MATHEMATICS OF COMPUTATION
VOLUME 36, NUMBER 153
JANUARY 1981

An $O(n^{1/10.89})$ Primality Testing Algorithm*

By Leonard Adleman and Frank Thomson Leighton

Abstract. In this paper, we describe an $O(n^{1/10.89})$ deterministic algorithm to decide primality. The algorithm incorporates several recent results in complexity theory.

1. Introduction. The problem of determining whether an integer is prime or composite in a polynomial amount of time on a deterministic machine is a well-known, unsettled problem in number theory and computational complexity theory. Miller [4] has shown that primality can be decided deterministically in $O(\log^4 n)$ steps assuming the Extended Riemann Hypothesis. Strassen and Solovay [9], Rabin [8], and Miller [4] have shown how to recognize composites in $O(\log^3(n))$ steps with a random algorithm. Thus, it is considered likely that primality can be decided deterministically in polynomial time. However, no such polynomial time algorithm is known. In fact, the best published upper bound on the amount of time needed to decide primality is $O(n^{1/8+\varepsilon})$ for any $\varepsilon > 0$ (Pollard [6]).

In this paper, we describe an $O(n^{1/(1+6\sqrt{e})+\varepsilon}) \leqslant O(n^{1/10.89})$ algorithm to decide primality. The algorithm is largely an extension of Miller's [4] $O(n^{1/7})$ algorithm but also incorporates several other recent results in complexity theory. In Section 2, we mention these results. The algorithm is described in Section 3 and its complexity is analyzed in Section 4. We conclude with some remarks in Section 5.

2. Preliminaries. We commence with some standard definitions. If $n = p_1^{v_1} \cdots p_m^{v_m}$, then the *Euler phi-function* is

$$\phi(n) = p_1^{v_1-1}(p_1 - 1) \cdots p_m^{v_m-1}(p_m - 1).$$

The *Carmichael function* is

$$\lambda(n) = \operatorname{lcm}\left(p_1^{v_1-1}(p_1 - 1), \ldots, p_m^{v_m-1}(p_m - 1)\right).$$

If $\lambda(n) \mid n - 1$, then n is called a *Carmichael number*. In addition, we define n to be *N-Carmichael-like* if, for every $m \geqslant 1$ and every prime $p \geqslant N$, $p^m \mid \lambda(n) \Rightarrow p^m \mid n - 1$. Finally, we denote, by $\sharp_q x$, the number of factors of q in x. For example, if $n = p_1^{v_1} \cdots p_m^{v_m}$, then $\sharp_{p_i} n = v_i$ for $1 \leqslant i \leqslant m$.

The validity of our algorithm relies heavily on several results from the literature. These results are included here as Lemmas 1–8. In each case, the reference given contains a proof of the lemma or some similar result. Often the results cited in the lemmas are slight generalizations of the original results.

Received November 19, 1979; revised June 24, 1980.
1980 *Mathematics Subject Classification.* Primary 10A15, 10A25, 10A30, 68C05, 68C25.
Key words and phrases. Algorithm, Carmichael number, composite, factor, prime, residue.
* Research sponsored by NSF Grant #78-04343.

0025-5718/81/0000-0023/$02.50

LEMMA 1 (POLLARD [7]). *For any $\varepsilon > 0$, there is a deterministic algorithm which, given n, $\alpha > 0$, finds all prime factors p of n with $p < n^{\alpha}$ in $O(n^{\alpha/2+\varepsilon})$ time.*

LEMMA 2 (NORTON [5]). *For any $\varepsilon > 0$, there exist constants C and N such that, for every n and every prime $q \geqslant N$ with $q \mid \phi(n)$, there is a qth nonresidue of n less than Cn^{ε}.*

LEMMA 3 (BURGESS [1]). *For any $\varepsilon > 0$, there is a constant C such that, for every pair of primes p and q with $q \mid p - 1$, there is a qth nonresidue of p less than $Cp^{(1/4\sqrt{e})+\varepsilon}$.*

LEMMA 4 (BURGESS [1]–[3]). *For any $\varepsilon > 0$, there is a constant C such that, for every pair of primes $p \neq q$, there is an $a \leqslant C(pq)^{(1/4\sqrt{e})+\varepsilon}$ such that $(a/pq) = -1$.*

