MATHEMATICS OF COMPUTATION, VOLUME 35, NUMBER 152
OCTOBER 1980, PAGES 1391–1417

Lucas Pseudoprimes

By Robert Baillie and Samuel S. Wagstaff, Jr.

Abstract. We define several types of pseudoprimes with respect to Lucas sequences and prove the analogs of various theorems about ordinary pseudoprimes. For example, we show that Lucas pseudoprimes are rare and we count the Lucas sequences modulo n with respect to which n is a Lucas pseudoprime. We suggest some powerful new primality tests which combine Lucas pseudoprimes with ordinary pseudoprimes. Since these tests require the evaluation of the least number $f(n)$ for which the Jacobi symbol $(f(n)/n)$ is less than 1, we evaluate the average order of the function f.

1. Introduction. *A pseudoprime to base a* (or psp(a)) is a composite number n such that $a^{n-1} \equiv 1 \pmod{n}$, i.e., n satisfies the conclusion of Fermat's "Little Theorem" even though n is not prime. Pseudoprimes have been studied intensively. (See [17] and the references there.) In the present work we consider various analogs of pseudoprimes in which $a^{n-1} - 1$ is replaced by a term of a Lucas sequence. We will assume that n is odd except in Theorem 1.

Let D, P and Q be integers such that $D = P^2 - 4Q \neq 0$ and $P > 0$. Let $U_0 = 0$, $U_1 = 1$, $V_0 = 2$, and $V_1 = P$. The Lucas sequences U_k and V_k are defined recursively for $k \geqslant 2$ by

$$U_k = PU_{k-1} - QU_{k-2}, \qquad V_k = PV_{k-1} - QV_{k-2}.$$

We will write $U_k(P, Q)$ for U_k when it is necessary to show the dependence on P and Q. For $k \geqslant 0$, we also have

$$U_k = (\alpha^k - \beta^k)/(\alpha - \beta), \qquad V_k = \alpha^k + \beta^k,$$

where α and β are the distinct roots of $x^2 - Px + Q = 0$. The values of the residues of U_k and V_k (mod n) may be computed quickly for individual large k by a sequence of operations determined by the binary expansion of k; see [1].

For odd positive integers n, let $\epsilon(n)$ denote the Jacobi symbol (D/n), and let $\delta(n) = n - \epsilon(n)$. If n is prime, and if $(n, Q) = 1$, then

$$U_{\delta(n)} \equiv 0 \pmod{n}. \tag{1}$$

If n is composite, but (1) still holds, then we call n a *Lucas pseudoprime with parameters P and Q* (or lpsp(P, Q)).

Received August 2, 1979; revised February 14, 1980.
1980 *Mathematics Subject Classification.* Primary 10A15; Secondary 10–04.
Key words and phrases. Pseudoprime, Lucas sequence, Lucas pseudoprime, strong pseudoprime, Euler pseudoprime, primality testing.

0025-5718/80/0000-0182/$07.75

There are two points of view one can take about lpsp's. One can study divisibility properties of Lucas sequences. This we do in Sections 2 and 3. In the former, we count the number of ways n can be an lpsp and derive some interesting corollaries. In the latter we consider analogs of Euler and strong pseudoprimes; see [17].

On the other hand, in Sections 5 and 6 we use lpsp's to devise tests for primality which are almost always correct. In Section 4, we lay the groundwork for these tests by showing that lpsp's are rare. Pseudoprimes have long been studied as special cases in simple primality tests for large numbers. The best tests for the primality of n which we propose require the selection of a D such that the Jacobi symbol $(D/n) = -1$. We estimate the cost of choosing such D in Section 7. Our conclusion is that only a couple of trials are necessary on the average before one is found.

Malm [13] has formulated a primality test which uses Lucas sequences, but his test is quite different from the ones we will propose.

Good general references for properties of Lucas sequences which we do not prove are the papers of Lucas [12] and Lehmer [10].

The authors thank Hugh Williams for valuable discussions, especially of Section 2. We thank Carl Pomerance for providing the second corollary to Theorem 1. Section 7 could not have been written without suggestions from P. D. T. A. Elliott. We are grateful to the Computer-Based Education Research Laboratory and to the Computing Services Office of the University of Illinois for providing the computer time used in this research.

2. Simple Divisibility Properties of Lucas Sequences. The following three congruences hold when n is an odd prime and $(n, Q) = 1$:

$$V_{\delta(n)} \equiv 2Q^{(1-\epsilon(n))/2} \pmod{n} \quad \text{provided } (n, D) = 1, \tag{2}$$

$$U_n \equiv \epsilon(n) \pmod{n}, \tag{3}$$

$$V_n \equiv V_1 = P \pmod{n}. \tag{4}$$

Congruences (1)–(4) hold rarely when n is an odd composite number. Assuming $(n, 2PQD) = 1$, any two of the congruences imply the other two.

Rotkiewicz [18] has shown that, when $Q = \pm 1$ and $(P, Q) \neq (1, 1)$, there are infinitely many odd composite numbers n satisfying (1), (3), and (4) simultaneously. Yorinaga [24], [25], [26] has studied the sequence of Fibonacci numbers ($P = 1$, $Q = -1$), and gives a table of the composite $n \leqslant 707000$ which satisfy (3). (Contrary to the last sentence of the review of [25], four psp(2)'s appear in Yorinaga's table, namely 219781, 252601, 399001, and 512461.) E. Lehmer [11] showed that there are infinitely many primes p for which $n = U_{2p}$ satisfies (1) for the Fibonacci numbers. Thus there are infinitely many lpsp$(1, -1)$.

Given n, how many pairs (P, Q) satisfy (1)? Let us first consider the corresponding question for pseudoprimes. We allow even n here.

THEOREM 1. *Let $n = \prod p_i^{\alpha_i}$ be a positive integer. Then the number of bases $a \pmod{n}$ for which n is a* psp(a) *is*

$$\prod(n-1, p_i - 1).$$

Proof. The number of such bases a is the number of solutions (mod n) of the congruence

$$f(x) = x^{n-1} - 1 \equiv 0 \pmod{n}. \tag{5}$$

Consider first the congruences

$$f(x) \equiv 0 \pmod{p_i^{\alpha_i}}, \tag{6}$$

$$f(x) \equiv 0 \pmod{p_i}. \tag{7}$$

By Theorem 2.27 of [15], congruence (7) has $s_i = (n-1, p_i - 1)$ distinct solutions (mod p_i). Note also that $s_i \geqslant 2$ if n is odd, for in that case, $n-1$ and $p_i - 1$ are both even. By Theorem 123 of [9], each solution y of (7) corresponds to one solution of (6) (since $f'(y) \not\equiv 0 \pmod{n}$) and vice versa, so (6) also has s_i distinct solutions (mod $p_i^{\alpha_i}$). Finally, according to the Chinese Remainder Theorem, (5) has $\prod s_i$ distinct solutions (mod n), including the two trivial solutions $x \equiv \pm 1 \pmod{n}$.

COROLLARY 1. *Every odd composite number n is a* psp *to at least two nontrivial bases* (mod n) *unless n is a power of* 3.

Let $B(n)$ denote the number of bases modulo n to which n is a pseudoprime. Let ϕ denote Euler's function.

COROLLARY 2 (POMERANCE). *If we ignore a set of n of asymptotic density zero, then we have $B(n) = o(n)$ as $n \longrightarrow \infty$.*

Proof. It is well known [6] that for a fixed prime q, the normal order of the number of prime factors of n which are $\equiv 1 \pmod{q}$ is $(\log\log n)/(q-1)$. Let S_q be the set of all positive multiples of q. By the fact just mentioned, the set T_q of n in S_q which have fewer than $(\log\log n)/(2(q-1))$ prime factors $\equiv 1 \pmod{q}$, has density zero. If n is in S_q but n is not in T_q, then $\phi(n)$ is divisible by q to at least the $(\log\log n)/(2q-2)$ power. But $q \nmid n-1$ for such n and hence

$$B(n) \leqslant \frac{\phi(n)}{q^{(\log\log n)/(2q-2)}} < \frac{n}{q^{(\log\log n)/(2q-2)}} = o(n),$$

as $n \longrightarrow \infty$, $n \in S_q$, $n \notin T_q$.

Now let $0 < \epsilon < 1$ be given. It follows easily from Mertens' theorem that there is a K so that the density of the set T_ϵ of n which have no prime factor below K, is less than ϵ. Let U_ϵ be the union of T_ϵ and all the sets T_q for each prime $q < K$. Then U_ϵ has density $< \epsilon$ and $B(n) = o(n)$ as $n \longrightarrow \infty$, $n \notin U_\epsilon$.

Let $x_0 = 10$. For $k \geqslant 1$, choose x_k so that (a) $x_k > x_{k-1}^2$, (b) for all $z \geqslant x_k$, the number of $n \leqslant z$ with $n \in U_{1/k}$ is $\leqslant 2z/k$, and (c) we have $B(n) < n/k$ for every $n > x_k$ with $n \notin U_{1/k}$. (Once x_{k-1} is chosen, any sufficiently large number will serve as x_k. This is clear for (a), true for (b) because $U_{1/k}$ has density $< 1/k$, and true for (c) because $B(n) = o(n)$ as $n \longrightarrow \infty$, $n \notin U_\epsilon$.)

Let $U = \bigcup_{k=1}^{\infty} \{n \in U_{1/k} : x_k < n \leqslant x_{k+1}\}$. It follows easily from properties (a) and (b) that U has density zero. Property (c) gives $B(n) = o(n)$ as $n \longrightarrow \infty$, $n \notin U$. This proves the corollary.

Remarks. 1. One can improve Corollary 2 if one uses the methods of Erdös [7]. One can prove that $B(n) = o(n)$ as $n \longrightarrow \infty$ avoiding a set of integers, the sum of whose reciprocals converges.

2. If n is odd, the bases to which n is a psp occur in pairs: if n is a psp(a), then n is a psp($n - a$). Every odd number is a psp(1) and a psp(-1) (the trivial bases).

