MATHEMATICS OF COMPUTATION, VOLUME 35, NUMBER 151
JULY 1980, PAGES 1003–1026

The Pseudoprimes to $25 \cdot 10^9$

By Carl Pomerance, J. L. Selfridge and Samuel S. Wagstaff, Jr.

Abstract. The odd composite $n \leqslant 25 \cdot 10^9$ such that $2^{n-1} \equiv 1 \pmod n$ have been determined and their distribution tabulated. We investigate the properties of three special types of pseudoprimes: Euler pseudoprimes, strong pseudoprimes, and Carmichael numbers. The theoretical upper bound and the heuristic lower bound due to Erdős for the counting function of the Carmichael numbers are both sharpened. Several new quick tests for primality are proposed, including some which combine pseudoprimes with Lucas sequences.

1. Introduction. According to Fermat's "Little Theorem", if p is prime and $(a, p) = 1$, then $a^{p-1} \equiv 1 \pmod p$. This theorem provides a "test" for primality which is very often correct: Given a large odd integer p, choose some a satisfying $1 < a < p - 1$ and compute $a^{p-1} \pmod p$. If $a^{p-1} \not\equiv 1 \pmod p$, then p is certainly composite. If $a^{p-1} \equiv 1 \pmod p$, then p is probably prime. Odd composite numbers n for which

$$a^{n-1} \equiv 1 \pmod n \tag{1}$$

are called *pseudoprimes to base a* (psp(a)). (For simplicity, a can be any positive integer in this definition. We could let a be negative with little additional work. In the last 15 years, some authors have used pseudoprime (base a) to mean any number $n > 1$ satisfying (1), whether composite or prime.) It is well known that for each base a, there are infinitely many pseudoprimes to base a. We have computed all psp(2)'s below $25 \cdot 10^9$.

The difficulty with using (1) for several bases a as a test for primality is that there are odd composite n, called *Carmichael* numbers, which are pseudoprimes to every base relatively prime to n. It is widely believed that there are infinitely many Carmichaels. Although this conjecture remains unproved, several different possible growth rates have been suggested for the counting function of the Carmichael numbers. We will explain in Section 5 why we support a growth rate like that proposed by Erdős [8].

In the present work, we consider two modifications of the pseudoprime test, which discriminate even better than (1) does between primes and composites. An odd composite n is an *Euler pseudoprime to base a* (epsp(a)) if $(a, n) = 1$ and

$$a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \pmod n, \tag{2}$$

Received December 11, 1978; revised November 2, 1979.
1980 *Mathematics Subject Classification*. Primary 10A15; Secondary 10–04.
Key words and phrases. Pseudoprime, strong pseudoprime, Euler pseudoprime, Carmichael number, primality testing, Lucas sequence.

where (a/n) is the Jacobi symbol. Euler's criterion states that (2) holds when n is prime, hence the name.* D. H. Lehmer [13] has shown that no odd composite number is an epsp(a) for every base a relatively prime to it. Solovay and Strassen [23] proved that no odd composite number is an epsp to more than half of the bases relatively prime to it. When a is small compared to n, the arithmetic of (1) and (2) require about the same computation time to perform. Using the quadratic reciprocity law, the Jacobi symbol is nearly as easy to compute as a greatest common divisor.

Now consider how the exponentiation of (1) is performed. One standard method is to write $n - 1 = d \cdot 2^s$, with d odd. Compute a^d (mod n), then square the result (mod n) s times. The second modification to the pseudoprime test (1) examines this process more carefully. An odd composite number n (with $n - 1 = d \cdot 2^s$, d odd, as above) either is a *strong pseudoprime to base a* (spsp(a)) if

(i) $a^d \equiv 1 \pmod{n}$, or

(ii) $a^{d \cdot 2^r} \equiv -1 \pmod{n}$, for some r in $0 \leqslant r < s$.

Note that if n is prime, then either (i) or (ii) must hold, because the equation $x^2 = 1$ has only the two solutions $1, -1$ in a field. Gary Miller [15] was the first to consider examining $a^{d \cdot 2^r}$ as in (ii), but his test was slightly different from ours. Michael Rabin [19] has proved that no odd composite is an spsp to more than half of the bases relatively prime to it. Malm [14] has shown that being epsp(a) is equivalent to being spsp(a) for numbers $n \equiv 3 \pmod{4}$. We show below that, for each base a, there are infinitely many spsp(a)'s, and that every spsp(a) is an epsp(a). The calculation of (i) and (ii) has at least one fewer multiplication and reduction (mod n) than is needed for (1), but it usually requires more comparisons. For large n, the arithmetic labor of an spsp test is practically the same as for a psp or epsp test.

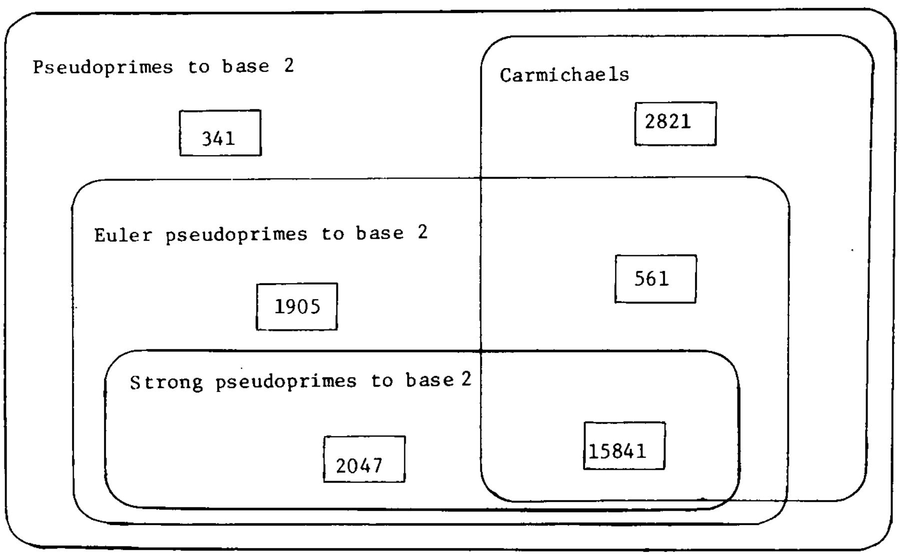

FIGURE 1

The least element of each set is shown

*The term "Euler pseudoprime" first appears in Shanks [22].

Figure 1 shows the least psp(2) of each of the possible types with respect to the preceding definitions. We note that 4369 and 4371 are the only twin psp(2)'s below $25 \cdot 10^9$.

Note that the set of bases to which an odd composite n is a pseudoprime forms a subgroup of the multiplicative group of reduced residue classes modulo n. The same is true for the Euler pseudoprime bases, because the Jacobi symbol is multiplicative. However, the following example shows that the set of bases to which n is a strong pseudoprime need not be closed under multiplication: Let $n = 2284453 = 1069 \cdot 2137$ and $e = (n-1)/2 = 1142226$. Then n is an spsp(2) and an spsp(7) because $2^e \equiv 7^e \equiv -1 \pmod{n}$, but n is not an spsp(14) because $14^e \equiv 1$, while $14^{e/2} \equiv 4275 \pmod{n}$. Nevertheless, it is true and easy to prove that if a and t are positive integers and n is an spsp(a), then n is an spsp(a^t).

TABLE 1

Count of pseudoprimes, Euler pseudoprimes, strong pseudoprimes and Carmichael numbers below x

x	$P_2(x)$	$E_2(x)$	$E_2(x)-S_2(x)$	$S_2(x)$	$C(x)$
10^3	3	1	1	0	1
10^4	22	12	7	5	7
10^5	78	36	20	16	16
10^6	245	114	68	46	43
10^7	750	375	213	162	105
10^8	2057	1071	583	488	255
10^9	5597	2939	1657	1282	646
10^{10}	14884	7706	4415	3291	1547
$25 \cdot 10^9$	21853	11347	6505	4842	2163

For each base a, let $P_a(x)$, $E_a(x)$, and $S_a(x)$ denote the number of psp(a), epsp(a), and spsp(a), respectively, not exceeding x. Write $C(x)$ for the number of Carmichaels not exceeding x. We have $S_a(x) \leqslant E_a(x) \leqslant P_a(x) < [x/2]$ for every a and $C(x) \leqslant P_2(x)$. (Only the very first inequality is not obvious; we will prove it as Theorem 3.) Table 1 gives the values of $P_2(x)$, $E_2(x)$, $S_2(x)$, and $C(x)$ for various x up to $25 \cdot 10^9$. Poulet [18] found the psp(2)'s and the Carmichaels below 10^8 and Swift [24] tabulated $C(x)$ for $x \leqslant 10^9$.

It is known [30], [8] that for all large x, we have

$$\frac{5}{8 \ln 2} \ln x < P_2(x) < x \cdot \exp(-c(\ln x \cdot \ln \ln x)^{1/2}).$$

We show in Theorem 1 that $S_2(x) > c' \ln x$ for all large x. Erdős [8] showed that there is a positive constant c'' such that for all sufficiently large x,

$$C(x) < x \cdot \exp(-c'' \ln x \cdot \ln \ln \ln x / \ln \ln x).$$

In Theorem 6 we will prove that one may take c'' arbitrarily close to 1.

We have deposited in the UMT files complete tables of the psp(2)'s, epsp(2)'s, spsp(2)'s, and Carmichaels below $25 \cdot 10^9$. We possess similar tables which also give the factorization and pseudoprime character to prime bases < 30 for each number, but these were too bulky to put in UMT.

The most time-consuming part of the work was determining the psp(2)'s. This project occupied one CPU of a dual processor DEC KI-10 at the University of Illinois for several months. A long sequence of 15-minute jobs was run, with each one submitting the next automatically. The algorithm used by the program is described in Section 2. We thank the University of Illinois Computing Services Office for permitting so much computer time to be used for this project. We thank Professor H. Diamond for valuable discussions concerning Section 5. We are grateful to H. W. Lenstra, Jr. and D. Shanks for their helpful criticisms of this paper.

