J. Symbolic Computation (2000) **30**, 151–160
doi:10.1006/jsco.1999.0343
Available online at http://www.idealibrary.com on IDEAL

Generalized Strong Pseudoprime Tests and Applications

PEDRO BERRIZBEITIA† AND T. G. BERRY‡

Departamento de Matematicas, Universidad Simón Bolívar, Caracas, Venezuela

We describe probabilistic primality tests applicable to integers whose prime factors are all congruent to 1 mod r where r is a positive integer; $r = 2$ is the Miller–Rabin test. We show that if ν rounds of our test do not find $n \neq (r+1)^2$ composite, then n is prime with probability of error less than $(2r)^{-\nu}$. Applications are given, first to provide a probabilistic primality test applicable to all integers, and second, to give a test for values of cyclotomic polynomials.

1. Introduction

For n odd, the strong pseudoprime primality test (also called the Miller–Rabin test c.f. Miller, 1976, Rabin, 1980, Koblitz, 1987) searches for $a \in \mathbf{Z}_n, a \neq \pm 1$ such that either $a^{n-1} \neq 1$ (so the little Fermat theorem fails) or $a^2 = 1$ (so there are at least three square roots of 1 in $\mathbf{Z}_n$); in either case n is composite. The test is a plausible advance on the Fermat test since by the Chinese remainder theorem if n is odd and has at least two distinct prime factors, then there are at least four square roots of 1 in $\mathbf{Z}_n$. In fact it is proved that if tests with ν distinct values of a fail to declare n composite, then n is probably prime with probability of error less than $4^{-\nu}$. Now, let r be a fixed positive integer and let A_r denote the set of integers all of whose prime factors are all congruent to 1 mod r. If $n \in A_r$ is composite with at least two distinct prime factors, then there are at least r^2 rth roots of 1 in $\mathbf{Z}_n$. This suggests generalizing the strong pseudoprime test by considering rth roots of 1 with $r > 2$, to give a probabilistic primality test for integers in A_r. In this paper we study these generalized tests, which we call "rth-order tests", and give some applications.

In Section 1 we give a formal definition of the rth-order test and prove a direct generalization of the Rabin–Monier theorem, to the effect that if the rth-order test fails to detect $n \in A_r$ composite in ν trials, then n is probably prime with probability of error less than $(2r)^{-\nu}$. If this is to be interesting, then we must either be able, given n, to choose r *a posteriori* so that $n \in A_r$, or find interesting subsets of A_r for given r. In Section 2 we describe applications involving each of these ideas. By choosing r, given n, we find a variant of the test used in Maple V. For a given error probability this variant is a probabilistic primality test which is more efficient than the strong pseudoprime test whenever factors of $n-1$ are known which are either odd primes or powers $2^j, j \geq 2$, and

†E-mail: `pedrob@usb.ve`
‡E-mail: `berry@usb.ve`

0747–7171/00/080151 + 10 $35.00/0

reduces to the strong pseudoprime test when 2^1 is the only known prime power factor of $n-1$. In view of finding interesting subsets of A_r for given r, we show that $\Phi_r(b) \in A_r$ for almost all integers b, where Φ_r denotes the rth cyclotomic polynomial. The rth-order test applies to such $\Phi_r(b)$ to give a probabilistic primality test faster than the strong pseudoprime test, for large r. There are evident applications to problems involving primality and factorization of values of cyclotomic polynomials.

There are connections between our work and that of Adleman *et al.* (1983). In fact, Adleman *et al.* (1983) described tests (both probabilistic and deterministic) based on calculations similar to those of our rth-order tests, but which involve working, not in the rational integers, but in the ring of integers of a cyclotomic field. As mentioned above, our general probabilistic primality test for an integer n is an improvement over the strong pseudoprime test only when we can find factors of $n-1$ other than 2, while the APR algorithms apply to arbitrary n. However, our tests, which involve working only in the ring of rational integers, are much simpler to implement, and have the advantage that we can give an explicit bound for the error probability. After finishing this paper, we received the preprint (Konyagin and Pomerance, 1997) which makes use of some of the same ideas, and some subtle analytic number theory, to obtain deterministic tests for those n for which a good part of the factorization of $n-1$ is known.

