MATHEMATICS OF COMPUTATION VOLUME 30, NUMBER 133
JANUARY 1976, PAGES 157–172

Determination of the Primality of N by Using Factors of $N^2 \pm 1$

By H. C. Williams and J. S. Judd

Abstract. Algorithms are developed which can be used to determine the primality of a large integer N when a sufficient number of prime factors of $N^2 + 1$ are known. A test for the primality of N which makes use of known factors of $N - 1$, $N + 1$ and $N^2 + 1$ and the factor bounds on these numbers is also presented. In order to develop the necessary theory, the properties of some functions which are a generalization of Lehmer functions are used. Several examples of numbers proved prime by employing these tests are given.

1. Introduction. Some of the most effective methods for determining the primality of a large integer N depend upon the knowledge of factors of $N - 1$ or $N + 1$. For an excellent discussion of many of these techniques see Brillhart, Lehmer and Selfridge [1] and Selfridge and Wunderlich [6]. It may, however, occur that we are more easily able to determine more factors of $N^2 + 1$, than of $N^2 - 1$. For example, if $N = (2^{198} + 1)41 - 2^{99}$, then

$$N - 1 = 2^3 \cdot 53 \cdot 2837 \cdot R_1,$$

$$N + 1 = 2 \cdot 3 \cdot R_2,$$

$$N^2 + 1 = 2 \cdot 5^2 \cdot 13 \cdot 37 \cdot 109 \cdot 397 \cdot 2113 \cdot 42373 \cdot 235621 \cdot 312709 \cdot R_4,$$

where R_1, R_2, R_4 are each composite and any prime factor of $R_1R_2R_4$ exceeds 10^6. This number is a special case of

$$N = x^2b - x + b \qquad (x = 2^{99}, b = 41).$$

For these numbers,

$$N^2 + 1 = (x^2 + 1)(b^2x^2 - 2bx + b^2 + 1);$$

hence, if $x^2 + 1$ can be easily factored, we can find factors of $N^2 + 1$. We also remark here that if f_n is the Fibonacci number $(\alpha^n - \beta^n)/(\alpha - \beta)$ and l_n is the Lucas number $\alpha^n + \beta^n$, where $\alpha + \beta = -\alpha\beta = 1$, then

$$f_{2n+1}^2 + 1 = f_{2n-1}f_{2n+3}, \qquad l_{2n}^2 + 1 = 5f_{2n-1}f_{2n+1};$$

thus, many of the Fibonacci and Lucas numbers are examples of numbers N such that $N^2 + 1$ may be fairly easily factored.

The purpose of this paper is to develop algorithms which can be used to determine

Received May 5, 1975.
AMS (MOS) subject classifications (1970). Primary 10A25; Secondary 10A35.
Key words and phrases. Primality testing, Lucas functions, Lehmer functions.
Copyright © 1976, American Mathematical Society

the primality of N when a sufficient number of prime factors of $N^2 + 1$ are known. We will also develop a combined test for primality which is an extension of that given in Section 7 of [1]. This test makes use of the knowledge of factors of $N - 1$, $N + 1$, $N^2 + 1$ and the factor bounds of these numbers in order to determine the primality of N. In order to do this, we review some properties of functions introduced by Williams [7] and then show how these functions may be utilized in the development of the desired primality criteria. Finally, we give some examples of numbers which were proved prime by using these algorithms.

2. The Functions V_m and U_m. Let ρ_1, ρ_2 be the two zeros of $x^2 - P_1 x + P_2$; and let α_i, β_i $(i = 1, 2)$ be the zeros of

$$x^2 - \rho_i x + Q \qquad (i = 1, 2),$$

where P_1, P_2, Q are integers such that $(P_1, P_2, Q) = 1$. Put $\delta = \rho_2 - \rho_1$ and define $\Delta = \delta^2 = P_1^2 - 4P_2$, $E = (P_2 + 4Q)^2 - 4QP_1^2$,

$$V_n = \frac{1}{\delta}\begin{vmatrix} \alpha_1^n + \beta_1^n & \rho_1 \\ \alpha_2^n + \beta_2^n & \rho_2 \end{vmatrix}, \qquad U_n = \frac{1}{\delta}\begin{vmatrix} 1 & \alpha_1^n + \beta_1^n \\ 1 & \alpha_2^n + \beta_2^n \end{vmatrix}.$$

The first few values for these functions are given in the table below.

n	V_n	U_n
0	2	0
1	0	1
2	$-P_2 - 2Q$	P_1
3	$-P_1P_2$	$P_1^2 - P_2 - 3Q$
4	$P_2^2 - P_1^2P_2 + 4P_2Q + 2Q^2$	$P_1^3 - 2P_1P_2 - 4P_1Q$

TABLE 1

Since

$$V_{n+4} = P_1V_{n+3} - (P_2 + 2Q)V_{n+2} + QP_1V_{n+1} - Q^2V_n,$$

$$U_{n+4} = P_1U_{n+3} - (P_2 + 2Q)U_{n+2} + QP_1U_{n+1} - Q^2U_n,$$

we see that V_n, U_n are integers for any integer $n \geqslant 0$. It should also be noted that

$$V_{n+m} = V_nV_m - P_2U_nU_m - Q^mV_{n-m}, \qquad U_{n+m} = U_nV_m + V_nU_m + P_1U_nU_m - Q^mU_{n-m},$$

for any integers n, m.