2. **Some Elementary Properties of Carmichael Numbers and Pseudoprimes.** Two classical facts about Carmichael numbers are these:

PROPOSITION 1 (CARMICHAEL [5]). *If the prime p divides the Carmichael number n, then $n \equiv 1 \pmod{p-1}$, and hence $n \equiv p \pmod{p(p-1)}$.*

PROPOSITION 2 (CARMICHAEL [5]). *Every Carmichael number is square free.*

Conversely, it is easy to see [10] that every odd composite squarefree number n which satisfies $n \equiv 1 \pmod{p-1}$ for each of its prime divisors p must be a Carmichael.

Ankeny remarked [1] that for odd composite squarefree n, n is Carmichael if and only if the denominator of the Bernoulli number B_{n-1} is $2n$. This rule is not quite correct, because the denominator often has many other prime factors. By the von Staudt-Clausen theorem, the denominator of B_{n-1} is the product of all primes p for which $p-1$ divides $n-1$. For example, the denominator of B_{560} is

$$2 \cdot 3 \cdot 5 \cdot 11 \cdot 17 \cdot 29 \cdot 41 \cdot 71 \cdot 113 \cdot 281 \neq 2 \cdot 561,$$

although 561 is a Carmichael. The correct formulation of his remark is that an odd composite squarefree number n is Carmichael if and only if n *divides* the denominator of the Bernoulli number B_{n-1}.

Note that it is usually much harder to show that a given large number is Carmichael than it is to show that it is a psp(a), spsp(a) or epsp(a). The most obvious test is to factor the number completely and then apply the converse of the propositions. But the corrected version of Ankeny's remark provides a means of deciding whether n is Carmichael, when we can factor $n-1$ completely, while n itself is hard to factor. In this case we determine the primes p for which $p-1$ divides $n-1$. (This process is usually easier than factoring n, especially if $n-1$ has not too many divisors.) The test is completed by checking whether n equals the product of those primes just discovered which divide n. If we learn that n is Carmichael in this manner, then we will have discovered its prime factorization as a by-product. However, we may prove that n is not Carmichael without factoring n at all.

We now prove two simple propositions which are analogs for psp(a)'s of the two facts above. Let $l_a(p)$ denote the least positive exponent h for which $a^h \equiv 1 \pmod p$.

PROPOSITION 3. *If the prime p divides the* psp(a) n, *then* $n \equiv 1 \pmod{l_a(p)}$, *and hence* $n \equiv p \pmod{p \cdot l_a(p)}$.

Proof. We have $a^{n-1} \equiv 1 \pmod p$, whence $l_a(p)$ divides $n - 1$.

PROPOSITION 4. *If n is a* psp(a) *and p^r divides n, where p is prime, then* $a^{p-1} \equiv 1 \pmod{p^r}$. *Conversely, if the last congruence holds for some odd prime p and some $r > 1$, then p^r is a* psp(a).

Proof. Write $n = p^r t$. Since $a^{n-1} \equiv 1 \pmod n$, so that $a^n \equiv a \pmod{p^r}$, we have

$$a^{p-1} \equiv (a^n)^{p-1} = a^{p^r t(p-1)} = (a^{\phi(p^r)})^{tp} \equiv 1 \pmod{p^r},$$

where ϕ denotes Euler's function. The converse is clear.

For fixed $a > 1$, solutions to the congruence $a^{p-1} \equiv 1 \pmod{p^2}$ are apparently quite rare. For example, among the primes $p < 3 \cdot 10^9$, the congruence $2^{p-1} \equiv 1 \pmod{p^2}$ holds only for $p = 1093$ and $p = 3511$; see [34]. Thus, Proposition 4 says that psp(a)'s are "nearly squarefree". Table 2 lists the nonsquarefree psp(2)'s below $25 \cdot 10^9$. Rotkiewicz [21] has exhibited two (larger) psp(2)'s which are divisible by 1093^2. No solution to the congruence $2^{p-1} \equiv 1 \pmod{p^3}$ is known.

TABLE 2

List of nonsquarefree pseudoprimes to base 2 *below* $25 \cdot 10^9$

Number	Factorization	spsp(2)?
1194649	1093^2	yes
12327121	3511^2	yes
3914864773	$29 \cdot 113 \cdot 1093^2$	yes
5654273717	$1093^2 \cdot 4733$	yes
6523978189	$43 \cdot 127 \cdot 1093^2$	no
22178658685	$5 \cdot 47 \cdot 79 \cdot 1093^2$	no

The program mentioned at the end of Section 1 used two sieves to find the psp(2)'s. A sieve of Eratosthenes generated the composites in some interval. Then a second sieve removed those odd composite numbers excluded by Propositions 3 and 4 with $a = 2$ and several small primes p. For example, since $l_2(5) = 4$, the residue class 15 (mod 20) contains no psp(2). Likewise, the second sieve deleted the classes 33, 55, 77, 99 (mod 110) because $l_2(11) = 10$. It also excluded the multiples of 9, 25, 49, etc., in accordance with Proposition 4. It was not efficient to use large primes in this sieve. The odd composites which survived were tested for being psp(2)'s by the definition. In this manner we obtained the list of psp(2)'s below $25 \cdot 10^9$, which was the basis for much of our other numerical work in this paper.

3. Some Theorems About Strong Pseudoprimes and Euler Pseudoprimes.

THEOREM 1. *If $n > 2$ is an integer, let $\Phi_n(x)$ denote the nth cyclotomic polynomial; and let $f_n(a) = \Phi_n(a)/(\Phi_n(a), n)$ for each integer $a > 1$. If $f_n(a)$ is composite, then $f_n(a)$ is an* spsp(a). *For all $a > 1$ and $x \geq a^{15a} + 1$, we have*

$$S_a(x) > \ln x/(4a \ln a).$$

Proof. It follows easily from the definition that n is an spsp(a) if and only if n is a psp(a) and there is an integer k such that $2^k \,\|\, l_a(p^b)$ for all prime powers p^b for which $p^b \,\|\, n$. Now $f_n(a)$ is $\Phi_n(a)$ with any intrinsic prime factor removed, so that if $f_n(a)$ has the prime factorization $\Pi_{i=1}^t p_i^{b_i}$, we have $l_a(p_i^{b_i}) = n$ for each i. Thus $f_n(a) \equiv 1 \pmod n$ and $f_n(a)$ is either prime or an spsp(a).

Let $k(a)$ be the squarefree kernel of a, that is, a divided by its largest square factor. Let $\eta = 1$ if $k(a) \equiv 1 \pmod 4$ and $\eta = 2$ if $k(a) \equiv 2$ or $3 \pmod 4$. Schinzel [6, Theorem 2] has proved that if h is an odd positive integer, then $f_{h\eta k(a)}(a)$ has at least two prime factors except in a few cases which have $h \leq 5$. Hence, $f_{h\eta k(a)}(a)$ is composite and therefore an spsp(a) for every odd $h \geq 7$. Since $f_{h\eta k(a)}(a) \leq a^{ah} + 1$ for each h, we have $S_a(a^{ah} + 1) \geq (h - 5)/2$ for each odd $h \geq 7$. Thus, for all $x \geq a^{15a} + 1$, we have

$$S_a(x) \geq \left[\frac{\ln(x-1)}{2a \ln a} - \frac{5}{2}\right] > \frac{\ln x}{4a \ln a}.$$

COROLLARY. *Each composite Mersenne number $2^p - 1$ (p prime) and each composite Fermat number $F_n = 2^{2^n} + 1$ is an* spsp(2).

Proof. We have $2^p - 1 = \Phi_p(2) = f_p(2)$ and $F_n = \Phi_{2^{n+1}}(2) = f_{2^{n+1}}(2)$.

In a forthcoming paper, the first author will show that $S_a(x)/\ln x \longrightarrow \infty$ for every natural number a.

THEOREM 2. *If n is a* psp(2), *then $2^n - 1$ is an* spsp(2). *There exist* spsp(2)'s *with arbitrarily many prime divisors.*

Proof. Let n be odd and $2^{n-1} \equiv 1 \pmod n$. Then $2^{n-1} - 1 = nt$ for some integer t, necessarily odd. We have $(2^n - 1) - 1 = nt \cdot 2^1$. Plainly, $2^n \equiv 1 \pmod{2^n - 1}$. Hence $2^{nt} \equiv 1 \pmod{2^n - 1}$, so $2^n - 1$ satisfies case (i) of the definition of spsp(2). Since n is composite, so is $2^n - 1$.

Erdős [36] (also see Szymiczek [25]) showed that there exist squarefree psp(2)'s n with arbitrarily many prime factors. By the above, $2^n - 1$ is an spsp(2). Since it is divisible by $2^p - 1$ for each divisor p of n, and since the numbers $2^p - 1$ with distinct primes p are relatively prime, $2^n - 1$ has at least as many prime factors as n.

Malm [14] has proved the following theorem for $n \equiv 3 \pmod 4$. The theorem for all odd n is mentioned in [22] and a variation of our proof appears in [35]. A. O. L. Atkin and R. Larson have obtained Theorem 3 independently.

THEOREM 3. *If n is an* spsp(a), *then n is an* epsp(a).