3. Experimentation indicates that the number of bases for which a composite n is a psp is usually small compared to n. We illustrate Corollary 2 for the 421502 odd composite numbers $n < 10^6$. We found that 255341 of them (that is, more than 60%) have fourteen or fewer nontrivial pseudoprime bases modulo n. The number of nontrivial psp bases for n is less than $0.0001n$ for 292440 (or nearly 70%) of them.

One may conveniently list all of the Lucas sequence parameters modulo n with fixed D as follows: Begin with any such pair (P_1, Q_1) and use the iterative scheme $P_{i+1} = P_i + 2$, $Q_{i+1} = P_i + Q_i + 1$.

When p is an odd prime not dividing Q, let $\omega(p) = \omega(p; P, Q)$ denote the *rank of apparition* of p in the Lucas sequence $U_k(P, Q)$, i.e., the least positive k such that $p \mid U_k$. The rank exists since (1) holds for prime n. Furthermore, $p \mid U_k$ if and only if $\omega(p) \mid k$.

THEOREM 2. *Let D be an integer. Let $n = \Pi p_i^{\alpha i}$ be an odd positive integer such that $(n, D) = 1$. Then the number of distinct values of P modulo n, for which there is a Q such that $P^2 - 4Q \equiv D \pmod{n}$ and (1) holds, is*

$$\prod_i ((\delta(n), \delta(p_i)) - 1) = \prod_i ((n - (D/n), p_i - (D/p_i)) - 1).$$

Remark. This formula counts the trivial Lucas sequence with $P \equiv 0 \pmod{n}$.

Proof. Let p^α exactly divide n. We first count the values of P modulo p, then modulo p^α. We have $p \mid U_{\delta(n)}(P, Q)$ if and only if $\omega(p; P, Q) \mid \delta(n)$, and hence if and only if $\omega(p; P, Q) \mid (\delta(n), \delta(p))$. By Theorem 2 of Williams [22], if $d \mid \delta(p)$ and $d > 1$, then there are $\phi(d)$ distinct values of P modulo p such that $\omega(p; P, Q) = d$. Since $U_1 = 1$, no P has $\omega(p; P, Q) = 1$. Thus the number of distinct P's modulo p is

$$\sum_{\substack{d \mid (\delta(n), \delta(p)) \\ d > 1}} \phi(d) = (\delta(n), \delta(p)) - 1.$$

Let

$$T_k(x) = \sum_{r=0}^{\lfloor k/2 \rfloor} \binom{k}{2r+1} x^{k-2r-1} D^r.$$

Then (see, e.g., Williams [22])

$$T_k(P) = 2^{k-1} U_k(P, Q).$$

Hence the values of P modulo p such that $p \mid U_{\delta(n)}(P, Q)$ (which we have just counted) are the zeros of $T_{\delta(n)}(x) \pmod p$. The derivative of $T_k(x)$ is $kT_{k-1}(x)$. We claim that

$$\delta(n)T_{\delta(n)-1}(P) \not\equiv 0 \pmod p,$$

whenever $T_{\delta(n)}(P) \equiv 0 \pmod p$. Clearly, $p \nmid \delta(n)$. If $p \mid T_{\delta(n)}(P)$ and $p \mid T_{\delta(n)-1}(P)$, then $p \mid U_{\delta(n)}$ and $p \mid U_{\delta(n)-1}$. This cannot happen unless $p \mid Q$ because $U_{\delta(n)} = PU_{\delta(n)-1} - QU_{\delta(n)-2}$. If $p \mid P$ also, then $p \mid D$, which is excluded. Finally, if $p \mid Q$, but $p \nmid P$, then $p \nmid U_k$ for every $k \geqslant 1$. This proves the claim.

From this claim and Newton's method modulo p^α (see Section 2.6 of [15]), it follows that for each zero of $T_{\delta(n)}(x)$ modulo p there is exactly one zero of $T_{\delta(n)}(x)$ modulo p^α congruent to it modulo p. Thus $T_{\delta(n)}(x)$ has exactly $(\delta(n), \delta(p)) - 1$ zeros modulo p^α. By Theorem 2.18 of [15], $T_{\delta(n)}(x)$ has $\prod((\delta(n), \delta(p_i)) - 1)$ zeros modulo n.

COROLLARY. *Every odd composite number n is an* lpsp(P, Q) *for at least three pairs P, Q with distinct values of P modulo n.*

Proof. It suffices to find a D for which $4 \mid \delta(n)$ and $4 \mid \delta(p)$ for some prime divisor p of n. If n is divisible by two distinct primes p, q and q exactly divides n to an odd power, then choose D so that $4 \mid \delta(p)$, $(D/r) = 1$ for each prime $r \mid n$, $r \neq p$ or q, and (D/q) has the proper sign to make $4 \mid \delta(n)$. Each condition restricts D modulo a different prime divisor of n, so all can be satisfied. If n is a square divisible by p, choose D so that $(D, n) = 1$ and $4 \mid \delta(p)$. Then $4 \mid \delta(n) = n - 1$. Finally, if n is an odd power of a prime p, choose D so that $4 \mid \delta(p)$. Then $4 \mid \delta(n)$ because $(D/n) = (D/p)$ and $n \equiv p \pmod 4$.

Another question one might ask is this: Given an odd n, for how many distinct D's, modulo n ($D \not\equiv 0 \pmod n$), do there exist at least one pair P, Q satisfying (1) and $P \not\equiv 0 \pmod n$? The answer depends on the prime factors of n. We illustrate the answer in the case when n is the product pq of two primes. According to Theorem 2, we should count D if and only if at least one of the GCD's,

$$(pq - (D/pq), p - (D/p)), (pq - (D/pq), q - (D/q)),$$

exceeds 2. Compute these GCD's for each of the four choices of ± 1 for (D/p), (D/q), and let H ($0 \leqslant H \leqslant 4$) be the number of choices for which the GCD exceeds 2. There are $((p - 1)/2)((q - 1)/2)$ distinct D's modulo n for each of the H choices of the signs. Thus the number of D's modulo n for which there is a pair P, Q satisfying (1) and $P \not\equiv 0 \pmod n$ is $H(p - 1)(q - 1)/4$.

In Sections 5 and 6, we shall consider lpsp n for which $\epsilon(n) = -1$. We remark here that the numbers $3(4k - 1)$ and $9(4k + 1)$, where the binomial factor is prime, cannot be such lpsp's, except for the trivial case $P \equiv 0 \pmod n$. For $n = 3(4k - 1) \equiv 1 \pmod 4$ implies that both GCD's

$$(n + 1, 3 \pm 1) = (n + 1, 4k - 1 \pm 1) = 2,$$

so that by Theorem 2, there is only one value of P modulo n which makes n an lpsp. With $n = 9(4k + 1)$, we have $(n + 1, 3 \pm 1) = 2$, as before. Now $\epsilon(4k + 1) = \epsilon(n) = -1$, whence $(n + 1, 4k + 1 - (-1)) = 2$, and the second assertion follows from Theorem 2.

3. Euler and Strong Lucas Pseudoprimes. We recall the definitions of Euler and strong pseudoprimes, which are introduced (see [17]) because these numbers are rarer than ordinary pseudoprimes.

An odd composite number n is an *Euler pseudoprime to base a* (or epsp(a)) if $(a, n) = 1$ and

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

An odd composite number n is a *strong pseudoprime to base a* (or spsp(a)) if, with $n - 1 = d \cdot 2^s$, d odd, we have either

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

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

We make the analogous definitions for Lucas pseudoprimes. An odd composite number n is an *Euler Lucas pseudoprime with parameters P, Q* (or elpsp(P, Q)) if $(n, QD) = 1$ and

$$U_{(n-\epsilon(n))/2} \equiv 0 \pmod{n} \quad \text{if } (Q/n) = +1$$

or

$$V_{(n-\epsilon(n))/2} \equiv 0 \pmod{n} \quad \text{if } (Q/n) = -1.$$

An odd composite number n is a *strong Lucas pseudoprime with parameters P, Q* (or slpsp(P, Q)) if $(n, D) = 1$ and, with $\delta(n) = d \cdot 2^s$, d odd, we have either

(i) $U_d \equiv 0 \pmod{n}$, or

(ii) $V_{d \cdot 2^r} \equiv 0 \pmod{n}$, for some r with $0 \leqslant r < s$.

Every prime n satisfies the conditions of each of these four definitions (with the word "composite" omitted), provided $(n, 2QD) = 1$.

Suppose n is an slpsp(P, Q), but $(n, Q) > 1$. Let the prime p divide (n, Q). If $p \nmid P$, then $p \nmid U_k$ for every $k \geqslant 1$. If $p \mid P$, then $p \mid D$ and $(n, D) > 1$. Thus, if n is an slpsp(P, Q), then $(n, 2QD) = 1$. This fact is the analog of the property: if n is an spsp(a), then $(n, 2a) = 1$.

Parberry [16, Theorems 4 and 1] has shown that there are infinitely many elpsp$(1, -1)$. Our Theorem 5 below generalizes his Theorem 1. Williams [22, Theorem 7] proved that there do not exist a composite number n and a discriminant D such that $(n, D) = 1$ and n is an elpsp(P, Q) for every pair P, Q for which $P^2 - 4Q = D$, $(P, Q) = 1$, and $(n, QD) = 1$.

Theorems 3 and 4 of [17] show that every spsp(a) is an epsp(a) and that every epsp(a) which is $\equiv 3 \pmod 4$ is an spsp(a). Theorems 3 and 4 which follow are the analogous results for Lucas pseudoprimes.

THEOREM 3. *If n is an* slpsp(P, Q), *then n is an* elpsp(P, Q).

