possible estimate (except for the constant c) for the running time. We are deeply indebted to him for allowing us to incorporate his insight in this paper.

In addition we owe a debt of gratitude to many others who have assisted us in this endeavor. Specifically we mention Jeff Lagarias, Hendrik Lenstra, Ram Murty, Claus Schmidt, Richard Schroeppel, and Harold Stark.

2. The ideas behind the algorithm

Let $\mathcal{I}$ denote a finite set of primes. We define a *Euclidean prime with respect to* $\mathcal{I}$ to be a prime q such that $q - 1$ is square-free and every prime factor of $q-1$ lies in $\mathcal{I}$.

We now give a rough outline of the algorithm. Say we are given a natural number n which we wish to test for primality. The "preparatory" stage in the algorithm is to find a small set $\mathcal{I} = \mathcal{I}(n)$ of primes, which we shall call the set of *initial primes*, such that the product of the Euclidean primes with respect to $\mathcal{I}$ exceeds $\sqrt{n}$. The running time of the algorithm is polynomial in the product of the initial primes, so it is important that this product be chosen as small as possible. In Section 6 we will show that $\mathcal{I}$ can be chosen so that

$$\prod_{p \in \mathcal{I}(n)} p < (\log n)^{c \log\log\log n}$$

for all $n > 100$, where c is a certain positive, calculable constant.

From now on p, p_i, p_j, etc. will denote initial primes, q, q_i, q_j, etc. will denote Euclidean primes, n will denote a large number to be tested for primality and r a possible prime factor of n, $0 < r \leq \sqrt{n}$.

The idea is to determine r (if it exists) by finding $r \bmod q$ for each Euclidean prime q. Indeed, if each $r \bmod q$ is known, since r is smaller than the product of the q's, the Chinese Remainder Theorem allows us to determine r. We can test directly if $q = r$ so we will henceforth assume $r \not\equiv 0 \bmod q$ for each q. Further, we will fix a primitive root t_q for each q and calculate indices with respect to it, writing $\operatorname{Ind}_q(x)$ for the least non-negative integer such that

$$x \equiv t_q^{\operatorname{Ind}_q(x)} \bmod q \tag{2.1}$$

when $(x, q) = 1$. Now, if $\operatorname{Ind}_q(r)$ is known, then obviously so is $r \bmod q$. Note further that we have carefully chosen the q's so that the order of the group $(\mathbf{Z}/q)^\times$ is square-free and divisible only by initial primes p. Thus, for a given q, if $\operatorname{Ind}_q(r) \bmod p$ is known for each initial prime $p \mid q - 1$, then the Chinese Remainder Theorem gives us $\operatorname{Ind}_q(r)$. In summary, if we know $\operatorname{Ind}_q(r) \bmod p$ for each pair p, q with $p \mid q - 1$, then we know r.

The crucial fact is that for each fixed initial prime p, it is possible to compute "transition data" relating the $\operatorname{Ind}_q(r) \bmod p$ for all q with $p \mid q - 1$, such that if one of them is known, the others can be found in terms of it. Knowing the $\operatorname{Ind}_q(r) \bmod p$ is equivalent to knowing certain p^{th} power residue symbols. The transition data are obtained by computing various "mock" p^{th} power residue symbols in the cyclotomic field $\mathbf{Q}(\zeta_p)$, which are linked to true power residue symbols by our "Extraction Lemma". The power residue symbols are related by the p^{th} Power Reciprocity Law. These computations form the "extraction" stage of the algorithm.

The final "consolidation" stage consists of systematically trying all possible values for $\operatorname{Ind}_q(r) \bmod p$ at one distinguished Euclidean prime $q = q(p)$ for each p. To exhaust all possibilities, it is thus necessary to try $\prod_{p \in \mathfrak{I}} p$ sets of values. For each set, a candidate divisor r of n is assembled and tested. If a divisor actually exists, then it corresponds to some set of values, and so will be constructed by this procedure.

Let us illustrate the computation and use of transition data in the case $p = 2$. Recall that for an odd prime v, and a number b not divisible by v, the Legendre symbol (b/v) is that root of unity defined by

$$\pm 1 = \left(\frac{b}{v}\right) \equiv b^{(v-1)/2} \bmod v.$$

Since (b/v) is $+1$ or -1 according as $\operatorname{Ind}_v(b)$ is even or odd, knowing (b/v) is equivalent to knowing $\operatorname{Ind}_v(b) \bmod 2$. The Legendre symbol can be extended by multiplicativity to give the Jacobi symbol (= quadratic power residue symbol): if an odd number c has the prime factorization $c = \pm v_1^{k_1} \cdots v_t^{k_t}$ and $(b, c) = 1$, then $(b/c) = \prod (b/v_i)^{k_i}$. Note that (b/c) does not depend on the sign of c but only on the ideal in $\mathbf{Z}$ it generates. If b is also odd, then (b/c) and (c/b) are related by the Quadratic Reciprocity Law:

$$\left(\frac{b}{c}\right) = \left(\frac{c}{b}\right) \cdot (-1)^{\frac{b-1}{2} \cdot \frac{c-1}{2} + \frac{\operatorname{sgn} b-1}{2} \cdot \frac{\operatorname{sgn} c-1}{2}}.$$

The key observation is that even if n is not prime, useful information can be obtained from the Legendre congruence. Define the *mock residue symbol* $\langle b/n \rangle_2$ by

$$\left\langle \frac{b}{n} \right\rangle_2 = \begin{cases} \pm 1 \equiv b^{(n-1)/2} \operatorname{mod} n, & \text{if such a congruence holds} \\ 0, & \text{otherwise.} \end{cases}$$

If $\langle b/n \rangle_2 = 0$, then n is composite (Fermat's Little Theorem). Our Extraction Lemma (see §4) says that relations between mock residue symbols also hold between the Legendre symbols at primes r dividing n. More precisely, if b is such that $\langle b/n \rangle_2 = -1$, then for any m, c,

$$\left\langle \frac{b}{n} \right\rangle_2^m = \left\langle \frac{c}{n} \right\rangle_2 \text{ implies } \left(\frac{b}{r}\right)^m = \left(\frac{c}{r}\right).$$

The Extraction Lemma will be proved in greater generality below.

In the algorithm we shall compute $\langle -q/n \rangle_2$ for each Euclidean prime $q > 2$. (The choice of $-q$ rather than q is made so that the factor in the Reciprocity Law will be trivial: in the algorithm, the odd q's will be congruent to $3 \operatorname{mod} 4$.) If some $\langle -q/n \rangle_2 = 0$ then n is composite, so assume they are all non-zero. Also assume for convenience that, say, $\langle -q_0/n \rangle_2 = -1$. (If each $\langle -q/n \rangle_2 = 1$, then in the probabilistic version of the algorithm we look for some γ such that $\langle \gamma/n \rangle_2 = -1$, while in the deterministic version we avoid the impasse by checking higher congruences akin to those in the strong pseudoprime test of Miller.) For each $q > 2$ there thus exists an $m_q = 0$ or 1 such that

$$\left\langle \frac{-q_0}{n} \right\rangle_2^{m_q} = \left\langle \frac{-q}{n} \right\rangle_2.$$

The m_q are the transition data. If r is a prime factor of n, then by the Extraction Lemma and the Quadratic Reciprocity Law

$$\left(\frac{-q_0}{r}\right)^{m_q} = \left(\frac{-q}{r}\right) = \left(\frac{r}{-q}\right) = \left(\frac{r}{q}\right).$$

Thus if we knew $(-q_0/r)$ $(= (-1)^{\operatorname{Ind} q_0(r) \operatorname{mod} 2})$, we could obtain (r/q), and hence $\operatorname{Ind}_q(r) \operatorname{mod} 2$, for all $q > 2$.

In generalizing the above for $p > 2$, we encounter the problem that in order to obtain a satisfactory p^{th} Power Reciprocity Law, it is necessary to work in $\mathbf{Q}(\zeta_p)$ rather than in $\mathbf{Q}$. This causes two further difficulties. First, in $\mathbf{Q}(\zeta_p)$ the ideal (q), where $q \equiv 1 \bmod p$, is no longer prime and the prime ideals into which it factors may be non-principal. Since the Reciprocity Law only permits one to "flip" field elements, not ideals, it is necessary to find a surrogate for q. Such an element is provided by an appropriate Jacobi sum. Second, the ideal (n) itself generally factors in $\mathbf{Q}(\zeta_p)$, so it is necessary to compute certain ideals which behave like the primes above n.

3. Some prerequisites

This section collects the relevant facts from algebraic number theory used in the algorithm. Much of what follows is standard and well-known.

Cyclotomic fields. We restrict our attention to cyclotomic fields of prime level p. A good reference is Birch's article in Cassels-Fröhlich [8]. Let

$$\zeta_p = e^{2\pi i/p}$$

be a primitive p^{th} root of 1, whose irreducible polynomial over $\mathbf{Q}$ is the p^{th} cyclotomic polynomial

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + 1.$$

The ring of algebraic integers in $\mathbf{Q}(\zeta_p)$ is $\mathbf{Z}[\zeta_p]$.

The factorization of a rational prime q into prime ideals in $\mathbf{Z}[\zeta_p]$ is determined by its congruence class mod p. In particular, (q) is ramified if and only if $q = p$: in fact

$$(p) = (\lambda)^{p-1}, \quad \text{where } \lambda = 1 - \zeta_p.$$

Otherwise (q) is the product of $g = (p-1)/f$ distinct prime ideals

$$(q) = \mathfrak{Q}_1 \cdots \mathfrak{Q}_g$$

where f is the order of q in $(\mathbf{Z}/p)^\times$. The norm of each of these primes is

$$N\mathfrak{Q}_i \overset{\text{def}}{=} \#\left[\mathbf{Z}[\zeta_p]/\mathfrak{Q}_i\right] = q^f \equiv 1 \bmod p. \tag{3.1}$$

The polynomial $\Phi_p(x)$ factors mod q as

$$\Phi_p(x) \equiv \prod_{i=1}^{g} h_i(x) \bmod q$$

where the $h_i(x)$ are distinct, monic polynomials of degree f which are irreducible mod q. From this factorization we can find the $\mathfrak{Q}_i$ precisely, using the following special case of Kummer's theorem.

Proposition 1. *The prime ideals in* $\mathbf{Z}[\zeta_p]$ *lying over* (q) *are*

$$\mathfrak{Q}_i = (q, h_i(\zeta_p)) \quad \textit{for } i = 1,\ldots,g.$$

The Galois group of $\mathbf{Q}(\zeta_p)/\mathbf{Q}$ is also known: it is canonically isomorphic to $(\mathbf{Z}/p)^\times$, the isomorphism being $\sigma_u \leftrightarrow u$, where $\sigma_u(\zeta_p) = \zeta_p^u$.

If n is a possibly composite number which behaves enough like a prime, then a variant of Kummer's Theorem applies to it as well.

