MATHEMATICS OF COMPUTATION, VOLUME 30, NUMBER 136
OCTOBER 1976, PAGES 867–886

Some Algorithms for Prime Testing Using Generalized Lehmer Functions

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

Abstract. Let N be an odd integer thought to be prime. The properties of special functions which are generalizations of the functions of Lehmer (*Ann. of Math.*, v. 31, 1930, pp. 419–448) are used to develop algorithms that produce information concerning the possible prime divisors of N. It is shown how the factors of $N \pm 1$, $N^2 + 1$, $N^2 \pm N + 1$, together with the factor bounds on these numbers, may all be used to calculate lower bounds for the possible prime divisors of N. Frequently, these bounds are large enough that N may be shown to be prime.

These tests were implemented on an IBM/370-158 computer and run on the pseudoprime divisors of the first 385 Fibonacci and Lucas numbers.

1. Introduction. In Brillhart, Lehmer, and Selfridge [1], it was shown how an odd integer N, suspected to be prime, may be proved prime provided a sufficient number of factors of $N - 1$ and/or $N + 1$ have been determined. Later Williams and Judd [10] showed that if there were not enough factors of $N \pm 1$ known to prove the primality of N, the factors of $N^2 + 1$ could also be used. In an attempt, however, to demonstrate the primality of

$$N = 134842925493450092180159677017134911374260731070173305763895 69$$

the large (62 digits) pseudoprime factor of the Lucas* number l_{368}, we find

$$N - 1 = 2^6 \cdot 11 \cdot 17 \cdot 23 \cdot R_1,$$

$$N + 1 = 2 \cdot 3 \cdot 5 \cdot 7^2 \cdot 389 \cdot R_2,$$

$$N^2 + 1 = 2 \cdot 193 \cdot 37217 \cdot 1717117 \cdot R_4,$$

with each of R_1, R_2, R_4 being composite and having any prime divisor greater than 4×10^6. This is not a sufficient number of factors to prove N a prime by using the tests of [1] and [10]; but, if we examine $N^2 - N + 1$, we find

$$N^2 - N + 1 = 3 \cdot 109 \cdot 216757 \cdot 1339903 \cdot R_6.$$

In this paper we will develop methods which allow the factors of $N \pm 1$, $N^2 + 1$, $N^2 \pm N + 1$ to be utilized in an attempt to show that N is a prime. As was done in [10], we make use of the properties of the generalized Lehmer functions of Williams [9] in order to develop the theoretical background necessary for establishing these

Received October 7, 1975.

AMS (MOS) subject classifications (1970). Primary 10A25; Secondary 10A35.

Key words and phrases. Primality testing, generalized Lehmer functions, Fibonacci numbers, Lucas numbers.

*We use the usual notations l_n and f_n for the nth Lucas number and Fibonacci number, respectively. That is, $l_0 = 2$, $l_1 = 1$, $f_0 = 0$, $f_1 = 1$, $l_{n+1} = l_n + l_{n-1}$, $f_{n+1} = f_n + f_{n-1}$.

algorithms. In the last two sections we discuss the results of a computer run on the numbers labelled pseudoprime in the table of factors of l_n and f_n in Jarden [2]. We also present several detailed examples.

It should be noted at this point that D. H. Lehmer [3], [4] has previously considered the possibility of using factors of $N^2 + N + 1$ to demonstrate the primality of N. His technique, however, involves the use of Pierce's [6] functions; and it also requires that $N^2 + N + 1$ be completely factored.

2. **The Function C_n.** Let $f(x)$ be a polynomial

$$x^s - P_1x^{s-1} + P_2x^{s-2} - \cdots + (-1)^sP_s$$

with integer coefficients and s distinct zeros $\rho_1, \rho_2, \ldots, \rho_s$.

Let Q be an integer such that $(P_1, P_2, \ldots, P_s, Q) = 1$; and let α_i, β_i $(i = 1, 2, \ldots, s)$ be the zeros of $x^2 - \rho_i x + Q$ $(i = 1, 2, \ldots, s)$. Put

$$\delta = \begin{vmatrix} 1 & \rho_1 & \rho_1^2 & \cdots & \rho_1^{s-1} \\ 1 & \rho_2 & \rho_2^2 & \cdots & \rho_2^{s-1} \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ 1 & \rho_s & \rho_s^2 & \cdots & \rho_s^{s-1} \end{vmatrix},$$