Proof. As was remarked above, we have $(n, 2QD) = 1$ and hence $(Q/n) \neq 0$. Let the prime factorization of n be $p_1 \cdots p_t$, where perhaps some primes are repeated. Define k_j by $2^{k_j} \| \delta(p_j)$ and assume $k_1 \leqslant k_2 \leqslant \cdots \leqslant k_t$. It follows easily from the definition of slpsp(P, Q) that there is an integer $k \geqslant 0$ with $2^k \| \omega(p^b)$ for all prime powers p^b for which $p^b \| n$. Since $\omega(p^b)/\omega(p)$ is 1 or a power of p, and hence odd, we have $2^k \| \omega(p_j)$ for each j. Then $k \leqslant k_1$. Let $i \geqslant 0$ be the number of j with $k_j = k$. Then (any empty product is 1)

$$n \equiv \prod_{j=1}^{i} (2^k + \epsilon(p_j)) \cdot \prod_{j=i+1}^{t} \epsilon(p_j) \equiv \epsilon(n) \left(1 + 2^k \sum_{j=1}^{i} \epsilon(p_j)\right) \pmod{2^{k+1}},$$

so that $2^k \| \delta(n)$ or $2^{k+1} \mid \delta(n)$ according as i is odd or even.

Since $U_{2h} = U_h V_h$ and n is an slpsp(P, Q), we know that either $n \mid U_{\delta(n)/2}$ or $n \mid V_{\delta(n)/2}$. Let $p^b \| n$. Since $2^k \| \omega(p^b)$, we have either $p^b \mid U_{\delta(n)/2}$ or $p^b \mid V_{\delta(n)/2}$ according as $2^{k+1} \mid \delta(n)$ or $2^k \| \delta(n)$. We conclude that either $n \mid U_{\delta(n)/2}$ or $n \mid V_{\delta(n)/2}$ according as i is even or odd.

Note that $(Q/p) = -1$ if and only if $p \mid V_{\delta(p)/2}$. The latter relation holds precisely when the exponent of 2 in $\omega(p)$ equals the exponent of 2 in $\delta(p)$. Thus $(Q/p_j) = -1$ or $+1$ according as $j \leqslant i$ or $j > i$. Hence

$$(Q/n) = \prod_{j=1}^{t} (Q/p_j) = (-1)^i,$$

and we have proved that $n \mid U_{\delta(n)/2}$ or $n \mid V_{\delta(n)/2}$ according as $(Q/n) = +1$ or $(Q/n) = -1$, i.e., that n is an elpsp(p, Q).

THEOREM 4. *If n is an* elpsp(P, Q) *and either* $(Q/n) = -1$ *or* $\delta(n) \equiv 2 \pmod 4$, *then n is an* slpsp(P, Q).

Proof. If $(Q/n) = -1$, then $n \mid V_{\delta(n)/2}$, so n is an slpsp(P, Q). If $\delta(n) \equiv 2 \pmod 4$, then $d = \delta(n)/2$ is the odd number in the definition of slpsp. Either U_d or V_d is divisible by n because n is an elpsp(P, Q). Thus one of the two cases of the definition of slpsp(P, Q) holds.

The following theorem has been proved by Parberry [16] in the case of the Fibonacci numbers. In that situation ($P = 1$, $Q = -1$), the hypothesis that n is an epsp(-1) holds trivially. A nontrivial example of our theorem is $n = 133$, $P = 25$, $Q = 31$.

THEOREM 5. *Suppose* $(n, 2QD) = 1$, $U_n \equiv \epsilon(n) \pmod n$, *and n is an* lpsp(P, Q). *If n is an* epsp(Q), *then n is an* elpsp(P, Q).

Proof. Begin with the well-known identity $U_{a+b} = U_a V_b + Q^a U_{b-a}$, valid for all positive integers a, b. Take $a = (n - \epsilon(n))/2$ and $b = (n + \epsilon(n))/2$. Then

$$U_n = U_{(n-\epsilon(n))/2} V_{(n+\epsilon(n))/2} + Q^{(n-\epsilon(n))/2} U_{\epsilon(n)} = \epsilon(n) \pmod n \tag{8}$$

by the second hypothesis. Since $U_1 = 1$ and $U_{-1} = -1/Q$, we have $Q^{(n-\epsilon(n))/2}U_{\epsilon(n)} = \epsilon(n)Q^{(n-1)/2}$. Hence, from (8),

$$U_{\delta(n)/2}V_{(n+\epsilon(n))/2} \equiv \epsilon(n)(1 - Q^{(n-1)/2}) \pmod{n}. \tag{9}$$

Thus, $U_{\delta(n)/2}V_{(n+\epsilon(n))/2} \equiv 0 \pmod{n}$ if and only if $Q^{(n-1)/2} \equiv 1 \pmod{n}$. The third hypothesis gives

$$U_{\delta(n)} = U_{\delta(n)/2}V_{\delta(n)/2} \equiv 0 \pmod{n}. \tag{10}$$

Now suppose $(Q/n) = +1$. Then $Q^{(n-1)/2} \equiv 1 \pmod{n}$ because n is an epsp(Q). We must show $n \mid U_{\delta(n)/2}$. Suppose instead that there is a prime p with $p^e \| n$, but $p^e \nmid U_{\delta(n)/2}$. Then $p \mid V_{\delta(n)/2}$ by (10), and $p \mid V_{(n+\epsilon(n))/2}$ by (9). Since $p \nmid Q$ because $(n, Q) = 1$, we find that $p \mid V_0 = 2$, a contradiction. Hence $n \mid U_{\delta(n)/2}$ when $(Q/n) = +1$.

If $(Q/n) = -1$, then $Q^{(n-1)/2} \equiv -1 \pmod{n}$, and so

$$U_{\delta(n)/2}V_{(n+\epsilon(n))/2} \equiv 2\epsilon(n) \pmod{n}$$

by (9). Hence $(U_{\delta(n)/2}, n) = 1$ and we have $n \mid V_{\delta(n)/2}$ by (10).

4. The Distribution of Lucas Pseudoprimes. The expression $(\log x \log\log x)^{1/2}$ will be used often in this section. Denote it by $S(x)$. Erdös [7] proved that the number of psp(2)'s not exceeding x is $< x \exp(-c_1 S(x))$ for some positive constant c_1 and all sufficiently large x. His proof is easily modified to yield the same inequality for the number of psp(a)'s ($a \neq -1, 1$) up to x. A simple consequence [19] of this inequality is that, for each $a \neq \pm 1$, the sum of the reciprocals of all the psp(a)'s is a convergent series. Thus the psp(a)'s are rare compared to the primes, and hence the odd n satisfying $a^{n-1} \equiv 1 \pmod{n}$ are almost exclusively primes. We call such odd n *probable primes to the base a.* (John Brillhart suggested the term "probable prime" with this meaning.) In this section we will prove that the lpsp's are rare compared to the primes. Then it makes sense to define a *Lucas probable prime with parameters P, Q* to be any odd n satisfying (1).

A *probable prime test to base a* is a testing of the truth of $a^{n-1} \equiv 1 \pmod{n}$. A *Lucas probable prime test* is a testing of the truth of (1). In the next section we will describe a combination of a probable prime test with a Lucas probable prime test which seems to distinguish primes from composites much more effectively than either test does alone.

We will need two lemmas for the proof that lpsp's are rare. The first appears in Erdös [7], where it is derived as an easy consequence of a theorem of de Bruijn [2]. The second follows from elementary divisibility properties of Lucas sequences and was mentioned in [17]. Recall that $\omega(p)$ is the rank of apparition of the prime p.

LEMMA 1. *Let $N(p_1, \ldots, p_k; x)$ denote the number of integers $\leq x$ composed only of the primes $p_1, \ldots, p_k$. Put $k^u = x$. Then, for $u < \log x/\log\log x$, we have*

$$N(p_1, \ldots, p_k; x) < x \exp(-c_2 u \log u),$$

where c_2 is a positive constant.

LEMMA 2. *If the prime p divides the* lpsp n, *then* $n \equiv \epsilon(n) \pmod{\omega(p)}$.

THEOREM 6. *Given P and Q, let $L(x)$ denote the number of* lpsp(P, Q)*'s not exceeding x. Then there is a positive constant c_3 such that*

$$L(x) < x \exp(-c_3 S(x)),$$

for all sufficiently large x.

Proof. Split the lpsp(P, Q)'s not exceeding x into two classes. Let the first class contain those lpsp's n for which $\omega(p) < \exp(S(x))$ for every prime factor p of n. Clearly these lpsp's are composed of the prime factors of

$$U_t, \qquad 1 \leqslant t < \exp(S(x)). \tag{11}$$

The smallest integer with at least t distinct prime factors is the product of the first t primes, which is approximately t^t, by the prime number theorem. Since $U_t = (\alpha^t - \beta^t)/(\alpha - \beta)$, the number of distinct prime factors of U_t cannot exceed a constant plus t. Hence, the total number k of prime factors of all the numbers (11) satisfies

$$k < \sum_{t=1}^{\exp(S(x))} (c_4 + t) < \exp(2S(x)),$$

for all large enough x. Apply Lemma 1 with $u = c_5(\log x/\log\log x)^{1/2}$. We find that the number of lpsp's of the first class up to x is less than $x \exp(-c_6 S(x))$.

Every lpsp n of the second class has a prime factor p with $\omega(p) \geqslant \exp(S(x))$. By Lemma 2, we have $n \equiv \epsilon(n) \pmod{\omega(p)}$. We also have $n \equiv 0 \pmod{p}$ and $n > p$, so that $n \geqslant p(\omega(p) - 1)$. Let $p_1, \ldots, p_r$ be the primes $\leqslant x$ such that $\omega(p) \geqslant \exp(S(x))$. Then the number of lpsp $\leqslant x$ of the second class is less than

$$x \sum_{i=1}^{r} \frac{2}{p_i \omega(p_i)} < 2x \exp(-S(x)) \sum_{p<x} \frac{1}{p} < x \exp(-c_7 S(x)).$$

This inequality and the corresponding one for the first class give Theorem 6.

COROLLARY. *For a fixed P and Q, the sum of the reciprocals of all* lpsp(P, Q)*'s converges.*

The details of the proof are just like those in the proof of Theorem 4 of [19] and so are omitted.

We have seen that probable prime tests and Lucas probable prime tests are each good tests for primality in that the probability of failure tends to zero as the number being tested increases without bound. We know that the probability of failure is less than $\exp(-c_8 S(x))$ for numbers near x. There is no good reason to believe that this probability approaches zero much more rapidly. (See the remarks on the density of Carmichael numbers in [17].)

We now prove that $L(x)$ exceeds a constant times $\log x$. The lpsp's which we construct are in fact slpsp's.