LEMMA 5 (MILLER [4]). *If $p \mid n$, $q^m \mid p - 1$ and $q^m \nmid n - 1$ for some $m \geqslant 1$, and a is a qth nonresidue of p, then $a^{n-1} \not\equiv 1 \bmod n$.*

LEMMA 6 (MILLER [4]). *If $p^2 \mid n$, and a is a pth nonresidue of p^2, then $a^{n-1} \not\equiv 1 \bmod n$.*

LEMMA 7 (MILLER [4]). *If $p \mid n$ and $p' \mid n$ for two primes p and p', $\sharp_q(p-1) > \sharp_q(p'-1) \geqslant 0$ for some prime q, a is a qth nonresidue of p, and $\lambda(n) \mid (n-1)s$ for some s, then either a or $(a^{(n-1)s/q^k} \bmod n) - 1$ has a nontrivial greatest common divisor with n for some $1 \leqslant k \leqslant \sharp_q([n-1]s)$.*

LEMMA 8 (MILLER [4]). *If $p \mid n$ and $p' \mid n$ for two different primes p and p', $\sharp_2(p-1) = \sharp_2(p'-1)$, $(a/pp') = -1$, and $\lambda(n) \mid (n-1)s$, then either a or $(a^{(n-1)s/2^k} \bmod n) - 1$ has a nontrivial greatest common divisor with n for some $1 \leqslant k \leqslant \sharp_2([n-1]s)$.*

3. The Algorithm. Given any small $\varepsilon > 0$, let the constant N be as defined in Lemma 2. In addition, let $\{p_1, \ldots, p_r\}$ be the set of primes less than N. Then define Algorithm A_ε as follows.

ALGORITHM A_ε:

Step (1): Input n.

Step (2): If $n \leqslant N$, check if $n \in \{p_1, \ldots, p_r\}$. If so, output "prime" and halt. If not, output "composite" and halt.

Step (3): Find all prime factors of $n-1$ which are less than $n^{2/(1+6\sqrt{e})}$. Let these factors be $q_1, \ldots, q_t$.

Step (4): Carry out (i) and (ii) for each $2 \leqslant a \leqslant \max(N, n^{1/(1+6\sqrt{e})})$. If at any stage (i) or (ii) holds, output composite and halt.

(i) $a^{n-1} \not\equiv 1 \bmod n$.

(ii) $((a^{(n-1)s/q^k} \bmod n) - 1, n) \neq 1, n$ for $1 \leqslant k \leqslant \sharp_q([n-1]s)$, $q \in \{q_1, \ldots, q_t, p_1, \ldots, p_r\}$, and $s = p_1^{b_1} \cdots p_r^{b_r}$ with $b_i = [\log n/\log p_i]$.

Step (5): Check if $(s_2 - s_1 + \sqrt{s_1^2 + s_2^2 + (4n-2)s_1 s_2}\,, n) \neq 1, n$ for any $s_1 = p_1^{u_1} \cdots p_r^{u_r}$ and $s_2 = p_1^{v_1} \cdots p_r^{v_r}$ with $0 \leqslant u_i, v_i \leqslant \lceil \log n/\log p_i \rceil$. If so, output "composite" and halt.

Step (6): Output "prime" and halt.

It is easily verified that if n is prime, then A_ϵ outputs "prime" and halts. It is also clear (noting Lemma 1) that A_ϵ runs in time $O(n^{1/(1+6\sqrt{\epsilon})+\epsilon}) \leqslant O(n^{1/10.89})$ for sufficiently small ϵ. It remains to be shown that if n is composite, then A_ϵ outputs "composite" and halts. In order to accomplish this, we divide the analysis up into several cases depending on the structure of n. The following is an outline of the subcase structure of the analysis. The portion of the total running time actually required to handle each subcase is also included in the outline.

Outline of Subcases.

I. n is not N-Carmichael-like $O(n^\epsilon)$.

II. n is N-Carmichael-like.

A. n is not square-free $O(n^\epsilon)$.

B. n is the product of distinct primes.

1. n is the product of two primes $O(n^\epsilon)$.

2. n is the product of four or more primes $O(n^{1/(8\sqrt{\epsilon})+\epsilon}) \leqslant O(n^{1/13})$.