$$\Delta = \delta^2, \qquad E = f(2\sqrt{Q})f(-2\sqrt{Q}),$$

$$v_n(\rho_i) = \alpha_i^n + \beta_i^n \qquad (i = 1, 2, \ldots, s)$$

and define $V_{j,n}$ $(j = 0, 1, 2, \ldots, s-1)$ as

$$V_{j,n} = \frac{1}{\delta}\begin{vmatrix} 1 & \rho_1 & \rho_1^2 & \cdots & \rho_1^{j-1} & v_n(\rho_1) & \rho_1^{j+1} & \cdots & \rho_1^{s-1} \\ 1 & \rho_2 & \rho_2^2 & \cdots & \rho_2^{j-1} & v_n(\rho_2) & \rho_2^{j+1} & \cdots & \rho_2^{s-1} \\ \cdot & \cdot & \cdot & \cdots & \cdot & \cdot & \cdot & \cdots & \cdot \\ 1 & \rho_s & \rho_s^2 & \cdots & \rho_s^{j-1} & v_n(\rho_s) & \rho_s^{j+1} & \cdots & \rho_s^{s-1} \end{vmatrix}.$$

The function C_n is then defined to be the greatest common divisor $(V_{1,n}, V_{2,n}, V_{3,n}, \ldots, V_{s-1,n})$ of $V_{1,n}, V_{2,n}, V_{3,n}, \ldots, V_{s-1,n}$.

As we shall be most concerned in this paper with the case $s = 3$, we conclude this section with some special properties of $V_{0,n}, V_{1,n}, V_{2,n}, C_n$ for $s = 3$. We first note that

$$\Delta = P_1^2P_2^2 + 18P_1P_2P_3 - 4P_2^3 - 4P_1^3P_3 - 27P_3^2,$$

$$E = (P_3 + 4QP_1)^2 - Q(2P_2 + 8Q)^2.$$

The first few values for the functions $V_{0,n}, V_{1,n}$ and $V_{2,n}$ are given in the following table.

n	$V_{0,n}$	$V_{1,n}$	$V_{2,n}$
0	2	0	0
1	0	1	0
2	$-2Q$	0	1
3	P_3	$-P_2 - 3Q$	P_1
4	$P_3P_1 + 2Q^2$	$P_3 - P_1P_2$	$P_1^2 - P_2 - 4Q$
5	$P_3P_1^2 - P_2P_3 - 5QP_3$	$P_2^2 - P_2P_1^2 + P_1P_3 + 5QP_2 + 5Q^2$	$P_1^3 - 2P_1P_2 - 5QP_1 + P_3$

Also, each of the functions $V_{0,n}$, $V_{1,n}$ and $V_{2,n}$ satisfies the recurrence

$$X_{n+6} = P_1X_{n+5} - (P_2 + 3Q)X_{n+4} + (2P_1Q + P_3)X_{n+3} - (3Q^2 + QP_2)X_{n+2} + P_1Q^2X_{n+1} - Q^3X_n$$

and

$$V_{0,n+1} = P_3V_{2,n} - QV_{0,n-1},$$
$$V_{1,n+1} = V_{0,n} - P_2V_{2,n} - QV_{1,n-1},$$
$$V_{2,n+1} = V_{1,n} + P_1V_{2,n} - QV_{2,n-1}.$$

If N is any integer and $(N, QP_3) = 1$, find M, S such that

$$QM \equiv P_3S \equiv 1 \pmod{N}$$

and put

$$X_k = \begin{cases} S^2M^{k/2}V_{0,k}, & k \text{ even}, \\ SM^{(k+1)/2}V_{0,k}, & k \text{ odd}; \end{cases}$$

$$Y_k = \begin{cases} S^2M^{k/2}V_{1,k}, & k \text{ even}, \\ SM^{(k+1)/2}V_{1,k}, & k \text{ odd}; \end{cases}$$

$$Z_k = \begin{cases} S^2M^{k/2}V_{2,k}, & k \text{ even}, \\ SM^{(k+1)/2}V_{2,k}, & k \text{ odd}. \end{cases}$$

Then,

$$X_{2m+1} = P_3(Y_{2m+2} + Y_{2m}) + P_2Z_{2m+1},$$

$$Y_{2m+1} = P_3(Z_{2m+2} + Z_{2m}) - P_1 Z_{2m+1},$$
$$Z_{2m+1} = X_{2m+2} + X_{2m}.$$

Also,

$$X_{2m} = Q(X_m^2 + 2Y_m Z_m P_3 + P_1 P_3 Z_m^2) - 2S^2,$$
$$Y_{2m} = Q(2X_m Y_m - 2P_2 Y_m Z_m + (P_3 - P_1 P_2)Z_m^2),$$
$$Z_{2m} = Q(Y_m^2 + 2Z_m X_m + 2P_1 Y_m Z_m + (P_1^2 - P_2)Z_m^2),$$

when m is odd. If m is even, replace the Q in these formulas by P_3^2. Using these formulas, we can evaluate Y_k, and Z_k in $O(\log k)$ operations. Since $(Y_k, Z_k, N) = (V_{1,k}, V_{2,k}, N)$, we see that this technique can be used for evaluating (C_k, N).