THEOREM 7. *Let P and Q be relatively prime positive integers for which $P^2 - 4Q$ is positive but not a square. Then there is a positive constant $c(P, Q)$ such that*

the number $R(x)$ *of* slpsp(P, Q)*'s not exceeding* x *satisfies* $R(x) > c(P, Q)\log x$, *for all sufficiently large* x.

Proof. Let Q' be Q divided by its largest square divisor. Let $\eta = 1$ if $Q' \equiv 1 \pmod 4$ and $\eta = 2$ if $Q' \equiv 2$ or $3 \pmod 4$. Rotkiewicz [27] has proved, under our hypotheses on P and Q, that if $h \geqslant 7$ is an odd integer and $m = h\eta Q'$, then U_m has at least two prime factors p and q not dividing $mU_1U_2 \cdots U_{m-1}$. Let $n = pq$. It is easy to see that n is an slpsp(P, Q) because $\omega(p) = \omega(q) = m$. Hence $R(U_m) \geqslant (h - 5)/2$ for odd h. There is a constant $k = k(P, Q) > 1$ such that $U_m < k^m$ for all $m \geqslant 5$. Since $m \leqslant 2hQ$ we have $R(k^{2hQ}) \geqslant (h - 5)/2$ for all odd $h \geqslant 7$. This inequality is enough to prove the theorem.

5. Powerful Tests for Primality. Let n be a large odd integer, and suppose we wish to determine whether n is prime or composite. The usual procedure is to first test n for "small" factors. If none is found, we perform a probable prime test to some convenient base. If n passes this test, (i.e., if n is a probable prime), we apply several more probable prime tests to different (perhaps randomly chosen) bases. If n passes all of these probable prime tests, then n is almost certainly prime, and then we proceed to attempt to prove that n is prime by using the factors of $n^2 - 1$, $n^2 + 1$, and $n^2 \pm n + 1$; see [1], [20], [21], [23].

The problem with this method is that the probable prime tests are dependent. Suppose a_1 and a_2 ($\not\equiv \pm 1 \pmod n$) are chosen in advance. If n is a psp(a_1), then n is very likely one of those few numbers which is psp to many bases, so that n is more likely than average to be a psp(a_2). For example, a psp(2) is psp to far more bases than is the average odd composite number of the same size. In fact, of the 21853 psp(2)'s $< 25 \cdot 10^9$, 4709 of them are also psp(3); 2522 of them are psp(2), psp(3), and psp(5) simultaneously; and 1770 of them are psp(2), psp(3), psp(5), and psp(7) simultaneously [17]. If the events "n is a psp(a_1)" and "n is a psp(a_2)" were independent, we would expect that none of the first 21853 psp(2)'s would be a pseudoprime to base 3, 5, or 7.

It would be better to use two probable prime tests which are independent, that is, where n being a probable prime of the first type does not affect the probability of n being a probable prime of the second type. In fact, we describe a method which seems to do slightly better than mere independence. Namely, we have observed empirically that if n is a psp(a), then n is less likely than a typical composite to be an lpsp(P, Q), provided P and Q are chosen properly, and vice versa. If n passes both a probable prime test and a Lucas probable prime test, we can be more certain that it is prime than if it merely passes several probable prime tests or several Lucas probable prime tests.

The "worst" composite numbers from the point of view of a probable prime test are the Carmichael numbers, i.e., odd composite n which will pass a probable prime test for any base a with $(a, n) = 1$. We noticed that when fifty small Carmichaels were checked for probable primality with a Lucas probable prime test, they all failed; i.e., the Lucas test indicated that they were composite. All of the 21853

psp(2)'s under $25 \cdot 10^9$ also failed our Lucas tests with P and Q chosen by methods A and B below. These were our first hints that a combination of a probable prime test and a Lucas probable prime test might be an excellent way to distinguish prime from composite numbers.

How should we choose P and Q? First, D should not be a square (mod n). For if $D = b^2$, so that $(D/n) = 1$ and $P = b + 2$, then $Q = b + 1$ and $U_{n-1} = (Q^{n-1} - 1)/(Q - 1)$, so that the Lucas test is merely an ordinary probable prime test in disguise. A good way to prevent such accidents is to require that $(D/n) = -1$. We state two algorithms for choosing the parameters:

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 first element of the sequence $5, 9, 13, 17, 21, \ldots$ for which $(D/n) = -1$. Let P be the least odd number exceeding $D^{1/2}$, and $Q = (P^2 - D)/4$.

Method A was suggested by John Selfridge. It does not try $D = -3$ first because then we would have $P = Q = 1$, and this produces a periodic Lucas sequence for which (1) holds for all odd n.

The first ten lpsp that arise when P and Q are chosen by method A are: 323, 377, 1159, 1829, 3827, 5459, 5777, 9071, 9179, and 10877. The first ten lpsp from method B are: 323, 377, 1349, 2033, 2651, 3569, 3599, 3653, 3827, and 4991.

Two points should be remembered in any practical implementation of these (or other) parameter selection methods. Our purpose is to devise a test for primality. If we encounter a D with $(D/n) = 0$ in the search for a D with $(D/n) = -1$, then we have found a factor of n and we should stop the test. Thus, we terminate the search with the first D for which $(D/n) < 1$. The second point is that if n is a square, then $(D/n) > -1$ for every D. Thus, if $(D/n) = 1$ for all of the first few D's, we should pause and check whether n is a square. (The number of iterations required by Newton's method to compute $[n^{1/2}]$ is $O(\log \log n)$, so this can be done quickly.) If n is a square, we stop the test. Otherwise, we resume the search for an appropriate D. In Section 7 we prove that the average number of D's which must be tried is less than 2.

Of course, the probable prime and Lucas probable prime tests can be made even more powerful by using their strong versions. To be specific, we recommend this test for primality of a large odd number n:

Step 1. If n is divisible by any prime less than some convenient limit (e.g.,1000), then n is composite.

Step 2. If n is not a strong probable prime to base 2, then n is composite.

Step 3. Choose parameters P and Q by method A or B. (This step might include a test whether n is a square.)

Step 4. If n is not a strong Lucas probable prime with parameters P and Q, then n is composite. Otherwise, n is almost certainly prime.

This procedure will always decide that primes above 1000 are prime. It can fail for numbers greater than 1000 only by asserting that a composite number is prime.

It certainly makes no mistakes for $n < 25 \cdot 10^9$. Does it always work correctly?

One could modify Steps 2 and 4 as follows. If n is a psp(2) or lpsp, Step 2′ or 4′ often produces at least one (not necessarily prime) factor of n. Let $n - 1 = d \cdot 2^s$, and $n + 1 = e \cdot 2^t$, with d and e odd.

Step 2′. Let $x_r \equiv 2^{d \cdot 2^r} \pmod{n}$, $(0 \leqslant r < s)$, and $g_r = (x_r - 1, n)$. If $1 < g_r < n$, so $g_r \mid n$, then n is composite. If n is not a strong probable prime to base 2, then n is composite.

Step 4′. Let $y_r \equiv V_{e \cdot 2^r} \pmod{n}$, for $0 \leqslant r < t$. If $1 < (U_e, n) < n$ or if $1 < (y_r, n) < n$, then n is composite. If n is not a strong Lucas probable prime, then n is composite.

Each GCD involves a loop of $O(\log n)$ iterations. If n is a psp(2), Step 2′ will give a factor of n unless n is an spsp(2). (For example, 341 can be factored this way, since $2^{85} \equiv 32 \pmod{341}$, and $(2^{85} - 1, 341) = 31$.) If n is a psp(a) but not an spsp(a), then n can be factored this way because the multiplicative order of the prime factors of n are not all divisible by the same power of 2. This means that for some r, $0 \leqslant r < s$, $a^{d \cdot 2^r}$ is congruent to 1 modulo some, but not all, of the prime powers that divide n. If n is an lpsp(P, Q) but not an slpsp(P, Q), then Step 4′ will give a factor of n.

If n is a prime power, then n can be factored very easily. If n is not a prime power, then one can show that there exists a base a such that n is a psp(a) but not an spsp(a). If one had a method for finding such an a, then one could factor n in just $O(\log n)$ additional steps!

Remarks. 1. Steps 4 and 4′ terminate at a subscript $\leqslant (n + 1)/2$. It is easy to continue and compute U_{n+1} and $V_{n+1} \pmod{n}$ by several doublings of the subscript.

2. If Step 4 or 4′ does not indicate that n is composite, then we can also check whether $V_{n+1} \equiv 2Q \pmod{n}$. This congruence must be satisfied if n is prime provided $(n, 2QD) = 1$. This check involves almost no additional work, because $V_{n+1} = (V_{(n+1)/2})^2 - 2Q^{(n+1)/2}$, where $V_{(n+1)/2}$ is used to compute U_{n+1}, and $Q^{(n+1)/2}$ is easily obtained from the previously computed power of Q.

3. There is another check we can do that is almost "free". If n is prime and $(n, Q) = 1$, then $Q^{(n+1)/2} = Q \cdot Q^{(n-1)/2} \equiv Q \cdot (Q/n) \pmod{n}$. This congruence can be easily checked, since $Q^{(n+1)/2} \pmod{n}$ is used to calculate V_{n+1}. If $Q = \pm 1$, this condition holds trivially. If the algorithm for selecting P and Q produces $Q = \pm 1$, we can simply choose a different (P, Q) pair having the same D; see methods A* and B* in Section 6. This check on the value of $Q^{(n+1)/2}$ amounts to a built-in Euler probable prime test. It is very rare to have both $U_{n+1} \equiv 0 \pmod{n}$ and $Q^{(n-1)/2} \equiv (Q/n) \pmod{n}$, (with $Q \neq \pm 1$) unless n is prime. The smallest n for which both congruences are true is $n = 65$, $Q = 14$, $|P| = 12$, 13, 17, 22, or 27, and $Q = -14$, $|P| = 6$, 19, 21, 26, or 31. (Of course, by "rare", we mean that unless you try many (P, Q) pairs for each n, you probably will not find one for which both congruences are true!)