3. n is the product of three primes.

a. n is not Carmichael $O(n^{1/(8\sqrt{\epsilon})+\epsilon}) \leqslant O(n^{1/13})$.

b. n is Carmichael $O(n^{1/(1+6\sqrt{\epsilon})+\epsilon}) \leqslant O(n^{1/10.89})$.

4. Complexity Analysis. We now analyze the complexity of each case outlined at the end of the previous section. Note that if $n \leqslant N$, then Step (2) of the algorithm correctly decides the primality of n in constant time. Thus, we henceforth assume that $n > N$.

Case I. n is not N-Carmichael-like.

By definition, if n is not N-Carmichael-like, then there exist an $m \geqslant 1$ and a prime $p \geqslant N$ such that $q^m \mid \lambda(n)$ but $q^m \nmid n - 1$. Assume that $q^m \mid p - 1$ for some prime $p \mid n$. Then, by Lemma 2, there is a qth nonresidue a of p less than $Cp^\epsilon \leqslant Cn^\epsilon$. By Lemma 5, $a^{n-1} \not\equiv 1 \bmod n$ and this case can be handled (by Step (4)(i)) in $O(n^\epsilon)$ time.

If $q^m \nmid p - 1$ for every prime $p \mid n$, then $q^m \mid \lambda(n)$ implies $q = p$ for some $p^2 \mid n$. As before, Lemmas 2 and 6 can be used to show that this case can be handled (by Step (4)(i)) in $O(n^\epsilon)$ time.

Case II: n is N-Carmichael-like.

Subcase A. n is not square-free.

If n is not square-free, then $p^2 \mid n$ for some prime p. Since n is N-Carmichael-like, $p \leqslant N$. Thus, n is found to be composite (by Step (4)(i)) in $O(n^\epsilon)$ time.

Subcase B. n is the product of distinct primes.

Subcase 1. n is the product of two primes.

Let $n = pq$. Since n is N-Carmichael-like, $p - 1 \mid (n - 1)s$ for some s composed solely of prime factors less than N. Thus,

$$p - 1 \mid (pq - 1)s \Rightarrow p - 1 \mid \big[(p - 1)q + q - 1\big]s \Rightarrow p - 1 \mid (q - 1)s.$$

Similarly, $q - 1 \mid (p - 1)s'$ for some s' composed solely of prime factors less than N. Thus, $p - 1 = xs_1$ and $q - 1 = xs_2$ for some selection of s_1 and s_2 where $s_1 = p_1^{u_1} \cdots p_r^{u_r}$, $s_2 = p_1^{v_1} \cdots p_r^{v_r}$ and $1 \leqslant u_i, v_i \leqslant \lceil \log n / \log p_i \rceil$ for $1 \leqslant i \leqslant r$. Thus, $n = pq = (xs_1 + 1)(xs_2 + 1) = s_1 s_2 x^2 + (s_1 + s_2)x + 1$. Using the quadratic

formula,

$$x = \frac{-s_1 - s_2 + \sqrt{s_1^2 + 2s_1s_2 + s_2^2 + 4(n-1)s_1s_2}}{2s_1s_2}$$

$$\Rightarrow p = s_1x + 1 = \frac{s_2 - s_1 + \sqrt{s_1^2 + s_2^2 + (4n-2)s_1s_2}}{2s_2}$$

$$\Rightarrow \left(s_2 - s_1 + \sqrt{s_1^2 + s_2^2 + (4n-2)s_1s_2}\ , n\right) \neq 1, n.$$

Since there are at most $(\log n)^{2r} \leqslant O(n^{\varepsilon})$ combinations of s_1 and s_2 to check, this case may be disposed of (by Step (5)) in $O(n^{\varepsilon})$ time.

Subcase 2. n is the product of four or more primes.

Let p and q be the two smallest prime factors of n. Then $pq \leqslant n^{1/2}$. Since n is square-free, $p \neq q$. If $\sharp_2(p-1) = \sharp_2(q-1)$, we know by Lemma 4 that there is a number a less than $C(pq)^{1/4\sqrt{e}+\varepsilon} \leqslant O(n^{1/8\sqrt{e}+\varepsilon})$ such that $(a/pq) = -1$. Since $\lambda(n) \mid (n-1)s$ for $s = p_1^{b_1} \cdots p_r^{b_r}$ with $b_i = \lceil \log n / \log p_i \rceil$ (by N-Carmichael-like property), we know by Lemma 8 that a or $(a^{(n-1)s/2^k} \bmod n) - 1$ has a nontrivial GCD with n for some $1 \leqslant k \leqslant \sharp_2[(n-1)s]$. There are at most $O(\log n)$ possibilities for k, so this case is handled (by Step (4)(ii)) in $O(n^{1/8\sqrt{e}+\varepsilon})$ time.