We are very grateful to Carl Pomerance who read an earlier version of this paper and provided us with helpful comments and a great deal of guidance with the literature. We also thank Luis Gomez Sanchez who read the first version, pointed out a number of misprints and made suggestions for improving the exposition.

2. Generalized Strong Pseudoprime Tests

For clarity of exposition we first define and analyse the tests for r a prime power, and then indicate how to proceed for general r. Thus let $r = q^e$ where q is prime. Let $n \in A_r$ (recall A_r denotes the set of integers whose prime factors are all congruent to 1 mod r) and let ω be an integer of exact order r mod n. Abusing language slightly, we refer to ω as a primitive rth root of 1 mod n. Such ω exist when $n \in A_r$: if $n = p^m$ is a prime power, then $\mathbf{Z}_n{}^*$ is cyclic, and $\phi(n) = p^m - p^{m-1} \equiv 0 \bmod r$, so $\mathbf{Z}_n{}^*$ contains a cyclic subgroup of order r and we choose a generator; in general use the Chinese remainder theorem to lift a set of primitive rth roots of 1 mod the prime power factors of n.

Definition 2.1. For $n \in A_r$ set $n-1 = q^s t$, where $(t,q) = 1$. Let $a \in \mathbf{N}$. Then n is an ω **-prime to base** a if either

$$\exists h \in \mathbf{Z} \mid a^t \equiv \omega^{qh} \bmod n \tag{2.1}$$

or

$$\exists i, j, (j,q) = 1, 0 \le i \le s-e, 1 \le j \le r-1 \mid a^{q^i t} \equiv \omega^j \bmod n. \tag{2.2}$$

By elementary congruence arguments, if $n \in A_r$ then $e \le s$ so the conditions of (2) make sense. If $r = 2, \omega = -1$ then Definition 1.1 reduces to that of strong pseudoprime to base a as used by Miller, Rabin and Monier. The point of the definition is that, if n is a pseudoprime to base a but *not* an ω-prime to base a, then some power of a^t is an rth root of 1 which is not a power of ω, hence n must be composite. (Slightly more detail is given in the proof of Proposition 2.4.)

We shall prove:

THEOREM 2.2. *With the notation of Definition* 1, *if* $n \in A_r$ *is* ω*-prime to base* a *for* ν *distinct bases* a, *and if* $n \neq (1+r)^2$, *then* n *is probably prime with probability of error less than* $(2r)^{-\nu}$.

For $r = 2$, Theorem 2.2 was proven independently by Rabin (1980) and Monier (1980).

The rest of this section is devoted to the proof of Theorem 2.2. For the proof we introduce a formalism which is of some interest in its own right.

DEFINITION 2.3. Let $A \subseteq \mathbf{N}$. An **elementary probabilistic primality test for integers in** A, denoted (T, A), is a collection $T = \{T_n, n \in A\}$ of sets with the properties:

(1) $T_n \subseteq \mathbf{Z}_n^*, \forall n \in A$
(2) If $n \in A$ is prime, then $T_n = \mathbf{Z}_n^*$
(3) If $n \in A, a \in \mathbf{Z}_n$, then the question whether $a \in T_n$ can be decided in time polynomial in $\log n$.

Examples. In the following examples, $[a]$ denotes the class of the integer a mod n.

(1) Fermat test $(F, \mathbf{N})$
$$F_n = \{[a] \in \mathbf{Z}_n^* \mid a^{n-1} \equiv 1 \bmod n\}.$$
(2) Solovay–Strassen test $(S, \mathbf{N})$
$$S_n = \left\{[a] \in \mathbf{Z}_n^* \mid a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \bmod n\right\}$$
where $\left(\frac{a}{n}\right)$ is the Jacobi symbol (c.f. Solovay and Strassen, 1977).
(3) The rth-order test $(T(\omega), A_r)$
$$T_n(\omega) = \{[a] \in \mathbf{Z}_n^* \mid n \text{ is } \omega\text{-prime to base } a\}.$$

In Proposition 2.4 below it is proved that Example 3 is in fact an elementary primality test. Observe that $(T(-1), A_2)$ is the strong pseudoprime test, and $(T(1), \mathbf{N})$ is the Fermat test.