Proof. Let n be an spsp(a) and let the prime factorization of n be $p_1 p_2 \cdots p_t$, where perhaps some prime factors are repeated. Define k_j by $2^{k_j} \| p_j - 1$ and assume $k_1 \leqslant k_2 \leqslant \cdots \leqslant k_t$. Since n is an spsp(a), there is an integer $k \geqslant 0$ with $2^k \| l_a(p^b)$ for all prime powers p^b for which $p^b \| n$. Since $l_a(p^b)/l_a(p)$ is 1 or a power of p, and hence odd, we have $2^k \| l_a(p_j)$ for each j. Then $k \leqslant k_1$. Let $i \geqslant 0$ be the number of j with $k_j = k$. Then $n \equiv (2^k + 1)^i \pmod{2^{k+1}}$, so that $2^k \| n - 1$ or $2^{k+1} \mid n - 1$ according as i is odd or even. Now if $p^b \| n$, then $a^{(n-1)/2}$ is -1 or $+1$ (mod p^b) according as $2^k \| n - 1$ or $2^{k+1} \mid n - 1$. We conclude that $a^{(n-1)/2}$ is -1 or $+1$ (mod n) according as i is odd or even.

Now $(a/p_j) = -1$ or $+1$ according as $j \leqslant i$ or $j > i$, since $(a/p) = -1$ if and only if the exponent on 2 in $l_a(p)$ is the same as the exponent on 2 in $p - 1$. Thus $(a/n) = \Pi(a/p_j) = (-1)^i$. We conclude that $a^{(n-1)/2} \equiv (a/n) \pmod n$.

THEOREM 4 (MALM [14]). *If $n \equiv 3 \pmod 4$ and n is an* epsp(a), *then n is an* spsp(a). *Thus, in the congruence class* 3 (mod 4), *strong and Euler pseudoprimes are the same.*

Proof. Since $n \equiv 3 \pmod 4$, we have $n - 1 = d \cdot 2^1$, where d is odd. The hypothesis that n is an epsp(a) tells us that $a^d \equiv (a/n) \pmod n$, which is $+1$ or -1, because $(a, n) = 1$. Thus, one of the two cases of the definition of spsp(a) is satisfied, depending on the sign of the Jacobi symbol.

THEOREM 5. *If n is an* epsp(a) *and* $(a/n) = -1$, *then n is an* spsp(a).

Proof. Write $n - 1 = d \cdot 2^s$. Then $a^{d \cdot 2^{s-1}} = a^{(n-1)/2} \equiv (a/n) = -1 \pmod n$, so that case (ii) of the definition of spsp(a) holds.

COROLLARY. *If $n \equiv 5 \pmod 8$, and n is an* epsp(2), *then n is an* spsp(2).

Proof. We have $(2/n) = -1$ for $n \equiv 5 \pmod 8$.

Likewise, one can show that if $n \equiv 5 \pmod{12}$ and n is an epsp(3), then n is an spsp(3); and many similar theorems.

4. The Controversy Concerning the Growth Rate of $C(x)$. Let $\ln_r x$ denote the r-fold iterated logarithm. We have already remarked that Erdös [8] showed that

$$C(x) < x \cdot \exp(-c \ln x \cdot \ln_3 x / \ln_2 x), \tag{3}$$

for some positive constant c and all sufficiently large x. In the same paper, Erdös claimed that he believed (3) to be nearly best possible. To substantiate this claim, Erdös gave an outline of a heuristic argument that had the conclusion that for every $\epsilon > 0$ and $x > x_0(\epsilon)$, we have $C(x) > x^{1-\epsilon}$.

The principal argument against the reasoning of Erdös is that the data appear to suggest a much slower growth rate for $C(x)$. Indeed, if one tries to approximate $C(x)$ by a function of the form Kx^u, one finds that $0.15x^{0.4}$ fits very well over most of the range for which $C(x)$ is known; see Table 3. Furthermore, $C(x)$ shows no tendency to increase more rapidly for x near $25 \cdot 10^9$, as one might expect if Erdös were correct. Swift computed the ratio $r(x) = C(10x)/C(x)$ in his summary [24]. We have $r(x) =$ 2.44, 2.43, and 2.53 for $x = 10^6$, 10^7, and 10^8, respectively. Swift commented that the increase in the ratio from 2.43 to 2.53 might be significant in support of Erdös's conjecture. However, $r(10^9) = 2.39$ and $r(10^{10}/4) = 2.34$. To investigate the possibility that the exponent 0.4 might increase for somewhat larger x, we searched for Carmichaels between 10^{15} and $10^{15} + 10^7$. We found 289394 primes in this interval, but not even one psp(2).

TABLE 3

Two approximations to $C(x)$

x	C(x)	Nearest integer to F(x)	Nearest integer to G(x)	C(x)/F(x)	C(x)/G(x)	k(x)
10^4	7	6	6	1.21	1.17	2.1955
10^5	16	13	15	1.20	1.07	2.0763
10^6	43	32	38	1.33	1.14	1.9795
10^7	105	81	95	1.30	1.11	1.9339
10^8	255	208	238	1.23	1.07	1.9049
$5\cdot10^8$	469	408	453	1.15	1.04	1.8920
10^9	646	547	597	1.18	1.08	1.8799
$5\cdot10^9$	1184	1090	1137	1.09	1.04	1.8722
10^{10}	1547	1470	1500	1.05	1.03	1.8687
$1.5\cdot10^{10}$	1782	1753	1764	1.017	1.010	1.8686
$2\cdot10^{10}$	1983	1986	1979	0.998	1.002	1.8678
$2.5\cdot10^{10}$	2163	2189	2164	0.9882	0.9995	1.8668

$$F(x) = x \cdot \exp(-\ln x \cdot (1 + \ln\ln\ln x)/\ln\ln x)$$

$$G(x) = 0.15 \cdot x^{0.4}$$

$$C(x) = x\cdot\exp(-k(x)\ln x\cdot\ln\ln\ln x/\ln\ln x)$$

The strong form of the prime k-tuple conjecture implies that $C(x) > c_1x^{1/3}/\ln^3 x$: If $6m + 1$, $12m + 1$, and $18m + 1$ are all prime, then their product is a Carmichael number. (See [22].)

In the next section we carefully rework Erdös's proof of (3), trying to get the constant c as large as possible. We also rework Erdös's heuristic argument, trying to find the largest lower bound for $C(x)$ for which there is a plausible supporting argument. We thus prove that for each $\epsilon > 0$ and $x > x_0(\epsilon)$, we have

$$C(x) < x \cdot \exp(-(1-\epsilon)\ln x \cdot \ln_3 x/\ln_2 x). \tag{4}$$

We also give a heuristic argument that for each $\epsilon > 0$ and $x > x_0(\epsilon)$, we have

$$C(x) > x \cdot \exp(-(2+\epsilon)\ln x \cdot \ln_3 x/\ln_2 x). \tag{5}$$

We are not sure which of (4) and (5) is closer to the truth about $C(x)$. The gap between (4) and (5) suggests the introduction of the function $k(x)$, defined by the equation

$$C(x) = x \cdot \exp(-k(x) \cdot \ln x \cdot \ln_3 x/\ln_2 x).$$

If there is an $\epsilon > 0$ such that $C(x) \ll x^{1-\epsilon}$ (as some people believe), then $k(x) \longrightarrow \infty$ as $x \longrightarrow \infty$. If our conjecture (5) is true, then $\limsup k(x) \leqslant 2$. Our theorem (4) asserts that $\liminf k(x) \geqslant 1$. We present values of $k(x)$ for selected values of $x \leqslant 25 \cdot 10^9$ in Table 3. These data certainly throw cold water on the assertion $k(x) \longrightarrow \infty$, since the values presented are steadily decreasing.

We submit the function

$$F(x) = x \cdot \exp(-\ln x \cdot (1 + \ln_3 x)/\ln_2 x),$$

which, as can be seen in Table 3, agrees fairly well with $C(x)$ for $x \leqslant 25 \cdot 10^9$. It may be that $C(x) \sim F(x)$. If so, then we would have $\lim k(x) = 1$. Also, we would expect $C(x) > x^{1/2}$ for all values of x surpassing a number near 10^{92}.

If we only assert the weaker statement $C(x) > x \cdot \exp(-2 \cdot \ln x \cdot \ln_3 x/\ln_2 x)$, which is true for every value of $x \geqslant 10^6$ in Table 3, then we would certainly have $C(x) > x^{1/2}$, if $x > 10^{2391}$.

We remark that the following approximate equalities hold in Table 1: $P_2(x)/\ln P_2(x) \approx C(x)$ and $E_2(x) \approx \frac{1}{2} P_2(x)$. (Compare [22].) If we assume the first formula and, respectively, $C(x) \approx x \cdot \exp(-\ln x \cdot \ln_3 x/\ln_2 x)$, $C(x) \approx F(x)$, and $C(x) \approx x \cdot \exp(-2 \cdot \ln x \cdot \ln_3 x/\ln_2 x)$, then in an interval of length 10^7 near 10^{15} we would expect to find, respectively, 775, 0.019 and 0.00086 psp(2)'s.

5. The Distribution of Carmichael Numbers. For the convenience of the reader we have made an effort to keep the notation in this section similar to that used by Erdös in [8].

If x and y are positive numbers, let $\psi(x, y)$ denote the number of positive integers $n \leqslant x$ such that n is divisible by no prime exceeding y. We have from de Bruijn [4]:

LEMMA 1. *For each $\epsilon > 0$, there is an $x_0(\epsilon)$ such that, whenever $x \geqslant x_0(\epsilon)$ and $\ln x \leqslant y \leqslant x$, we have*

$$\psi(x, y) \leqslant x \cdot \exp(-(1-\epsilon)u \ln u),$$

where $u = \ln x/\ln y$.

Remark. Although there has been much work on the function $\psi(x, y)$, precise estimates when y is in the vicinity of $\exp((\ln x)^{1/2})$ remain a murky area. Unfortunately, this is exactly the range of y we seem to need in our study of Carmichael numbers. An improvement in Lemma 1 for this range of y will give us corollary improvements both in Lemma 2 and in the main result of this section, Theorem 6.