If $\sharp_2(p-1) \neq \sharp_2(q-1)$, then (WLOG) $\sharp_2(p-1) > \sharp_2(q-1)$. Using a similar argument, it is easy to show by Lemmas 3 and 7 that this case may also be handled (by Step (4)(ii)) in $O(n^{1/8\sqrt{e}+\varepsilon})$ time.

Subcase 3. n is the product of three primes.

Let $n = pqr$ with $p < q < r$. There are two further subcases to consider.

Subcase a. n is not Carmichael.

If $r \geqslant n^{1/2}$, then $pq \leqslant n^{1/2}$ and we may apply the arguments of the case when n has four or more factors to dispatch this possibility (by Step (4)(ii)) in $O(n^{1/8\sqrt{e}+\varepsilon})$ time. Thus, we may assume that $r < n^{1/2}$. Since n is not Carmichael, there is a prime q' and an $m \geqslant 1$ such that (WLOG) $q'^m \mid r-1$ but $q'^m \nmid n-1$. Since n is N-Carmichael-like, $q' \leqslant N$. Since $n - 1 = pqr - 1 = (p-1)(q-1)(r-1) + (q-1)(r-1) + (p-1)(r-1) + (p-1)(q-1) + (p-1) + (q-1) + (r-1)$, this means that $q'^m \nmid p-1$ or $q'^m \nmid q-1$. (WLOG) assume $q'^m \nmid p-1$. Then $\sharp_{q'}(r-1) > \sharp_{q'}(p-1)$. Applying Lemmas 3 and 7 together with the knowledge that $r \leqslant n^{1/2}$, we find that this case can be handled (by Step (4)(ii)) in $O(n^{1/8\sqrt{e}+\varepsilon})$ time.

Subcase b. n is Carmichael.

If n is Carmichael, then $p-1 \mid n-1 \Rightarrow p-1 \mid [(q-1)(r-1) + (q-1) + (r-1)] \Rightarrow (p-1, q-1) \mid (r-1)$. Similarly, $(p-1, r-1) \mid q-1$ and $(q-1, r-1) \mid p-1$. Let $d = (p-1, q-1) = (p-1, r-1) = (q-1, r-1)$. Define $p-1 = dx$, $q-1 = dy$ and $r-1 = dz$ where x, y, z are relatively prime in pairs. Then

$$\lambda(n) \mid n-1 \Rightarrow xyzd \mid d^2(xy + yz + xz) + d(x + y + z)$$

$$\Rightarrow 1 \leqslant d\left(\frac{1}{x} + \frac{1}{y} + \frac{1}{z}\right) + \left(\frac{1}{xy} + \frac{1}{xz} + \frac{1}{yz}\right) \Rightarrow x \leqslant 3d.$$

Otherwise,

$$z \geqslant y \geqslant x \geqslant 3d+1 \Rightarrow d\left(\frac{1}{x}+\frac{1}{y}+\frac{1}{z}\right)+\left(\frac{1}{xy}+\frac{1}{xz}+\frac{1}{yz}\right)$$
$$\leqslant \frac{3d}{3d+1}+\frac{3}{(3d+1)^2}=\frac{9d^2+3d+3}{9d^2+6d+1}<1$$

since $d \geqslant 1$.

Since $p \leqslant n^{1/3}$ and $x \leqslant 3d$, we know that $x \leqslant \sqrt{3}n^{1/6}$. In the case where $x > 1$, the prime factors of x are among the prime factors of $n-1$ which are less than $\sqrt{3}n^{1/6}$. We may find all such small factors in $O(n^{1/12+\varepsilon})$ time by Lemma 1. Any such factor must divide $p-1$ more often than $q-1$ and, thus, we may apply Lemmas 3 and 7 to show that only $O(n^{1/12\sqrt{e}+\varepsilon})$ additional time is needed to decide that n is composite (by Step (4)(ii)).