We note that F_n, S_n are multiplicative subgroups of $\mathbf{Z}_n^*$ for all n, but that $T_n(\omega)$ is not in general a group.

We shall say that a test (T, A) is *sharp* if $T_n = \mathbf{Z}_n^*$ implies n prime. For example, the Solovay–Strassen test is sharp, but the Fermat test is not because of the existence of the Carmichael numbers. Alford *et al.* (1994) recently proved the existence of infinitely many Carmichael numbers.

Elementary primality tests are partially ordered by $(T, A) \leq (T', A')$ if $A \subseteq A'$ and, $\forall n \in A, T_n \subseteq T'_n$. Monier (1980) shows $(T(-1), A_2) < (S, \mathbf{N}) < (\mathbf{F}, \mathbf{N})$.

PROPOSITION 2.4. *With the notation of Definition* 2.3.

(1) $(T_n(\omega), A_r)$ *is an elementary probabilistic primality test;*
(2) *for all* $r, d \in \mathbf{N}$, $(T(\omega), A_r) \leq (T(\omega^d), A_{r'})$, *where* $r' = r/(r, d)$. *In particular, for all* r, $(T(\omega), A_r) \leq (F, N)$.

PROOF. (1) The first condition of Definition 2.3 is immediate. Next, suppose n prime; we must show that n is ω-prime to all bases a. Now if a^t is not a q^sth root of 1, then the little Fermat theorem fails in $\mathbf{Z}_n$ and n is certainly composite. Assume then that a^t has order $\mu | q^s$ in $\mathbf{Z}_n^*$. If $\mu < r = q^e$ then unless a^t is a power of ω of order less than r, i.e. a power of ω^q, there are too many rth roots of 1 in $\mathbf{Z}_n$ and n is composite. On the other hand, if $\mu \geq q^e$ write $\mu = q^{i+e}$, with $i \leq s - e$. Then $a^{q^i t}$ has exact order q^e and must be ω^j for some $j, (j, q) = 1$, otherwise n again is composite. This proves condition (2) of Definition 2.3. Condition (3) is immediate from the well-known fact that exponentiation mod n is polynomial in $\log n$.

(2) It is enough to prove that, for all n, $T_n(\omega) \subseteq T_n(\omega^q)$. This follows from Definition 1.1, taking into account that, ω being a primitive q^eth root of 1, we have that ω^q is a primitive $q^{(e-1)}$th root of 1. The final remark follows from (1), since $(T_1(1), A_1) = (F, \mathbf{N})$.□

Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ be the prime factorization of n, so that in particular k denotes the number of distinct prime factors of n. As usual ϕ denotes the Euler phi-function. Finally, let $K_m = \{c \in \mathbf{Z}_n^* \mid c^m = 1\}$ denote the kernel of the mth power map on $\mathbf{Z}_n^*$. Thus $F_n = K_{n-1} = K_t \times K_{q^s}$.

The following lemma can be found in Monier (1980, Lemma 1).

LEMMA 2.5. *For $i = 1 \ldots r$, let g_i be a generator mod $p_i^{\alpha_i}$, let y be an integer prime to n and l an arbitrary positive integer. Then the congruence $x^l \equiv y \bmod n$ has a solution if and only if $(l, \phi(p_i^{\alpha_i}))$ divides $\mathrm{ind}_{g_i} y, i = 1 \ldots l$. If this condition is satisfied, then the congruence has exactly $\prod_{i=1}^k (l, \phi(p_i^{\alpha_i}))$ solutions.*

From this, we have:

LEMMA 2.6. *The order of F_n is given by*

$$|F_n| = \prod_{i=1}^k (\phi(p^{\alpha_i}), n-1) \tag{2.3}$$
$$= \prod_{i=1}^k (p_i - 1, n-1). \tag{2.4}$$

PROOF. The first equality is an immediate consequence of Lemma 2.5, and the second follows from the first using the formula for $\phi(p^e)$ and the fact that p_i is prime to $n-1, i = 1 \ldots k$. □

Results equivalent to Lemma 2.6 can be found in Monier (1980) and Baillie and Wagstaff (1980).