3. Properties of C_n. In [9] several divisibility properties of C_n are presented; for example, $C_n \mid C_{mn}$ if $n \mid m$. The following definition is also given.

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

$$(*) \qquad C_1, C_2, C_3, \ldots, C_n, \ldots$$

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 that C_{τ_j} is the first term of the sequence $(*)$ such that $m \mid C_{\tau_j}$ 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 $\tau_j(m)$.

It is then demonstrated that if $(m, Q) = 1$, then any order of apparition $\tau(m)$ must be a divisor of $2\Phi(m)$, where $\Phi(m)$ is a rather complicated function which depends on m, Q, and the polynomial $f(x)$. When $f(x)$ is irreducible modulo a prime p and s is odd, we can obtain some special results about the orders of apparition of p. We first give some simple lemmas.

LEMMA 1. *If $f(x)$ is irreducible modulo p, then $p \mid C_n$ if and only if $v_n(\rho^*) \in \mathrm{GF}[p]$, where ρ^* is a root of $f(x) = 0$ in $\mathrm{GF}[\rho^s]$.*

Proof. Let

$$v_n(\rho^*) = \sum_{j=0}^{s-1} V_{j,n}^* \rho^{*j},$$

where $V_{j,n}^* \in \mathrm{GF}[p]$ $(j = 0, 1, 2, \ldots, s-1)$.

Now $p \mid C_n$ if and only if $V_{1,n}^* = V_{2,n}^* = V_{3,n}^* = \cdots = V_{s-1,n}^* = 0$; thus, if $p \mid C_n$, $v_n(\rho^*) \in \mathrm{GF}[p]$. If $v_n(\rho^*) \in \mathrm{GF}[p]$, then

$$A = \sum_{j=0}^{s-1} V_{j,n}^* \rho^{*j} \in \mathrm{GF}[p].$$

But, since $f(x)$ is irreducible modulo p, we must have

$$V_{0,n}^* = A, \qquad V_{1,n}^* = V_{2,n}^* = \cdots = V_{s-1,n}^* = 0;$$

hence, $P \mid C_n$.

LEMMA 2. *Let* $A, B \in K = \mathrm{GF}[p^{2s}]$, *where* $AB \neq 0$ *and* s *is odd. If* $A + B \in \mathrm{GF}[p^s]$, $AB \in \mathrm{GF}[p]$, $A^k + B^k \in \mathrm{GF}[p]$ *and* $A^m + B^m \in \mathrm{GF}[p]$, *then* $A^r + B^r \in \mathrm{GF}[p]$, *where* $m = qk + r$.

Proof. In K we have

$$A^{kp^2} = A^k, \quad B^{kp^2} = B^k, \quad A^{mp^2} = A^m, \quad B^{mp^2} = B^m;$$

hence,

$$A^{qk+r} = A^{mp^2} = A^{qkp^2+rp^2} = A^{qk+rp^2}$$

and $A^r = A^{rp^2}$, also $B^r = B^{rp^2}$. Since $A^r + B^r \in \mathrm{GF}[p^s]$, we have

$$(A^r + B^r)^{p^s} = A^r + B^r, \quad (A^r + B^r)^{p^2} = A^r + B^r.$$

Since s is odd, it follows that $(A^r + B^r)^p = A^r + B^r$; and consequently, $A^r + B^r \in \mathrm{GF}[p]$.

COROLLARY. *If the conditions of the lemma are true, then* $A^d + B^d \in \mathrm{GF}[p]$, *where* $d = (k, m)$.

We are now able to prove the following

THEOREM. *If* $p \nmid 2\Delta EQ$ *and* $f(x)$ *is of odd degree* s *and irreducible modulo* p, *then there is only one order of apparition* τ *of* p *and* $\tau \mid (p^s - \epsilon)/(p - \epsilon)$, *where* $\epsilon = (E \mid p)$ (*Legendre Symbol*).