If N is any integer and $(N, QP_2) = 1$, find M, S such that

$$QM \equiv -P_2S \equiv 1 \pmod{N}$$

and put

$$X_k \equiv \begin{cases} S^2M^{k/2}V_k & (k \text{ even}) \\ SM^{(k+1)/2}V_k & (k \text{ odd}) \end{cases} \pmod{N},$$

$$W_k \equiv \begin{cases} S^2 M^{k/2} U_k & (k \text{ even}) \\ S M^{(k+1)/2} U_k & (k \text{ odd}) \end{cases} \pmod{N}.$$

From the formulas given above, we see that

$$W_{2m+1} \equiv X_{2(m+1)} + X_{2m},$$

$$X_{2m+1} \equiv -P_2(W_{2m+2} + W_{2m}) - P_1 W_{2m+1} \pmod{N},$$

and

$$X_{2m} \equiv \begin{cases} Q(X_m^2 - P_2 W_m^2) - 2S^2 & (m \text{ odd}) \\ P_2^2(X_m^2 - P_2 W_m^2) - 2S^2 & (m \text{ even}) \end{cases} \pmod{N},$$

$$W_{2m} \equiv \begin{cases} Q(2X_m W_m + P_1 W_m^2) & (m \text{ odd} \\ P_2^2(2X_m W_m + P_1 W_m^2) & (m \text{ even}) \end{cases} \pmod{N}.$$

Using these formulas, we can evaluate $W_k \pmod{N}$ for any $k > 0$ in $O(\log k)$ operations (Lehmer [3]). Since $(U_k, N) = (W_k, N)$, we see that this technique for evaluating $W_k \pmod{N}$ may be used in the evaluation of (U_k, N).

3. Properties of U_m. Several divisibility properties of the functions U_n may be deduced from the more general results of [7]. We list here some of the properties that will be needed in later sections of the paper.

We first note that if n and m are positive integers, then $U_n \mid U_{mn}$.

We now require a few definitions. Let the function U_n be given by parameters P_1, P_2, Q. For each prime p such that $(p, 2\Delta EQ) = 1$, we associate with U_n the functions

$$\delta(p) = (\Delta \mid p), \quad \epsilon(p) = (E \mid p), \quad \eta(p) = (e(p) \mid p),$$

where the symbol $(x \mid p)$ is the Legendre symbol,

$$e(p) = P_1^2 + \Delta - 16Q + 2P_1 d \quad \text{and} \quad d^2 \equiv \Delta \pmod{p}.$$

We see that the function $\eta(p)$ is defined only when $\delta(p) = +1$. We also define the function $\Psi(p)$ by putting

$$\Psi(p) = \begin{cases} (p^2 - \epsilon)/2 & \text{when } \delta = -1, \\ (p^2 - 1)/2 & \text{when } \delta = +1, \epsilon = -1, \\ p - \eta & \text{when } \delta = \epsilon = 1, \end{cases}$$

where $\delta = \delta(p), \epsilon = \epsilon(p), \eta = \eta(p)$.

Let m be any integer such that $(m, Q) = 1$ and let U_{τ_0} be the first term of the sequence

$$(*) \qquad U_1, U_2, U_3, \ldots, U_n, \ldots$$

in which m occurs as a factor. We define the increasing sequence of integers $\tau_0, \tau_1, \tau_2, \ldots, \tau_j, \ldots$ by saying U_{τ_j} is the first term of the sequence $(*)$ such that $m \mid U_{\tau_j}$

and $\tau_i \nmid \tau_j$ $(i = 0, 1, 2, \ldots, j-1)$. We call these τ's the *orders of apparition of* m and denote them by $\tau_j(m)$. We are now able to give the following important theorem.

THEOREM. *If p is a prime and $(p, 2\Delta EQ) = 1$, there exists at least one order of apparition of p. Further, if $\tau_j(p)$ is any order of apparition of p, then $\tau_j(p) \mid 2\Psi(p)$.*

Proof. This follows as a result of Theorems 6.6, 7.1, and 7.2 of [7].

With this result we easily deduce

THEOREM 1. *Let $(N, 2\Delta QE) = 1$ and $N \mid U_m$. If q is any odd prime divisor of m and $N \nmid U_{m/q}$, then any prime divisor p of N which does not divide $U_{m/q}$ must satisfy the congruence*

$$\Psi(p) \equiv 0 \pmod{q^\alpha},$$

where $q^\alpha \| m$.

Proof. Let τ be an order of apparition of p such that $\tau \mid m$. Clearly, since $p \mid U_m$, such a τ must exist. Now $p \nmid U_{m/q}$; hence, $\tau \nmid m/q$ and, consequently, $q^\alpha \mid \tau$. Since q is odd and $\tau \mid 2\Psi(p)$, the theorem follows.

4. Some Criteria for Primality. In this section we develop some results which will allow us to test an integer N for primality when we know a sufficient number of divisors of $N^2 + 1$. We let the completely factored part of $N^2 + 1$ be denoted by F_4 and the unfactored part by R_4;* then $N^2 + 1 = F_4 R_4$ and $(F_4, R_4) = 1$.

We select integers D, C such that $(D \mid N) = (C^2 - 16D \mid N) = -1$, where the symbol $(X \mid N)$ is the Jacobi symbol. If H and K are integers and

$$\begin{aligned} P_1 &= 4(2H^2 + HKC + 2K^2D), \\ 4P_2 &= P_1^2 - 16D, \\ 16Q &= P_1^2 - 16(H^2C + K^2CD + 8HKD) + 16D, \end{aligned}$$

we have

$$\Delta = 16D,$$

$$P_1^2 + \Delta - 16Q + 2P_1\sqrt{\Delta} = 16(H + K\sqrt{D})^2(C + 4\sqrt{D}),$$

$$\begin{aligned} E &= (P_1^2 + \Delta - 16Q + 2P_1\sqrt{\Delta})(P_1^2 + \Delta - 16Q - 2P_1\sqrt{\Delta})/16 \\ &= 16(H^2 - K^2D)^2(C^2 - 16D). \end{aligned}$$

If p is any prime such that $(p, 2(H^2 - K^2D)(C^2 - 16D)D) = 1$ and $(D \mid p) = +1$, then $e(p) = 16(H + K\bar{d})^2(C + 4\bar{d})$, where $\bar{d}^2 \equiv D \pmod{p}$. Hence, for U_n given by P_1, P_2, Q above, we see for any prime p such that $(p, 2(H^2 - K^2D)(C^2 - 16D)D) = 1$,

$$\delta(p) = (D \mid p), \quad \epsilon(p) = (C^2 - 16D \mid p), \quad \eta(p) = (C + 4\bar{d} \mid p).$$

These are all independent of the values of H, K; and consequently, we see that the value of $\Psi(p)$ is independent of H and K.