Now define a subset $B_r \subseteq K_{q^s}$ by

$$B_r = \{\beta \in K_{q^s} \mid \exists h, \beta = \omega^{qh} \tag{2.5}$$
$$\text{or } \exists i, j, (j, q) = 1, 0 \leq i \leq s - e, 1 \leq j \leq r - 1 | \beta^{q^i} \equiv \omega^j \bmod n\}. \tag{2.6}$$

LEMMA 2.7.

$$T_n(\omega) \cong K_t \times B_r.$$

Proof. Suppose $c \in T_n(\omega)$. Then $c = \tau\beta$ for some $\tau \in K_t, \beta \in K_r$ since $T_n(\omega) \subseteq F_n = K_t \times K_r$. Since $c \in T_n(\omega)$ there are two possibilities for $c^t = \tau^t\beta^t = \beta^t$: in the first case $c^t = \omega^{qh}$ for some $h \in \mathbf{N}$ and thus $\beta^t = \omega^{qh}$. In the second case $c^{q^i t} = \beta^{q^i t}$ is a power of ω of order r. In the first case, since t is prime to r we can write $1 = at + br$ for some integers a, b, whence $\beta = \beta^{at}.\beta^{br} = \omega^{aqh}$ since $\beta^{br} = 1$, because $\beta \in K_r$. We conclude $\beta = \omega^{qh'}$, for some integer h', therefore $\beta \in B_r$. In the second case $\beta^{q^i t} = \omega^j$ for some j prime to r; again arguing as in the first case, using $(t, r) = 1$ we have $\beta = \beta^{at}$ for some integer a, with $(a, r) = 1$. Then $\beta^{q^i} = \beta^{q^i at} = \omega^{aj}$ where $(aj, r) = 1$ and again $\beta \in B_r$. Thus $T_n(\omega) \subseteq K_t \times B_r$. The opposite inclusion follows immediately from the definitions of $T_n(\omega), K_t$ and B_r. □

For each p_i let f_i be the exact power of q which divides $p_i - 1$. Then $f_i \geq e$ since $n \in A_r$. Set $e' = \min f_i, i = 1 \ldots k$.

Lemma 2.8. $|B_r| = q^{e-1} + (q-1)q^{e-1}(1 + q^k + q^{2k} + \cdots q^{(e'-e)k})$.

Proof. The first term q^{e-1} is the order of the subgroup of $\mathbf{Z}_n^*$ generated by ω^q, i.e. is the cardinality of the set of β's satisfying the first condition in the definition of B_r. It remains to count the β's satisfying the second condition. Fix l, j with $0 \leq l \leq s - e, 1 \leq j \leq r - 1, (j, q) = 1$. Apply Lemma 2.5 to count the solutions of $x^{q^l} \equiv \omega^j \bmod n$. For any generator $g_i \bmod p_i^{\alpha_i}$, the condition on $ind_{g_i}\omega^j$ is satisfied if and only if $l \leq f_i - e$. Thus the condition is satisfied for all p_i if and only if $l \leq e' - e$. If this condition is satisfied, then, by the count in Lemma 2.5, the number of solutions is q^{lk}. The lemma follows summing over l and the $\phi(r) = \phi(q^e)$ possible j. □

Proposition 2.9. *For all $n \in A_r$,*

$$\frac{|T_n(\omega)|}{|F_n|} \leq \frac{1}{r^{k-1}}.$$

Proof. By Lemma 2.7, $|T_n(\omega)| = |K_t| \times |B_r|$, and as we have already observed $F_n = K_t \times K_{q^s}$. Thus it is enough to prove $|B_r|/|K_{q^s}| \leq 1/r^{k-1}$. By the Chinese remainder theorem K_{q^s} contains a copy of the direct product of k cyclic groups of order at least $q^{e'}$, hence $|K_{q^s}| \geq q^{e'k}$. Thus

$$\frac{|B_r|}{|K_{q^s}|} \leq \frac{|B_r|}{q^{e'k}}.$$

Now, applying the elementary inequality

$$1 + (1 + x + x^2 + \cdots x^m)(y - 1) \leq x^m y.$$

valid for $y \leq x$, to Lemma 2.8, with $x = q^k, m = e' - e$ and $y = q$, we obtain

$$|B_r| \leq q^e.q^{(e'-e)k}$$

and the proposition follows. □

Corollary 2.10. *If $n \in A_r, n \neq (1+r)^2$ and n is not prime, then $|T_n(\omega)| \leq \phi(n)/2r < n/2r$.*