Now if $k \geqslant 2$ is an integer, let $f(k)$ denote the least common multiple of the $p - 1$ for prime divisors p of k. Also, let $f(1) = 1$. By Propositions 1 and 2 and their converse, the Carmichael numbers are precisely those composite, squarefree n satisfying $n \equiv 1 \pmod{f(n)}$.

Let $\#A$ denote the cardinality of the set A.

LEMMA 2. *For each $\epsilon > 0$, there is a $y_0(\epsilon)$ such that for all $y \geqslant y_0(\epsilon)$ and all t,*

$$\#\{k \leqslant y\colon\ f(k) = t\} \leqslant y \cdot \exp(-(1 - \epsilon)\ln y \cdot \ln_3 y/\ln_2 y).$$

Proof. We may assume $t \geqslant 2$. Let $q_1 < q_2 < \cdots$ be the primes q with $q - 1 \mid t$ and $q \leqslant \exp((\ln_2 y)^2/\ln_3 y)$, and let $r_1 < r_2 < \cdots$ be the remaining primes r with $r - 1 \mid t$. Let $\alpha = \ln_3 y/\ln_2 y$, and let $\delta > 0$. We now show that if $y > y_1(\delta)$, we have for each i such that r_i exists

$$r_i > P_i^{1 + (1 - 3\delta)\alpha}, \tag{6}$$

where P_i is the ith prime. Since $r_1 > 4 = P_1^2$, (6) is true if $i = 1$. Now assume $1 < i \leqslant \exp((\ln_2 y)^2/6 \ln_3 y)$. Then

$$r_i > i^6 > (2i \ln i)^2 > P_i^2 > P_i^{1 + (1 - 3\delta)\alpha},$$

since by Rosser [20], $P_i < 2i \ln i$ holds for all $i > 1$. So we now assume $i > \exp((\ln_2 y)^2/6 \ln_3 y)$. Noting that $\delta\alpha \ln i - 2 \ln_2 i$ is an increasing function of i for $i > (\ln y)^{2/\delta \ln_3 y}$ and that for large y we have

$$i > (\ln y)^{3/\delta} > (\ln y)^{2/\delta \ln_3 y},$$

we thus have for $y > y_2(\delta)$

$$\begin{aligned}\delta\alpha \ln i - 2 \ln_2 i &> \delta\alpha(3/\delta)\ln_2 y - 2 \ln(3/\delta) - 2 \ln_3 y\\ &= \ln_3 y - 2 \ln(3/\delta) > \ln 4.\end{aligned}$$

Thus, for $y > y_2(\delta)$ and $i > \exp((\ln_2 y)^2/6 \ln_3 y)$, we have

$$i^{\delta\alpha} > (2 \ln i)^2. \tag{7}$$

Now let $s_1, \ldots, s_j$ be the distinct primes in t. Clearly, i is at most the number of integers less than r_i composed only of $s_1, \ldots, s_j$. Thus, i is at most the number of integers less than r_i composed only of $P_1, \ldots, P_j$. Note that there is an absolute constant c such that $P_j < c \ln t$ for all $t \geqslant 2$. Since $t < k \leqslant y$, we have for $y > y_3(\delta)$ by Lemma 1, that

$$i \leqslant \psi(r_i, c \ln t) \leqslant \psi(r_i, c \ln y) \leqslant r_i \exp(-(1 - \delta)u_i \ln u_i),$$

where $u_i = \ln r_i/\ln_2 y$. Since $r_i > \exp((\ln_2 y)^2/\ln_3 y)$, we have $u_i > \ln_2 y/\ln_3 y$. Hence,

$$i \leqslant r_i \exp(-(1 - 2\delta)u_i \ln_3 y) = r_i \exp(-(1 - 2\delta)\alpha \ln r_i),$$

so that

$$r_i \geqslant i^{(1-(1-2\delta)\alpha)^{-1}} > i^{1+(1-2\delta)\alpha}.$$

Thus using (7), we have for $y > y_1(\delta) = \max\{y_2(\delta), y_3(\delta)\}$,

$$r_i > (2i \ln i)^{1+(1-3\delta)\alpha} > P_i^{1+(1-3\delta)\alpha},$$

which proves (6).

Now let $1 = Q_1 < Q_2 < \cdots$ be the integers composed of just the primes q_i, and let $1 = R_1 < R_2 < \cdots$ be the integers composed of just the primes r_i. Then for $y > y_4(\delta)$ and any $z \geqslant 1$, we have by (6) that

$$(8) \qquad N(R, z) \overset{\text{def}}{=} \#\{R_i\colon\ R_i \leqslant z\} \leqslant z^{(1+(1-3\delta)\alpha)^{-1}} \leqslant z^{1-(1-4\delta)\alpha}.$$

Also, if $z > y^\delta$, we have by Lemma 1 for $y > y_5(\delta)$,

$$N(Q, z) \overset{\text{def}}{=} \#\{Q_i\colon\ Q_i \leqslant z\} \leqslant \psi(z, \exp((\ln_2 y)^2/\ln_3 y))$$

$$\leqslant z \exp(-(1 - \delta)u \ln u),$$

where $u = \ln z \cdot \ln_3 y/(\ln_2 y)^2$. Thus, for $y > y_5(\delta)$, $z > y^\delta$,

$$(9) \qquad N(Q, z) \leqslant z \exp(-(1 - 2\delta)\alpha \ln z) = z^{1-(1-2\delta)\alpha}.$$

We thus have by (8) and (9), that if $y > y_6(\delta) = \max\{y_1(\delta), y_4(\delta), y_5(\delta)\}$, then

$$\begin{aligned}
\#\{k \leqslant y\colon\ f(k) = t\} &\leqslant \#\{k \leqslant y\colon\ k = Q_iR_j \text{ for some } i, j\} \\
&= \sum_{Q_i \leqslant y} \sum_{R_j \leqslant y/Q_i} 1 \leqslant \sum_{Q_i \leqslant y} (y/Q_i)^{1-(1-4\delta)\alpha} \\
&= y^{1-(1-4\delta)\alpha} \left\{ \sum_{Q_i \leqslant y^\delta} Q_i^{(1-4\delta)\alpha-1} + \sum_{y^\delta < Q_i \leqslant y} Q_i^{(1-4\delta)\alpha-1} \right\} \\
&\leqslant y^{1-(4\delta)\alpha} \left\{ \sum_{n \leqslant y^\delta} n^{(1-4\delta)\alpha-1} + \frac{N(Q, y)}{y^{1-(1-4\delta)\alpha}} + 2\int_{y^\delta}^{y} \frac{N(Q, z)\,dz}{z^{2-(1-4\delta)\alpha}} \right\} \\
&< y^{1-(1-4\delta)\alpha} \left\{ y^{2\delta\alpha} + y^{-2\delta\alpha} + 2\int_{y^\delta}^{y} z^{-1-2\delta\alpha}\,dz \right\} \\
&< y^{1-(1-7\delta)\alpha}.
\end{aligned}$$

So letting $\delta = \epsilon/7$ and $y_0(\epsilon) = y_6(\epsilon/7)$, we have Lemma 2.

THEOREM 6. *For each $\epsilon > 0$, there is an $x_0(\epsilon)$ such that for all $x \geqslant x_0(\epsilon)$, we have $C(x) \leqslant x \exp(-(1 - \epsilon)\ln x \cdot \ln_3 x/\ln_2 x)$.*

Proof. Let $\delta > 0$. We divide the Carmichael numbers $n \leqslant x$ into three classes:

(i) $n \leqslant x^{1-\delta}$,

(ii) $x^{1-\delta} < n \leqslant x$ and n has a prime factor $p \geqslant x^{\delta}$,

(iii) $x^{1-\delta} < n \leqslant x$ and all prime factors of n are below x^{δ}.

For each prime $p \geqslant x^{\delta}$ the number of Carmichael numbers $n \leqslant x$ and divisible by p is at most $x/p(p-1)$ by Proposition 1. Thus, the number N_2 of Carmichael numbers in the second class satisfies

$$N_2 \leqslant x \sum_{p \geqslant x^{\delta}} 1/p(p-1) < 2x^{1-\delta}.$$

We now consider Carmichael numbers n in the third class. Every such n necessarily has a divisor k with $x^{1-2\delta} < k \leqslant x^{1-\delta}$. The number of Carmichael numbers $n \leqslant x$ divisible by an integer k is at most $1 + x/kf(k)$, since any such n satisfies $n \equiv 0 \pmod{k}$ and $n \equiv 1 \pmod{f(k)}$ (so if there are any such n, then $(k, f(k)) = 1$). Thus N_3, the number of Carmichaels in the third class, satisfies

$$N_3 \leqslant x^{1-\delta} + \sum_{x^{1-2\delta} < k \leqslant x^{1-\delta}} x/kf(k) = x^{1-\delta} + \sum_{d \leqslant x} \frac{x}{d} \sum_{\substack{x^{1-2\delta} < k \leqslant x^{1-\delta} \\ f(k)=d}} \frac{1}{k}.$$

We now assume x is sufficiently large and apply Lemma 2 and partial summation to the inner sum. We get

$$\sum_{\substack{x^{1-2\delta} < k \leqslant x^{1-\delta} \\ f(k)=d}} \frac{1}{k} < \ln x \cdot \exp(-(1-3\delta)\ln x \cdot \ln_3 x/\ln_2 x).$$

Thus

$$N_3 \leqslant x^{1-\delta} + x \ln^2 x \cdot \exp(-(1-3\delta)\ln x \cdot \ln_3 x/\ln_2 x)$$
$$< x^{1-\delta} + x \cdot \exp(-(1-4\delta)\ln x \cdot \ln_3 x/\ln_2 x).$$

Thus, the number of Carmichael numbers below x is at most

$$x^{1-\delta} + N_2 + N_3 < 4x^{1-\delta} + x \cdot \exp(-(1-4\delta)\ln x \cdot \ln_3 x/\ln_2 x)$$
$$< x \cdot \exp(-(1-5\delta)\ln x \cdot \ln_3 x/\ln_2 x).$$

Hence, by letting $\delta = \epsilon/5$, we have Theorem 6.