Proposition 2. *Suppose* $n \geq 2$ *is an integer,* n *has order* f *in* $(\mathbf{Z}/p)^\times$, *and* $g = (p-1)/f$. *Also suppose*

$$\Phi_p(x) \equiv \prod_{i=1}^{g} h_i(x) \bmod n$$

where the $h_i(x)$ *are monic polynomials in* $\mathbf{Z}[x]$ *each of degree* f. *Consider the ideals* $\mathfrak{A}_i = (n, h_i(\zeta_p))$ *in* $\mathbf{Z}[\zeta_p]$. *If* r *is a prime factor of* n, *then in* $\mathbf{Z}[\zeta_p]$

$$(r) = \prod_{i=1}^{g} (r, \mathfrak{A}_i)$$

and each $(r, \mathfrak{A}_i)$ *is divisible by the same number of prime ideals of* $\mathbf{Z}[\zeta_p]$ *lying over* r.

Proof. Let

$$\Phi_p(x) \equiv \prod_{j=1}^{k} v_j(x) \bmod r$$

be the decomposition into monic irreducible factors in $(\mathbf{Z}/r)[x]$. There are no repeated factors since $p \neq r$ (using $p \nmid n$). By Proposition 1, the primes over r are the ideals

$$\mathfrak{R}_j = (r, v_j(\zeta_p)), \qquad j = 1,\ldots,k.$$

But each $h_i(x)$ is uniquely a product mod r of certain $v_j(x)$ and each $v_j(x)$ is a divisor mod r of some $h_i(x)$ since $\mathbf{Z}/r$ is a field. Thus each $(r, \mathfrak{A}_i)$ is precisely the product of those $\mathfrak{R}_j$ corresponding to the $v_j(x)$ which divide $h_i(x) \bmod r$. Our assertions then follow.

Remark. It is not difficult to show that if d is any divisor of n, then $(d) = \prod_{i=1}^{g} (d, \mathfrak{A}_i)$.

The p^{th} *Power Reciprocity Law.* In $\mathbf{Q}(\zeta_p)$ it is possible to formulate a p^{th} Power Reciprocity Law. Let $\mathfrak{Q}$ be a non-zero prime of $\mathbf{Q}(\zeta_p)$ not dividing p, and let $v_{\mathfrak{Q}}(\ )$ denote the corresponding exponential valuation. Note that by (3.1), $N\mathfrak{Q} - 1$ is divisible by p. For any $\alpha \in \mathbf{Q}(\zeta_p)$ with $v_{\mathfrak{Q}}(\alpha) = 0$, define the p^{th}

power residue symbol $(\alpha/\mathfrak{Q})_p$ to be the unique p^{th} root of unity satisfying the congruence

$$\left(\frac{\alpha}{\mathfrak{Q}}\right)_p = \zeta_p^i \equiv \alpha^{(N\mathfrak{Q}-1)/p} \bmod \mathfrak{Q}.$$

Just as with the Jacobi symbol, the p^{th} power residue symbol can be extended by multiplicativity in its lower argument. It can further be extended to field elements by setting

$$\left(\frac{\alpha}{\gamma}\right)_p \overset{\text{def}}{=} \prod_{\mathfrak{Q}\nmid p,\, \alpha} \left(\frac{\alpha}{\mathfrak{Q}}\right)^{v_{\mathfrak{Q}}(\gamma)}.$$

Proposition 3 (p^{th}*Power Reciprocity Law*). *Take $p > 2$ and let α, γ be elements of $\mathbf{Q}(\zeta_p)$ relatively prime to λ and to each other. Then there is an independently defined p^{th} root of unity $(\alpha, \gamma)_\lambda$ (called the norm residue symbol) such that*

$$\left(\frac{\alpha}{\gamma}\right)_p = \left(\frac{\gamma}{\alpha}\right)_p (\alpha, \gamma)_\lambda.$$

This result is a somewhat specialized form of the corollary on p. 171 of Artin-Tate [4]. (The norm residue symbols for archimedean valuations have been omitted, since as noted on p. 172 of [4], they are trivial at valuations where the completion is **C**.) The symbol $(\alpha, \gamma)_\lambda$ is multiplicative in both arguments and is not changed when α or γ is multiplied by a p^{th} power (see pp. 150–151 of [4]).

There exist closed formulas for the norm residue symbol, but here we simply need

Proposition 4. *If $\alpha \equiv 1 \bmod \lambda^i$, $\gamma \equiv 1 \bmod \lambda^j$ and $i + j \geq p + 1$, then $(\alpha, \gamma)_\lambda = 1$.*

The proposition is given as Exercise 2.13b, p. 354 of [8], and is an immediate consequence of Lemma 3, p. 158 and Theorem 9, p. 163 of [4].

We also note the functoriality of the power residue symbol under the Galois group: for any $\sigma \in \text{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q})$ it follows from the defining congruence that

$$\left(\frac{\sigma\alpha}{\sigma\mathfrak{Q}}\right)_p = \sigma\left(\frac{\alpha}{\mathfrak{Q}}\right)_p. \tag{3.2}$$

We now consider power residue symbols in the special case where q is a rational prime and $p \mid q - 1$. Let $t = t_q$ be a primitive root for q. Then

$$\Phi_p(x) \equiv \prod_{i=1}^{p-1} \left(x - t^{((q-1)/p)i}\right) \bmod q,$$

so by Proposition 1 there is a "canonical" prime $\mathfrak{Q}$ lying over q in $\mathbf{Z}[\zeta_p]$

(canonical in terms of the choice of t_q):

$$(3.3)\qquad \mathfrak{Q} = \left(q, \zeta_p - t^{(q-1)/p}\right).$$

If x is a rational integer, then similarly to the case $p = 2$ we have

$$(3.4)\qquad \left(\frac{x}{\mathfrak{Q}}\right)_p = \zeta_p^{\mathrm{Ind}_q(x)}$$

where we compute indices with respect to t. Indeed

$$(3.5)\qquad \left(\frac{x}{\mathfrak{Q}}\right)_p \equiv x^{(q-1)/p} \equiv t^{\mathrm{Ind}_q(x)(q-1)/p} \equiv \zeta_p^{\mathrm{Ind}_q(x)} \bmod \mathfrak{Q}$$

by the definition of $\mathfrak{Q}$. Thus knowing $(x/\mathfrak{Q})_p$ for the canonical prime $\mathfrak{Q}$ is equivalent to knowing $\mathrm{Ind}_q(x) \bmod p$.

Jacobi sums. The power residue symbols can also be used to compute Jacobi sums, certain elements of $\mathbf{Z}[\zeta_p]$ with known factorizations into prime ideals. Their use enables us to circumvent the difficulties that might be expected to arise when the class number of $\mathbf{Q}(\zeta_p)$ exceeds 1. The principal virtues of Jacobi sums are their computability and their known factorization; but they satisfy congruence properties helpful in the p^{th} Power Reciprocity Law, as well.

In general, if $\mathfrak{Q}$ is a prime of $\mathbf{Q}(\zeta_p)$ not dividing p and if $a, b \in \mathbf{Z}$, we define the Jacobi sum

$$J_{a,b}(\mathfrak{Q}) = \sum{}' \left(\frac{x}{\mathfrak{Q}}\right)_p^{-a} \left(\frac{1-x}{\mathfrak{Q}}\right)_p^{-b}$$

where Σ' denotes the sum over a set of coset representatives x of $\mathbf{Z}[\zeta_p]/\mathfrak{Q}$ other than $0, 1 \bmod \mathfrak{Q}$. The prime factorization of $(J_{a,b}(\mathfrak{Q}))$ is given by the following result; recall that $[x]$ denotes the greatest integer not exceeding x.

PROPOSITION 5 (Stickelberger). *Suppose $a, b \in \mathbf{Z}$ with $ab(a+b) \not\equiv 0 \bmod p$. For $u \in \mathbf{Z}$, let*

$$\theta_{a,b}(u) = \left[\frac{a+b}{p}u\right] - \left[\frac{a}{p}u\right] - \left[\frac{b}{p}u\right],$$

so that $\theta_{a,b}(u) = 0$ or 1. Then

$$(J_{a,b}(\mathfrak{Q})) = \prod_{u=1}^{p-1} \sigma_u^{-1}(\mathfrak{Q})^{\theta_{a,b}(u)}.$$

(This result is Theorem 11, p. 98 in Lang [14], except that the conditions on a and b are omitted there.)

We shall also need the following two results. The first is used to show that in our cases of the p^{th} Power Reciprocity Law, the norm residue symbols are trivial.

The second will imply that Jacobi sums are "good" surrogates for primes $\mathfrak{Q}$ in $\mathbf{Q}(\zeta_p)$; that is, useful information can be extracted from them.

PROPOSITION 6. (Iwasawa [13], Theorem 1). *For all* $a, b \in \mathbf{Z}$,

$$-J_{a,b}(\mathfrak{Q}) \equiv 1 \bmod \lambda^2.$$

PROPOSITION 7. *If* $p > 2$, *there exist* $a, b \in \mathbf{Z}$ *such that* $ab(a+b) \not\equiv 0 \bmod p$ *and*

$$\hat{\theta}_{a,b} \overset{\text{def}}{=} \sum_{u=1}^{p-1} \theta_{a,b}(u) \cdot u^{-1} \not\equiv 0 \bmod p$$

where u^{-1} *denotes an inverse to* $u \bmod p$.

Proof. Note that for $1 \leq u \leq p-1$, we have $[u/p] = 0$ and

$$[((p-1)/p)u] = u - 1.$$

Hence

$$\sum_{m=1}^{p-2} \hat{\theta}_{m,1} = \sum_{m=1}^{p-2} \sum_{u=1}^{p-1} \left(\left[\frac{(m+1)u}{p} \right] - \left[\frac{mu}{p} \right] \right) u^{-1}$$

$$= \sum_{u=1}^{p-1} \left[\frac{(p-1)}{p} u \right] u^{-1} = \sum_{u=1}^{p-1} (u-1)u^{-1} \equiv p - 1 \not\equiv 0 \bmod p.$$

So there is at least one "good" pair (a, b) among $(m, 1)$ for $m = 1, \ldots, p-2$.

We remark that $\hat{\theta}_{a,b} \equiv ((a+b)^p - a^p - b^p)/(p) \bmod p$, so that for all $p < 10^9$ except for $p = 1093$ and 3511, one can take $a = b = 1$.

4. The probabilistic version of the algorithm

We are now in a position to present the algorithm in detail. In this section we shall describe an informal probabilistic version for clarity of presentation. In the next section we shall carry out the changes needed to make the algorithm deterministic and give a more formal statement.

Primality Algorithm (probabilistic version).

Let n be a natural number. (If the algorithm is actually being implemented, assume n has passed standard pseudo-primality tests and so is almost certainly prime.)