Proof. Let ρ^* be a zero of $f(x)$ in $\mathrm{GF}[p^s]$; then the other zeros are given by $\rho^{*p}, \rho^{*p^2}, \ldots, \rho^{*p^{s-1}}$ also $\rho^{*p^s} = \rho^*$. Let α^*, β^* be the two zeros of $x^2 - \rho^* x + Q$ in $\mathrm{GF}[p^{2s}]$. We have

$$v_n(\rho^*) = \alpha^{*n} + \beta^{*n}.$$

Now $(2\alpha^* - \rho^*)^2 = \rho^{*2} - 4Q$; hence,

$$\begin{aligned}(2\alpha^* - \rho^*)^{p^s-1} &= (\rho^{*2} - 4Q)^{(p^s-1)/2} \\ &= [(\rho^{*2} - 4Q)^{p^{s-1}}(\rho^{*2} - 4Q)^{p^{s-2}} \cdots (\rho^{*2} - 4Q)]^{(p-1)/2} \\ &= [((\rho^{*p^{s-1}})^2 - 4Q)((\rho^{*p^{s-2}})^2 - 4Q) \cdots (\rho^{*2} - 4Q)]^{(p-1)/2} \\ &= E^{(p-1)/2} = \epsilon.\end{aligned}$$

We see that $(2\alpha^* - \rho^*)^{p^s} = \epsilon(2\alpha^* - \rho^*)$ and

$$\alpha^{*p^s} = \begin{cases} \alpha^* & \text{if } \epsilon = 1, \\ \beta^* & \text{if } \epsilon = -1. \end{cases}$$

Putting $k = (p^s - \epsilon)/(p - \epsilon)$, we get

$$\begin{aligned}v_k(\rho^*)^p &= \alpha^{*kp} + \beta^{*kp} = \alpha^{*(p-\epsilon)k+\epsilon k} + \beta^{*(p-\epsilon)k+\epsilon k} \\ &= \alpha^{*(p^s-\epsilon)}\alpha^{*\epsilon k} + \beta^{*(p^s-\epsilon)}\beta^{*\epsilon k} = v_k(\rho^*).\end{aligned}$$

It follows that $p \mid C_k$.

We have shown that there exists one order of apparition τ of p and that $\tau \mid k$. Suppose there exists a second order of apparition τ_1 of p. We have

$$\alpha^{*\tau} + \beta^{*\tau} \in \mathrm{GF}[p], \quad \alpha^{*\tau_1} + \beta^{*\tau_1} \in \mathrm{GF}[p];$$

hence,

$$\alpha^{*d} + \beta^{*d} \in \mathrm{GF}[p],$$

where $d = (\tau, \tau_1)$. Now $d < \tau$, $d \mid \tau$ and $p \mid C_d$. By definition of τ this is impossible and the theorem is proved.

Let $f(x)$ be a polynomial of odd degree s such that, for any prime $p \nmid \Delta$, $f(x)$ is either irreducible modulo p or completely reducible. For example, the cyclotomic period equation [5] is such a polynomial. (For $s = 3$ the necessary and sufficient condition for $f(x)$ to be this type of polynomial is that Δ be a perfect square.) For C_n defined for such an f, we define

$$\psi(p) = \begin{cases} (p^s - \epsilon)/(p - \epsilon) & \text{if } f(x) \text{ is irreducible (mod } p), \\ 2[p - \eta_1, p - \eta_2, p - \eta_3, \ldots, p - \eta_s] & \text{if } f(x) \text{ is reducible (mod } p), \end{cases}$$

where $\eta_i = (r_i^2 - 4Q \mid p)$ and $r_1, r_2, r_3, \ldots, r_s$ are the s roots of $f(x) \equiv 0 \pmod{p}$.

With this definition of f and C_n we have the following two theorems.

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

Proof. This follows easily from the Law of Apparition of [9] and the previous theorem.

THEOREM. *Let $(N, 2\Delta QE) = 1$ and $N \mid C_m$. If q is any prime divisor of m and $N \nmid C_{m/q}$, then any prime divisor p of N which does not divide $C_{m/q}$ 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 $p \mid C_m$, such a τ must exist. Now $p \nmid C_{m/q}$; hence, $\tau \nmid m/q$; and consequently, $q^\alpha \mid \tau$. Since $\tau(p) \mid \psi(p)$, we have

$$\psi(p) \equiv 0 \pmod{q^\alpha}.$$

4. The Sequences $\{C_n^{(i)}\}$. In the remainder of this paper we will consider s to have the value 3.

Let N be an integer which we wish to test for primality. Select a prime P such that $P \equiv 1 \pmod 3$ and $(N \mid P)_3 \neq 1$, and let $4P = S^2 + 27T^2$, where $S \equiv 1 \pmod 3$. Then, if N is a prime and $(N, PT) = 1$, $x^3 - ax - b$, where $a = 3P$, $b = PS$, is irreducible modulo N. Let G be a fixed integer and put $\theta = (G \mid N)$, where $|\theta| = 1$.