We next present a heuristic argument for the following lower bound for $C(x)$.

CONJECTURE 1. *For each* $\epsilon > 0$, *there is an* $x_0(\epsilon)$ *such that for all* $x \geqslant x_0(\epsilon)$,

$$C(x) > x \cdot \exp(-(2+\epsilon)\ln x \cdot \ln_3 x/\ln_2 x).$$

Let $\psi'(x, y)$ denote the number of primes $p \leqslant x$ for which $p-1$ is squarefree and all prime factors of $p-1$ do not exceed y. We now make the following

CONJECTURE 2. *For each* $\epsilon > 0$, *there is an* $x_0(\epsilon)$ *such that whenever* $x \geqslant x_0(\epsilon)$ *and* $\exp((\ln x)^{1/2}/2) \leqslant y \leqslant \exp((\ln x)^{1/2})$, *we have*

$$\psi'(x, y) \geqslant \pi(x)\exp(-(2+\epsilon)u \ln u),$$

where $u = \ln x/\ln y$ *and* $\pi(x)$ *is the number of primes not exceeding* x.

Let $\delta > 0$, let x be large, and let $A = A(x)$ denote the product of the primes $p \leqslant \ln x/\ln_2 x$. Then for all sufficiently large x, we have $A < x^{2/\ln_2 x}$. Let $r_1, \ldots, r_k$ be the primes in the interval $(\ln x/\ln_2 x, (\ln x)^{\ln_2 x})$ with $r_i - 1 \mid A$. Thus, by Conjecture 2, we have for large x,

$$k \geqslant \pi((\ln x)^{\ln_2 x}) \exp(-(2 + \delta) \ln_2 x \cdot \ln_3 x). \tag{10}$$

Let now $m_1, \ldots, m_N$ be the composite squarefree integers not exceeding x composed only of the r_i. We now prove (cf. Erdös [7]) that for all sufficiently large x,

$$N > x \cdot \exp(-(2 + 2\delta) \ln x \cdot \ln_3 x/\ln_2 x). \tag{11}$$

Let $l = [\ln x/(\ln_2 x)^2]$, $c = \exp(-(2 + \delta)\ln_2 x \cdot \ln_3 x)$. Since any product of l distinct r_i is less than $(\ln x)^{l \ln_2 x} \leqslant x$, we have that

$$N \geqslant \binom{k}{l} = \frac{k}{l} \cdot \frac{k-1}{l-1} \cdot \ \cdots \ \cdot \frac{k-l+1}{1} \geqslant \left(\frac{k}{l}\right)^l .$$

Thus, by (10) we have

$$N > \left(\frac{c (\ln x)^{\ln_2 x} / 2 (\ln_2 x)^2}{\ln x/(\ln_2 x)^2} \right)^{\ln x/(\ln_2 x)^2}$$

$$= \exp\left(\ln x \cdot \left\{ \frac{\ln(c/2)}{(\ln_2 x)^2} + \frac{-1 + \ln_2 x}{\ln_2 x} \right\} \right)$$

$$= x \cdot \exp\left(\ln x \cdot \left\{ \frac{-(2 + \delta)\ln_3 x}{\ln_2 x} - \frac{\ln 2}{(\ln_2 x)^2} - \frac{1}{\ln_2 x} \right\} \right)$$

$$\geqslant x \cdot \exp(-(2 + 2\delta) \ln x \cdot \ln_3 x/\ln_2 x).$$

This proves (11). We now note that each m_i is relatively prime to A.

CONJECTURE 3. *We have $m_1, \ldots, m_N$ at least roughly uniformly distributed in the residue classes modulo A that are relatively prime to A. Specifically, there are at least N/A^2 choices of i for which $m_i \equiv 1 \pmod{A}$.*

Since $A < x^{2/\ln_2 x}$, it follows from Conjecture 3 and (11) (which follows from Conjecture 2) that for all large x the number of $m_i \equiv 1 \pmod{A}$ is at least $x \cdot \exp(-(2 + 3\delta)\ln x \cdot \ln_3 x/\ln_2 x)$. But each such m_i is a Carmichael number, since m_i is composite, squarefree and $f(m_i) | A | m_i - 1$. If we now let $\delta = \epsilon/3$, we have Conjecture 1.

We thus see that Conjecture 1 follows in straightforward fashion from Conjectures 2 and 3. We now give plausibility arguments for the latter two assertions.

Concerning Conjecture 2, we first believe that the condition that $p - 1$ is squarefree in the definition of $\psi'(x, y)$ is not very important. Specifically, we believe (compare with Mirsky [16]) that $\psi''(x, y)$, the number of primes $p \leqslant x$ for which $p - 1$ is divisible only by primes not exceeding y, should be of the same order of magnitude as $\psi'(x, y)$ but for values of y that are ridiculously small (note that $\psi'(x, y)$ is bounded as $x \longrightarrow \infty$ for fixed y, while $\psi''(x, y)$ need not be bounded, or at least it appears so on the surface). Moreover, with a little extra effort, we could have dispensed with $\psi'(x, y)$ in the argument, using instead of Conjecture 2, the corresponding (weaker) conjecture for $\psi''(x, y)$. Secondly, and more importantly, we believe that $\psi''(x, y)/\pi(x)$ should be of the same order of magnitude as $\psi(x, y)/x$ (again one would want to exclude very small values of y). This belief fits nicely into the framework of the Titchmarsh divisor problem and other results (cf. [7]) which assert that the shifted primes $p - 1$ behave like ordinary integers. Furthermore, from de Bruijn [4], we in fact do have

$$\frac{1}{x}\,\psi(x, y) > \exp(-(2 + \epsilon)u \ln u)$$

for $u = \ln x/\ln y$, $\exp((\ln x)^{1/2}/2) \leqslant y \leqslant \exp((\ln x)^{1/2})$, and $x \geqslant x_0(\epsilon)$. In a forthcoming paper, the first author shows that $\psi''(x, y)/\pi(x)$ and $\psi(x, y)/x$ are in fact the same order of magnitude for the smaller range $y \geqslant x^{4/9}$. It also should be noted that a conjecture of Halberstam and Richert that Bombieri's prime number theorem holds for all moduli $k < x^{1-\epsilon}$ can be used to prove that $\psi''(x, x^u)/\pi(x) \sim \psi(x, x^u)/x$ for each fixed u, $0 < u \leqslant 1$. Thus, we feel that Conjecture 2 is a reasonable assertion.

On the subject of Conjecture 3, we note that in [9], Erdös and Rényi treat a similar situation. They have an arbitrary finite abelian group G and elements $a_1, \ldots, a_k$. Their conclusion is that if k is somewhat larger than $\ln \#G$, then for most choices of $a_1, \ldots, a_k$, the 2^k products $\Pi\, a_i^{\epsilon_i}$, where each $\epsilon_i = 0$ or 1, are uniformly distributed in G. For us, our group G is the multiplicative group of reduced residue classes modulo A and our given group elements are $r_1, \ldots, r_k$. We have the additional condition that we are only looking at those products $\Pi\, r_i^{\epsilon_i}$ which do not exceed x, but we do not feel this side condition is of overwhelming importance, since $\#G$ is much smaller than x ($\#G < x^{2/\ln_2 x}$). Thus, for Conjecture 3 to fail there must be something very peculiar about our set $r_1, \ldots, r_k$. Now our group G is isomorphic to the direct sum $\Sigma_{p|A}\, \mathbf{Z}_{p-1}$, where $\mathbf{Z}_{p-1}$ is the cyclic group of order $p - 1$. A necessary condition for a set $a_1, \ldots, a_k$ in G to be "random" (i.e., not "peculiar") is that the projections of $a_1, \ldots, a_k$ on the various $\mathbf{Z}_{p-1}$ should be uniformly distributed. But it is certainly not unreasonable for us to assume there are just as many $r_i \equiv 1 \pmod 3$ as $r_i \equiv 2 \pmod 3$, etc. Although this may not be a sufficient condition for Conjecture 3, it seems to be a step in the right direction. We, thus, believe Conjecture 3 to be at least plausible.

6. Distribution of Pseudoprimes in Residue Classes. Table 4 gives the number of psp(2)'s, epsp(2)'s, spsp(2)'s, and Carmichaels below $25 \cdot 10^9$ which lie in various residue classes with small moduli. We have a similar table for all moduli $\leqslant 200$. The distribution is similar for larger moduli, except that the irregularities become less pronounced for large prime moduli. For most $m \leqslant 200$, the residue class 1 (mod m) contains the largest number of psp(2)'s. The first exception is $m = 37$. There are 1267 psp(2)'s divisible by 37, while only 1152 lie in 1 (mod 37). The other 35 classes (mod 37) have about 500 to 600 psp(2)'s in each.

TABLE 4

Number of pseudoprimes below $25 \cdot 10^9$ in each residue class

Modulus	Class	Psp(2)	Euler	Euler but not strong	Strong	Carmichael
3	0	628	314	313	1	25
	1	18413	9501	5677	3824	2118
	2	2812	1532	515	1017	20
4	1	19269	10314	6505	3809	2116
	3	2584	1033	0	1033	47
5	0	1474	757	702	55	203
	1	12721	6460	4136	2324	1652
	2	2743	1492	547	945	82
	3	2685	1440	586	854	102
	4	2230	1198	534	664	124
7	0	2025	968	935	33	401
	1	8730	4491	2803	1688	1096
	2	2049	1054	499	555	105
	3	2491	1351	583	768	152
	4	2039	1119	549	570	129
	5	2258	1176	567	609	138
	6	2261	1188	569	619	142
8	1	12654	8887	6505	2382	1781
	3	1295	505	0	505	20
	5	6615	1427	0	1427	335
	7	1289	528	0	528	27
9	1	11395	5833	3782	2051	1609
	2	935	517	172	345	9
	3	318	160	160	0	11
	4	3513	1805	895	910	259
	5	937	498	170	328	6
	6	310	154	153	1	14
	7	3505	1863	1000	863	250
	8	940	517	173	344	5
12	1	16281	8666	5677	2989	2071
	3	29	0	0	0	0
	5	2389	1334	515	819	20
	7	2132	835	0	835	47
	9	599	314	313	1	25
	11	423	198	0	198	0

The missing residue classes contain no psp(2)'s.