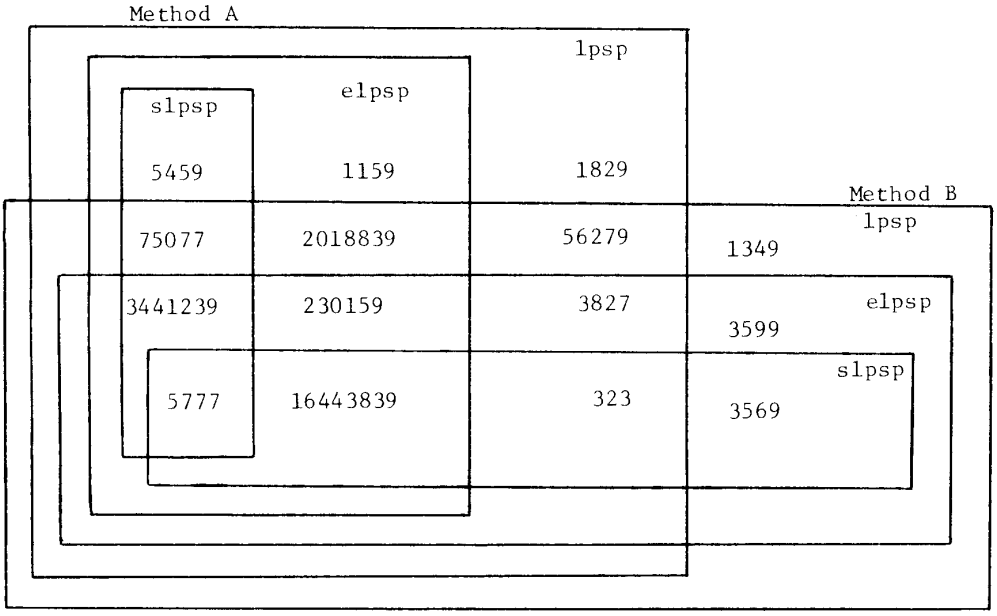
We will see in Section 6 that these additional checks are extremely powerful, especially if $Q \neq \pm 1$.

Now let us look at the results of the computer calculations and the evidence for independence of the probable prime and Lucas probable prime tests. First, as noted above, the psp(2) under $25 \cdot 10^9$ and several small Carmichaels failed our Lucas probable prime test.

By Theorem 3, every slpsp is an elpsp. Of course, every elpsp is an lpsp. Figure 1 shows the least integer of each of these three types with respect to each of the two methods of choosing parameters. For example, 3827 is the first lpsp but not elpsp for method A which is an elpsp but not slpsp for method B.

FIGURE 1

The least element of each set is shown



In Table 1, we give the number of lpsp's up to x with respect to parameter selection methods A and B. Once the parameters have been chosen, we can consider Euler and strong lpsp's. The numbers of these lpsp's are also given in Table 1. That table also shows the number of numbers $\leqslant x$ which are lpsp, elpsp, or slpsp for both methods simultaneously. The growth rates are very much like those of the psp(a)'s which are reported in [17]. Note that there are more lpsp for method B than for method A. This occurs because on those occasions where $(5/n) = 1$, method A eliminates multiples of 7, 11, etc., but method B does not. If we consider only those numbers that have no prime factor < 1000 (as in Steps 1–4 above), then there is little difference between methods A and B.

It is certainly not true that no psp is an lpsp. (Recall Corollary 1 to Theorem 1 and the Corollary to Theorem 2.) Our experience is that if n is a psp(a), and you try many Lucas sequences with $(D/n) = -1$, you can often find one for which n is an lpsp. For example, $n = 341$ is a psp(2); it is also an lpsp(7, 2). (We exclude all the trivial cases $a \equiv 0$ or $\pm 1 \pmod{n}$ and $n \mid P$ here.) Likewise, most lpsp n with $(D/n) = -1$ are psp(a)'s for only a few bases a. The point is that if you prescribe a base a and a method for choosing Lucas sequence parameters so that $(D/n) = -1$, then very few n will be both psp(a)'s and lpsp's. Indeed, it appears that such n are far less numerous than either psp(a)'s or lpsp's.

TABLE 1

Count of Lucas pseudoprimes up to x

	x = 10^3	10^4	10^5	10^6	10^7	10^8
Method A.						
lpsp	2	9	57	219	659	1911
elpsp	0	3	17	80	269	833
slpsp	0	2	12	58	178	505
Method B.						
lpsp	2	15	70	248	750	2119
elpsp	2	7	40	142	441	1265
slpsp	2	4	23	84	261	711
Methods A and B simultaneously.						
lpsp	2	4	29	87	246	660
elpsp	0	1	5	18	57	156
slpsp	0	1	5	17	49	125

Further support for our proposal is provided by Theorems 1 and 2. When D is fixed, and $(D/n) = -1$, the number of distinct values of P modulo n for which $n \mid U_{n+1}$ is $\Pi((n+1, p_i \pm 1) - 1)$, where $n = \Pi p_i^{\alpha i}$, and the choice of ± 1 depends on D and p_i. Most of the GCD's $(n+1, p_i \pm 1)$ would have to be large for there to be many Lucas sequences with respect to which n is an lpsp. Likewise, n is a psp(a) for $\Pi(n-1, p_i - 1)$ distinct values of a modulo n. Thus, most of the GCD's $(n-1, p_i - 1)$ must be large for n to be a pseudoprime to many bases. Now, the GCD's $(n+1, p_i - 1)$ and $(n-1, p_i - 1)$ cannot both exceed 2. Furthermore, it seems very difficult for both GCD's $(n+1, p_i + 1)$ and $(n-1, p_i - 1)$ to be large fractions of p_i, at least for most prime factors p_i of n. Hence it is nearly impossible for a number to be both a psp to many bases and an lpsp for many values of P, as long as $(D/n) = -1$.

On the other hand, suppose that $(D/n) = +1$. The GCD's in question are $(n-1, p_i - (D/p_i))$ and $(n-1, p_i - 1)$. As above, $(n-1, p_i + 1)$ and $(n-1, p_i - 1)$ cannot both exceed 2, but whenever $(D/p_i) = +1$, then the GCD's are the same, so that both can be large. Thus, in many cases we would expect that if n is an lpsp(P, Q) for many values of P with $(D/n) = +1$, then n might also be a psp(a) for many values of a. The computer calculations bear this out.

Table 2 gives the distribution modulo m of the lpsp's under 10^8 for several small m. Note that the residue class $-1 \pmod m$ has more lpsp's than any other class. This shows that if n is a typical lpsp (with $(D/n) = -1$), then $n+1$ has many small prime divisors. The analogous table to Table 2 for psp(2)'s is given in [17]. It

shows that the class $+1 \pmod{m}$ contains the lion's share of the psp(2)'s, at least for small m. If n is a typical psp(2), then $n-1$ has many small prime divisors. Since $(n-1, n+1) = 2$, these facts support our proposal that the combination of a probable prime test with a Lucas probable prime test is a very discriminating test for primality. In fact, since the psp(2) and lpsp have a tendency to fall into different residue classes (mod m), it may even be that any dependence between the probable prime and Lucas probable prime tests works in our favor. If this were so, or even if the tests were independent, we would not expect to find a number which is both a psp(2) and an lpsp until far beyond our search limit.

TABLE 2

Number of Lucas pseudoprimes below 10^8 *in each residue class*

Modulus	Class	Method A			Method B		
		lpsp	elpsp	slpsp	lpsp	elpsp	slpsp
3	0	47	24	4	16	9	0
	1	251	107	72	281	135	92
	2	1613	702	429	1822	1121	619
4	1	419	167	167	558	280	280
	3	1492	666	338	1561	985	431
5	1	271	130	81	279	150	92
	2	274	64	64	391	274	169
	3	237	41	41	364	237	132
	4	1129	598	319	1085	604	318
7	0	11	0	0	120	53	6
	1	224	90	63	243	155	85
	2	248	106	73	269	169	108
	3	123	39	30	237	149	87
	4	191	95	65	252	148	86
	5	130	57	47	250	141	78
	6	984	446	227	748	450	261
8	1	212	80	80	267	138	138
	3	563	161	137	571	278	203
	5	207	87	87	291	142	142
	7	929	505	201	990	707	228
9	1	86	41	28	99	44	30
	2	349	154	93	419	251	141
	3	22	11	2	7	4	0
	4	74	27	16	86	43	29
	5	352	146	97	414	261	146
	6	25	13	2	9	5	0
	7	91	39	28	96	48	33
	8	912	402	239	989	609	332
12	1	55	27	27	82	39	39
	3	47	24	4	13	9	0
	5	364	140	140	473	241	241
	7	196	80	45	199	96	53
	9	0	0	0	3	0	0
	11	1249	562	289	1349	880	378

Note that if $(D/n) = -1$ and $n \equiv 1 \pmod 4$, then n is an elpsp(P, Q) if and only if n is an slpsp(P, Q) by Theorem 4, because in this case, $\delta(n) \equiv 2 \pmod 4$.

TABLE 3

Number and percentage of numbers below 10^8 *with exactly k prime divisors, counting multiplicity*

	k = 2	3	4	5	6	7
All composites %	17	24	24	17	10	5
Method A						
lpsp	1127	485	267	32	0	0
%	59	25	14	2	0	0
elpsp	509	188	119	17	0	0
%	61	23	14	2	0	0
slpsp	430	63	12	0	0	0
%	85	12	2	0	0	0
Method B						
lpsp	1295	561	219	38	6	0
%	61	26	10	2	0	0
elpsp	815	312	119	15	4	0
%	64	25	9	1	0	0
slpsp	595	104	10	2	0	0
%	84	15	1	0	0	0

Table 3 shows the numbers of lpsp, elpsp, and slpsp below 10^8 with exactly k prime divisors, counting multiplicity. The values shown for all composites were computed from the asymptotic formula

$$\frac{x}{\log x} \cdot \frac{(\log \log x)^{k-1}}{(k-1)!}$$

for the number of integers up to x with exactly k prime factors. The lpsp and elpsp are somewhat skewed in the direction of having fewer prime divisors than the "average" number. The slpsp are even more skewed in this direction. This tendency is similar to that reported in [17] for psp(2), epsp(2) and spsp(2).