For our fixed values of D and C we now define the functions $U_n^{(i)}$ $(i = 1, 2, \ldots)$

*We use the notation F_4 and R_4 because $N^2 + 1$ is the fourth cyclotomic polynomial in N.

by using the parameters $P_1^{(i)}$, $P_2^{(i)}$, $Q^{(i)}$ $(i = 1, 2, \ldots)$, where

$$P_1^{(i)} = 4(2H_i^2 + H_iK_iC + 2K_i^2D),$$
$$P_2^{(i)} = 4(2H_i^2 + H_iK_iC + 2K_i^2D)^2 - 4D,$$
$$Q^{(i)} = (2H_i^2 + H_iK_iC + 2K_iD)^2 - (H_i^2C + 8H_iK_iD + K_i^2CD) + D,$$

and H_i, K_i $(i = 1, 2, \ldots)$ are any two integers such that $(N, H_i^2 - K_i^2D) = 1$.

As it will be necessary to refer to the following statements several times, we put $\overline{F}_4 = F_4/2$ and put

(α) *For each prime $q \mid \overline{F}_4$ there exists some H_i, K_i such that for the function $U_n^{(i)}$*

$$N \mid U_{N^2+1}^{(i)} \quad \text{and} \quad (U_{(N^2+1)/q}^{(i)}, N) = 1.$$

(β) *For some H_i, K_i we have*

$$N \mid U_{N^2+1}^{(i)} \quad \text{and} \quad (U_{(N^2+1)/R_4}^{(i)}, N) = 1.$$

It should be noted here that, if N is not a divisor of $U_{N^2+1}^{(i)}$, then N is composite.

We now describe, by means of the two following theorems, some properties of possible prime divisors of N when either (α) or (β) is true. We first give a theorem which is analogous to a recent theorem of Morrison [4].

THEOREM 2. *If (α) is true and p is any prime divisor of N, then*

$$\Psi(p) \equiv 0 \pmod{\overline{F}_4}.$$

Proof. Since $\Psi(p)$ has a value which depends only on the fixed values of D and C, it follows that, if q is any prime divisor of $\overline{F}_4$ and (α) is true, then $q^\nu \mid \Psi(p)$, where $q^\nu \| \overline{F}_4$; hence, $\overline{F}_4 \mid \Psi(p)$.

THEOREM 3. *If (β) is true and all possible prime divisors of R_4 are greater than B_4, then each prime factor p of N must satisfy a congruence of the form*

$$\Psi(p) \equiv 0 \pmod{q},$$

where q is some prime divisor of R_4 depending on p.

Proof. Let $\tau = \tau(p)$ be an order of apparition of p such that $\tau \mid (N^2 + 1)$; then $\tau \nmid F_4$ and, consequently, $(R_4, \tau) > 1$. Thus, there must exist a prime q such that $q \mid R_4$ and $q \mid \tau$. Since $\tau \mid \Psi(p)$, the theorem follows.

We are now in a position to give the main result of this section.

THEOREM 4. *If (α) and (β) are both true, all prime factors of R_4 are greater than B_4 and $B_4F_4 > N^{2/3} + 1$, then N is a prime.*

Proof. If p_i is some prime divisor of N, then

$$\Psi(p_i) \equiv 0 \pmod{q_i\overline{F}_4},$$

where q_i is a prime divisor of R_4.

Suppose $N = p_1p_2p_3a$ and a is any integer such that $a \geqslant 1$. Since $\Psi(p_i) \mid p_i^2 \pm 1$, $p_i^2 \pm 1$ is even, and $\overline{F}_4$ is odd, we have

$$p_i^2 \geqslant q_iF_4 - 1, \qquad p_i > \sqrt{B_4F_4 - 1},$$

and

$$N > (B_4F_4 - 1)^{3/2}.$$

Thus, if N is composite, it must be the product of two distinct primes p_1 and p_2. (Since $(D|N) = -1$, N cannot be a perfect square.) Since $(D|p_1p_2) = (C^2 - 4D|p_1p_2) = -1$, we have

$$\delta(p_1) = -\delta(p_2), \qquad \epsilon(p_1) = -\epsilon(p_2).$$

Assume p_1 to be that prime such that $\delta(p_1) = +1$; then $\delta(p_2) = -1$,

$$p_2^2 \equiv \epsilon(p_2) \pmod{q_2F_4} \quad \text{and} \quad p_1^2 \equiv 1 \pmod{q_1F_4}.$$

If $F_4 = 2$, we have

$$p_1^2 \equiv 1 \pmod{q_1} \quad \text{and} \quad p_2^2 \equiv \pm 1 \pmod{q_2};$$

hence,

$$p_1 \geqslant 2q_1 - 1 > 2B_4 - 1, \qquad p_2 > \sqrt{2B_4 - 1},$$

and $N > (B_4F_4 - 1)^{3/2}$.