A. "*Preparation Step*"

A.1. **Compute** $f(n)$, **the least square-free natural number such that**

$$\prod_{\substack{q-1 \mid f(n) \\ q \text{ prime}}} q > n^{1/2}.$$

Define the *initial primes* for n to be the prime factors p of $f(n)$. Define the *Euclidean primes* for n to be the primes q for which $q - 1 \mid f(n)$. Since there are infinitely many primes q such that $q - 1$ is square-free (Mirsky [21]), $f(n)$ always exists. We will show in Section 6 that

$$f(n) \leq (\log n)^{c_0 \log\log\log n}$$

for all large n. We believe (but cannot prove) that taking the product of the initial segment of primes up to

$$\frac{1+\varepsilon}{\log 2} \log\log n \log\log\log n$$

will provide enough Euclidean primes. An unimaginative but sure way of computing $f(n)$ is to compute sequentially for each square-free $k = 1, 2, 3, 5, 6, \ldots$ the product

$$\prod_{\substack{q-1 \mid k \\ q \text{ prime}}} q$$

stopping as soon as a value of k is found for which the product exceeds $n^{1/2}$. The number of computational operations required for each k is at most k^c for some constant c, so the time needed to compute $f(n)$ is at most $f(n)^{c+1}$.

A.2. **Compute and fix a primitive root t_q for each Euclidean prime q (for example, the smallest positive primitive root). Also check that n is divisible by no p or q.**

A.3. **For each initial prime $p > 2$, find $a, b \in \mathbf{Z}$ such that $0 < a,\ b < p$, $a + b \equiv 0 \bmod p$, and**

$$\hat{\theta}_{a,b} = \sum_{u=1}^{p-1} \theta_{a,b}(u) \cdot u^{-1} \not\equiv 0 \bmod p$$

as guaranteed by Proposition 7. For $p = 2$, let $a = b = \hat{\theta}_{a,b} = 1$.

A.4. **Compute a "Jacobi sum" $J_p(q)$ for each initial prime p and Euclidean prime q with $p \mid q - 1$ as follows.**

If $p = 2$, put $J_p(q) = -q$.

If $p > 2$, let

$$J_p(q) = -J_{a,b}(\mathcal{Q}) = -\sum_{x=2}^{q-1} \left(\frac{x}{\mathcal{Q}}\right)_p^{-a} \left(\frac{1-x}{\mathcal{Q}}\right)_p^{-b} \in \mathbf{Q}(\zeta_p),$$

where a, b are the integers computed in A.3 and $\mathcal{Q}$, defined by (3.3), is the "canonical" prime over q with respect to t_q. (Since $\mathbf{Z}[\zeta_p]/\mathcal{Q} \cong \mathbf{Z}/q$, rational integers can be used as coset representatives in computing the Jacobi sum.) To

compute a power residue symbol $(x/\mathfrak{Q})_p = \zeta_p^j$ it suffices to make a table of $t^{j(q-1)/p}$ for $j = 0, 1, \ldots, p-1$, compute and look up $x^{(q-1)/p}$, and thus determine j as in (3.5). Moreover, if $p > 2$ and if r is any rational number prime to p, then the norm residue symbol $(J_p(q), r)_\lambda$ is trivial. Indeed,

$$\big(J_p(q), r\big)_\lambda = \big(J_p(q), r^{1-p}\big)_\lambda = \left(J_p(q), (r^{-1})^{p-1}\right)_\lambda$$

since the norm residue symbol is unaffected by p^{th} powers. But

$$(r^{-1})^{p-1} \equiv 1 \bmod \lambda^{p-1}$$

by Fermat's Little Theorem and the fact that $(\lambda^{p-1}) = (p)$. Also

$$J_p(q) \equiv 1 \bmod \lambda^2$$

by Proposition 6. Thus our assertion that $(J_p(q), r)_\lambda = 1$ follows from Proposition 4.

A.5. **For each p, factor n into ideals in $\mathbf{Z}[\zeta_p]$ as it would split if it were prime (no computations are needed if $p = 2$).** We attempt to do this as follows. Let f be the order of n in $(\mathbf{Z}/p)^\times$, put $g = (p-1)/f$, and try to factor

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + 1 \equiv \prod_{i=1}^{g} h_i(x) \bmod n$$

where each $h_i(x) \in \mathbf{Z}[x]$ is monic and has degree f. If n is in fact prime, then with high probability of success $\Phi_p(x)$ can be so factored over $\mathbf{Z}/n$ by the probabilistic method of Berlekamp [5] or of Rabin [31] in time polynomial in p and $\log n$. Note that the algorithm may diverge here, even if n is prime. But for a probabilistic algorithm, it is only necessary that if n is prime, there is high probability that a proof of primality will eventually be found. If the factorization can be carried out, we will be in the situation of Proposition 2 of Section 3. Put

$$\mathfrak{Q}_i = \big(n, h_i(\zeta_p)\big), \qquad i = 1, \ldots, g.$$

B. "*Extraction Step*"

Suppose $\mathfrak{Q}$ is an ideal of $\mathbf{Z}[\zeta_p]$ not dividing (λ) and $\alpha \in \mathbf{Z}[\zeta_p]$. We saw in Section 3 that if $\mathfrak{Q}$ is a proper prime ideal and if $\alpha \notin \mathfrak{Q}$, then $\alpha^{(N\mathfrak{Q}-1)/p}$ is congruent mod $\mathfrak{Q}$ to a p^{th} root of 1. This may still occur even if $\mathfrak{Q}$ is not prime, so that $\mathfrak{Q}$ would be analogous to a rational pseudoprime. However, since $\mathfrak{Q} \nmid (\lambda)$, this can hold for at most one such root of unity. We define the *mock residue symbol* $\langle \alpha/\mathfrak{Q} \rangle_p$ to be

$$\left\langle \frac{\alpha}{\mathfrak{Q}} \right\rangle_p = \begin{cases} \zeta_p^j \equiv \alpha^{(N\mathfrak{Q}-1)/p} \bmod \mathfrak{Q}, & \text{if such a congruence holds,} \\ 0, & \text{otherwise.} \end{cases}$$

B.1. **For each initial prime p and each Euclidean prime q with $p \mid q-1$, compute the mock residue symbols**

$$\left\langle \frac{J_p(q)}{\mathfrak{A}_i} \right\rangle_p \quad \text{for } i = 1, \ldots, g$$

for the ideals $\mathfrak{A}_i$ found in A.5 and the $J_p(q)$ defined in A.4. Note that g and the $\mathfrak{A}_i$ depend on p. **If any of the mock residue symbols are 0, declare n composite.**

In the next section we will show that the computation of a mock residue symbol can be accomplished in time polynomial in p and $\log n$ ($\leq f(n)$). We need to compute $g \leq p-1$ mock residue symbols for each pair p, q with $p \mid q-1$. It is clear that the number of Euclidean primes is less than $f(n)$, so this step of the algorithm can be completed in time polynomial in $f(n)$.

B.2. **For each initial prime p do the following. If the mock residue symbols for p are not all equal to 1, choose some nontrivial one, $\langle \gamma/\mathfrak{A}\rangle_p$, and call it the distinguished symbol corresponding to p. If they are all 1, compute mock residue symbols $\langle \gamma/\mathfrak{A}_i\rangle_p$ for other γ's chosen at random in $\mathbf{Z}[\zeta_p]$, until one is found to be not 0 or 1 and designate it the distinguished symbol.** (Again, the algorithm may diverge here, but if n is prime the probability of an arbitrarily chosen γ working is roughly $(p-1)/p$.)

B.3. **For each pair p, q with $p \mid (q-1)$, compute the exponents $m_{i,q}$ such that**

$$\left\langle \frac{\gamma}{\mathfrak{A}} \right\rangle_p^{m_{i,q}} = \left\langle \frac{J_p(q)}{\mathfrak{A}_i} \right\rangle_p, \quad 0 \leq m_{i,q} < p. \tag{4.1}$$

These relations are preserved for the power residue symbols at prime ideals dividing the $\mathfrak{A}_i$ as we now see.

Extraction Lemma. *Let $\mathfrak{A}$ and $\mathfrak{A}_1$ be ideals of $\mathbf{Z}[\zeta_p]$ such that $p \nmid N\mathfrak{A} = N\mathfrak{A}_1$ and let $\mathfrak{R}, \mathfrak{R}_1$ be conjugate prime ideals dividing $\mathfrak{A}$ and $\mathfrak{A}_1$ respectively. Suppose there is some $\gamma \in \mathbf{Z}[\zeta_p]$ such that $\langle \gamma/\mathfrak{A}\rangle_p$ is not 0 or 1. Then for any $\alpha_1 \in \mathbf{Z}[\zeta_p]$, the relation (where $m \in \mathbf{Z}$)*

$$\left\langle \frac{\gamma}{\mathfrak{A}} \right\rangle_p^{m} = \left\langle \frac{\alpha_1}{\mathfrak{A}_1} \right\rangle_p \tag{A}$$

implies

$$\left(\frac{\gamma}{\mathfrak{R}} \right)_p^{m} = \left(\frac{\alpha_1}{\mathfrak{R}_1} \right)_p. \tag{B}$$

Proof. The initial hypothesis is that $\gamma^{(N\mathfrak{A}-1)/p} \equiv \zeta_p^j \bmod \mathfrak{A}$ for some $j \not\equiv 0 \bmod p$. Reducing this congruence mod $\mathfrak{R}$, we see that

$$v_p(N\mathfrak{R}-1) > v_p\left(\frac{N\mathfrak{A}-1}{p}\right) \tag{4.2}$$

(where $v_p(t)$ is defined by $p^{v_p(t)} \,\|\, t$) since $\zeta_p^j \not\equiv 1 \bmod \mathfrak{R}$ and $N\mathfrak{R} - 1$ is the order of $(\mathbf{Z}[\zeta_p]/\mathfrak{R})^{\times}$.

First suppose $\mathfrak{R} = \mathfrak{R}_1$. Then reducing the relation (A) mod $\mathfrak{R}$ and using $N\mathfrak{Q} = N\mathfrak{Q}_1$, we obtain

$$(4.3) \qquad \left(\gamma^{(N\mathfrak{Q}-1)/p}\right)^m \equiv \left\langle \frac{\gamma}{\mathfrak{Q}} \right\rangle_p^m = \left\langle \frac{\alpha_1}{\mathfrak{Q}_1} \right\rangle_p \equiv \alpha_1^{(N\mathfrak{Q}-1)/p} \bmod \mathfrak{R}.$$

The multiplicative group of a finite field is cyclic, so we may compute indices with respect to some primitive root τ. Thus (4.3) may be rewritten

$$(4.4) \qquad \tau^{(m \operatorname{Ind}(\gamma) - \operatorname{Ind}(\alpha_1))(N\mathfrak{Q}-1)/p} \equiv 1 \bmod \mathfrak{R}.$$

Since the order of τ is $N\mathfrak{R} - 1$, (4.2) and (4.4) imply

$$p \mid \left(m \operatorname{Ind}(\gamma) - \operatorname{Ind}(\alpha_1)\right).$$

But this in turn means that (4.4) holds with "$N\mathfrak{R}$" replacing "$N\mathfrak{Q}$". Making the substitution and unwinding the resulting congruence give

$$\left(\gamma^{(N\mathfrak{R}-1)/p}\right)^m \equiv \alpha_1^{(N\mathfrak{R}-1)/p} \bmod \mathfrak{R};$$

that is, (B).