For any three integers h_i, k_i, l_i, put

$$m_1 = h_i^2 + 2bl_ik_i - G, \qquad m_2 = bl_i^2 + 2h_ik_i + 2ak_il_i,$$

$$m_3 = k_i^2 + al_i^2 + 2h_il_i,$$

$$d_1 = m_1^2 + 2am_3m_1 + a^2m_3^2 - am_2^2 - bm_2m_3, \qquad d_2 = bm_3^2 - m_1m_2,$$

$$d_3 = m_2^2 - m_1m_3 - am_3^2.$$

Let

$$R = d_1m_1 + bd_2m_3 + bd_3m_2,$$

$$A = 4Gd_1 + 2R, \qquad B = 4Gd_2, \qquad C = 4Gd_3.$$

We define the sequence $C_n^{(i)}$ by using the parameters below:

$$P_1^{(i)} = 3A + 2aC, \qquad P_2^{(i)} = 3A^2 + 4aAC - aB^2 - 3bBC + a^2C^2,$$

$$P_3^{(i)} = A^3 + bB^3 + b^2C^3 - 3bABC - aAB^2 - abBC^2 + a^2AC^2 + 2aA^2C,$$

$$Q^{(i)} = R^2.$$

If σ_1, σ_2, σ_3 are the zeros of $x^3 - ax - b$, we see that $\rho_j = A + B\sigma_j + C\sigma_j^2$ $(j = 1, 2, 3)$ are the three zeros of

$$f(x) = x^3 - P_1^{(i)}x^2 + P_2^{(i)}x - P_3^{(i)}.$$

Now let σ be any one of the three zeros σ_1, σ_2, σ_3 and put

$$\rho = A + B\sigma + C\sigma^2, \qquad X(\sigma) = h_i + k_i\sigma + l_i\sigma^2,$$

$$Y(\sigma) = d_1 + d_2\sigma + d_3\sigma^2.$$

Then

$$m_1 + m_2\sigma + m_3\sigma^2 = (X(\sigma))^2 - G,$$

$$R = Y(\sigma)(m_1 + m_2\sigma + m_3\sigma^2) = Y(\sigma)((X(\sigma))^2 - G),$$

$$\rho = 4Y(\sigma)G + 2R.$$

It follows that

$$\rho^2 - 4Q = [4Y(\sigma)X(\sigma)]^2G.$$

Since $E^{(i)} = (\rho_1^2 - 4Q)(\rho_2^2 - 4Q)(\rho_3^2 - 4Q)$, we have $E^{(i)} = V^2G$, where $V = 4^3GY(\sigma_1)Y(\sigma_2)Y(\sigma_3)X(\sigma_1)X(\sigma_2)X(\sigma_3)$.

Also,

$$\Delta^{(i)} = (B^3 - aBC^2 - bC^3)^2 \begin{vmatrix} 1 & \sigma_1 & \sigma_1^2 \\ 1 & \sigma_2 & \sigma_2^2 \\ 1 & \sigma_3 & \sigma_3^2 \end{vmatrix}^2$$

$$= 3^6(B^3 - aBC^2 - bC^3)^2(PT)^2.$$

Thus, if p is any prime such that $(p, 2\Delta^{(i)}E^{(i)}Q^{(i)}) = 1$, then $(\Delta^{(i)}|p) = 1$, $(E^{(i)}|p) = (G|p) = \theta(p)$ and if $f(x)$ is reducible, $\eta_i = \theta(p)$ $(i = 1, 2, 3)$. We see that these are independent of the values of h_i, k_i, l_i. Also, if $x^3 - ax - b$ is irreducible (mod p), then so is $f(x)$; thus, $\psi(p)$ is always the same for any sequence $\{C_n^{(i)}\}$. Also $\psi(p) = 2(p - \theta(p))$ when $f(x)$ is reducible modulo p.

5. Some Criteria for Primality. Denote by F_3 the completely factored part of $N^2 + N + 1$ and by F_6 the completely factored part of $N^2 - N + 1$. Then $N^2 + N + 1 = F_3R_3$, $N^2 - N + 1 = F_6R_6$, where $(R_3, F_3) = (F_6, R_6) = 1$. For $\theta = 1$, put

(1) *For each prime $q|F_3$, there exists some h_i, k_i, l_i such that $(N, \Delta^{(i)}E^{(i)}Q^{(i)}) = 1$ for the sequence $\{C_n^{(i)}\}$,*

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

(2) *For some h_i, k_i, l_i such that $(N, \Delta^{(i)}E^{(i)}Q^{(i)}) = 1$ for the sequence $\{C_n^{(i)}\}$, we have*

$$N \mid C^{(i)}_{N^2+N+1} \quad \text{and} \quad (C^{(i)}_{(N^2+N+1)/R_3}, N) = 1.$$