If $F_4 > 2$, we have

$$N^2 = p_1^2p_2^2 \equiv -1 \pmod{F_4} \quad \text{and} \quad p_1^2 \equiv 1 \pmod{F_4};$$

consequently,

$$p_2^2 \equiv \epsilon(p_2) \equiv -1 \pmod{F_4}$$

and $\epsilon(p_2) = -1$. It follows that $\epsilon(p_1) = +1$ and

$$p_1 \equiv \pm 1 \pmod{q_1F_4}.$$

Putting this result together with

$$p_2^2 \equiv -1 \pmod{q_2F_4},$$

we see that $N > (B_4F_4 - 1)^{3/2}$; thus, N cannot be the product of two or more primes and, therefore, must be a prime.

5. A Further Refinement. If (α) and (β) are true and $F_4 > B_4 \geqslant 5$, we can lower the bound given in Theorem 4 on F_4 and still test N for primality. In order to do this it is necessary to show that neither of two cubic equations has three integer roots. This improved result, given as Theorem 5, is similar to the results obtained in [1] by using the properties of the hyperbola $x^2 - y^2 = N$. In order to prove Theorem 5, it should first be noted that if $f = \epsilon_1 + rF_4$ and $g = \epsilon_2 + sF_4$, where $|\epsilon_1| = |\epsilon_2| = 1$ and $r, s > B_4$, then $fg = \epsilon_1\epsilon_2 + tF_4$, where $t > B_4$. Thus, if (α) and (β) are true and N is composite, we see by results obtained in the proof of Theorem 4 that there exist three integers k, l, m such that

$$N^2 = (\epsilon_1 + kF_4)(\epsilon_2 + lF_4)(\epsilon_3 + mF_4),$$

where $|\epsilon_1| = |\epsilon_2| = |\epsilon_3| = 1$, $\epsilon_1\epsilon_2\epsilon_3 = -1$, and $k, l, m > B_4$. We also assume here that $(N, 3) = 1$.

THEOREM 5. *Put*

$$R_4 = \lambda_1 + \mu_1(3F_4) + \nu_1(3F_4)^2 \qquad (|\lambda_1|, |\mu_1| < 3\overline{F}_4).$$

Let

$$F_4 \equiv \gamma \pmod 3 \qquad (|\gamma| = 1),$$

$$(R_4 + \gamma F_4^2)/3 \equiv \lambda_2 \pmod{F_4} \qquad (|\lambda_2| < \overline{F}_4),$$

$$1 + 2\lambda_2\gamma \equiv \theta \pmod 3 \qquad (|\theta| \leqslant 1),$$

$$((R_4 + \gamma F_4^2)/3 - \lambda_2 - \theta F_4 + (\gamma\theta + \gamma)F_4^2)/3F_4 = \mu_2 + \nu_2 F_4,$$

where $|\mu_2| < \overline{F}_4$.

If either of the cubic equations

(1) $$x^3 - \lambda_1 x^2 - 3\mu_1 x - 9\nu_1 = 0 \qquad (\nu_1 \neq 0),$$

(2) $$x^3 - 3\lambda_2 x^2 - 3(3\mu_2 + \theta)x - 3(3\nu_2 - \gamma(\theta + 1)) + \gamma = 0,$$

has three integer roots, then N is composite. If neither of these equations has three integer roots, $N^2 < C$, *where*

$$C = (B_4F_4 - 1)(-1 + (B_4 - 3|\lambda_2|)F_4 + (3\overline{F}_4 - 1)F_4^2),$$

and (α), (β) *are both true, then N is a prime.*

Proof. If (2) has three integer roots x_1, x_2, x_3, we have

$$x_1 + x_2 + x_3 = 3\lambda_2,$$

$$x_1x_2 + x_2x_3 + x_3x_1 = -3(3\mu_2 + \theta),$$

$$x_1x_2x_3 = 3(3\nu_2 - \gamma\theta - \theta) - \gamma \neq 0.$$

Also,

$$(R_4 + \gamma F_4^2)/3 = \lambda_2 + (3\mu_2 + \theta)F_4 + (3\nu_2 - \gamma\theta - \gamma)F_4^2;$$

hence,

$$R_4 = 3\lambda_2 + 3(3\mu_2 + \theta)F_4 + (3(3\nu_2 - \gamma\theta - \gamma) - \gamma)F_4^2$$

and

$$\begin{aligned} N^2 &= -1 + 3\lambda_2F_4 + 3(3\mu_2 + \gamma)F_4^2 + (3(3\nu_2 - \gamma\theta - \gamma) - \gamma)F_4^3 \\ &= (x_1F_4 - 1)(x_2F_4 - 1)(x_3F_4 - 1). \end{aligned}$$

Thus, if (2) has three integer roots, N^2 has at least three factors greater than 1; consequently, N is composite. It can also be shown, by similar reasoning, that N is composite if (1) has three integer roots.

Suppose now that neither (1) nor (2) has three integer roots, that (α), (β) are both true, that $N^2 < C$, and that N is composite. Then

$$N^2 = (\epsilon_1 + kF_4)(\epsilon_2 + lF_4)(\epsilon_3 + mF_4),$$

where $|\epsilon_i| = 1$, $\epsilon_1\epsilon_2\epsilon_3 = -1$, $k, l, m > B$. Putting $r = \epsilon_1\epsilon_2 m + \epsilon_2\epsilon_3 k + \epsilon_1\epsilon_3 l$, $s = \epsilon_1 ml + \epsilon_2 mk + \epsilon_3 lk$, $t = klm$, we have $R_4 = r + sF_4 + tF_4^2$.