In general, let σ be an automorphism of $\mathbf{Q}(\zeta_p)$ such that $\sigma\mathfrak{R} = \mathfrak{R}_1$. Then, as is immediately seen from the definitions,

$$\left\langle \frac{\alpha_1}{\mathfrak{Q}_1} \right\rangle_p = \sigma \left\langle \frac{\sigma^{-1}\alpha_1}{\sigma^{-1}\mathfrak{Q}_1} \right\rangle_p = \left\langle \frac{\sigma^{-1}\alpha_1}{\sigma^{-1}\mathfrak{Q}_1} \right\rangle_p^j$$

if $\sigma(\zeta_p) = \zeta_p^j$. Hence replacing α_1 by $\sigma^{-1}\alpha_1$, $\mathfrak{Q}_1$ by $\sigma^{-1}\mathfrak{Q}_1$, and m by mj^{-1} where j^{-1} is an inverse of $j \bmod p$, we are reduced to the previous case, completing the proof.

The Extraction Lemma and the relations (4.1) among the mock residue symbols allow us to compute many power residue symbols in terms of one unknown one, via the following calculation.

Suppose r is a prime number dividing n. Let $p > 2$ be an initial prime. Suppose $\langle \gamma/\mathfrak{Q} \rangle_p$ is the distinguished symbol corresponding to p. Knowing this mock residue symbol does not allow us to compute the power residue symbol $(\gamma/(r, \mathfrak{Q}))_p$, but there are only p possibilities for it. We now show that the value of $(\gamma/(r, \mathfrak{Q}))_p$ completely determines each $\operatorname{Ind}_q(r) \bmod p$ for every Euclidean prime q with $p \mid q - 1$.

This idea is to evaluate $(J_p(q)/r)_p$ in two ways. First, note that

$$\left(\frac{J_p(q)}{r}\right)_p = \left(\frac{r}{J_p(q)}\right)_p \left(J_p(q), r\right)_\lambda = \left(\frac{r}{J_p(q)}\right)_p$$

by the Power Reciprocity Law (Proposition 3) and step A.4. On the one hand

$$\left(\frac{r}{J_p(q)}\right)_p = \prod_{u=1}^{p-1}\left(\frac{r}{\sigma_u^{-1}\mathcal{Q}}\right)_p^{\theta_{a,b}(u)} = \prod_{u=1}^{p-1}\sigma_u^{-1}\left(\frac{r}{\mathcal{Q}}\right)_p^{\theta_{a,b}(u)}$$

$$= \prod_{u=1}^{p-1}\left(\frac{r}{\mathcal{Q}}\right)_p^{u^{-1}\theta_{a,b}(u)} = \left(\frac{r}{\mathcal{Q}}\right)_p^{\hat{\theta}_{a,b}}$$

where $\mathcal{Q}$ is the canonical prime lying over q. We have used the factorization of Jacobi sums (Proposition 5) and functoriality (equation (3.2)). On the other hand

$$\left(\frac{J_p(q)}{r}\right)_p = \prod_{i=1}^{g}\left(\frac{J_p(q)}{(r,\mathfrak{A}_i)}\right)_p = \prod_{i=1}^{g}\left(\frac{\gamma}{(r,\mathfrak{A})}\right)_p^{m_{i,q}} = \left(\frac{\gamma}{(r,\mathfrak{A})}\right)_p^{\Sigma_{i=1}^{g} m_{i,q}}$$

by Proposition 2, (4.1) and the Extraction Lemma. (Note that by Proposition 2 there is a one-to-one correspondence between the primes dividing $(r, \mathfrak{A}_i)$ and $(r, \mathfrak{A})$.)

Now a and b were specifically chosen in A.3 so that $\hat{\theta}_{a,b}$ is invertible mod p. Hence

$$\left(\frac{r}{\mathcal{Q}}\right)_p = \left(\frac{\gamma}{(r,\mathfrak{A})}\right)_p^{\hat{\theta}_{a,b}^{-1}\Sigma_{i=1}^{g} m_{i,q}}.$$

Thus from (3.4), if $(\gamma/(r,\mathfrak{A}))_p = \zeta_p^k$ then

$$\operatorname{Ind}_q(r) \equiv k\,\hat{\theta}_{a,b}^{-1}\sum_{i=1}^{g} m_{i,q} \bmod p. \tag{4.5}$$

C. "*Consolidation Step*"

If $p_1,\ldots,p_d$ are the initial primes and $\langle\gamma_i/\mathfrak{A}_i\rangle_{p_i}$ are the corresponding distinguished symbols found in step B.2, then for each prime factor r of n, there are integers $k_1,\ldots,k_d$ such that

$$\left(\frac{\gamma_i}{(r,\mathfrak{A}_i)}\right)_{p_i} = \zeta_{p_i}^{k_i}, \qquad i = 1,\ldots,d. \tag{4.6}$$

By the Chinese Remainder Theorem there is a single integer k defined modulo Πp_i, such that

$$\left(\frac{\gamma_i}{(r,\mathfrak{A}_i)}\right)_{p_i} = \zeta_{p_i}^{k}, \qquad i = 1,\ldots,d.$$

For each k, $1 \le k \le f(n) = \Pi p_i$, we assemble and test a possible divisor $r = r(k)$ of n.

C.1. **Use the Chinese Remainder Theorem to compute for each $q > 2$ integers $I(k, q)$ such that**

$$I(k, q) \equiv k\ \hat{\theta}_{a,b}^{-1} \sum_{i=1}^{g} m_{i,q} \bmod p$$

for each p with $p \mid q - 1$. Also let $I(k, 2) = 1$. If k corresponds to an actual prime factor r of n, then the $I(k, q)$ are the $\mathrm{Ind}_q(r) \bmod p$ (see (4.5)).

C.2. **For each q, compute the least positive integer**

$$r(k, q) \equiv t_q^{I(k, q)} \bmod q.$$

Again, if k corresponds to an actual prime factor r of n, then the $r(k, q)$ are the $r \bmod q$.

C.3. **Use the Chinese Remainder Theorem to compute the least positive integer $r(k)$ such that for each q, $r(k) \equiv r(k, q) \bmod q$.** Thus, if k corresponds to an actual prime factor r of n, then $r(k) \equiv r \bmod Q$ where Q is the product of the Euclidean primes. If $r \leq \sqrt{n} < Q$, then $r(k) = r$.

C.4. **Check whether $r(k) \mid n$. If it does and $r(k) \neq 1$, n declare n composite and halt. Otherwise continue with the next value of k.**

C.5. **Declare n prime.** For if n is composite it must have a prime factor $r \leq \sqrt{n}$.

From the above considerations, we have

THEOREM 1. *The above algorithm correctly determines whether n is prime or composite, if it terminates. There is an absolute, calculable constant $c_1 > 0$ such that for every $k \geq 1$, if n is prime, the algorithm terminates within $T_k(n)$ steps with probability greater than $1 - 2^{-k}$, where*

$$f(n) \leq T_k(n) \leq kf(n)^{c_1}.$$

Remark 4.1. If n is composite, and passes all the pseudo-primality tests in the Extraction Step, then it will be factored during the Consolidation Step. Thus it might appear that our algorithm gives a method for factoring. In fact, this is not so, for any composite n will almost certainly be rejected before or during the Extraction Step.

Remark 4.2. H. W. Lenstra, Jr. and R. Schroeppel independently noted that the map $k \to r(k)$ is a homomorphism from the additive group $\mathbf{Z}/f(n)$ to the multiplicative group $(\mathbf{Z}/Q)^{\times}$, where Q is the product of the Euclidean primes. Thus, after computing $r(1)$ by steps C.1–C.3, one immediately obtains $r(k)$ for $k > 1$ by the formula $r(k) \equiv r(1)^k \bmod Q$.

Lenstra went further, and showed that n itself is a generator for the group of $r(k) \bmod Q$, eliminating the need even to compute $r(1)$. As this is only a small facet of his recasting of the algorithm, we again refer the reader to his paper [19] and that of Cohen [9].

Remark. 4.3. The quantity $f(n)$ is deeply embedded in the algorithm, appearing in the computation of the Euclidean primes, the calculation of primitive roots and Jacobi sums for the larger Euclidean primes, and the number of trial divisors of n in the Consolidation Step. If there are large initial primes (a possibility we cannot a priori rule out) then it appears in the computation of mock residue symbols as well.

5. The deterministic version of the algorithm

As presented in the previous section, the algorithm failed to be deterministic at two points: the factorization of the polynomial $\Phi_p(x)$ mod n in step A.5, which was necessary to factor (n) into ideals in $\mathbf{Z}[\zeta_p]$; and the construction of an element $\gamma \in \mathbf{Z}[\zeta_p]$ such that the mock residue symbol $\langle \gamma/\mathfrak{C} \rangle_p$ was nontrivial in step B.2, which was needed to construct the transition data $m_{i,q}$ and to apply the Extraction Lemma.

We will deal with both problems simultaneously, replacing the factorization of (n) into ideals by a process involving forming the greatest common divisor of ideals, which will also construct the transition data. We then prove a strengthened version of the Extraction Lemma which eliminates the need for a "γ".

The mock residue symbols $\langle J_p(q)/\mathfrak{C}_i \rangle_p$ are a suggestive way of codifying congruences, but they obscure the fact that further information can be gained from higher congruences in the event that all of the mock residue symbols for a fixed p turn out to be 1. So, in the following, we drop the formalism of mock residue symbols and work directly with congruences.

Suppose steps A.1–A.4 of the probabilistic version of the algorithm have been carried out. Fix an initial prime p and let f be the order of n in $(\mathbf{Z}/p)^\times$. If n is prime and $\mathfrak{R}$ is a prime in $\mathbf{Z}[\zeta_p]$ lying over (n), then $N\mathfrak{R} = n^f$. Suppose $\alpha \in \mathbf{Z}[\zeta_p] - \mathfrak{R}$. If $(\alpha/\mathfrak{R})_p = 1$ and $p^2 \mid n^f - 1$, then $\alpha^{(n^f-1)/p^2}$ is a p^{th} root of 1 mod $\mathfrak{R}$; that is,

$$\alpha^{(n^f-1)/p^2} \equiv \zeta_p^j \bmod \mathfrak{R}$$

for some j. If $\zeta_p^j = 1$ and $p^3 \mid n^f - 1$, we similarly find that $\alpha^{(n^f-1)/p^3}$ is a p^{th} root of 1 mod $\mathfrak{R}$, and so on. Thus if $p^k \| n^f - 1$, then there is some s, $1 \le s \le k$, and some j with

(i) $\alpha^{(n^f-1)/p^s} \equiv \zeta_p^j \bmod \mathfrak{R}$ and

(ii) either $\zeta_p^j \ne 1$ or $s = k$.

If we have h numbers $\alpha_1, \ldots, \alpha_h \notin \mathfrak{R}$, then there is some s, $1 \le s \le k$, and integers $j_1, \ldots, j_h$ with

$$(5.1)\qquad \begin{aligned} &\text{(i)}\quad \alpha_i^{(n^f-1)/p^s} \equiv \zeta_p^{j_i} \bmod \mathfrak{N} \quad \text{for } i = 1, \ldots, h,\\ &\text{(ii)}\quad \text{either at least one } \zeta_p^{j_i} \neq 1 \quad \text{or} \quad s = k. \end{aligned}$$

If (5.1) holds simultaneously for several primes $\mathfrak{N}_l$ over (n) (that is, with the identical numbers $s, j_1, \ldots, j_h$) then (5.1) holds with the modulus $\mathfrak{A} = \Pi \mathfrak{N}_l$. Our goal is to find such a nontrivial ideal factor of (n) in the specific case when the $\alpha_1, \ldots, \alpha_h$ are the $J_p(q)$ for each Euclidean prime q with $p \mid q - 1$ and their conjugates $\sigma J_p(q)$ in $\mathbf{Z}[\zeta_p]$.