6. Other Congruence Conditions. We have defined Lucas pseudoprimes to be odd composite numbers n that satisfy congruence (1), and we have seen that if we require $(D/n) = -1$, the lpsp tend to be psp to very few bases. We now consider the other congruences, namely, (2), (3), and (4), which must hold if n is prime and $(n, 2QD) = 1$. Unless stated otherwise, in this section n will be an odd composite number which is not a square.

The n's which are squares were omitted from the calculations. (Squares are easy to spot, and are of little interest in prime testing.) Congruence (2) is satisfied, for example, if n is the square of an odd prime p, if $Q = 1$, and $(D/p) = +1$. (Proof: $2V_{p-1} = (V_{(p-1)/2})^2 + D(U_{(p-1)/2})^2$, and $V_{p-1} = (V_{(p-1)/2})^2 - 2Q^{(p-1)/2}$, so $V_{p-1} = D(U_{(p-1)/2})^2 + 2Q^{(p-1)/2} \equiv 0 + 2 \pmod{p^2}$. Then use $2V_{a+b} = V_aV_b + DU_aU_b$ repeatedly, to obtain $2^{k-1}V_{k(p-1)} \equiv (V_{p-1})^k \pmod{p^2}$, for $k = 2, 3, \ldots, p + 1$.)

TABLE 4

Counts of odd, composite, nonsquare $n \leqslant x$ satisfying congruence (1), (2), (3), *or* (4); *D, P, Q from method* A *or* A*

Congruence	(D/n)	Method A or A*	x 10^3	10^4	10^5	10^6	10^7	10^8
(1)	-1	A	2	9	57	219	659	1911
(1)	1	A	0	7	37	134		
(2)	-1	A	0	2	4	18		
(2)	-1	A*	1	1	1	1	1	1
(2)	1	A	0	9	34	103		
(3)	-1	A	7	62	471	3789		
(3), (3,n)=1	-1	A	0	4	22	172		
(3), (39,n)=1	-1	A	0	1	3	13		
(3), (39,n)=1	-1	A*	0	0	1	2	9	13
(3)	1	A	10	70	494	3868		
(3), (39,n)=1	1	A	0	4	26	91		
(4)	-1	A	0	2	4	20		
(4)	-1	A*	2	3	3	4	9	17
(4)	1	A	0	4	22	78		
(1,2,3,4)	-1	A	0	1	3	11	38	105

TABLE 5

Counts of odd, composite, nonsquare $n \leqslant x$ satisfying congruence (1), (2), (3), *or* (4); *D, P, Q from method* B *or* B*

Congruence	(D/n)	Method B or B*	x = 10^3	10^4	10^5	10^6	10^7	10^8
(1)	-1	B	2	15	70	248	750	2119
(1)	1	B	5	25	93	289		
(2)	-1	B	3	8	41	124		
(2)	-1	B*	1	1	2	2	2	2
(2)	1	B	1	22	79	259		
(3)	-1	B	4	7	29	91	249	
(3)	-1	B*	0	0	1	1	3	3
(3)	1	B	2	18	73	230		
(4)	-1	B	2	8	32	116		
(4)	-1	B*	2	3	3	4	9	29
(4)	1	B	2	24	87	298		
(1,2,3,4)	-1	B	2	4	25	81	228	620

Tables 4 and 5 show the counts of the $n \leqslant x$ which satisfy at least one of the congruences (1)–(4). We first tested all four congruences with both choices of sign of (D/n), where P and Q were chosen by methods A and B. Most of the n satisfying (3) when P and Q were chosen by method A were divisible by 3 or 13. (For example, let $n = 3p$, p prime, $p \equiv \pm 1 \pmod 8$, and let $D = -7$ so that $P = 1$ and $Q = 2$. Then $(D/3) = -1$. If $(D/p) = 1$, then it is not hard to show that $U_n \equiv -1 \pmod p$ and that $U_n \equiv -1 \pmod 3$, so that $U_n \equiv -1 \pmod n$.) If we exclude n with $(39, n) > 1$ in congruence (3), we find that when $(D/n) = -1$, almost every n which satisfies congruence (2), (3), or (4) had $Q = \pm 1$. The only exceptions were:

Congruence	Method	n	D	P	Q	Searched $n \leqslant$
(3)	A	186961	−7	1	2	10^6
(4)	A	530881	−11	1	3	10^6
(2)	B	64469	13	5	3	10^6
(3)	B	1940611	17	5	2	10^7
(4)	B	137149	17	5	2	10^6

By contrast, many n satisfied (1) with $Q \neq \pm 1$.

We decided to test these congruences again, but this time we would force Q to be other than ± 1. In particular, we used these methods for choosing D, P, and Q (with $(D/n) = -1$):

A*. Choose D, P, and Q as in method A above. If $Q = -1$, reset P and Q according to: $P \Leftarrow 5$, $Q \Leftarrow 5$.

B*. Choose D, P, and Q as in method B above. If $Q = 1$, reset P and Q according to: $Q \Leftarrow P + Q + 1$, $P \Leftarrow P + 2$.

In A*, we get $P = Q = 5$ from two applications of the transformation $Q \Leftarrow P + Q + 1$, $P \Leftarrow P + 2$, starting with $P = 1$, $Q = -1$. If $D = 5$, methods A* and B* are equivalent: both give $P = Q = 5$. Also, as in methods A and B, if we encounter a D with $(D/n) = 0$, we consider n to be composite and we do not do a Lucas test on this n.

We checked congruences (2), (3), and (4) using methods A* and B* for $n < 10^8$, and these counts are also shown in Tables 4 and 5. All of the $n < 10^8$ that satisfied congruences (2), (3), or (4) are listed in Table 6. We do not know why the n satisfying congruence (2), (3), or (4) are so rare when $(D/n) = -1$ and $Q \neq \pm 1$. Note that when P and Q are chosen by method A*, there is only one composite $n < 10^8$ for which (2) holds!

Hugh Williams noticed that if n is prime, $(D/n) = -1$, and $(2Q, n) = 1$, then

$$(*) \qquad V_{n+1} \equiv 2Q^{(n+1)/2} \cdot (Q/n) \pmod{n^2}.$$

This follows from the identity $V_{2k}^2 = DU_{2k}^2 + 4Q^{2k}$. From this we obtain $V_{n+1}^2 \equiv 4Q^{n+1} \pmod{n^2}$. The proper sign for the right side of (*) is determined from the fact that $V_{n+1} \equiv 2Q \pmod{n}$.

Congruence (*) is even stronger than, and implies, congruence (2). The two composite n listed in Table 6 which satisfy (2) were tested in congruence (*) with the same P and Q as in Table 6. Neither of these n satisfied (*). Thus, (*), with D, P, and Q chosen by method A* or B*, detects all composites $<10^8$.

Another result we noticed in the calculations was that the n which satisfied congruences (1), (2), or (3) were almost always pseudoprimes to few or many bases depending on whether $(D/n) = -1$ or $(D/n) = +1$. The n satisfying (4) with either $(D/n) = \pm 1$, however, often seem to be psp to more bases than are the n which satisfy (1), (2), or (3) with $(D/n) = -1$.

TABLE 6

Odd, composite, $n < 10^8$ satisfying congruence (2), (3), or (4); D, P, Q from method A or B*. $(D/n) = -1$*

	Method A*			Method B*			
	n	D	P	Q	n	D	P	Q
Congruence (2)								
	913	5	5	5	913	5	5	5
					64469	13	5	3
Congruence (3)								
	61807	5	5	5	61807	5	5	5
	186961	-7	1	2	1 940611	17	5	2
	1 012051	-7	1	2	8 226373	5	5	5
	1 821419	-7	1	2				
	3 043921	-7	1	2				
	5 665981	-7	1	2				
	6 317009	-7	1	2				
	6 684221	-7	1	2				
	8 226373	5	5	5				
	28 083221	-7	1	2				
	50 273929	-7	1	2				
	57 644501	-7	1	2				
	66 784709	-7	1	2				
Congruence (4)								
	27	5	5	5	27	5	5	5
	203	5	5	5	203	5	5	5
	7083	5	5	5	7083	5	5	5
	530881	-11	1	3	137149	17	5	2
	2 861101	-7	1	2	1 024651	17	5	2
	3 342827	5	5	5	2 704801	13	5	3
	3 581761	-11	1	3	3 342827	5	5	5
	6 906901	17	1	-4	4 504501	17	5	2
	8 163167	5	5	5	8 163167	5	5	5
	12 490201	-7	1	2	10 024561	29	7	5
	14 834403	5	5	5	13 199089	13	5	3
	17 064007	5	5	5	14 676481	17	5	2
	20 964961	-7	1	2	14 834403	5	5	5
	34 745047	5	5	5	16 666651	29	7	5

TABLE 6 (*continued*)

40 160737	5	5	5	17 064007	5	5	5
55 462177	5	5	5	26 582219	33	7	4
70 561921	-7	1	2	29 993761	13	5	3
				30 958201	17	5	2
				30 996001	17	5	2
				31 405501	17	5	2
				34 196401	13	5	3
				34 745047	5	5	5
				40 160737	5	5	5
				43 620409	17	5	2
				47 706949	21	7	7
				55 462177	5	5	5
				75 447101	13	5	3
				90 698401	21	7	7
				99 085829	13	5	3

Note: Of those n satisfying (3) with P and Q chosen by Method A*, only those with (39, n) = 1 were counted.

We also tested the psp(2)'s under $25 \cdot 10^9$ in congruences (1) through (4), with D, P, and Q chosen by methods A, B, A*, and B*, with $(D/n) = -1$. No psp(2) satisfied (1) or (2). There was one solution ($n = 1210\ 383801$, $D = 13$, $P = 1$, and $Q = -3$ chosen with A and A*) to congruence (3). There were many solutions to congruence (4).

We now consider the n for which two (and hence all) of congruences (1)–(4) are true simultaneously, assuming $(n, 2PQD) = 1$.