Since $F_4 | N^2 + 1$, we may assume without any loss of generality that $\epsilon_1 + kF_4$ is the square of a prime and that $\epsilon_1 = -1$. Hence,

$$\epsilon_2 mF_4 + \epsilon_3 lF_4 + mlF_4^2 \equiv 0 \pmod 3.$$

From this result we easily deduce that

$$\epsilon_2 mF_4 \equiv \epsilon_3 lF_4 \equiv \kappa \pmod 3,$$

where $\kappa = 0, 1$.

Case 1. $\kappa = 0$. In this case, we have

$$s \equiv 0 \pmod 3, \quad t \equiv 0 \pmod 9;$$

thus,

$$R_4 = r + (s/3)(3F_4) + (t/9)(3F_4)^2$$

and

$$\lambda_1 \equiv r \pmod{3F_4}.$$

If $r \neq \lambda_1$, we have $|r| > 3\overline{F}_4$; consequently, one of k, l, m must exceed $\overline{F}_4$ and

$$N^2 > (-1 + B_4F_4)^2(-1 + F_4\overline{F}_4) > C.$$

Thus, $r = \lambda_1$ and $s/3 \equiv \mu_1 \pmod{3F_4}$. If $s/3 \neq \mu_1$, we must have one of kl, lm, or km greater than $3\overline{F}_4$. Hence

$$N^2 > (-1 + B_4F_4)(-1 + F_4(B_4 - |\lambda_1|) + 3\overline{F}_4F_4^2) > C.$$

It follows that $r = \lambda_1$, $s/3 = \mu_1$, $t/9 = \nu_1$, and we see that (1) must have three integer roots.

Case 2. $\kappa = 1$. In this case we have $3|r$, $3|s$ and

$$t = klm \equiv -\gamma \pmod 3.$$

Also,

$$s \equiv 3 + 2\gamma r \pmod 9, \qquad t \equiv 2\gamma + r \pmod 9.$$

Since

$$(R_4 + \gamma F_4^2)/3 \equiv r/3 \pmod{F_4},$$

we have

$$r/3 \equiv \lambda_2 \pmod{F_4}.$$

If $r/3 \neq \lambda_2$, then $|r| > 3\overline{F}_4$, which is not possible; hence,

$$r/3 = \lambda_2,$$

$$s/3 \equiv 1 + 2\gamma\lambda_2 \equiv \theta \pmod 3,$$

$$(t+\gamma)/3 \equiv -\gamma - \gamma\theta \pmod 3.$$

Now

$$((R_4 + \gamma F_4^2)/3 - \lambda_2 - \theta F_4 + (\gamma + \gamma\theta)F_4^2)/3F_4$$
$$= (s/3 - \theta)/3 + F_4((t+\gamma)/3 + \gamma + \gamma\theta)/3;$$

thus,

$$(s/3 - \theta)/3 \equiv \mu_2 \pmod{F_4}.$$

If $\mu_2 \neq (s/3 - \theta)/3$, we have

$$|s/3 - \theta| \geqslant 3\overline{F}_4 \quad \text{or} \quad |s/3| \geqslant 3\overline{F}_4 - 1.$$

One of kl, lm, km must be greater than $3\overline{F}_4 - 1$ and

$$N^2 > (B_4F_4 - 1)(-1 + (B_4 - 3|\lambda_2|)F_4 + (3\overline{F}_4 - 1)F_4^2) = C.$$

Hence,

$$r/3 = \lambda_2, \qquad (s/3 - \theta)/3 = \mu_2, \qquad ((t+\gamma)/3 + \gamma + \gamma\theta)/3 = \nu_2,$$

and (2) has the three integer roots $\epsilon_1\epsilon_2 m$, $\epsilon_2\epsilon_3 k$, $\epsilon_1\epsilon_3 l$. Since this is impossible, N cannot be composite.

6. A Combined Theorem. Let F_1 be the completely factored part of $N-1$, F_2 be the completely factored part of $N+1$, $R_1 = (N-1)/F_1$, $R_2 = (N+1)/F_2$. For convenience of reference, we give the following tests of [1].

(I) For each prime p_i dividing F_1 there exists an a_i such that

$$a_i^{N-1} \equiv 1 \pmod N \quad \text{and} \quad (a_i^{(N-1)/p_i} - 1, N) = 1.$$

(II) For some a,

$$a^{N-1} \equiv 1 \pmod N \quad \text{and} \quad (a^{(N-1)/R_1} - 1, N) = 1.$$

(III) For each prime q_i dividing F_2 there exists a Lucas sequence $\{u_k^{(i)}\}$ with discriminant D' for which $(D'|N) = -1$,

$$N | u_{N+1}^{(i)} \quad \text{and} \quad (u_{(N+1)/q_i}^{(i)}, N) = 1.$$

(IV) For some Lucas sequence $\{u_k\}$ for which $(D'|N) = -1$,

$$N | u_{N+1} \quad \text{and} \quad (u_{(N+1)/R_2}, N) = 1.$$

In [1] the following theorem is proved.

THEOREM. *Assume* (I), (II), (III), (IV), *and suppose all prime factors of* R_1 *and* R_2 *are respectively* $\geqslant B_1$ *and* B_2. *Define* r *and* s *by* $R_1 = \overline{F}_2 s + r$ $(0 \leqslant r < \overline{F}_2)$, *and*

let

$$G = \max(B_1F_1 + 1, B_2F_2 - 1, mF_1\overline{F}_2 + rF_1 + 1) \qquad (m \geqslant 1).$$

Further, in the case that $G = mF_1\overline{F}_2 + rF_1 + 1$, *assume* $(\lambda F_1\overline{F}_2 + rF_1 + 1) \nmid N$, $\delta_0^r \leqslant \lambda < m$, *where* δ_0^r *is the Kronecker delta.*

If $N < G(B_1B_2F_1\overline{F}_2 + 1)$, *then* N *is prime.*

In this section we will obtain an extension of this theorem which takes into account the factors of $N^2 + 1$ and, to a lesser extent, the factor bound of R_4. In order to do this we first give some notation.