The distribution of spsp(2)'s is slightly different. For most $m \leqslant 200$, the residue class 1 (mod m) contains the greatest number of spsp(2)'s and the class 0 (mod m) contains the least number of them, often none at all. The first exception to either statement is $m = 109$, for which each of the 109 classes contains between 28 and 70 spsp(2)'s. The classes 0 and 1 (mod 109) contain 46 and 59 spsp(2)'s, respectively. For $m = 157$, the class 0 (mod m) contains 51 spsp(2)'s, which is more than any other class modulo 157. For every odd prime $m < 200$, except $m = 167$, there is at least one spsp(2) below $25 \cdot 10^9$ divisible by m, but usually there is only a handful of them.

The single spsp(2) that we found which is a multiple of 3 is $5455590801 = 3 \cdot 691 \cdot 1481 \cdot 1777$. Although there are 54 multiples of 167 below $25 \cdot 10^9$ which are psp(2)'s, none of them is strong.

The distribution of epsp(2)'s in residue classes is very similar to that of all psp(2)'s on the average. However, as Shanks [22] has noted, the fraction of psp(2)'s which are epsp(2)'s is much larger for the class 1 (mod 8) than for the other three classes modulo 8. Also, no epsp(2) below $25 \cdot 10^9$ is $\equiv 3 \pmod{12}$, because then it would have to be strong by Theorem 4, but there is only one spsp(2) divisible by 3, and it happens to be $\equiv 9 \pmod{12}$.

The distribution of Carmichael numbers differs from that of all psp(2)'s, in that many more residue classes have no Carmichaels below $25 \cdot 10^9$, partly because of the action of Proposition 1. (Proposition 2 is no more restrictive than Proposition 4 for moduli below 1093^2.) Some empty classes not explained by the propositions are 3 and 11 (mod 12); 2, 3, 8, and 12 (mod 15); and 9, 11, and 20 (mod 21). But see a forthcoming paper by D. E. Penney and the first author, where examples are shown for some of these classes. For large odd m in our table, the class 0 (mod m) often has more Carmichaels than 1 (mod m). For example, we found 144 Carmichaels divisible by 181, while the other 180 classes each contain between 4 and 22 of them. For $m = 179$, however, every class has between 5 and 24 Carmichaels below $25 \cdot 10^9$. This great discrepancy may be explained as follows. In order for n to be a Carmichael we must have $f(n) \mid n - 1$. Now $f(n)$ usually is divisible by most small primes, but it is rarely divisible by a particular large prime. Thus, if p is a prime for which $p - 1$ has only small prime factors, then we will have $p - 1 \mid f(n)$ for most n, and so there will be many Carmichael numbers divisible by p. This is the case for 181, since $181 - 1 = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5$. On the other hand, if $p - 1$ is divisible by a large prime, then we will have $p - 1 \nmid f(n)$ for most n, and so there will be few Carmichael numbers divisible by p (at least in the range where p is still considered "large"). An example is $p = 179$, because $179 - 1 = 2 \cdot 89$.

For each integer $k \geq 0$, let c_k denote the relative density in all primes of the primes p for which $2^k \| l_2(p)$. It follows from the Čebotarev density theorem that each $c_k > 0$. (In fact, $c_0 = c_1 = 7/24$, $c_2 = 1/3$, and $c_k = 2^{-k}/3$ for $k \geq 3$.) It thus follows that for each fixed k, all but density 0 integers n have a prime factor p with $2^k \| l_2(p)$. Thus, for every fixed k, all but density 0 odd integers n have $2^k \mid l_2(n)$. But if such an n is a psp(2), then $2^k \mid n - 1$. Thus, we believe it is reasonable to conjecture that for each fixed k, all but a set of relative density 0 of the psp(2)'s n have $2^k \mid n - 1$. This argument would seem to explain the popularity of the class 1 (mod 4) over the class 3 (mod 4) for psp(2)'s and also the popularity of the class 1 (mod 8) over the class 5 (mod 8). In fact, a similar argument can explain the popularity of the class 1 (mod m) for psp(2)'s over other classes modulo m for every "small" m.

This heuristic argument also supports a conjecture of Shanks [22] that $S_2(x) = o(P_2(x))$. In fact, the argument suggests that most psp(2)'s are divisible by two primes p, q with $l_2(p)$ odd and $l_2(q)$ even. But such a psp(2) cannot be an spsp(2).

7. Distribution of Pseudoprimes According to Number of Prime Divisors. Table 5 gives the number of psp(2), spsp(2), and Carmichaels below $25 \cdot 10^9$ which have exactly k prime factors (counted according to multiplicity). Observe that the spsp(2)'s usually have only two prime factors and that the Carmichaels have more prime factors than the typical psp(2). Of course, the Carmichaels must have at least three prime factors, but the discrepancy is more than can be so explained.

TABLE 5

Number and percentage of numbers below $25 \cdot 10^9$ *with exactly* k *prime divisors, counting multiplicity*

k	All composites	psp(2)'s		spsp(2)'s		Carmichaels	
	%	#	%	#	%	#	%
2	14	9582	44	4200	87	0	0
3	22	3145	14	407	8	412	19
4	23	4843	22	205	4	795	38
5	18	3455	16	29	1	756	35
6	12	786	4	1	0	192	9
7	6	42	0	0	0	8	0
8	3	0	0	0	0	0	0

The percentages in the column headed "all composites" were computed from the formula $\Pi_k(x)/(x - \Pi_1(x))$ with $x = 25 \cdot 10^9$, where $\Pi_k(x)$ is the number of integers below x which have exactly k prime factors, counting multiplicity. We used the well-known asymptotic estimate

$$\Pi_k(x) \sim \frac{x}{\ln x} \frac{(\ln \ln x)^{k-1}}{(k-1)!}.$$

It is a mystery to us, why so many of the psp(2)'s have exactly two prime factors, or why more psp(2)'s have four or five prime factors than three of them.

The spsp(2) with six prime factors is

$$10761055201 = 13 \cdot 29 \cdot 41 \cdot 61 \cdot 101 \cdot 113.$$

It is a Carmichael number, too. Strong pseudoprimes with at least three prime factors often are Carmichaels, but not always.

Let $C_k(x)$ denote the number of Carmichael numbers $n \leqslant x$ which have exactly k distinct prime factors. We now show that for all large x, we have $C_k(x) \leqslant x^{(k-1)/k}$. Thus, if Conjecture 1 is true, then for each k, $C_k(x) = o(C(x))$. Let n be a Carmichael number with exactly k distinct prime factors and $x/2 < n \leqslant x$. Thus, n has a prime factor $p \geqslant (x/2)^{1/k}$. Also, $n \equiv 1 \pmod{p-1}$ and $n > p$. Thus, for each prime p, the number of Carmichael numbers $n \leqslant x$ which are divisible by p is less than $x/(p(p-1))$. Hence,

$$C_k(x) - C_k(x/2) \leqslant \sum_{p \geqslant (x/2)^{1/k}} x/(p(p-1)) \leqslant \frac{1}{4} x^{(k-1)/k}$$

for all large x. Thus,

$$C_k(x) \leqslant x^{1/2} + \sum_{1 \leqslant 2^i \leqslant \sqrt{x}} \{C_k(x \cdot 2^{-i}) - C_k(x \cdot 2^{-i-1})\}$$

$$\leqslant x^{1/2} + \frac{1}{4} x^{(k-1)/k} \sum_{i \geqslant 0} 2^{-i(k-1)/k} \leqslant x^{(k-1)/k}$$

for all large x.

We can show a similar result for psp(2)'s. For each d, the number of primes p with $l_2(p) = d$ is clearly less than d (since their product divides $2^d - 1$). Hence, there are fewer than $x^{2\epsilon}$ primes p with $l_2(p) < x^{\epsilon}$. Consequently, there are at most $x^{2k\epsilon}$ integers n composed of exactly k primes p with $l_2(p) < x^{\epsilon}$. Now consider psp(2)'s $n \leqslant x$ composed of exactly k primes, one of which, p, satisfies $l_2(p) \geqslant x^{\epsilon}$. Any such n satisfies $n \equiv 0 \pmod p$, $n \equiv 1 \pmod{l_2(p)}$, and $n > p$. Thus, the number of such $n \leqslant x$ is at most

$$\sum_{\substack{l_2(p) \geqslant x^{\epsilon} \\ p \leqslant x}} \frac{x}{p l_2(p)} \leqslant x^{1-\epsilon} \sum_{x^{\epsilon} \leqslant p \leqslant x} \frac{1}{p} \ll x^{1-\epsilon}.$$

Hence, letting $\epsilon = 1/(2k+1)$, we have that the number of psp(2)'s $n \leqslant x$ with exactly k prime factors is $O_k(x^{2k/(2k+1)})$. Thus, if Conjecture 1 holds, then the psp(2)'s with exactly k prime factors form a set of relative density 0 in the set of all psp(2)'s.