For $\theta = -1$, put

(3) *For each prime $q|F_6$, there exists some h_i, k_i, l_i such that $(N, E^{(i)}\Delta^{(i)}Q^{(i)}) = 1$ for the sequence $\{C_n^{(i)}\}$,*

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

(4) *For some h_i, k_i, l_i such that $(N, \Delta^{(i)}E^{(i)}Q^{(i)}) = 1$ for the sequence $\{C_n^{(i)}\}$, we have*

$$N \mid C^{(i)}_{N^2-N+1} \quad \text{and} \quad (C^{(i)}_{(N^2-N+1)/R_6}, N) = 1.$$

It should be noted that if $N \nmid C^{(i)}_{N^2+\theta N+1}$, then N is composite.

We are now able to prove some theorems which give some information about possible prime factors of N should any of (1), (2), (3), or (4) be true.

THEOREM. *If $\theta = 1$, (1) is true, and p is any prime divisor of N, then*

$$\psi(p) \equiv 0 \pmod{F_3}.$$

Proof. Since the value of $\psi(p)$ is the same for any of the sequences $\{C_n^{(i)}\}$ $(i = 1, 2, \ldots)$, it follows that if q is any prime divisor of F_3 and (1) is true, then $q^\nu \mid \psi(p)$, where $q^\nu \| F_3$; hence $F_3 \mid \psi(p)$.

THEOREM. *If $\theta = 1$, (2) is true, and p is any prime divisor of N, then*

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

where q is some prime divisor of R_3 depending on p.

Proof. Let $\tau = \tau(p)$ be an order of apparition of p such that $\tau \mid N^2 + N + 1$; then $\tau \nmid F_3$; and consequently, $(R_3, \tau) > 1$. Thus there must exist a prime q such that $q \mid R_3$ and $q \mid \tau$. Since $\tau \mid \psi(p)$, the theorem follows.

THEOREM. *If* $\theta = -1$ *and* (3) *is true, and* p *is any prime divisor of* N, *then*

$$\psi(p) \equiv 0 \pmod{F_6}.$$

THEOREM. *If* $\theta = -1$, (4) *is true and* p *is any prime divisor of* N, *then*

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

where q *is some prime divisor of* R_6 *depending on* p.

The theorems requiring the truth of either (2) or (4) are unfortunately not as useful here as their analogues in [1] or even [10]; however, we will show in a later section how these theorems can occasionally be useful.

We conclude this section with two results which allow us to demonstrate the primality of N when either $N^2 + N + 1$ or $N^2 - N + 1$ is sufficiently factored.

THEOREM. *If* $\theta = 1$, (1) *is true,* N *is not a perfect square and* $F_3 > N^{2/3} > 36$, *then* N *is a prime.*

Proof. Suppose $N = p_1p_2p_3a$ and a is any positive integer. Since

$$\psi(p_i) \equiv 0 \pmod{F_3}$$

and $\psi(p_i) = p_i^2 \pm p_i + 1$ or $p_i \pm 1$, we have $p_i > \sqrt{F_3} - 1$. If $F_3 \mid p_i \pm 1$, then $p_i > F_3 - 1 > \sqrt{3}\sqrt{F_3} - 1$. Since N is not a perfect cube there must be at least two distinct prime divisors p_1 and p_2. If $F_3 \mid p_1^2 \pm p_1 + 1$ and $F_3 \mid p_2^2 \pm p_2 + 1$, then for one of these p's, say p_1, it must be true that

$$p_1^2 \pm p_1 + 1 \geqslant 3F_3.$$

Thus, we have

$$N = p_1p_2p_3a > (\sqrt{F_3} - 1)^2(\sqrt{3}\sqrt{F_3} - 1) > F_3^{3/2},$$

which is impossible.

Hence, if N is not a prime, it must be the product of two primes p_1, p_2.