Proof. Suppose first that n is a prime power, $n = p^f$. Then $|\mathbf{Z}_n^*| = \phi(n) = p^f - p^{f-1}$, and, using Lemma 2.6 we find $|\mathbf{Z}_n^*|/|F_n| = p^{f-1}$. Since $p \equiv 1 \bmod r$ and we are excluding the possibility $n = (1+r)^2$, we have $|\mathbf{Z}_n^*|/|F_n| > 2r$. The corollary now follows from the fact that $(T(\omega), A_r) < (F, \mathbf{N})$. Thus suppose n has $k \geq 2$ prime divisors. Then by Proposition 2.9 $|T_n(\omega)| \leq |F_n|/r^{k-1}$; if $k \geq 3$ then $|F_n|/r^{k-1} \leq \phi(n)/r^{k-1} < \phi(n)/2r$. If $k = 2$ then n is not a Carmichael number since Carmichael numbers have at least three distinct prime divisors (see Koblitz, 1987, p. 115). Thus F_n is a proper subgroup of $\mathbf{Z}_n^*$, whose index in $\mathbf{Z}_n^*$ is therefore ≥ 2, and the desired result follows. □

Theorem 2.2 is an immediate consequence.

2.1. THE TEST FOR ARBITRARY r

Let $r = \prod_{i=1}^m q_i^{e_i}$, be the prime factorization of an arbitrary positive integer r, let $n \in A_r$ and let ω be a primitive rth root of 1 mod n. Set $\omega_i = \omega^{r/q_i^{e_i}}, i = 1 \ldots m$, and let $n - 1 = t \prod_{i=1}^m q_i^{s_i}$, where $(t, r) = 1$ and $s_i \geq e_i, i = 1 \ldots m$.

Definition 2.11. For $a \in \mathbf{N}$, n is ω-prime to base a if n is ω_i-prime to base a for $i = 1 \ldots m$.

It follows immediately that the primality test $(T(\omega), A_r)$ is given by the sequence

$$T_n(\omega) = \bigcap_{i=1}^m T_n(\omega_i).$$

We claim that Propositions 2.4, 2.9 and Corollary 2.10, and therefore Theorem 1, hold also in this case. In fact, parts (1) and (2) of Proposition 2.4 are immediate. For Proposition 2.9 observe that

$$T_n(\omega) = K_t \times \textstyle\prod_{i=1}^m B_{q_i^{e_i}} \tag{2.7}$$

$$F_n = K_t \times \textstyle\prod_{i=1}^m K_{q_i^{s_i}} \tag{2.8}$$

from which 2.9 follows as in the case r a prime power.

We make a final remark on deriving deterministic tests prom probabilistic. Let us call an elementary probabilistic primality test *algebraic* if T_n is a group, for all n.

A probabilistic test becomes deterministic if we can bound the smallest witness for composite n, i.e. for a primality test (T, A) if we can find $\tau = \tau(n) | \exists a < \tau, \quad [a] \in \mathbf{Z}_n^* \setminus T_n$. Miller (1976) showed, assuming the extended Riemann hypothesis (ERH), that the smallest witness for composite n for the strong pseudoprime test is $O(\log n^2)$. His result was improved by Bach (1985) whose result, in our language, is:

Theorem 2.12. *Assuming ERH, if (T, A) is a sharp algebraic elementary primality test and n is composite, then the smallest witness for n is $< 2(\log n)^2$.*

Since the strong pseudoprime test is dominated, in the partial order defined in Section 1, by the Solovay–Strassen test, which is algebraic, it follows that the smallest witness for the strong pseudoprime test is also $< 2(\log n)^2$. We conjecture that the same is true for rth-order tests, and that it can be proved by showing that rth-order tests are dominated by generalizations of the Solovay–Strassen test defined by general norm-residue symbols.