We now outline a procedure which will either do this, or show that n is composite.

Note that if n is prime, then by Proposition 1, any ideal in $\mathbf{Z}[\zeta_p]$ containing n will be generated by n and $h(\zeta_p)$, where $h(x)$ is a polynomial with integer coefficients with the property that $\bar{h} = (h \bmod n)$ divides $x^{p-1} + \cdots + x + 1$ in $(\mathbf{Z}/n)[x]$. If one adjoins an element $h_1(\zeta_p)$ of $\mathbf{Z}[\zeta_p]$ to $(n, h(\zeta_p))$, the result is the ideal $(n, h_2(\zeta_p))$ where $\bar{h}_2 = \gcd(\bar{h}, \bar{h}_1)$. This gcd may be computed by the ordinary Euclidean algorithm for polynomials, which involves division (by leading coefficients) in $\mathbf{Z}/n$. This latter division may be done using the Euclidean algorithm for integers. A moment's reflection shows that even if n is not prime, if the Euclidean algorithm for polynomials can be carried out for $\bar{h}$ and $\bar{h}_1$ then $(n, h(\zeta_p), h_1(\zeta_p)) = (n, h_2(\zeta_p))$. But the only way the Euclidean algorithm can fail is if at some stage, a nontrivial common divisor of n and some leading coefficient is found. In that case, n will have been factored.

The GCD *Process*. Let $\mathfrak{A}^0 = (n) = n\mathbf{Z}[\zeta_p]$.

Say now $1 \leq i \leq h$ and $\mathfrak{A}^{i-1}$ has been constructed. Consider the ideals $(\mathfrak{A}^{i-1}, \alpha_i^{(n^f-1)/p} - \zeta_p^j)$ for $j = 1, \ldots, p$, by the procedure above. If n factors, or if all the ideals are the identity ideal, declare n composite and halt. Otherwise, let $\mathfrak{A}^i$ be the first one which is nontrivial.

If, after constructing $\mathfrak{A}^h$, it has been possible to choose $\zeta_p^j \neq 1$ at some step, or if $p \nmid (n^f - 1)/p$, set $\mathfrak{A} = \mathfrak{A}^h$. Otherwise, continue the process, but with the exponent $(n^f - 1)/p^2$ in place of $(n^f - 1)/p$. If $1 \leq i \leq h$ and $\mathfrak{A}^{h+i-1}$ has been constructed, consider the ideals $(\mathfrak{A}^{h+i-1}, \alpha_i^{(n^f-1)/p^2} - \zeta_p^j)$ for $j = 1, \ldots, p$, and either declare n composite, or find an ideal $\mathfrak{A}^{h+i}$. If, after constructing $\mathfrak{A}^{2h}$ some ideal has been obtained for which $\zeta_p^j \neq 1$, or if $p \nmid (n^f - 1)/p^2$, put $\mathfrak{A} = \mathfrak{A}^{2h}$. Otherwise, continue with $(n^f - 1)/p^3$, and so on, until finally some s is reached such that it has been possible to choose some $\zeta_p^j \neq 1$, or $p \nmid (n^f - 1)/p^s$. Put $\mathfrak{A} = \mathfrak{A}^{sh}$. Clearly $s < (p/\log p) \log n$.

If n is prime, the GCD process will construct an ideal $\mathfrak{A}$ (in fact with minimal "s"), and will not falsely declare n composite.

It may be good to emphasize that the above operations with ideals can be carried out in time polynomial in p and $\log n$. All arithmetic operations may be done with polynomials modulo $\Phi_p(x) = x^{p-1} + \cdots + x + 1$ and modulo n, so there will not be too many coefficients and no coefficient will grow too large. Exponentiations can be done by the process of repeated squarings, and for the operation of the Galois group, if σ_t is an automorphism of $\mathbf{Q}(\zeta_p)/\mathbf{Q}$, and $h(\zeta_p) \in \mathbf{Z}[\zeta_p]$ is represented by $h(x)$, then $\sigma_t(h(\zeta_p))$ is represented by $h(x^t)$.

Finally, we remark that this construction is applicable to the ideals $\mathfrak{A}_i$ in steps B.1 and B.2 of the probabilistic version of the algorithm, showing that the mock residue symbols there can be computed in time polynomial in p and $\log n$ as well.

Generalized Extraction Lemma. *Let f denote the order of $n \bmod p$ and let $\mathfrak{A}$ be an ideal in $\mathbf{Z}[\zeta_p]$ dividing n. Let $\alpha_1, \ldots, \alpha_h \in \mathbf{Z}[\zeta_p]$ be given and suppose there is an integer $s \geq 1$ and integers j_i for $1 \leq i \leq h$ with*

(i) *each* $\alpha_i^{(n^f-1)/p^s} \equiv \zeta_p^{j_i} \bmod \mathfrak{A}$,

(ii) *either* $p \nmid (n^f - 1)/p^s$ *or some* $\zeta_p^{j_i} \neq 1$.

Then for any $\alpha, \beta \in \{\alpha_1, \ldots, \alpha_h\}$ and any integer m, the statement

(A) $(\alpha^{(n^f-1)/p^s})^m \equiv \beta^{(n^f-1)/p^s} \bmod \mathfrak{A}$,

implies the statement

(B) *for each prime ideal* $\mathfrak{R} \mid \mathfrak{A}$, $(\alpha/\mathfrak{R})_p^m = (\beta/\mathfrak{R})_p$.

Proof. For any $\mathfrak{R}$ dividing $\mathfrak{A}$ the congruence (A) also holds mod $\mathfrak{R}$, so that writing $I(\nu)$ for the index of ν with respect to a fixed generator τ of $(\mathbf{Z}[\zeta_p]/\mathfrak{R})^\times$, we obtain

$$\tau^{(I(\alpha)m - I(\beta))(n^f-1)/p^s} \equiv 1 \bmod \mathfrak{R}.$$

Since $\tau \bmod \mathfrak{R}$ has order $N\mathfrak{R} - 1$, this implies that

$$(I(\alpha)m - I(\beta))\frac{n^f - 1}{p^s} = l(N\mathfrak{R} - 1) \tag{5.2}$$

for some integer l. Since $p \nmid n$ and $n \in \mathfrak{R}$, we have $p \mid N\mathfrak{R} - 1$. Thus if we are in the case $p \nmid (n^f - 1)/p^s$, (5.2) implies

$$p \mid (I(\alpha)m - I(\beta)). \tag{5.3}$$

On the other hand, if some $\alpha_i^{(n^f-1)/p^s} \equiv \zeta_p^{j_i} \not\equiv 1 \bmod \mathfrak{A}$, then

$$N\mathfrak{R} - 1 \nmid I(\alpha_i)\frac{n^f - 1}{p^s}, \qquad N\mathfrak{R} - 1 \mid I(\alpha_i)\frac{n^f - 1}{p^{s-1}}.$$

Thus we have

$$v_p(N\mathfrak{R} - 1) > v_p\left(\frac{n^f - 1}{p^s}\right). \tag{5.4}$$

Using (5.4) in (5.2) shows that (5.3) holds in this case as well.

Hence

$$\tau^{(I(\alpha)m - I(\beta))(N\mathfrak{R}-1)/p} \equiv 1 \bmod \mathfrak{R},$$

so that $(\alpha^{(N\mathfrak{R}-1)/p})^m \equiv \beta^{(N\mathfrak{R}-1)/p} \bmod \mathfrak{R}$; that is, (B) holds.

If in the GCD process some $\alpha_i^{(n^f-1)/p^s} \equiv \zeta_p^{j_i} \not\equiv 1 \bmod \mathfrak{A}$, choose such an α_i and call it γ. Recall now that the α_i are the conjugates for the various $J_p(q)$, where $p \mid q - 1$ (p is fixed). Write $m(\sigma, q)$ for the unique integer with $0 \leq m(\sigma, q) \leq p - 1$ and

$$\left(\gamma^{(n^f-1)/p^s}\right)^{m(\sigma, q)} \equiv \left(\sigma J_p(q)\right)^{(n^f-1)/p^s} \bmod \mathfrak{A}. \tag{5.5}$$

If, on the other hand, each $\zeta_p^{j_i} = 1$, set $\gamma = \alpha_1$ and each $m(\sigma, q) = 0$. Note that (5.5) holds in this case as well. The $m(\sigma, q)$ form "transition data" which can be used similarly to the $m_{i,q}$ in the probabilistic version of the algorithm.

Indeed, suppose r is a prime factor of n. Let $\mathfrak{R}$ be a prime lying over r in $\mathbf{Z}[\zeta_p]$ which divides $\mathfrak{A}$ and suppose the order of $r \bmod p$ is $d = d_p$. Then for each q with $p \mid q - 1$ we have, as in step B.3 of the probabilistic version,

$$\left(\frac{J_p(q)}{r}\right)_p = \left(\frac{r}{J_p(q)}\right)_p = \left(\frac{r}{\mathfrak{Q}}\right)_p^{\hat{\theta}_{a,b}}$$

where $\hat{\theta}_{a,b}$ was chosen in step A.3 and $\mathfrak{Q} = (q, \zeta_p - t_q^{(q-1)/p})$ is the canonical prime lying over q described in step A.4. On the other hand, since $(r)^d = \prod_{j=1}^{p-1} \sigma_j \mathfrak{R}$, we have

$$\begin{aligned}\left(\frac{J_p(q)}{r}\right)_p^d &= \prod_{j=1}^{p-1} \left(\frac{J_p(q)}{\sigma_j \mathfrak{R}}\right)_p = \prod_{j=1}^{p-1} \sigma_j \left(\frac{\sigma_j^{-1} J_p(q)}{\mathfrak{R}}\right)_p \\ &= \prod_{j=1}^{p-1} \left(\frac{\sigma_j^{-1} J_p(q)}{\mathfrak{R}}\right)_p^j = \prod_{j=1}^{p-1} \left(\frac{\gamma}{\mathfrak{R}}\right)_p^{j \cdot m(\sigma_j^{-1}, q)} \\ &= \left(\frac{\gamma}{\mathfrak{R}}\right)_p^{\sum_{j=1}^{p-1} j \cdot m(\sigma_j^{-1}, q)}\end{aligned}$$

where we use (3.2), (5.5) and the Generalized Extraction Lemma.