Now $(p_1p_2 \mid P)_3 \neq 1$ and $(G \mid p_1p_2) = 1$; hence $\theta(p_1) = \theta(p_2) = \epsilon$, say. If $(p_1 \mid P)_3 = 1$, then $(p_2 \mid P)_3 \neq 1$ and

$$p_1 \equiv \epsilon \pmod{F_3} \quad \text{and} \quad p_2^2 + \epsilon p_2 + 1 \equiv 0 \pmod{F_3}.$$

We have

$$p_1 > 2F_3 - 1 \quad \text{and} \quad p_2 > \sqrt{F_3} - 1;$$

consequently,

$$N = p_1p_2 > (F_3)^{3/2}.$$

If $(p_1 \mid P)_3 \neq 1$, $(p_2 \mid P)_3 \neq 1$,

$$p_1^2 + \epsilon p_1 + 1 \equiv p_2^2 + \epsilon p_2 + 1 = p_1^2p_2^2 + p_1p_2 + 1 \equiv 0 \pmod{F_3}.$$

It follows that

$$(p_1 - p_2)(p_1 + p_2 + \epsilon) \equiv 0 \pmod{F_3}.$$

If $q \mid F_3$ and $q \nmid p_1 - p_2$, then $q \mid p_1 + p_2 + \epsilon$ and

$$p_1^2 \equiv \epsilon p_2, \quad p_2^2 \equiv \epsilon p_1 \pmod{q};$$

hence,

$$q \mid 2p_1p_2 + 1 \quad \text{and} \quad q \mid 3.$$

Thus,

$$p_1 \equiv p_2 \pmod{\bar{F}_3},$$

where**

$$\bar{F}_3 = \begin{cases} F_3/3 & \text{if } 3 \mid F_3, \\ F_3 & \text{otherwise.} \end{cases}$$

If $3 \mid F_3$, then $p_1^2 + \epsilon p_1 + 1 \equiv 0 \pmod 3$ and $p_1 \equiv \epsilon \pmod 3$, also $p_2 \equiv \epsilon \pmod 3$. Since $(3, \bar{F}_3) = 1$, we have

$$p_1 \equiv p_2 \pmod{F_3}.$$

Since $p_1 \neq p_2$, we have $p_1 > p_2$ and

$$p_1 = p_2 + 2kF_3 \quad \text{and} \quad p_1 > 2F_3 + 1.$$

Hence

$$N = p_1p_2 > (2F_3 + 1)(\sqrt{F_3} - 1) > F_3^{3/2}.$$

Thus N is a prime.

THEOREM. *If $\theta = -1$, (3) is true and $F_6 > N^{2/3} > 36$, then N is a prime.*

6. Prime Testing. Let F_1 be the completely factored part of $N - 1$, F_2 be the completely factored part of $N + 1$, and F_4 be the completely factored part of $N^2 + 1$. Put

$$R_1 = (N-1)/F_1, \quad R_2 = (N+1)/F_2, \quad R_4 = (N^2+1)/F_4,$$

$$\bar{F}_1 = F_1/2, \quad \bar{F}_2 = F_2/2, \quad \bar{F}_4 = F_4/2,$$

$$R_2 = r + S\bar{F}_1, \qquad 0 \leqslant r < \bar{F}_1,$$

$$2R_1R_2 \equiv s \pmod{\bar{F}_4},$$

$$S + sN \equiv t \pmod{\bar{F}_4}, \qquad 0 < s, t < \bar{F}_4,$$

$$\mu_1 = -1 + rF_2 + tF_1\bar{F}_2, \quad \mu_2 = 1 + sF_1\bar{F}_2.$$

In [10] it was shown that if C and D are selected such that

**We also define

$$\bar{F}_6 = \begin{cases} F_6/3 & \text{if } 3 \mid F_6, \\ F_6 & \text{otherwise.} \end{cases}$$

$$(D\,|N) = (C^2 - 16D\,|N) = -1,$$

tests can be developed for demonstrating the primality of N. For very large N we sometimes are unable to demonstrate the primality of N but can use a result (Theorem 6) of [10] to show that N is either a prime or $N = p_1p_2$, where p_1 and p_2 are primes,

$$p_1 = \mu_1 + m_1F_1\bar{F}_2\bar{F}_4, \qquad p_2 = \mu_2 + m_2F_1\bar{F}_2\bar{F}_4,$$

and $(D\,|p_2) = +1$, $(D\,|p_1) = -1$, $(C^2 - 16D|p_2) = +1$, $(C^2 - 16D|p_1) = -1$. (We call a prime p such that $(D|p) = (C^2 - 16D|p) = -1$ a prime of the first kind; otherwise, we say it is a prime of the second kind [10].) When this occurs, the tests (1) and (3) can be used to attempt to show the primality of N.

If we select G such that $G \equiv u^2 \pmod N$, then $(G\,|N) = +1$; and if N is the product of the two primes p_1, p_2, then $(G|p_1) = (G|p_2) = 1$. If (1) is true, we have three possible cases.