3. Applications

3.1. A PROBABILISTIC PRIMALITY TEST FOR ODD n

For the rth-order test to be useful, we must find interesting numbers in A_r. An elementary method to determine integers in A_r, when r is a prime power, is given by the following slight generalization of a theorem of Pocklington (see Pocklington, 1916):

THEOREM 3.1. *Let $n \in \mathbf{N}$,and let $n-1 = q^s t$ where q is prime and t is prime to q. If $\exists e, 1 \le e \le s | (a^{tq^{e-1}} - 1, n) = 1$, but $(a^{tq^e} - 1, n) = n$, then $n \in A_{q^e}$ and a^t is a primitive q^eth root of 1 mod n.*

We next define an elementary probabilistic test, in the sense of Definition 2.3. Let r be a positive integer, and let N_r denote the set of positive integers $\equiv 1 \bmod r$. We use the notation introduced in the final subsection of Section 1. Then the test $(P(r), N_r)$ is defined by:

DEFINITION 3.2. (1) Suppose q is prime, and $n \in N_q$. Set $n-1 = q^s t$ where $(t,q) = 1$.

$$P_n(q) = \left\{ [a] \in F_n | \quad \forall i, 0 \le i \le s-1, (a^{tq^i} - 1, n) \in \{1, n\} \right\}.$$

(2) For general r,where $n-1 = rt$, $(r,t) = 1$ let $q_i, i = 1 \cdots m$ be the prime factors of r

$$P_n(r) = \bigcap_{i=1}^{m} P_n(q_i).$$

Definition 3.2(2) makes sense since $q_i^{e_i}$ divides r implies $N_{q_i^{e_i}} \subseteq N_r$.

We leave it to the reader to verify that $(P(2), N_2)$ coincides with the strong pseudoprime test.

For small q, it is more efficient to avoid all gcd computations by means of the following lemma.

LEMMA 3.3. *Let $r = q^s$, q prime, and $n \in N_r$. Let $[a] \in F_n$. If $[a] \notin P_n(r)$ then there exists a positive integer $e < n-1$, such that $a^e \not\equiv 1 \bmod n$, $a^{eq} \equiv 1 \bmod n$, and $\left(\frac{a^{eq}-1}{a^e-1}\right) \not\equiv 0 \bmod n$.*

The proof is straightforward.

The function "Isprime" of Maple V implements tests $(P(r), N_r)$ with $r = 2^a 3^b 5^c 7^d$ where $n-1 = 2^a 3^b 5^c 7^d t, (t,r) = 1$, followed by a Lucas test. We propose a variant of this procedure, motivated by the observation that in the course of verifying $n \in P_n(r)$, with high probability we will find an rth root of 1 mod n, and then by Pocklington's theorem $n \in A_r$. If this happens, then we can apply the rth-order test instead of the Lucas test. Specifically, in case the case of $r = q$ a prime we proceed as follows.

1. Factor $n-1 = q^s t$, where q is prime and $(t,q) = 1$.
2. Choose a random a. If $a \notin P_n(q)$ then return "n composite".

3. If $a \in P_n(q)$, and, for some e, $1 \le e \le s$, $(a^{tq^{e-1}} - 1, n) = 1$, $(a^{tq^e} - 1, n) = n$ then set $\omega = a^t \bmod n$ and test n with the q^eth-order test $T_n(\omega)$.
4. If $a \in P_n(q)$ and $a^t \equiv 1 \bmod n$ (so that no primitive eth root of 1 mod n is found, re-enter at (2).

If n is prime, then for random $a \in P_n(q)$ the probability that step (4) is reached is $t/(n-1) = 1/q^s$. Thus, ν passes through step (4) indicate that n is probably composite, with probability of error $\le (1/q)^{s\nu}$. This is useful when the algorithm is being used as a prime-generating algorithm: if $q \ge 3$ and step (4) is reached, then n should be discarded as possible prime. If $a \in P_n(q)$ is found, it is not worth doing a further $P_n(q)$ test with a new base b, but it is well worth doing a ω-prime test. Indeed, suppose n is composite and the new base $b \in F_n$; then b has probability $O(1/q)$ of being a witness for the $P_q(n)$ test, whereas it has probability $\ge 1 - 1/q$ of being a witness for the qth-order test.