Note that neither $(\gamma/\mathfrak{R})_p$ nor d is known, but that if $i = i_p$ is such that $(\gamma/\mathfrak{R})_p = \zeta_p^i$, then the above calculations together with (3.4) show that

$$\operatorname{Ind}_q(r) \equiv \left(d\hat{\theta}_{a,b}\right)^{-1} i \sum_{j=1}^{p-1} j \cdot m\left(\sigma_j^{-1}, q\right) \bmod p.$$

We conclude that there is some integer k, $1 \le k \le f(n)$, such that

$$\operatorname{Ind}_q(r) \equiv k\hat{\theta}_{a,b}^{-1} \sum_{j=1}^{p-1} j \cdot m\left(\sigma_j^{-1}, q\right) \bmod p$$

for every pair p, q with $p \mid q-1$. Indeed we just choose k so that $k \equiv d_p^{-1} i_p \bmod p$ for each p.

We now give a more formal statement of the algorithm.

Primality Algorithm (Deterministic Version)

On input n:

A′. “*Preparation Step*”

A′.1. Compute the least positive square-free integer $f(n)$ such that

$$\prod_{\substack{q-1 \mid f(n) \\ q \text{ prime}}} q > n^{1/2}.$$

Define the initial primes to be the prime factors of $f(n)$. Define the Euclidean primes to be the primes q with $q - 1 \mid f(n)$.

A′.2. Test whether any initial or Euclidean prime divides n; if one does and is not equal to n, declare n composite and halt. Compute the least positive primitive root t_q for each Euclidean prime q.

A′.3. For each initial prime $p > 2$, find integers a, b with $0 < a$, $b < p$, $a + b \equiv 0 \bmod p$, and

$$\hat{\theta}_{a,b} = \sum_{u=1}^{p-1} \theta_{a,b}(u) \cdot u^{-1} \equiv 0 \bmod p$$

as guaranteed by Proposition 7. For $p = 2$, put $a = b = \hat{\theta}_{a,b} = 1$.

A′.4. For each initial prime p and each Euclidean prime q with $p \mid q - 1$, fix the prime ideal

$$\mathfrak{Q}_q = \left(q, \zeta_p - t_q^{(q-1)/p}\right)$$

lying over q in $\mathbf{Z}[\zeta_p]$, where $\zeta_p = e^{2\pi i/p}$. Compute the Jacobi sum $J_p(q) \in \mathbf{Q}(\zeta_p)$:

if $p = 2$, put $J_p(q) = -q$,

if $p > 2$, put $J_p(q) = -J_{a,b}(\mathfrak{Q}_q) = -\sum_{x=2}^{q-1} \left(\frac{x}{\mathfrak{Q}_q}\right)_p^{-a} \left(\frac{1-x}{\mathfrak{Q}_q}\right)_p^{-b}$,

where a, b are the integers (depending on p) computed in A′.3 above.

B′. "*Extraction Step*"

B′.1. For each initial prime p, carry out the GCD process in $\mathbf{Q}(\zeta_p)$ with respect to n and the set of $\sigma J_p(q)$ where q ranges over all Euclidean primes with $p \mid q-1$ and σ ranges over $\mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q})$. Thus either declare n composite or construct a proper ideal $\mathfrak{A}$ in $\mathbf{Z}[\zeta_p]$, an integer $s \geq 1$, and integers $j(\sigma, q)$, with $1 \leq j(\sigma, q) \leq p$, such that

(i) each $(\sigma J_p(q))^{(n^f-1)/p^s} \equiv \zeta_p^{j(\sigma, q)} \bmod \mathfrak{A}$,

(ii) either $p \nmid (n^f - 1)/p^s$ or some $\zeta_p^{j(\sigma, q)} \neq 1$,

where f denotes the order of $n \bmod p$.

B′.2. For each initial prime p, do the following. If some $j(\sigma_0, q_0) \neq p$, let $\gamma = \sigma_0 J_p(q_0)$. In this case, construct integers $m(\sigma, q)$ for all σ, q such that $0 \leq m(\sigma, q) \leq p-1$ and

$$\left(\gamma^{(n^f-1)/p^s}\right)^{m(\sigma, q)} \equiv \left(\sigma J_p(q)\right)^{(n^f-1)/p^s} \bmod \mathfrak{A}.$$

If all $j(\sigma, q) = p$, set all $m(\sigma, q) = 0$.

C′. "*Consolidation Step*"

For each integer k, $1 \leq k \leq f(n)$, do C′.1 to C′.4.

C′.1. For each $q > 2$ use the Chinese Remainder Theorem to compute integers $I(k, q)$ such that

$$I(k, q) \equiv k\hat{\theta}_{a,b}^{-1} \sum_{j=1}^{p-1} j \cdot m\left(\sigma_j^{-1}, q\right) \bmod p$$

for each $p \mid q-1$. Also let $I(k, 2) = 1$.

C′.2. For each q, compute the least positive integer $r(k, q) \equiv t_q^{I(k, q)} \bmod q$.

C′.3. Use the Chinese Remainder Theorem to compute the least positive integer $r(k)$ such that $r(k) \equiv r(k, q) \bmod q$ for each q.

C′.4. Check whether $r(k) \mid n$. If it does and $r(k) \neq 1$ or n, declare n composite and halt. Otherwise continue with the next value of k.

C′.5. Declare n prime.

We have

THEOREM 2. *On input* $n > 1$, *the above algorithm correctly determines whether* n *is prime or composite. There is an absolute, positive, calculable* *constant c_2 such that the running time $T(n)$ satisfies*

$$f(n) \le T(n), \quad \text{if } n \text{ is prime},$$
$$T(n) \le f(n)^{c_2}, \quad \text{for all } n.$$

6. The running time

Recall that $f(n)$ denotes the least positive square-free integer such that the product of the primes q with $q - 1 \mid f(n)$ exceeds $\sqrt{n}$. We have seen above that the running time for either the probabilistic or deterministic algorithms is bounded above by $f(n)^c$, where c is a positive, absolute, calculable constant. Moreover, if n is prime, the running time is at least $f(n)$. In this section we obtain estimates for $f(n)$ and a closely related function $g(n)$ which appears in the Lenstra-Cohen variations of the algorithm. The function $g(n)$ is defined as the least positive integer (not necessarily square-free) such that the product of the primes q with $q - 1 \mid g(n)$ exceeds $\sqrt{n}$. Thus $g(n) \le f(n)$. While in practice $g(n)$ can be much smaller than $f(n)$, the main theorem of this section shows they are of the same rough order of magnitude.

THEOREM 3. *There are positive, absolute, calculable constants c_3, c_4 such that for all $n > 100$,*

$$(\log n)^{c_3 \log\log\log n} < g(n) \le f(n) < (\log n)^{c_4 \log\log\log n}.$$

The lower bound in Theorem 3 is relatively simple. What is needed is an upper bound for the number $d(k)$ of divisors of an integer k, such as that provided by a well-known theorem of Wigert [37]:

$$d(k) \le 2^{(1+o(1))\log k/\log\log k}. \tag{6.1}$$

However, we require a more explicit result than (6.1) to insure that the constant c_3 be calculable. This is easily provided by tracing through the proof of Wigert's theorem given by Ramanujan [32]. He uses the geometric mean-arithmetic mean inequality and partial summation to show (see displays (3), (19), (20) in [32])

$$\log d(k) \le \pi(P)\log\left(1 + \frac{\log k}{\theta(P)}\right) + \int_2^P \frac{1}{u\log^2 u}\int_2^u \frac{\pi(t)}{t}\,dt\,du$$

where P is the $\omega(k)$-th prime. Here, $\omega(k)$ is the number of distinct prime factors of k and

$$\pi(x) = \sum_{p \le x} 1, \qquad \theta(x) = \sum_{p \le x} \log p.$$

Using solely Chebyshev-type upper and lower bound estimates for $\pi(x)$ and $\theta(x)$ (e.g., see Davenport [10], Ch. 7), Ramanujan goes on (display (28)) to show that

$$d(k) \le 2^{\log k/\log\log k + O(\log k/(\log\log k)^2)}.$$

From his proof and the fact that the Chebyshev estimates can be made effectively, an upper bound for the implied constant is calculable.

Thus for all k beyond some computable point

$$d(k) \le (2.5)^{\log k/\log\log k}. \tag{6.2}$$

We conclude that if n is beyond some computable point and $k \le (\log n)^{\log\log\log n}$, then

$$\begin{aligned}\prod_{q-1|k} q &\le \prod_{d|k}(d+1) \le \prod_{d|k}(2d) = (2k^{1/2})^{d(k)}\\ &\le \left(2(\log n)^{(1/2)\log\log\log n}\right)^{(2.5)^{\log\log n}}\\ &= \exp\left\{\left(\log 2 + \tfrac{1}{2}\log\log n \log\log\log n\right)(\log n)^{\log(2.5)}\right\}\\ &< n^{1/2}.\end{aligned}$$

This calculation shows that $(\log n)^{\log\log\log n} < g(n)$ for all n beyond some computable point, and introducing the constant c_3 gives the lower bound in the theorem, for all $n > 100$.

The rest of this section will be devoted to the upper bound. To show $f(n)$ is small, it will be sufficient to show there is some small square-free integer with an inordinately large number of divisors of the form $p - 1$ with p prime. Prachar [29] has obtained such a result (without the square-free requirement) by showing, on the average, that all multiples of the product of a long initial segment of primes are such numbers. Our general strategy will be to follow Prachar's proof, but with two important differences. First, as mentioned in Section 1, we do not follow Prachar in using the result of Tatuzawa [36] that asserts that most arithmetic progressions $a \bmod k$ with $k < x^{c/\log\log x}$ have the "proper" number of primes below x. Instead we use a result of Gallagher as applied by Bombieri that essentially allows us to replace "$x^{c/\log\log x}$" with "x^{δ}" where $\delta > 0$ is a constant. This is Proposition 8 below. The second difference is that we wish to count only primes p for which $p - 1$ is square-free. This task is routinely accomplished in Proposition 9 by an inclusion-exclusion argument that is made simpler by the observation that most non-square-free numbers are divisible by a small square exceeding 1.

In this section the letter p denotes a variable prime and φ denotes Euler's function.

Proposition 8. *For every* $\varepsilon > 0$ *there are calculable positive numbers* $x_0 = x_0(\varepsilon)$, $\delta = \delta(\varepsilon)$ *such that if* $x \ge x_0(\varepsilon)$ *and* k, a *are coprime integers with*

$0 < k < x^{\delta}$, *then*

$$\left| \sum_{\substack{p \equiv a \bmod k \\ p \le x}} \log p - \frac{x}{\varphi(k)} \right| < \frac{\varepsilon x}{\varphi(k)},$$

except possibly for those k *which are multiples of a certain integer* $k_0(x) > (\log x)^{3/2}$.

This result follows from the proof of Linnik's theorem given on pp. 54–56 of Bombieri [6]. The main tool used on those pages is a result of Gallagher [12] on the number of non-exceptional zeros near the line $\sigma = 1$ of all L-series corresponding to primitive characters with conductor not exceeding some parameter. We use the result of Landau-Page (see Bombieri [6], p. 39) to estimate $k_0(x)$ rather than Siegel's theorem so as to assure our constants will be calculable. Proposition 8 is related to the result of Tatuzawa [36]. There the error term is smaller, but k is not permitted to be so large.