8. **Bases *a* Other Than 2.** In addition to the primary calculation of the psp(2)'s to $25 \cdot 10^9$, we found the psp(a)'s below 10^7 for $a = 3, 5$, and 7. The results are summarized in Table 6. The data suggest that $P_a(x)$ and $P_b(x)$ have roughly the same growth rate as $x \longrightarrow \infty$. However, the fact that a number is a psp(a) appears to enhance its chances for being a psp(b). This observation may be explained by a heuristic argument (given elsewhere [26]) which concludes that $l_a(p)$ and $l_b(p)$ have a large common factor for a substantial fraction of all primes p. Hence, when $l_a(p) \mid n-1$ is known, it is much easier to have $l_b(p) \mid n-1$ as well.

No one has ever proved that infinitely many numbers are simultaneously pseudoprimes to two distinct given bases, except for the trivial case when both bases are powers of the same integer. Our data supports the conjecture that for any given finite set of bases, infinitely many numbers are a psp(a) for each a in the set. When a number is known to be a pseudoprime to several bases, it has a much improved chance of being a Carmichael number. For example, while only 10% of the psp(2)'s below $25 \cdot 10^9$ are Carmichael, 1572 or 89% of the 1770 pseudoprimes to bases 2, 3, 5, and 7 are Carmichaels.

Shanks [22] has observed that $(12m + 1)(24m + 1)$ is both a psp(2) and a psp(3), whenever both factors are prime. Thus, the strong form of the prime k-tuples conjecture implies that at least $cx^{1/2}/\ln^2 x$ integers below x are simultaneously psp(2) and psp(3).

TABLE 6

Number of pseudoprimes to bases 2, 3, 5, 7 *below a limit*

Bases	First example	Limit 10^3	10^5	10^7	10^9	$25 \cdot 10^9$
2	$341 = 11 \cdot 31$	3	78	750	5597	21853
3	$91 = 7 \cdot 13$	5	76	749	-	-
5	$217 = 7 \cdot 31$	3	66	726	-	-
7	$25 = 5 \cdot 5$	5	69	651	-	-
2,3	$1105 = 5 \cdot 13 \cdot 17$	0	23	187	1272	4709
2,5	$561 = 3 \cdot 11 \cdot 17$	1	16	159	1086	3897
2,7	$561 = 3 \cdot 11 \cdot 17$	1	11	125	970	3573
3,5	$1541 = 23 \cdot 67$	0	14	137	-	-
3,7	$703 = 19 \cdot 37$	1	13	141	-	-
5,7	$561 = 3 \cdot 11 \cdot 17$	1	9	112	-	-
2,3,5	$1729 = 7 \cdot 13 \cdot 19$	0	11	95	685	2522
2,3,7	$1105 = 5 \cdot 13 \cdot 17$	0	7	90	688	2499
2,5,7	$561 = 3 \cdot 11 \cdot 17$	1	4	73	576	2046
3,5,7	$29341 = 13 \cdot 37 \cdot 61$	0	4	69	-	-
2,3,5,7	$29341 = 13 \cdot 37 \cdot 61$	0	3	63	501	1770

9. A Fast Test for Primality. We next consider another "test" for primality. The one at the beginning of this paper would work infallibly, if we could tell somehow when we are considering a pseudoprime. Several lists of psp(2)'s were published ([18] and [12]) for precisely this purpose. The defining of Euler and strong pseudoprimes were attempts to formulate a quick test for primality which never fails, or, at least, has a shorter list of special cases than the test (1). In view of the rarity of pseudoprimes, we are justified in defining a *probable prime to base a* (or prp(a))** to be any

** This terminology was suggested in a conversation with John Brillhart.

odd $n > 1$ satisfying (1). It may be either a psp(a) or a prime not dividing a. We define eprp(a) and sprp(a) similarly. Note that we can determine very quickly whether a large number is a prp(a), while it might be quite difficult to decide whether it is a psp(a).

We propose the following criterion for the primality of an odd number $n < 25 \cdot 10^9$.

Step 1. Check whether n is an sprp(2). If not, then n is composite.

Step 2. Check whether n is an sprp(3). If not, then n is composite.

Step 3. Check whether n is an sprp(5). If not, then n is composite.

Step 4. If n is one of the 13 numbers listed in Table 7, then n is composite. Otherwise n is prime.

TABLE 7

List of strong pseudoprimes to all of the bases 2, 3, *and* 5

	number	psp? to base: 7	11	13	carm?	factorization	form
A	25 326001	no	no	no	no	2251·11251	(k+1)(5k+1)
B	161 304001	no	spsp	no	no	7333·21997	(k+1)(3k+1)
C	960 946321	no	no	no	no	11717·82013	(k+1)(7k+1)
D	1157 839381	no	no	no	no	24061·48121	(k+1)(2k+1)
E	3215 031751	spsp	psp	psp	yes	151·751·28351	①
F	3697 278427	no	no	no	no	30403·121609	(k+1)(4k+1)
G	5764 643587	no	no	spsp	no	37963·151849	(k+1)(4k+1)
H	6770 862367	no	no	no	no	41143·164569	(k+1)(4k+1)
I	14386 156093	psp	psp	psp	yes	397·4357·8317	②
J	15579 919981	psp	spsp	no	no	88261·176521	(k+1)(2k+1)
K	18459 366157	no	no	no	no	67933·271729	(k+1)(4k+1)
L	19887 974881	psp	no	no	no	81421·244261	(k+1)(3k+1)
M	21276 028621	no	psp	spsp	no	103141·206281	(k+1)(2k+1)

① (k+1)(4k+1), where 4k + 1 = (m+1)(5m+1). Here k = 28350, m = 150.

② (k+1)(208k+1), where 208k + 1 = (m+1)(11m+1). Here k = 8316, m = 396.

Since Table 7 lists the numbers below $25 \cdot 10^9$ which are strong pseudoprimes to all three of the bases 2, 3, and 5, this algorithm correctly decides the primality of any number $n < 25 \cdot 10^9$. Note that virtually all composite numbers are discovered in Step 1. On the other hand, if we reach Step 2, then n is almost certainly prime, and we must continue to Step 4. Only very rarely does the algorithm terminate in Step 2 or Step 3.

Several obvious modifications of this algorithm are possible. If one were willing to use a longer list, one could follow the first two steps by looking up n in a table of the 184 spsp(2)'s below $25 \cdot 10^9$ which are also spsp(3)'s. (It would be slightly better to drop the second step instead of the third, since there are only 157 spsp(2)'s which are also spsp(5)'s and $< 25 \cdot 10^9$.) If one preferred to have no table look-up at all, e.g., on a small programmable calculator, then one could simply use strong probable prime tests to bases 2, 3, 5, 7, and 11. No number below $25 \cdot 10^9$ is a strong pseudoprime to all five of those bases (and only 3215031751 to the first four). Since most numbers are composite and most composites have a small prime factor, it is faster on the average to test n for divisibility by the first few primes, say, those < 100, before embarking on the above algorithm.

Let us now consider the numbers which are spsp(a)'s to several bases a. The first spsp(2) is $2047 = 23 \cdot 89$. The first number which is both an spsp(2) and an spsp(3) is $1373653 = 829 \cdot 1657$. The corresponding first numbers for bases 2, 3, 5, and bases 2, 3, 5, 7 are given in Table 7 (numbers A and E).

Notice that the 13 numbers in Table 7 are of the form $(k + 1)(rk + 1)$, where r is a small positive integer and $k + 1$ is prime. This suggests that there might be a divisibility condition (like Proposition 3, but stronger) for strong pseudoprimes. If one has to factor a large number known to be a strong pseudoprime to several bases, one should probably first try for a factorization of the form $(k + 1)(rk + 1)$ with small positive r. Actually, many pseudoprimes have the form $(k + 1)(rk + 1)$, but the tendency to have this form is more marked for the strong ones.

10. Lucas Pseudoprimes. When P and Q are integers such that $D = P^2 - 4Q \neq 0$, we define the Lucas sequence $\{U_k\}$ with parameters D, P, Q by

$$U_k = (\alpha^k - \beta^k)/(\alpha - \beta), \qquad k \geq 0,$$

where α and β are the two roots of $x^2 - Px + Q = 0$. (See Section 4 of [3] for a discussion of Lucas sequences from our point of view.) Fermat's "Little Theorem" has an analog for Lucas sequences: If p is an odd prime, $p \nmid Q$, and $(D/p) = -1$, then $p \mid U_{p+1}$. An odd composite number n such that $n \nmid Q$, $(D/n) = -1$, and $n \mid U_{n+1}$ is called a *Lucas pseudoprime* (lpsp) with parameters D, P, Q. One can compute a particular term, say U_{n+1}, of a Lucas sequence by means of recursion formulas at a cost of about three times the arithmetic labor of the exponentiation in (1).

By analogy to pseudoprimes, one might guess that the number of Lucas pseudoprimes below x would be about $P_2(x)$. The data we have indicates that this is approximately true.

R. Baillie [2] noticed that if one chooses the parameters D, P, Q as in B below, the first 50 Carmichael numbers and several other psp(2)'s were never Lucas pseudoprimes. His discovery led to the belief that a combination of a probable prime test and a Lucas probable prime test might be an infallible test for primality. (An lprp is a prime or lpsp.)

Numerous papers [33], [11], [17], [27], [28], [29], [31], [32] concerning Lucas pseudoprimes have appeared. Malm [14] used Lucas sequences in a practical pseudoprime test, but his test was quite different from ours. He discusses the computational cost of finding the Jacobi nonresidue D.

If one wishes to perform an ordinary prp test on an odd number n, one may select almost any number a for the base. In contrast, only about half of the parameter triples D, P, Q satisfying $D = P^2 - 4Q \neq 0$ may be used in constructing an lprp test because of the Jacobi symbol condition. Various methods of choosing the parameters are discussed in [2]. We mention two possibilities here. Baillie uses B while Selfridge prefers A.

A. Let D be the first element of the sequence $5, -7, 9, -11, 13, \ldots$ for which $(D/n) = -1$. Let $P = 1$ and $Q = (1 - D)/4$.