Thus, we may assume that $x = 1$. Define reals α_1, α_2 and β so that $y = n^{\alpha_1}$, $z = n^{\alpha_2}$, and $d = n^{\beta}$. Note that $n^{\alpha_1+\alpha_2+3\beta} = (p-1)(q-1)(r-1) < n$ so $\alpha_1 + \alpha_2 + 3\beta < 1$. We first consider the case when $\beta \geqslant (2\sqrt{e}-1)/(1+6\sqrt{e})$. Then $\alpha_1 + \alpha_2 < 1 - 3\beta \leqslant 4/(1+6\sqrt{e})$. Since $\alpha_1 \leqslant \alpha_2$, we know that $\alpha_1 < 2/(1+6\sqrt{e})$. Thus, the prime factors of y are $< O(n^{2/(1+6\sqrt{e})})$. Since all factors of $n-1$ of this size can be found in $O(n^{1/(1+6\sqrt{e})+\varepsilon})$ time, we have achieved the desired bound for this case.

If $\beta \leqslant (2\sqrt{e}-1)/(1+6\sqrt{e})$, then

$$\alpha_1 + 2\beta \leqslant \frac{\alpha_1+\alpha_2}{2}+2\beta < \frac{1+\beta}{2} \leqslant \frac{4\sqrt{e}}{1+6\sqrt{e}}$$

and $pq < O(n^{4\sqrt{e}/(1+6\sqrt{e})})$. By arguments similar to those described in the case when n has four or more prime factors, this case can be handled in $O((pq)^{1/4\sqrt{e}+\varepsilon})$ $\leqslant O(n^{1/(1+6\sqrt{e})+\varepsilon})$ time.

This completes the analysis of the complexity of the algorithm. We summarize our result in the following theorem.

THEOREM. *For sufficiently small $\varepsilon > 0$, Algorithm A_ε decides whether or not any integer n is prime in $O(n^{1/(1+6\sqrt{e})+\varepsilon}) \leqslant O(n^{1/10.89})$ steps.*

5. Remarks. It is quite likely that the algorithm presented in this paper can be improved substantially. In particular, an improved method of dealing with Carmichael numbers (very highly structured numbers) would directly lead to an improvement in the running time of the algorithm.

It is also likely that the practical efficiency of the algorithm can be improved substantially. Though we have not made an attempt to do so here, such an improvement would be of great interest and could lead to a practical algorithm for deterministically deciding primality. In particular, Step 5 is very fast asymptotically but is prohibitively time consuming in practice.

One alternate approach to the problem involves the behavior of $a^{(n^k-1)/(n-1)q'} \bmod n$ where $a \in GF(n^k)$ for $k \geqslant 2$. Several improvements on the algorithm can be made on the assumption that nonresidues are no more difficult to

find in $GF(p^k)$ for $k \geqslant 2$ than they are to find in $GF(p)$. This assumption may well be very hard to verify, however.

Department of Mathematics
Massachusetts Institute of Technology
Cambridge, Massachusetts 02139

1. D. A. BURGESS, "The distribution of quadratic residues and nonresidues," *Mathematika*, v. 4, 1957, pp. 106–112.

2. D. A. BURGESS, "On character sums and primitive roots," *Proc. London Math. Soc.* (3), v. 12, 1962, pp. 179–192.

3. D. A. BURGESS, "On character sums and L-series," *Proc. London Math. Soc.* (3), v. 12, 1962, pp. 193–206.

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

5. K. K. NORTON, "Numbers with small prime factors and the least kth power non-residue," *Mem. Amer. Math. Soc.*, No. 106, Amer. Math. Soc., Providence, R. I., 1971.

6. J. M. POLLARD, "An algorithm for testing the primality of any integer," *Bull. London Math. Soc.*, v. 3, 1971, pp. 337–340.

7. J. M. POLLARD, "Theorems on factorization and primality testing," *Proc. Cambridge Philos. Soc.*, v. 76, 1974, pp. 521–528.

8. M. O. RABIN, "Probabilistic algorithms," *Algorithms and Complexity, New Directions and Present Results* (J. Traub, Ed.), Academic Press, New York, 1976, pp. 21–40.

9. R. SOLOVAY & V. STRASSEN, "A fast Monte Carlo test for primality," *SIAM J. Comput.*, v. 6, 1977, pp. 84–85.