Put

$$\overline{F}_1 = F_1/2, \qquad \overline{F}_2 = F_2/2,$$

$$R_2 = r + S\overline{F}_1, \quad \text{where } 0 \leqslant r < \overline{F}_1,$$

$$S \equiv k, \quad 2R_1R_2 \equiv h, \quad hN \equiv g \pmod{\overline{F}_4},$$

where $0 \leqslant k, h, g < \overline{F}_4$.

Let f be any unitary divisor of $\overline{F}_4$, i.e. $(\overline{F}_4/f, f) = 1$. Define

$$L(f) = -1 + rF_2 + bF_1F_2,$$

where

$$b \equiv k - fgy \pmod{\overline{F}_4} \qquad (0 \leqslant b < \overline{F}_4),$$

and (x, y) is a solution of the linear Diophantine equation $x(\overline{F}_4/f) - yf = 1$. Put $\Lambda = \min_{f \mid \overline{F}_4} L(f)$, where the minimum is taken over all unitary divisors of $\overline{F}_4$ including 1 and $\overline{F}_4$.

LEMMA. *If*

$$z \equiv 1 \pmod{F_1}, \qquad z \equiv -1 \pmod{F_2}, \qquad z^2 \equiv -1 \pmod{F_4},$$

then

$$z \equiv L(f) \pmod{F_1\overline{F}_2\overline{F}_4}$$

for some unitary divisor f *of* $\overline{F}_4$.

Proof. Since

$$z^2 \equiv -1 \equiv N^2 \pmod{F_4},$$

we have

$$z \equiv N \pmod{f}, \qquad z \equiv -N \pmod{\overline{F}_4/f},$$

for some factor f of $\overline{F}_4$. Since $(x - N, x + N) \mid 2N$ and $(2N, \overline{F}_4) = 1$, f must be a unitary factor of $\overline{F}_4$. Thus,

$$z \equiv N \pmod{fF_1\overline{F}_2}, \qquad z \equiv -N \pmod{\overline{F}_4/f}.$$

It follows that

$$z \equiv N(1 - (N^2 - 1)yf) \pmod{F_1\overline{F}_2\overline{F}_4},$$

where $x(\overline{F}_4/f) - yf = 1$. The result follows on noting that

$$N^3 - N \equiv gF_1\overline{F}_2 \pmod{F_1\overline{F}_2\overline{F}_4}$$

and

$$N \equiv -1 + rF_2 + kF_1\overline{F}_2 \pmod{F_1\overline{F}_2\overline{F}_4}.$$

We are now able to give our combined theorem as

THEOREM 6. *Assume that* $\overline{F}_4 > 1$, (I), (II), (III), (IV), (α) *and* (β) *are all true with the value of* D' *used in* (III) *and* (IV) *being a square multiple of the value of* D *used in* (α) *and* (β). *If* $L(f)$ *is not a divisor of* N *for each unitary divisor* f *of* $\overline{F}_4$ *and* $1 + hF_1\overline{F}_2 \nmid N$, *then* N *is prime if* $N < T$, *where* $T = \min(M_1M_2, M_3^3, MM_3)$ *and*

$$M = 1 + B_1B_2B_4F_1\overline{F}_2\overline{F}_4,$$

$$M_1 = \max(-1 + B_4F_4, 1 + B_1B_2F_1\overline{F}_2, 1 + hF_1\overline{F}_2 + F_1\overline{F}_2\overline{F}_4),$$

$$M_2 = \max(1 + B_1F_1, -1 + B_2F_2, L(1) + mF_1\overline{F}_2\overline{F}_4),$$

$$M_3 = \max(1 + B_1F_1, -1 + B_2F_2, \Lambda + F_1\overline{F}_2\overline{F}_4),$$

and $L(1) + tF_1\overline{F}_2\overline{F}_4$ *is not a divisor of* N *for* $1 \leqslant t < m$.

Proof. We will say that a prime divisor p of N is of the first kind if $\epsilon(p) = \delta(p) = -1$; otherwise, we call p a prime of the second kind. If p is a prime of the first kind, we must have, by results proved in [1] together with Theorem 2,

$$p \equiv 1 \pmod{F_1}, \quad p \equiv -1 \pmod{F_2}, \quad p^2 \equiv -1 \pmod{F_4}.$$

Hence,

$$p \geqslant \max(\Lambda + F_1\overline{F}_2\overline{F}_4, 1 + B_1F_1, -1 + B_2F_2) = M_3.$$

If p is a prime of the second kind we have

$$p \equiv 1 \pmod{q_1F_1}, \quad p \equiv \pm 1 \pmod{q_2F_2}, \quad p^2 \equiv 1 \pmod{q_4F_4},$$

where $q_i | R_i$ $(i = 1, 2, 4)$; thus,

$$p^2 \equiv 1 \mod(q_1q_2q_4F_1\overline{F}_2\overline{F}_4)$$

and $p \geqslant \sqrt{M}$. Since $N^2 \equiv -1 \pmod{\overline{F}_4}$ and $\overline{F}_4 > 2$, we must have at least one prime divisor of N which is of the first kind.

If N is the product of three primes, one of them must be of the first kind and since $(D|N) = (C^2 - 16D|N) = -1$, the other two must be of the same kind. Hence, $N \geqslant \min(M_3^3, MM_3)$, which is impossible.

If N is the product of four or more primes, one is of the first kind, and at least two others must be of the same kind; and we have already seen that this is not possible.