3.2. REMARKS ON THE IMPLEMENTATION

The test for general r works by implementing the test for one prime at a time. A feasible implementation is as follows.

Let B be a set of small primes, containing 2. Then attempt to factorize $n - 1 = \left(\prod_{q \in B} q^*\right) t$, where t has no factor in B and q^* denotes the exact power of q which divides $n-1$. Then apply the test $P_q(n)$ for each prime q starting with the largest q^*. At worst this reduces to the strong pseudoprime test, and is much faster if some odd prime of B or high power of 2 divides $n-1$. The test in fact becomes deterministic if the factored part of $n-1$ is sufficiently large (c.f. Brillhart *et al.*, 1988; Konyagin and Pomerance, 1997; Pocklington, 1916).

3.3. A PRIMALITY TEST FOR VALUES OF CYCLOTOMIC POLYNOMIALS

We show that, for given r, integers in A_r can be generated from values of Φ_r, where Φ_r denotes the rth cyclotomic polynomial.

We shall make use of the following elementary but extremely useful identity

$$\left(\frac{a^n - 1}{a - 1}, a - 1\right) = (n, a - 1).$$

The proof is left to the reader. Results similar to, and more general than, the following lemma can be found in the literature. We prove no more than we need.

LEMMA 3.4. *If the prime q divides $(r, \Phi_r(b))$, then q^2 does not divide $\Phi_r(b)$.*

PROOF. As usual, denote by $v_p(m)$ the exact power of the prime p which divides the integer m. With this notation, the lemma states that, if q divides r then $v_q(\Phi_r(b)) \le 1$.

First, suppose $r = q$. Since q divides $b^q - 1$ if and only if q divides $b - 1$, we find $v_q(\Phi_q(b)) = 0$ unless $b \equiv 1 \bmod q$. On the other hand, if $b \equiv 1 \bmod q$ then applying 3.1 with $n = q$ gives $v_q(\Phi_q(b)) = 1$. Thus the lemma is established for $r = q$. Now suppose $r = qs, s > 1$. We claim that $\Phi_r(b)$ divides $\Phi_q(b^s)$. Indeed we have

$$b^r - 1 = (b^s - 1)\Phi_q(b^s)$$

and, on the other hand, the factorization of $b^r - 1$ as product of $\Phi_d(b)$, $d|r$ can be rewritten as

$$b^r - 1 = (b^s - 1) \prod_{d|s} \Phi_{dq}(b)$$

where the right-hand side contains in particular the factor $\Phi_{qs}(b) = \Phi_r(b)$. The claim follows by comparing these two factorizations of $b^r - 1$. Thus $v_q(\Phi_r(b)) \leq v_q(\Phi_q(b^s)) \leq 1$ where the final inequality is the case $r = q$. This is the lemma for general r. □

DEFINITION 3.5. For $b \in \mathbf{Z}$ the **non-trivial factor** of $\Phi_r(b)$ is $\Phi_r(b)/(r, \Phi_r(b))$.

We have the following.

PROPOSITION 3.6. *For $r \in \mathbf{N}, b \in \mathbf{Z}$, let n be the non-trivial factor of $\Phi_r(b)$. Then $n \in A_r$ and b is a primitive rth root of* 1 *mod* n.