B. Let D be the least element of the sequence $5, 9, 13, \ldots$ for which $(D/n) = -1$. Let P be the least odd number exceeding $D^{1/2}$ and let $Q = (P^2 - D)/4$.

If no such D exists, then n is a square and hence not an lpsp for any choice of parameters. In the following, we assume that a particular algorithm for selecting the parameters D, P, Q in terms of n is given, and that it detects and removes squares n. Write $L(x)$ for the number of lpsp's up to x with parameters so chosen.

The analog for Lucas pseudoprimes of Proposition 3 is this:

PROPOSITION 5. *If the prime p divides the* lpsp *n, then $n \equiv -1 \pmod{\rho(p)}$, where $\rho(p)$ is the least positive k such that $p \mid U_k$. Hence, $n \equiv -(D/p)p \pmod{p \cdot \rho(p)}$, where D is the associated Jacobi nonresidue of n.*

Proof. The proposition follows immediately from Theorem 10 of [3].

For each of the algorithms A and B above, we have performed lpsp tests on the odd nonsquare composites up to 10^8 as well as on the nonsquare psp(2)'s below $25 \cdot 10^9$. We found that $L(x)$ has roughly the same growth rate as $P_2(x)$ for $x \leqslant 10^8$. We noticed several differences between the lpsp's and the psp(2)'s. While the pseudoprimes tend to be $\equiv 1 \pmod{m}$ for most m, the lpsp's preferred the class $-1 \pmod{m}$. Just as many pseudoprimes have the form $(k + 1)(rk + 1)$, many lpsp's have one of the forms $(k + 1)(rk - 1)$ or $(k - 1)(rk + 1)$, where r is a small positive integer. Perhaps these phenomena are related to the minus sign which distinguishes Propositions 3 and 5. The numerical data suggest that an lpsp with respect to a given parameter selection algorithm has an improved chance of being an lpsp for other algorithms, but that it is very unlikely to be a psp(a) for any base a specified in advance. In short, the lpsp's are different kinds of numbers than psp's. Not a single one of the first 21853 psp(2)'s is an lpsp for either algorithm A or B. Thus we have another test for primality for odd n below $25 \cdot 10^9$:

Step 1. Check whether n is an sprp(2). If not, then n is composite.

Step 2. Check whether n is an lprp for algorithm A (or B). If not, then n is composite. Otherwise n is prime.

We have explained why numbers which are both an spsp(2) and an lpsp should be rare. We challenge the reader to exhibit one. If there are none, then we have a primality test which is faster than that of Gary Miller [15] by a factor of ln n on the average when n is prime. For composite n which are not spsp(2)'s (and these are most of the composite numbers), Miller's test and ours are nearly equally swift.

The authors offer a prize of \$30 to the first person who communicates to us either (i) a number which is both an spsp(2) and an lpsp for either algorithm A or algorithm B, or (ii) a proof that no such number exists (for one of the algorithms). Claimants must state the prime factorization of any numbers submitted.

Department of Mathematics
University of Illinois at Urbana-Champaign
Urbana, Illinois 61801
and
Department of Mathematics
University of Georgia
Athens, Georgia 30602

Mathematical Reviews
611 Church Street
Ann Arbor, Michigan 48104
and
Department of Mathematical Sciences
Northern Illinois University
DeKalb, Illinois 60115

Department of Mathematics
University of Illinois at Urbana-Champaign
Urbana, Illinois 61801

1. N. C. ANKENY, Review #4935, *Math. Rev.*, v. 21, 1959, p. 905.

2. R. J. BAILLIE & S. S. WAGSTAFF, JR., "Lucas pseudoprimes," *Math. Comp.*, v. 35, 1980, pp. 000–000.

3. JOHN BRILLHART, D. H. LEHMER & J. L. SELFRIDGE, "New primality criteria and factorizations of $2^m \pm 1$," *Math. Comp.*, v. 29, 1975, pp. 620–647. MR 52 #5546.

4. N. G. DE BRUIJN, "On the number of positive integers $\leqslant x$ and free of prime factors $> y$," *Nederl. Acad. Wetensch. Proc. Ser. A*, v. 54, 1951, pp. 50–60. Also II, *ibid.*, v. 69, 1966, pp. 239–247. MR 13, 724; 34 #5770.

5. R. D. CARMICHAEL, "On composite numbers P which satisfy the Fermat congruence $a^{P-1} \equiv 1 \bmod P$," *Amer. Math. Monthly*, v. 19, 1912, pp. 22–27.

6. A. SCHINZEL, "On primitive prime factors of $a^n - b^n$," *Proc. Cambridge Philos. Soc.*, v. 58, 1962, pp. 555–562. MR 26 #1280.

7. P. ERDÖS, "On the normal number of prime factors of $p - 1$ and some other related problems concerning Euler's ϕ-function," *Quart. J. Math. Oxford Ser.*, v. 6, 1935, pp. 205–213.

8. P. ERDÖS, "On pseudoprimes and Carmichael numbers," *Publ. Math. Debrecen*, v. 4, 1956, pp. 201–206. MR 18, 18.

9. P. ERDÖS & A. RÉNYI, "Probabilistic methods in group theory," *J. Analyse Math.*, v. 14, 1965, pp. 127–138.

10. W. KNÖDEL, "Carmichaelsche Zahlen," *Math. Nachr.*, v. 9, 1953, pp. 343–350. MR 14, 1062.

11. EMMA LEHMER, "On the infinitude of Fibonacci pseudo-primes," *Fibonacci Quart.*, v. 2, 1964, pp. 229–230.

12. D. H. LEHMER, "On the converse of Fermat's theorem. II," *Amer. Math. Monthly*, v. 56, 1949, pp. 300–309. MR 10, 681.

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

14. D. E. G. MALM, "On Monte-Carlo primality tests," *Notices Amer. Math. Soc.*, v. 24, 1977, p. A-529; Abstract #77T-A22.

15. G. L. MILLER, "Riemann's Hypothesis and tests for primality," *Proc. Seventh Annual ACM Symposium on the Theory of Computing*, May 4–7, 1975, Albuquerque, pp. 234–239.

16. L. MIRSKY, "The number of representations of an integer as a sum of a prime and a k-free integer," *Amer. Math. Monthly*, v. 56, 1949, pp. 17–19. MR 10, 431.

17. E. A. PARBERRY, "On primes and pseudo-primes related to the Fibonacci sequence," *Fibonacci Quart.*, v. 8, 1970, pp. 49–60. MR 41 #6809.

18. P. POULET, "Table des nombres composés vérifiant le théorème de Fermat pour le module 2 jusqu'à 100 000 000," *Sphinx*, v. 8, 1938, pp. 42–52. For corrections see *Math. Comp.*, v. 25, 1971, pp. 944–945, MTE 485; v. 26, 1972, p. 814, MTE 497.

19. MICHAEL O. RABIN, "Probabilistic algorithms," in *Symposium on New Directions and Recent Results in Algorithms and Complexity* (J. F. Traub, Ed.), Academic Press, New York, 1976, pp. 21–39.

20. B. ROSSER, "The n-th prime is greater than $n \log n$," *Proc. London Math. Soc.* (2), v. 45, 1939, pp. 21–44.

21. A. ROTKIEWICZ, "Sur les progressions arithmétiques et géométriques formées de trois nombres pseudopremiers distincts," *Acta Arith.*, v. 10, 1964, pp. 325–328. MR 30 #1995.

22. D. SHANKS, *Solved and Unsolved Problems in Number Theory*, 2nd ed., Chelsea, New York, 1978.

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

24. J. D. SWIFT, "Table of Carmichael numbers to 10^9," *Math. Comp.*, v. 29, 1975, pp. 338–339. Review #13.

25. K. SZYMICZEK, "On pseudoprimes which are products of distinct primes," *Amer. Math. Monthly*, v. 74, 1967, pp. 35–37. MR 34 #5746.

26. S. S. WAGSTAFF, JR., "Pseudoprimes and a generalization of Artin's conjecture." *Acta Arith.* (To appear.)

27. M. YORINAGA, "A technique of numerical production of a sequence of pseudo-prime numbers," *Math. J. Okayama Univ.*, v. 19, 1976, pp. 1–4. MR 55 #5510.

28. M. YORINAGA, "On a congruencial property of Fibonacci numbers—numerical experiments," *Math. J. Okayama Univ.*, v. 19, 1976, pp. 5–10. MR 55 #5513.

29. M. YORINAGA, "On a congruencial property of Fibonacci numbers—considerations and remarks," *Math. J. Okayama Univ.*, v. 19, 1976, pp. 11–17. MR 55 #5514.

30. A. ROTKIEWICZ, "On the number of pseudoprimes $\leqslant x$," *Univ. Beograd. Publ. Elektrotehn. Fak. Ser. Mat. Fiz.*, No. 381–409, 1972, pp. 43–45. MR 48 #256.

31. A. ROTKIEWICZ, "On the pseudoprimes with respect to the Lucas sequences," *Bull. Acad. Polon. Sci. Sér. Sci. Math. Astronom. Phys.*, v. 21, 1973, pp. 793–797.

32. H. C. WILLIAMS, "On numbers analogous to the Carmichael numbers," *Canad. Math. Bull.*, v. 20, 1977, pp. 133–143.

33. D. H. LEHMER, "An extended theory of Lucas' functions," *Ann. of Math.*, v. 31, 1930, pp. 419–448.

34. J. BRILLHART, J. TONASCIA & P. WEINBERGER, "On the Fermat quotient," *Computers in Number Theory*, Academic Press, London, 1971, pp. 213–222.

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

36. P. ERDÖS, "On the converse of Fermat's theorem," *Amer. Math. Monthly*, v. 56, 1949, pp. 623–624. MR 11, 331.