If $N = p_1p_2$ where p_1, p_2 are distinct primes, we know by the reasoning of Theorem 4, that

$$p_1 \equiv 1 \pmod{q_1F_1}, \quad p_1 \equiv 1 \pmod{q_2F_2}, \quad p_1 \equiv \pm 1 \pmod{q_4F_4},$$

where $q_i | R_i$ $(i = 1, 2, 4)$. It follows that

$$p_1 \equiv 1 \pmod{q_1F_1}, \quad p_2 \equiv -1 \pmod{q_2F_2}, \quad p_2 \equiv \pm N \pmod{q_4F_4}.$$

If $p_1 \equiv 1 \pmod{q_4F_4}$, we have

$$p_1 \equiv 1 \pmod{q_1q_2q_4F_1F_2F_4}, \quad p_2 \equiv L(\overline{F}_4) \pmod{F_1\overline{F}_2\overline{F}_4}$$

and $N = p_1p_1 \geqslant MM_3$. If $p_1 \equiv -1 \pmod{q_4F_4}$, we have

$$p_1 \equiv 1 + hF_1\overline{F}_2 \pmod{F_1\overline{F}_2\overline{F}_4}$$

and

$$p_1 \equiv 1 \pmod{q_1q_2F_1\overline{F}_2};$$

consequently,

$$p_1 \geqslant \max(-1 + B_4F_4, 1 + B_1B_2F_1\overline{F}_2, 1 + hF_1\overline{F}_2 + F_1\overline{F}_2\overline{F}_4) = M_1.$$

Also,

$$p_2 \geqslant \max(1 + B_1F_1, -1 + B_2F_2, L(1) + mF_1\overline{F}_2\overline{F}_4) = M_2;$$

and we have $N \geqslant M_1M_2$. Since N cannot be the product of two or more primes, it must be a prime.

COROLLARY. *If the conditions of Theorem* 6 *are all true except that* $M_1M_2 < N < \min(MM_3, M_3^3)$, *then* N *must be the product of two primes and both of these primes must exceed* $\min(M_1, M_2)$. *If, on the other hand, we have* $N > \min(MM_3, M_3^3)$, *then the smallest prime divisor of* N *must exceed* $\min(M_3, R)$, *where*

$$R = \max(\sqrt{M}, 1 + B_1F_1, -1 + B_2F_2).$$

Remark 1. We note here that it is an easy matter to factor $N^2 + 1$ by trial division at the same time as $N + 1$ and $N - 1$. If d is a trial divisor of $N - 1$ and leaves a remainder of r, then $d | N^2 + 1$ if and only if $d | r(r + 2) + 2$.

Remark 2. It should be emphasized that it is not always necessary, in determining the primality of a particular N, to verify all the assertions (I), (II), (III), (IV), (α) and (β). For example, if $T = M_1M_2$, $M_1 = 1 + hF_1\overline{F}_2 + F_1\overline{F}_2\overline{F}_4$ and $M_2 = L(1) + mF_1\overline{F}_2\overline{F}_4$, it would not be necessary to verify each of (II), (IV) and (β). For, if $B_1 > m$, which is usually the case, then $M > M_2$ and it would be sufficient to verify (I), (II), (III), and (α) only.

Remark 3. In practice T is usually M_1M_2 with $M_1 = 1 + B_1B_2F_1\overline{F}_2$ and $M_2 = L(1) + mF_1\overline{F}_2\overline{F}_4$. Also, very frequently a simple method of factoring like Pollard's method [5] is successful in finding a fairly large factor of $N^2 + 1$.

Remark 4. In finding a value for m in the theorem, it is not necessary to attempt to divide $L(1) + tF_1\overline{F}_2\overline{F}_4$ into N for each value of t such that $1 \leqslant t \leqslant m$. Since this number must represent a prime factor of N, it suffices to divide N by it only when it has no prime factor. For many values of t, $L(1) + tF_1\overline{F}_2\overline{F}_4$ has a small prime factor; when this occurs no trial division by $L(1) + tF_1\overline{F}_2\overline{F}_4$ is required.

Remark 5. Frequently, at least one of the cofactors R_1, R_2, R_4 is a pseudoprime.

Suppose R_i is a pseudoprime. Then, if we do not have enough factors of $N^2 \pm 1$ to demonstrate the primality of N, we can attempt to demonstrate the primality of R_i. If we succeed in this, it becomes a fairly easy matter to verify the primality of N. If, on using our theorem, we fail to prove R_i a prime, the corollary allows us to find a bound on the largest prime divisor of R_i. This usually increases the size of B_i and very often with this increased value for B_i we are able to demonstrate the primality of N. (The authors are indebted to John Selfridge for this suggestion.)

7. **Some Examples.** These tests were implemented on a computer and used to determine the primality of some numbers of special forms. In the following three lists we present some of the primes which were discovered using the tests of Theorems 4 and 5.

For

$$L = (10^{2n} + 1)a + 10^n, \qquad M = (2^{2n} + 1)b - 2^n,$$

and

$$N = (2^{2n} + 1)c + 2^{3n},$$

some values of (a, n), (b, n) and (c, n) for which L, M, or N are prime are given in Tables 2, 3 and 4, respectively.

A computer program was written to implement the algorithm of Theorem 6 on an IBM/370-158 computer. We present below some selected results of running this program.

For

$$N = 3598020110125739154986036092356326252597494924799183218$$
$$7257385201689,$$

the sixty-eight digit pseudoprime factor of f_{353} (see Jarden [2]), we have for $B_1 = B_2 = B_4 = 4 \times 10^6$,

$$F_1 = 2^3 \cdot 3^3 \cdot 13 \cdot 353 \cdot 6163 \cdot 349291,$$

$$F_2 = 2 \cdot 5 \cdot 7 \cdot 1543,$$

$$F_4 = 2 \cdot 123757 \cdot 331081.$$

For $m > 4122$, we have $N < T$, where $T = M_1 M_2$, $M_1 = B_1 B_2 F_1 \overline{F}_2 + 1$, and $M_2 = L(1) + mF_1\overline{F}_2\overline{F}_4$. N was easily found by the program to be prime.