Rotkiewicz [18] proved several theorems to the effect that if $Q = \pm 1$ and if $(P, Q) \neq (1, 1)$, then there are infinitely many composite n for which (1), (3), and (4) are true simultaneously, but he says little about what happens if $Q \neq \pm 1$. He does state the following result: $U_{n-(D/n)} \equiv 0 \pmod{n}$ and $U_n \equiv (D/n) \pmod{n}$ are true simultaneously if and only if $\alpha^n \equiv \alpha$, $\beta^n \equiv \beta \pmod{n}$ when $(D/n) = +1$, or $\alpha^n \equiv \beta$, $\beta^n \equiv \alpha \pmod{n}$ when $(D/n) = -1$. These latter congruences imply that, with $(D/n) = \pm 1$, we have $Q^n \equiv Q \pmod{n}$ (since $\alpha\beta = Q$). But if n and Q are given and if $Q \neq \pm 1$, then $Q^n \equiv Q \pmod{n}$ holds very rarely. Are there infinitely many composite n satisfying all of (1)–(4) for a given $Q \neq \pm 1$? The first such n with $(D/n) = -1$ is $n = 51$, with $P = \pm 17$, $Q = 35$, and $P = \pm 24$, $Q = 16$.

Tables 4 and 5 also show the counts of the lpsp $< 10^8$ with P and Q chosen by methods A and B which also satisfy (2), (3), and (4); for all of these n, the Q's deter-

mined by algorithm A or B were either ± 1. The first few for method A are: $n = 5777$, $n = 10877$, $n = 75077$, and $n = 100127$ (for these, $P = 1$, $Q = -1$). The first few for method B are: $n = 323$, $n = 377$, $n = 3827$, and $n = 5777$ (for these, $P = 3$, $Q = 1$).

When we tested the $n < 10^8$ with methods A* and B*, we found that no n satisfied more than one congruence (1)–(4). Also, we found no n where both $U_{n+1} \equiv 0$ and $Q^{n-1} \equiv 1 \pmod{n}$. These results, along with the rarity of n satisfying (2) with $Q \neq \pm 1$, justify the remarks in Section 5 that, in a probable prime test, one should check the conditions $V_{n+1} \equiv 2Q$ and $Q^{(n+1)/2} \equiv Q \cdot (Q/n) \pmod{n}$.

To summarize, a good primality test might include these congruence tests:

(1) Test whether n is an sprp(2);

then, with D, P, and Q chosen by method A* or B*:

(2) test whether n is an slprp(P, Q);

(3) verify congruence (2);

(4) verify that the (known) value of $Q^{(n+1)/2}$ is congruent to $Q \cdot (Q/n) \pmod{n}$;

(5) verify congruence (*).

7. The Cost of Choosing D with $(D/n) < 1$. In Section 5 we described two ways of choosing the parameters for a Lucas sequence. Both methods began by finding the first D in a certain sequence, for which $(D/n) < 1$. We compute here the average number of D's which must be tried until a suitable one is found. The maximum number of D's tested in the worst case is also discussed. We will assume in this section that n is known not to be a square, even though this differs from what we did in Section 5.

We begin with the related problem of the size of the least positive integer D such that $(D/n) < 1$. For odd nonsquare n, let $f(n)$ denote the least positive D for which $(D/n) < 1$. Let $f(n) = 0$ when n is an odd square. Then $f(n)$ is prime whenever it is positive.

An upper bound for $f(n)$ follows easily from a general character sum estimate; see Theorem 1 of Burgess [3]. His theorem yields $f(n) < n^{1/4+\epsilon}$ for all large squarefree n. Suppose $n = d^2m$, where m is squarefree and larger than 1. Clearly $f(n) \leqslant f(m)$. If m is large enough for the theorem of Burgess to apply, then $f(n) < m^{1/4+\epsilon} \leqslant n^{1/4+\epsilon}$. Otherwise, m is bounded, and we may assume $n > m^4$. Then $f(n) \leqslant f(m) \leqslant m < n^{1/4+\epsilon}$. Thus, we have the following result.

THEOREM 8. *For all sufficiently large n, $f(n) < n^{1/4+\epsilon}$.*

The same proof produces the same upper bound for the size of the first suitable D in the two methods for choosing parameters. Assuming the Extended Riemann Hypothesis one can show $f(n) = O(\log^2 n)$. See [14] and the references there.

Let q_j denote the jth prime and let $\pi(x)$ be the number of primes $\leqslant x$. Erdös [8] has computed the average order of $f(p)$, where p is restricted to the set of all odd primes. He proved that

$$\lim_{x\to\infty} \frac{1}{\pi(x)} \sum_{\substack{p\leqslant x \\ p \text{ prime}}} f(p) = \sum_{j=1}^{\infty} q_j 2^{-j}.$$

The value of the limit is approximately 3.674643966.

THEOREM 9.

$$\lim_{x\to\infty} \frac{1}{x/2} \sum_{\substack{n\leqslant x \\ n \text{ odd}}} f(n) = 1 + \sum_{j=2}^{\infty} \frac{q_j + 1}{2^{j-1}} \prod_{i=1}^{j-1} \left(1 - \frac{1}{q_i}\right).$$

The right-hand side is approximately 3.147755149. The proof of Theorem 9 parallels that of a theorem of Elliott [4], which generalizes the result of Erdös just stated. We need two lemmas which are similar to Elliott's Lemmas 2 and 5. (Lemma 2 of [4] is identical to Lemma 10 of [5].)

LEMMA 3. *Let $x \geqslant 3$ and $H \geqslant 2$. Let $a_1, a_2, \ldots$ be a sequence of complex numbers. Then*

$$\sum_{\substack{n\leqslant x \\ n \text{ odd}}} \left| \sum_{m\leqslant H} a_n \left(\frac{m}{n}\right) \right|^2 \ll x \sum\sum_{\substack{m,n\leqslant H \\ m,n=t^2,2t^2}} |a_m a_n| + H \log H \left(\sum_{n\leqslant H} |a_n| \right)^2.$$

Proof. The proof of Lemma 10 of Elliott [5] applies verbatim with the proviso that p therein represents an odd number, not necessarily prime.

LEMMA 4. *For any $x \geqslant 3$ and $N \geqslant 2$, the number of odd $n \leqslant x$ for which $f(n) > N$ is*

$$\ll xN^{-2}(\log N)^{15} + N^2 \log N.$$

Proof. The proof of Lemma 5 of Elliott [4] applies with minor changes in notation and the omission of the first and last paragraphs. Use our Lemma 3 in place of his Lemma 2.

Proof of Theorem 9. Let $\nu_x(n\colon \ldots)$ denote the frequency of odd $n \leqslant x$ such that . . . .

It follows from the Chinese Remainder Theorem and quadratic reciprocity that if p, q are distinct primes and x is a multiple of $4pq$, then

$$\nu_x(n\colon (p/n) = (q/n) = +1) = \nu_x(n\colon (p/n) = +1) \cdot \nu_x(n\colon (q/n) = +1).$$

More generally, whenever x is a multiple of $4N!$, we have

$$\nu_x(n\colon f(n) > N) = \nu_x(n\colon (p/n) = +1 \text{ for each prime } p \leqslant N)$$

$$= \prod_{\substack{p\leqslant N \\ p \text{ prime}}} \nu_x(n\colon (p/n) = +1).$$

Thus, for all sufficiently large x, and $M \leqslant N$, we have

$$\nu_x(n: f(n) > M) = \prod_{\substack{p \leqslant M \\ p \text{ prime}}} \nu_x(n: (p/n) = +1) + O(4N!/x)$$

$$= \left(\frac{1}{2} + O(1/x)\right) \prod_{\substack{p \leqslant M \\ p \text{ odd prime}}} \left(\left(\frac{p-1}{2p}\right) + O(1/x)\right) + O(4N!/x).$$

Now let $N = [(\log\log x)^{1/2}]$ and suppose x is so large that $q_j \leqslant N$. Note that for large x, we have

$$4N! \leqslant 4\exp(N\log N) < \exp((\log\log x)^{3/4}) < \log x.$$

Then

$$\nu_x(n: f(n) > q_j) = 2\prod_{i=1}^{j}\left(\frac{q_i - 1}{2q_i}\right) + O(j/x) + O(\log x/x).$$

Let $d_1 = 1/2$, and

$$d_j = 2\prod_{i=1}^{j-1}\left(\frac{q_i - 1}{2q_i}\right) - 2\prod_{i=1}^{j}\left(\frac{q_i - 1}{2q_i}\right) = \frac{q_j + 1}{2^{j-1}q_j}\prod_{i=1}^{j-1}\left(1 - \frac{1}{q_i}\right),$$

for $j \geqslant 2$. Then

$$\begin{aligned}\nu_x(n: f(n) = q_j) &= \nu_x(n: f(n) > q_{j-1}) - \nu_x(n: f(n) > q_j) \\ &= d_j + O(\log x/x).\end{aligned} \tag{12}$$

By Mertens' theorem, with γ denoting Euler's constant,

$$\prod_{i=1}^{j-1}\left(1 - \frac{1}{q_i}\right) = (1 + O(1/q_j))/(e^{\gamma}\log q_j).$$

Hence $d_j = O(2^{-j}/\log j)$, so that, with N as before,

$$\sum_{q_j > N} q_j d_j << \sum_{j > \pi(N)} j2^{-j} << \pi(N)2^{-\pi(N)} << (\log\log x)^{-1/2}. \tag{13}$$

Next we use Lemma 4 with $2^k N$ in place of N, and get

$$\frac{1}{x/2} \sum_{\substack{n \leqslant x \\ n \text{ odd} \\ 2^k N < f(n) \leqslant 2^{k+1}N}} f(n) << \frac{1}{x/2}(2^{k+1}N)(x(2^kN)^{-2}(\log(2^kN))^{15} + (2^kN)^2\log(2^kN))$$

$$<< 2^{-k/2}N^{-1/2} + (2^kN)^3\log(2^kN)/x.$$

Now sum this inequality over the $O(\log x)$ possible values of k for which $2^kN \leqslant x^{0.26}$. With $\epsilon = 0.01$ in Theorem 8, we find that

$$\begin{aligned}\frac{1}{x/2} \sum_{\substack{n \leqslant x \\ n \text{ odd} \\ f(n) > N}} f(n) &<< N^{-1/2}\sum_{k=0}^{\infty} 2^{-k/2} + (x^{0.26})^3\log(x^{0.26})/x \\ &<< N^{-1/2} << (\log\log x)^{-1/4}.\end{aligned} \tag{14}$$

From (12) and (13), we have

$$\frac{1}{x/2}\sum_{\substack{n<x\\ n\text{ odd}\\ f(n)\leqslant N}} f(n) = \sum_{q_j\leqslant N} q_j \nu_x(n\colon f(n)=q_j) = \sum_{q_j\leqslant N} q_j(d_j + O(\log x/x))$$

$$= \sum_{j=1}^{\infty} q_j d_j + O(N^2 \log x/x) + O((\log\log x)^{-1/2})$$

$$= \sum_{j=1}^{\infty} q_j d_j + O((\log\log x)^{-1/2}).$$

This estimate and the complementary one given in (14) show that

$$\frac{1}{x/2}\sum_{\substack{n\leqslant x\\ n\text{ odd}}} f(n) = \sum_{j=1}^{\infty} q_j d_j + O((\log\log x)^{-1/4}),$$

which proves Theorem 9.