PROOF. We can prove both assertions by proving that, if m is any divisor of n, then $m \equiv 1 \bmod r$ and b has order r mod m. To see this, we first observe that, since m divides $b^r - 1$, the order of b mod m is a divisor of r, say d. If $d < r$ then m is a divisor of $((b^r - 1)/(b^d - 1), b^d - 1) = (r/d, b^d - 1)$ (applying the identity 3.3). This implies that m divides r, which is impossible by Lemma 3.2 and the definition of n. Thus $d = r$, i.e. b has order r mod m. If m is prime, then this implies that r divides $m-1$, i.e. $m \equiv 1 \bmod r$ and the proof is complete. □

As an example, consider the test for numbers $M_p = \Phi_p(3) = \dfrac{3^p - 1}{2}$, where p is an odd prime. We have $M_p \equiv 1 \bmod p$, so that $(p, M_p) = 1$ and the non-trivial factor of M_p is M_p itself, and moreover $M_p - 1 \equiv 0 \bmod p$. By Lemma 3.6 $M_p \in A_p$ and 3 is a primitive pth root of 1 mod M_p. We apply the pth-order test with $\omega = 3$ and base 2. This runs: if $2^{(M_p - 1)/p}$ is a power of $3 \bmod M_p$, then M_p is probably prime with probability of error less than $1/2p$, otherwise M_p is certainly composite. For large p we need only perform one round of the test to obtain a low probability of error. The strong pseudoprime test, in order to achieve a similar error probability, will have to perform $\lceil (1 + \log_2 p)/2 \rceil$ rounds. A single round of either the pth power or the strong pseudoprime test has asymptotic complexity $O(p)$ modular operations. Thus the asymptotic complexity of the strong pseudoprime test with probability of error less than $1/2p$ is $O(p \log p)$. Rather more precisely, note that, by computing 3^p in the naive manner, with p multiplications, we obtain simultaneously with the computation of M_p a table of powers of 3. Moreover, since we require powers only up to 3^{p-1}, there is no need to reduce mod M_p and the table is naturally sorted in increasing order. Using this, one finds that the number of modular operations in one round of the pth-order test is less than or equal to twice the number of operations in one round of the strong pseudoprime test, which is around $p \log_2 3$. To obtain an error probability less than $1/2p$ then, one must perform about $\lceil (1 + \log_2 p)/2 \rceil$ rounds of the strong pseudoprime test, and thus about $p \lceil (1 + \log_2 p)/2 \rceil$ operations, as opposed to at most $2p \log_2 3$ operations of the pth-order test.

References

Adleman, L., Pomerance, C., Rumely, R. S. (1983). On distinguishing prime numbers from composite numbers. *Ann. Math.*, **117**, 173–206.

Alford, W., Granville, A., Pomerance, C. (1994). There are infinitely many Carmichael numbers. *J. Am. Math. Soc.*, **140**, 703–722.

Bach, E. (1985). *Analytic Methods in the Analysis and Design of Number-Theoretic Algorithms*, Boston, MIT Press.

Brillhart, J., Lehmer, D., Selfridge, J., Tuckerman, B., Wagstaff j., S. S. (1988). *Factorizations of* $b^n \pm 1, b = 2, 3, 5, 6, 710, 11, 12$ *up to High Powers,* Number 22 in *Contemporary Mathematica*, Providence, RI, American Mathematic Society.

Koblitz, N. (1987). *A Course in Number Theory and Cryptography*, Berlin, NY, Springer.

Konyagin, S., Pomerance, C. (1997). On primes recognizable in deterministic polynomial time. In Graham, R. L., Nesetril, J. eds, *The Mathematics of Paul Erdos, Vol. 1,* volume 13 of *Algorithms and Combinatorics*, Berlin, NY, Springer.

Miller, G. (1976). Riemann's hypothesis and a test for primality. *J. Theor. Comput. Sci.*, 300–317.

Monier, L. (1980). Evaluation and comparison of two efficient probabilistic primality testing algorithms. *J. Theor. Comp. Sci.*, **12**, 97–108.

Pocklington, H. (1914–1916). The determination of the prime or composite nature of large numbers by Fermat's theorem. *Proc. Camb. Phil. Soc.*, **18**, 29–30.

Rabin, O. (1980). Probabilistic algorithm for testing primality. *J. Numer. Theory*, **12**, 128–138.

Baillie, R., Wagstaff, S. (1980). Lucas pseudoprimes. *Math. Comput.*, **35**, 1391–1417.

Solovay, R., Strassen, V. (1977). The fast Monte-Carlo test for primality. *Siam J. Comput.*, **6**, 84–85.

Originally Received 25 May 1998
Accepted 9 December 1999