Let

$$\theta(x, k, a) = \sum_{\substack{p \le x \\ p \equiv a \bmod k}} \log p,$$

$$\theta_0(x, k, a) = \sum_{\substack{p \le x \\ p \equiv a \bmod k}} \mu^2(p - 1) \cdot \log p,$$

where μ denotes the Moebius function. Thus in the second sum we only count those primes p with $p - 1$ square-free. Let α denote Artin's constant,

$$\alpha = \prod_p \frac{p^2 - p - 1}{p^2 - p} \doteq 0.3740.$$

Let $\psi(k)$ denote the multiplicative function whose value at the prime power p^d is $(p^2 - p)/(p^2 - p - 1)$. Note that for all k, $\alpha \le \alpha\psi(k) < 1$.

PROPOSITION 9. *For every* $\varepsilon > 0$, *there exist calculable positive numbers* δ, x_0, T *such that if* $0 < k < x^{\delta}$, k *is square-free, and* $x \ge x_0$, *then*

$$\left| \theta_0(x, k, 1) - \frac{\alpha\psi(k)x}{k} \right| < \varepsilon \frac{x}{k}$$

provided $k_0(x) \nmid k^2 \prod_{p < T,\, p \nmid k} p^2$.

Proof. We consider separately the residue classes $a_1, \ldots, a_{\varphi(k)} \bmod k^2$ which satisfy $a_i \equiv 1 \bmod k$, $((a_i - 1)/k, k) = 1$. Let a denote one of these classes. If $(k, j) = 1$, let $R(j)$ denote the least positive integer which satisfies

$$R(j) \equiv a \bmod k^2, \qquad R(j) \equiv 1 \bmod j.$$

If $q_1 < q_2 < \ldots$ are the primes which do not divide k, we have by an inclusion-exclusion argument that

$$\theta_0(x, k^2, a) = \theta(x, k^2, a) - \sum_i \theta(x, k^2 q_i^2, R(q_i^2)) + \sum_{i<j} \theta(x, k^2 q_i^2 q_j^2, R(q_i^2 q_j^2)) - \cdots + \cdots. \tag{6.3}$$

Let $M(T)$ denote the right side of (6.3) where we only consider primes $q_i < T$. Thus if $Q = \Pi_{q_i < T} q_i$, then

$$\begin{aligned} M(T) &= \sum_{d|Q} (-1)^{\omega(d)} \theta(x, k^2 d^2, R(d^2)) \\ &= \theta_0(x, k^2, a) + \sum{}' \log p \\ &\leq \theta_0(x, k^2, a) + \sum_{\substack{m \geq T \\ (m, k) = 1}} \theta(x, k^2 m^2, R(m^2)), \end{aligned} \tag{6.4}$$

where Σ' denotes the sum over those $p < x$ such that $q_i^2 \mid p - 1$ for some $q_i \geq T$ and for no $q_i < T$. Note that if $m \geq x^{1/2}$, then $\theta(x, k^2m^2, R(m^2)) = 0$, since $k^2m^2 \geq x$ and $R(m^2) \geq m^2 + 1 > x$. Thus

$$\begin{aligned} &\sum_{\substack{m \geq T \\ (m, k) = 1}} \theta(x, k^2 m^2, R(m^2)) \\ &= \left(\sum_{\substack{x^{1/4} > m \geq T \\ (m,k)=1}} + \sum_{\substack{x^{1/2} > m \geq x^{1/4} \\ (m,k)=1}} \right) \theta(x, k^2 m^2, R(m^2)) \\ &\leq 3c_5 \sum_{\substack{m \geq T \\ (m,k)=1}} x/\varphi(k^2 m^2) + \log x \sum_{x^{1/2} > m \geq x^{1/4}} (1 + x/(k^2 m^2)) \\ &\leq \frac{(3c_5 c_6 + 1)x}{\varphi(k^2)T}. \end{aligned} \tag{6.5}$$

Here we assume $k < x^{1/12}$ and use the Brun-Titchmarsh inequality

$$\theta(x, K, a) \leq c_5 \frac{x}{\varphi(K)} \cdot \frac{\log x}{\log(x/K)}$$

(c_5 an absolute constant) for the first sum; we use a trivial estimate for the second sum; and we use

$$\sum_{m \geq T} \frac{1}{\varphi(m^2)} < \frac{c_6}{T} \tag{6.6}$$

(c_6 an absolute constant) for the last estimate. (To see (6.6), let $h(n)$ denote the multiplicative function such that $h(p) = (p-1)^{-1}$ for primes p and $h(p^i) = 0$ for $i \geq 2$. Then

$$\begin{aligned}\sum_{m\geq T}\frac{1}{\varphi(m^2)} &= \sum_{m\geq T}\frac{1}{m^2}\frac{m}{\varphi(m)} = \sum_{m\geq T}\frac{1}{m^2}\sum_{d|m}h(d)\\ &= \sum_{d=1}^{\infty}h(d)\sum_{l\geq T/d}\frac{1}{l^2d^2} < \sum_{d=1}^{\infty}\frac{h(d)}{d^2}\frac{2}{T/d}\\ &= \frac{2}{T}\prod_p\left(1+\frac{1}{p(p-1)}\right),\end{aligned}$$

so we may take $c_6 = 2\Pi_p(1 + 1/(p^2 - p)) = 2\zeta(2)\zeta(3)/\zeta(6)$.) We shall choose

$$T = \frac{3}{\varepsilon}(3c_5c_6 + 1),$$

so that from (6.4) and (6.5) we have

$$0 \leq M(T) - \theta_0(x, k^2, a) < \frac{\varepsilon x}{3\varphi(k^2)}. \tag{6.7}$$

We now estimate $M(T)$. Letting $\varepsilon' = \varepsilon/3c_6$ and applying Proposition 8 to ε', we have an x_0 and a $\delta > 0$ such that if $0 < k < x^\delta$, $x \geq x_0$, and $k_0(x) \nmid k^2Q^2$, then

$$\begin{aligned}\left|M(T) - \frac{\alpha\psi(k)x}{\varphi(k^2)}\right| &= \left|M(T) - \sum_{(d,k)=1}\mu^2(d)(-1)^{\omega(d)}\frac{x}{\varphi(k^2d^2)}\right|\\ &\leq \left|\sum_{d|Q}(-1)^{\omega(d)}\left\{\theta(x, k^2d^2, R(d^2)) - \frac{x}{\varphi(k^2d^2)}\right\}\right| + \sum_{d\geq T}\frac{x}{\varphi(k^2)\varphi(d^2)}\\ &< \sum_{d|Q}\frac{\varepsilon' x}{\varphi(k^2d^2)} + \frac{c_6x}{\varphi(k^2)T}\\ &< \frac{c_6\varepsilon' x}{\varphi(k^2)} + \frac{c_6x}{\varphi(k^2)T} < \frac{2\varepsilon x}{3\varphi(k^2)}.\end{aligned}$$

Combining this estimate with (6.7) we have

$$\left|\theta_0(x, k^2, a) - \frac{\alpha\psi(k)x}{\varphi(k^2)}\right| < \frac{\varepsilon x}{\varphi(k^2)}.$$

Adding these estimates for the $\varphi(k)$ choices of a mod k^2 and using $\varphi(k)/\varphi(k^2) = 1/k$, we finally have

$$\left|\theta_0(x, k, 1) - \frac{\alpha\psi(k)x}{k}\right| < \frac{\varepsilon x}{k},$$

which was to be proved.

Remark 6.1. A corollary of Proposition 9 is that $\theta_0(x, k, 1) \sim (\alpha\psi(k)/k)x$ as $x \to \infty$ when k is square-free. These methods show more generally that if $(k, a) = 1$, if $l = (k, a - 1)$ is square-free, and if m is the product of the primes $q \mid l$ for which $q^2 \mid k$, then

$$\theta_0(x, k, a) \sim \frac{\alpha\psi(k)\varphi(l/m)}{\varphi(k)l/m} x \text{ as } x \to \infty.$$

PROPOSITION 10. *There is a positive, absolute, calculable constant c_7 such that for all $x > 10$ there is a square-free number $M < x^2$ with*

$$\sum_{\substack{p-1|M \\ p \text{ prime}}} 1 > e^{c_7 \log x/\log\log x}.$$

Proof (cf. Prachar [29]). Let $\varepsilon = 1/4$ in Proposition 9 and fix the corresponding quantities T, x_0, δ. Let $x \geq x_0$ and let k_1 denote the product of the primes $p \leq \max\{\frac{1}{2}\delta \log x, T\}$. Note that then for all x beyond a computable point x_1 we have $k_1 < x^\delta$. (To compute x_1, one could use the estimates of Rosser and Schoenfeld [34].) If $(k_1, k_0(x))$ has a prime factor $p_0 \geq T$, let $k = k_1/p_0$. Otherwise let $k = k_1$. Then $k_0(x) \nmid k^2$. Indeed, if $k_0(x) \mid k^2$, then every prime factor of $k_0(x)$ would be smaller than T. Since $k_0(x) > (\log x)^{3/2}$, we would have $p^3 \mid k_0(x)$ for some prime p, provided x exceeded some computable point x_2. This would contradict $k_0(x) \mid k^2$.

Thus if $d \mid k$, we have by Proposition 9 that

$$\begin{aligned} (6.8) \qquad \pi_0(x, d, 1) &\overset{\text{def}}{=} \sum_{\substack{p \leq x \\ p \equiv 1 \bmod d}} \mu^2(p - 1) \geq \frac{1}{\log x}\theta_0(x, d, 1) \\ &\geq \left(\alpha\psi(d) - \frac{1}{4}\right)\frac{x}{d \log x} > \frac{x}{10\, d \log x}. \end{aligned}$$

Let A denote the number of solutions of

$$(6.9) \qquad m(p - 1) \equiv 0 \bmod k$$

where $m \leq x$ and $p \leq x$ is prime with $p - 1$ square-free. For each $d \mid k$, let A_d denote the number of solutions of (6.9) with $d \mid p - 1$, $(m, k) = k/d$.

From (6.8), the number of primes $p \leq x$ with $p - 1$ square-free and $d \mid p - 1$ is at least $x/(10\, d \log x)$. The number of $m \leq x$ with $(m, k) = k/d$ is at least $[x/k]\varphi(d)$. Thus

$$A_d \geq \frac{x}{10\, d \log x}\left[\frac{x}{k}\right]\varphi(d) > \frac{x^2}{20\, k \log x} \cdot \frac{\varphi(d)}{d}.$$

Thus for all x beyond a computable point

$$\begin{aligned} A = \sum_{d|k} A_d &> \frac{x^2}{20\,k\log x} \sum_{d|k} \frac{\varphi(d)}{d} \\ &= \frac{x^2}{20\,k\log x} \prod_{p|k} \left(2 - \frac{1}{p}\right) \\ &\geq \frac{x^2}{20\,k\log x} \left(\frac{3}{2}\right)^{\omega(k)} \\ &> \frac{x^2}{20\,k\log x} \left(\frac{3}{2}\right)^{(1/4)\,\delta\log x/\log\log x} \end{aligned}$$

Now the number of integers $n \leq x^2$ for which $k \mid n$ is at most x^2/k. Also, for each solution m, p of (6.9), $m(p-1)$ is such an n. Thus there is some $n \leq x^2$ with $k \mid n$ and n has at least

$$\begin{aligned} \frac{A}{x^2/k} &> \frac{1}{20\log x} \left(\frac{3}{2}\right)^{(1/4)\,\delta\log x/\log\log x} \\ &> e^{c_7 \log x/\log\log x} \end{aligned}$$

representations as $m(p-1)$. If we let M denote the largest square-free divisor of this n, then M fulfills the assertions of the proposition. Technically, we had to take x beyond some computable point, so the constant c_7 may have to be adjusted to take into account values of x between this point and 10.