Now consider method A. Let $g(n)$ denote the first element D of the sequence $5, -7, 9, -11, 13, \ldots$ for which $(D/n) < 1$. Let $g(n) = 0$ when n is a square. We claim that the positive part of the range of $|g(\cdot)|$ is

$$5, 7, 9, 11, 13, 15, 17, 19, 23, 29, 31, 37, \ldots, \tag{15}$$

in which 9 and 15 are the only composite numbers. Suppose $|g(n)| = D$. Then $((-1)^{(D-1)/2}D/n) < 1$, while $((-1)^{(E-1)/2}E/n) = 1$ for every odd E in the interval $3 < E < D$. Suppose $p > 3$ is a prime dividing D. Write $E = D/p$. Then

$$((-1)^{(D-1)/2}D/n) = ((-1)^{(p-1)/2}p/n)((-1)^{(E-1)/2}E/n).$$

If $E > 3$, then both Jacobi symbols on the right side are $+1$, and hence so is the one on the left side, which is a contradiction. Thus, either D is a prime > 3 or $D = 3p$, where p is an odd prime. Clearly, every odd prime >3 appears in (15). Also $D = 9$ can occur, for example, with $n \equiv 1 \pmod{35}$, $n \equiv 0 \pmod 3$. Moreover, $|g(n)| = 15$ for $n \equiv 1 \pmod{5\cdot 7\cdot 11\cdot 13}$, $n \equiv 2 \pmod 3$, for instance. However, no further multiples of 3 appear in (15) because $(5/n) = (-15/n) = 1$ implies $(-3/n) = 1$, so that if $((-1)^{(p-1)/2}p/n) = 1$, then $((-1)^{(3p-1)/2}3p/n) = 1$. This proves the claim.

Write the sequence (15) as $r_1, r_2, \ldots$. We will compute the limiting frequencies

$$e_j = \lim_{x\to\infty} \nu_x(n\colon |g(n)| > r_j).$$

Then, with $e_0 = 1$ and $d_j = e_{j-1} - e_j$, for $j \geqslant 1$, we can prove

$$\lim_{x\to\infty} \frac{1}{x/2}\sum_{\substack{n\leqslant x\\ n\text{ odd}}} |g(n)| = \sum_{j=1}^{\infty} r_j d_j, \tag{16}$$

by the methods used to prove Theorem 9. Similarly, we can compute

$$\lim_{x\to\infty} \frac{1}{x/2}\sum_{\substack{n\leqslant x\\ n\text{ odd}}} \frac{|g(n)|-3}{2} = \sum_{j=1}^{\infty} \frac{r_j - 3}{2} d_j, \tag{17}$$

which is the average number of D's which must be tried until a suitable one for method A is found. We can also evaluate

$$\sum_{j=1}^{\infty} jd_j, \tag{18}$$

which is the average number of D's which must be tried if we have a table of the r_j's and try only these numbers for D.

Clearly, $e_j = \Pi_{i=1}^{j} z_i$, where z_i is the conditional limiting frequency of odd n such that $(r_i/n) = 1$, given that $(r_k/n) = 1$ for all $k < i$. Whenever r_i is prime, we have $z_i = (r_i - 1)/(2r_i)$. For $r_3 = 9$, we find $z_3 = 2/3$, which is the probability that $3 \nmid n$. Finally, the probability that $(-15/n) = 1$, given that $(5/n) = (9/n) = 1$, is $z_6 = 1/2$, which is the probability that $(-3/n) = +1$, given that $3 \nmid n$. Using these values of z_i, we find that the values of the sums in (16), (17), and (18) are approximately 6.580958182, 1.790479091, and 1.784417556, respectively.

Only a few changes need be made in the foregoing argument to obtain the corresponding results for method B. Let $h(n) = 0$ if n is a square. Otherwise, let $h(n)$ be the least element D of the sequence 5, 9, 13, 17, . . . , for which $(D/n) < 1$. We sketch a proof of the fact that the positive part of the range of h consists of all primes $p \equiv 1 \pmod 4$ together with the numbers $3q$ for each prime $q \equiv 3 \pmod 4$ (including $q = 3$). If $D > 0$ is in the range of h and D is divisible by a prime $p \equiv 1 \pmod 4$, then $D = p$. Other positive D in the range of h must have the form $D = pq$, where $p \equiv q \equiv 3 \pmod 4$ are primes. If both p and q exceed 3, then $3 \nmid n$ and $(D/n) = (3p/n)(3q/n) = 1 \cdot 1 = 1$ because $3p < D$ and $3q < D$. Hence, at least one of the p, q is 3.

Let $r_1, r_2, \ldots$ be the range of h. We compute the limiting frequencies z_i as for method A. We find $z_i = (r_i - 1)/(2r_i)$ whenever r_i is prime. For $r_2 = 9$, we have $z_2 = 2/3$. Finally, when $r_i = 3p$, where p is a prime >3, we find that $z_i = (p - 1)/(2p)$, which is the probability that $(3p/n) = 1$, given that $3 \nmid n$. These values of z_i produce approximate values of 8.690967494 and 1.895078260 for the sums (16) and (18), respectively. The average number of D's which must be tried until a suitable one for method B is found is

$$\lim_{x\to\infty} \frac{1}{x/2} \sum_{\substack{n\leqslant x \\ n \text{ odd}}} \frac{h(n) - 1}{4} = \sum_{j=1}^{\infty} \frac{r_j - 1}{4} d_j,$$

which is approximately 1.922741874. Note that having a table of r_j's accelerates the search for D very little in either method.

Computer-Based Education Research Laboratory
University of Illinois at Urbana-Champaign
Urbana, Illinois 61801

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

and

Department of Mathematical Sciences
Northern Illinois University
DeKalb, Illinois 60115

1. 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.

2. N. G. DE BRUIJN, "On the number of positive integers $\leqslant x$ and free of prime factors $> y$," *Indag. Math.*, v. 13, 1951, pp. 50–60. MR **13**, 724.

3. D. A. BURGESS, "On character sums and L-series," *Proc. London Math. Soc.* (3), v. 12, 1962, pp. 193–206. MR **24** #A2570.

4. P. D. T. A. ELLIOTT, "A conjecture of Erdös concerning character sums," *Indag. Math.*, v. 31, 1969, pp. 164–171. MR **39** #4107.

5. P. D. T. A. ELLIOTT, "On the mean value of $f(p)$," *Proc. London Math. Soc.* (3), v. 21, 1970, pp. 28–96. MR **42** #1783.

6. P. ERDÖS & M. KAC, "The Gaussian law of errors in the theory of additive number theoretic functions," *Amer. J. Math.*, v. 62, 1940, pp. 738–742. MR **2**, 42.

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

8. P. ERDÖS, "Számelméleti megjegyzések I," *Mat. Lapok*, v. 12, 1961, pp. 10–17. MR **26** #2410.

9. G. H. HARDY & E. M. WRIGHT, *An Introduction to the Theory of Numbers*, 4th ed., Oxford Univ. Press, London, 1959.

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

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

12. E. LUCAS, "Théorie des fonctions numériques simplement périodiques," *Amer. J. Math.*, v. 1, 1878, pp. 184–240, 289–321.

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

14. G. L. MILLER, "Riemann's Hypothesis and tests for primality," *Proc. of the Seventh Annual ACM Symposium on the Theory of Computing*, May 4–7, 1975, Albuquerque, N.M., pp. 234–239. MR **58** #470b.

15. I. NIVEN & H. S. ZUCKERMAN, *An Introduction to the Theory of Numbers*, 3rd ed., Wiley, New York, 1972.

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

17. C. POMERANCE, J. L. SELFRIDGE & S. S. WAGSTAFF, JR., "The pseudoprimes to $25 \cdot 10^9$," *Math. Comp.*, v. 35, 1980, pp. 1003–1026.

18. 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.

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

20. H. C. WILLIAMS & J. S. JUDD, "Determination of the primality of N by using factors of $N^2 \pm 1$," *Math. Comp.*, v. 30, 1976, pp. 157–172. MR **53** #257.

21. H. C. WILLIAMS & J. S. JUDD, "Some algorithms for prime testing using generalized Lehmer functions," *Math. Comp.*, v. 30, 1976, pp. 867–886. MR **54** #2574.

22. H. C. WILLIAMS, "On numbers analogous to the Carmichael numbers," *Canad. Math. Bull.*, v. 20, 1977, pp. 133–143. MR **56** #5414.

23. H. C. WILLIAMS & R. HOLTE, "Some observations on primality testing," *Math. Comp.*, v. 32, 1978, pp. 905–917. MR **57** #16184.

24. 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.

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

26. 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.

27. A. ROTKIEWICZ, "On Lucas numbers with two intrinsic prime divisors," *Bull. Acad. Polon. Sci. Sér. Sci. Math. Astronom. Phys.*, v. 10, 1962, pp. 229–232. MR **25** #3024.