For

$$N = 22966686648632120276391228028485200841318497622533370591664502461,$$

the sixty-five digit pseudoprime factor of f_{331}, we have for $B_1 = B_2 = B_4 = 3 \times 10^6$,

$$F_1 = 2^2 \cdot 3^2 \cdot 5 \cdot 11 \cdot 331,$$

$$F_2 = 2 \cdot 7 \cdot 2137,$$

$$F_4 = 2 \cdot 41 \cdot 125813.$$

n	a
19	3
20	11
20	161
21	77
25	21

TABLE 2

n	b
87	9
87	57
90	73
99	41

TABLE 3

n	c
83	7
83	13
91	31
91	75
93	85
97	15
97	55
97	111
103	13
103	87
105	13
105	109
107	105

TABLE 4

This is not enough information to prove this number prime; however, R_1 was found to be a pseudoprime.

Now if we put

$$N' = R_1 = 350433132665508869303171107273416961782759584096675868338467,$$

(59 digits)

we find with $B_1' = B_2' = B_4' = 3 \times 10^6$,

$$F_1' = 2 \cdot 3 \cdot 7 \cdot 87631 \cdot 100183,$$

$$F_2' = 2 \cdot 2 \cdot 71 \cdot 1093,$$

$$F_4' = 2 \cdot 5.$$

Here $N' > \min(M_3'^3, M'M_3')$; thus, the program determined that any prime divisor of N' must exceed

$$B_1'F_1' + 1 = 1106171195598000001;$$

and, consequently, B_1 for R_1 can be increased to the value 1106171195598000001. This, however, is still not enough to prove N prime. It was then discovered that R_1' is also a pseudoprime.

We put

$$N'' = R_1' = 950394841395404888259688590644377706963288701 01 \quad (48 \text{ digits}).$$

We find with $B_1'' = B_2'' = B_4'' = 3 \times 10^6$,

$$F_1'' = 2^2 \cdot 5^2 \cdot 67,$$

$$F_2'' = 2 \cdot 3^2 \cdot 53,$$

$$F_4'' = 2 \cdot 41 \cdot 997 \cdot 1519313.$$

Then

$$M_1''M_2'' < N'' < \min((M_3'')^3, M''M_3'').$$

The program verified that any prime divisor of N'' must exceed M_2'', which has the value

$$L''(1) + F_1''\overline{F}_2''\overline{F}_4'' = 309165997822073801;$$

thus, we can now increase the size of B_1' to 3×10^{17}. Using this value for B_1', the program found N' and then N to both be primes.

We also used Pollard's method to attempt to factor R_4'' and this produced the additional prime factor 565909422161; this together with the previous factors was enough for the program to determine N'' a prime.

At the suggestion of J. Selfridge, the number

$$N = 326564995911857479727767473965124258858383644229 81 \quad (50 \text{ digits})$$

$$= \sum_{k=1}^{41} (-1)^{k-1}k!$$

was run on the computer. For $B_1 = B_2 = B_4 = 2 \times 10^6$, we have

$$F_1 = 2^2 \cdot 5 \cdot 13 \cdot 37,$$

$$F_2 = 2 \cdot 3 \cdot 41,$$

$$F_4 = 2.$$

This is not enough to prove N a prime; however, R_2 is a pseudoprime. Putting

$$N' = R_2 = 132749998338153447043807916245985471080643757817 \quad (48 \text{ digits})$$

and $B_1' = B_2' = B_4' = 2 \times 10^6$, we get

$$F_1' = 2^3 \cdot 3 \cdot 167 \cdot 3593,$$

$$F_2' = 2 \cdot 1307,$$

$$F_3' = 2 \cdot 5 \cdot 61 \cdot 614177.$$

Hence

$$M_1'M_2' < N' < \min(M_3'^3, M'M_3')$$

and

$$M_2' = L'(1) + F_1\overline{F}_2\overline{F}_4 = \min(M_1', M_2')$$
$$= 4964870743200170113.$$

Thus, any prime divisor of N' must exceed M_2' and B_2 can now be increased to 4.9×10^{18}. With this new value of B_2, the program was able to prove N prime.

8. **Acknowledgments.** The authors gratefully acknowledge the suggestions given them by John Selfridge and John Brillhart. They also wish to thank J. Brillhart for making available to them a preprint of [1].

Department of Computer Science
University of Manitoba
Winnipeg, Manitoba, Canada R3T 2N2

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.

2. DOV JARDEN, *Recurring Sequences*, 3rd ed., Riveon Lemathematika, Jerusalem, 1973, pp. 41–59.

3. D. H. LEHMER, "Computer technology applied to the theory of numbers," *Studies in Number Theory*, Math. Assoc. Amer.; distributed by Prentice-Hall, Englewood Cliffs, N. J., 1969, pp. 117–151. MR **40** #84.

4. M. A. MORRISON, "A note on primality testing using Lucas sequences," *Math. Comp.*, v. 29, 1975, pp. 181–182.

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

6. J. L. SELFRIDGE & M. C. WUNDERLICH, "An efficient algorithm for testing large numbers for primality," *Proc. Fourth Manitoba Conf. on Numerical Math.*, Winnipeg, Manitoba, 1974, pp. 109–120.

7. H. C. WILLIAMS, "A generalization of Lehmer's functions," *Acta Arith.* (To appear).