Remark 6.2. The proof gives no clue as to the nature of the number M except for a predisposition to the primes below $\frac{1}{2}\delta\log x$. We conjecture that if $m(x)$ is the product of the longest initial segment of primes for which $m(x) \leq x$, then

$$\sum_{p-1|m(x)} 1 = 2^{(1+o(1))\log x/\log\log x}.$$

All we can prove, however, is that

$$\sum_{p-1|m(x)} 1 \geq (\log x)^{9/4}$$

for all large x. This result follows from the methods of Pomerance [24].

We can now prove the second inequality in Theorem 3. Let

$$x = (\log n)^{(2/c_7)\log\log\log n}.$$

By Proposition 10 there is a square-free $M \le x^2$ such that

$$\begin{aligned}\sum_{p-1|M} 1 &\ge e^{c_7 \log x/\log\log x}\\ &= \exp\left\{\frac{2\log\log n \log\log\log n}{\log(2/c_7) + \log\log\log n + \log\log\log\log n}\right\}\\ &\ge \exp(\log\log n) = \log n,\end{aligned}$$

if n exceeds some computable point. Thus

$$\prod_{p-1|M} p \ge 2^{\Sigma_{p-1|M} 1} \ge 2^{\log n} > n^{1/2},$$

so that we may take $f(n) \le M$. But

$$M \le x^2 = (\log n)^{(4/c_7)\log\log\log n}.$$

To complete the proof of the theorem one has to adjust the constant $4/c_7$ so as to include those n that are not covered by the above argument and are larger than 100.

Remark 6.3. A slightly more careful treatment of the lower bound in Theorem 3 would show that $g(n)$ is at least

$$(6.10) \qquad (\log n)^{(1/\log 2 + o(1))\log\log\log n}.$$

From the conjecture in Remark 6.2 we get the same expression as an upper bound for $f(n)$. Thus, $g(n)$ and $f(n)$ should both be given by (6.10), the only difference being in the "$o(1)$" term.

In Lenstra [19], a variation of the tests of Williams is described which runs in time polynomial in $h(n)$, where $h(n)$ is the least positive integer such that the product of the primes $q < h(n)^2$ with $q \mid n^{h(n)} - 1$ exceeds $\sqrt{n}$. If n has no small prime factors, then $h(n) \le g(n)$. We now present a heuristic argument suggesting that $h(n)$ should also be given by an expression of the form (6.10), the same as for $g(n)$ and $f(n)$. Only an argument for the lower bound is needed.

For each $k \mid h(n)$, consider primes q of the form $ak + 1 < h(n)^2$. Then we guess that q divides $n^k - 1$ with "probability" $1/a$. Thus the "expected" number of such q's is at most

$$\sum_{a<h(n)^2/k} \frac{1}{a} < 2\log h(n) + 1,$$

and, in all, the "expected" number of primes $q \mid n^{h(n)} - 1$ with $q < h(n)^2$ is at most

$$(2\log h(n) + 1)d(h(n)) \le 2^{(1+o(1))\log h(n)/\log\log h(n)},$$

where we use (6.1). From this the desired lower bound follows by an argument similar to the one used for the lower bound in Theorem 3.

Remark 6.4. For values of $n < 10^{11356}$ we may choose the initial primes from among the first 13 primes, as the following table shows. Let $E(t)$ denote the number of Euclidean primes with respect to the first t primes. As in Remark 6.2, we conjecture that $E(t) = 2^{(1+o(1))t}$. The data suggest that $E(t)$ could be compared with $2^t/(t\sqrt{\log t})$. The ratio of these functions shows fairly stable behavior and it may be there is a constant C with

$$E(t) \sim C2^t/\left(t\sqrt{\log t}\right) \quad \text{as } t \to \infty.$$

We have a heuristic argument to support this conjecture, but we shall not present it here.

TABLE

t	Product of first t primes	Number of Euclidean primes	Square of product of Euclidean primes
1	2	2	36
2	6	3	1764
3	30	5	$2.0512 \cdot 10^{8}$
4	210	8	$8.5119 \cdot 10^{19}$
5	2310	13	$2.5354 \cdot 10^{43}$
6	$3.0030 \cdot 10^{4}$	21	$5.3723 \cdot 10^{89}$
7	$5.1051 \cdot 10^{5}$	32	$6.5191 \cdot 10^{166}$
8	$9.6997 \cdot 10^{6}$	54	$2.8537 \cdot 10^{350}$
9	$2.2309 \cdot 10^{8}$	83	$5.2088 \cdot 10^{620}$
10	$6.4697 \cdot 10^{9}$	149	$8.2520 \cdot 10^{1364}$
11	$2.0056 \cdot 10^{11}$	251	$2.3443 \cdot 10^{2715}$
12	$7.4207 \cdot 10^{12}$	450	$3.0596 \cdot 10^{5635}$
13	$3.0425 \cdot 10^{14}$	807	$1.4135 \cdot 10^{11356}$

(Table computed by William Dubuque)

MASSACHUSETTS INSTITUTE OF TECHNOLOGY, CAMBRIDGE, MASS. and UNIVERSITY OF SOUTHERN CALIFORNIA, LOS ANGELES (first author)
UNIVERSITY OF GEORGIA, ATHENS (second and third authors)

REFERENCES

[1] L. M. ADLEMAN, Number theoretic aspects of computational complexity, Ph.D. Thesis, U.C. Berkeley (1976).

[2] ______, On distinguishing prime numbers from composite numbers (Abstract), 21st FOCS (1980).

[3] L. M. Adleman and F. T. Leighton, An $O(n^{1/10.89})$ primality testing algorithm, Math. Comp. **36** (1981), 261–266.

[4] E. Artin and J. Tate, *Class Field Theory*, W. A. Benjamin (New York, Amsterdam), 1967.

[5] E. R. Berlekamp, Factoring polynomials over large finite fields, Math. Comp. **24** (1970), 713–735.

[6] E. Bombieri, Le grand crible dans la théorie analytique des nombres, Astérisque **18** (1974), 1–87.

[7] J. Brillhart, D. H. Lehmer, and J. L. Selfridge, New primality criteria and factorizations of $2^m \pm 1$, Math. Comp. **29** (1975), 620–647.

[8] J. W. S. Cassels and A. Fröhlich (editors), *Algebraic Number Theory*, Thompson (Washington, D.C.), 1967.

[9] H. Cohen, Tests de primalité d'après Adleman, Rumely, Pomerance et Lenstra, publ. Laboratoire de Math. Pures associé au CNRS, Grenoble, France, 1981.

[10] H. Davenport, *Multiplicative Number Theory*, 2nd edition, Springer-Verlag, New York, 1980.

[11] J. D. Dixon, Asymptotically fast factorization of integers, Math. Comp. **36** (1981), 255–260.

[12] P. X. Gallagher, A large sieve density estimate near $\sigma = 1$, Inv. Math. **11** (1970), 329–339.

[13] K. Iwasawa, A note on Jacobi sums, Symposia Math. **15** (1975), 447–459.

[14] S. Lang, *Algebraic Number Theory*, Addison-Wesley (Reading, Mass.), 1970.

[15] D. H. Lehmer, Strong Carmichael numbers, J. Austral. Math. Soc. Ser. A **21** (1976), 508–510.

[16] ______, Computer technology applied to the theory of numbers, in W. J. LeVeque, ed., MAA Stud. Math. **6** (1969), 117–151.

[17] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász, Factoring polynomials with rational coefficients, Report 82–05, Department of Mathematics, University of Amsterdam, 1982.

[18] H. W. Lenstra, Jr., Primality testing, in H. W. Lenstra, Jr. and R. Tijdeman, eds., *Computational Methods in Number Theory*, Math. Centrum, to appear.

[19] ______, Primality testing algorithms (after Adleman, Rumely and Williams), Séminaire Bourbaki (June, 1981) # 576.

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

[21] L. Mirsky, The number of representations of an integer as a sum of a prime and a k-free integer, Amer. Math. Monthly **56** (1949), 17–19.

[22] M. A. Morrison and J. Brillhart, A method of factoring and the factorization of F_7, Math. Comp. **29** (1975), 183–205.

[23] J. M. Pollard, Theorems on factorization and primality testing, Proc. Cambridge Phil. Soc. **76** (1974), 521–528.

[24] C. Pomerance, Popular values of Euler's function, Mathematika **27** (1980), 84–89.

[25] ______, On the distribution of pseudoprimes, Math. Comp. 37 (1981), 587–593.

[26] ______, A new lower bound for the pseudoprime counting function, Illinois J. Math., **26** (1982), 4–9.

[27] ______, Recent developments in primality testing, Math. Intelligencer 3 (1981), 97–105.

[28] ______, Analysis and comparison of some integer factoring algorithms, in H. W. Lenstra, Jr. and R. Tijdeman, eds., *Computational Methods in Number Theory*, Math. Centrum, to appear.

[29] K. Prachar, Über die Anzahl der Teiler einer natürlichen Zahl, welche die Form $p-1$ haben, Monatsh. Math. **59** (1955), 91–97.

[30] M. O. Rabin, Probabilistic algorithms, in J. Traub, Ed., *Algorithms and Complexity, New Directions and Recent Results*, Academic Press (New York) 1976, 21–24.

[31] ______, Probabilistic algorithms in finite fields, SIAM J. Comput. 9 (1980), 273–280.

[32] S. Ramanujan, Highly composite numbers, Proc. London Math. Soc., ser. 2, **14** (1915), 347–409.

[33] R. Rivest, A. Shamir, and L. M. Adleman, A method for obtaining digital signatures and public key cryptosystems, Comm. ACM **21** (1978), 120–128.

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

[35] R. Solovay and V. Strassen, A fast Monte-Carlo test for primality, SIAM J. Comput. **6** (1977), 84–85; Erratum, **7** (1978), 118.

[36] T. Tatuzawa, On the number of the primes in an arithmetic progression, Japan J. Math. **21**(1951), 93–111.

[37] S. Wigert, Sur l'ordre de grandeur du nombre des diviseurs d'un entier, Arkiv für Math. Astr. Fys. **3**, no. 18 (1907), 1–9.

[38] H. C. Williams, Primality testing on a computer, Ars Combinatoria **5** (1978), 127–185.

[39] H. C. Williams and R. Holte, Some observations on primality testing, Math. Comp. **32** (1978), 905-917.

[40] H. C. Williams and J. S. Judd, Some algorithms for prime testing using generalized Lehmer functions, Math. Comp. **30** (1976), 867–886.

(Received October 30, 1981)