Case 1. $(p_1\,|P)_3 = 1$, $(p_2\,|P)_3 \neq 1$. Here

$$p_1 \equiv 1 \pmod{F_3}, \qquad p_2 \equiv N \pmod{F_3}.$$

Case 2. $(p_1\,|P)_3 \neq 1$, $(p_2\,|P)_3 = 1$. Here

$$p_2 \equiv 1 \pmod{F_3}, \qquad p_1 \equiv N \pmod{F_3}.$$

Case 3. $(p_1\,|P)_3 \neq 1$, $(p_2\,|P)_3 \neq 1$. Here

$$p_1 \equiv p_2 \pmod{F_3},$$

$$p_1^2 \equiv p_2^2 \equiv N \pmod{F_3} \quad \text{and} \quad p_1^2 + p_1 + 1 \equiv p_2^2 + p_2 + 1 \equiv 0 \pmod{F_3};$$

hence,

$$p_1 \equiv p_2 \equiv -N - 1 \pmod{F_3}.$$

If $HF_1\bar{F}_2\bar{F}_4 \equiv 1 \pmod{\bar{F}_3}$, we see that we must have

$$m_1 \equiv (1 - \mu_1)H, \qquad m_2 \equiv (N - \mu_2)H \pmod{\bar{F}_3},$$

or

(a)
$$m_1 \equiv (N - \mu_1)H, \qquad m_2 \equiv (1 - \mu_2)H \pmod{\bar{F}_3},$$

or

$$m_1 \equiv (-N - 1 - \mu_1)H, \qquad m_2 \equiv (-N - 1 - \mu_2)H \pmod{\bar{F}_3}.$$

If we select G such that $G \equiv u^2(C^2 - 16D) \pmod N$, then $(G\,|N) = -1$; and if N is the product of the two primes p_1, p_2, then $(G\,|p_2) = +1$, $(G\,|p_1) = -1$; and if (3) is true, we again have three possible cases.

Case 1. $(p_1\,|P)_3 = 1$, $(p_2\,|P)_3 \neq 1$. Here

$$p_1 \equiv -1 \pmod{F_6}, \qquad p_2 \equiv -N \pmod{F_6}.$$

Case 2. $(p_1 \mid P)_3 \neq 1$, $(p_2 \mid P)_3 = 1$. Here

$$p_2 \equiv 1 \pmod{F_6}, \qquad p_1 \equiv N \pmod{F_6}.$$

Case 3. $(p_1 \mid P)_3 \neq 1$, $(p_2 \mid P)_3 \neq 1$. In this case

$$p_1 \equiv -p_2 \pmod{F_6}, \qquad p_1^2 \equiv p_2^2 \equiv -N \pmod{F_6},$$

and

$$p_2^2 + p_2 + 1 \equiv p_1^2 - p_1 + 1 \equiv 0 \pmod{F_6};$$

hence,

$$p_2 \equiv N - 1 \pmod{F_6} \quad \text{and} \quad p_1 \equiv -N + 1 \pmod{F_6}.$$

If $H'F_1\bar{F}_2\bar{F}_4 \equiv 1 \pmod{\bar{F}_6}$, we see that we must have

$$m_1 \equiv (-1 - \mu_1)H', \qquad m_2 \equiv (-N - \mu_2)H' \pmod{\bar{F}_6},$$

or

(b)
$$m_1 \equiv (N - \mu_1)H', \qquad m_2 \equiv (1 - \mu_2)H' \pmod{\bar{F}_6},$$

or

$$m_1 \equiv (-N + 1 - \mu_1)H', \qquad m_2 \equiv (N - 1 - \mu_2)H' \pmod{\bar{F}_6}.$$

By using (a) or (b) or both, we can often increase the possible size of m_1 and m_2 to the point where we get $p_1p_2 > N$; when this occurs we have proved N a prime.

If by using the tests of [10] we are unable to show that N is either prime or the product of two primes, we can use the tests (1) and (3) of this paper to increase M_3, the minimum size of a prime divisor of the first kind of N. This can be done by finding all the positive solutions $S_1, S_2, S_3, \ldots, S_n$ which are less than $K = F_1\bar{F}_2\bar{F}_3\bar{F}_4\bar{F}_6$ of the system

$$Z \equiv 1 \pmod{F_1\bar{F}_3}, \qquad Z \equiv -1 \pmod{F_2\bar{F}_6}, \qquad Z^2 \equiv -1 \pmod{F_4},$$

and all the positive solutions $S'_1, S'_2, S'_3, \ldots, S'_k$, which are less than K of the system

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

$$Z^2 + Z + 1 \equiv 0 \pmod{F_3}, \quad Z^2 - Z + 1 \equiv 0 \pmod{F_6}.$$

If $S = \min\{S_1, S_2, S_3, \ldots, S_n, S'_1, S'_2, S'_3, \ldots, S'_k\}$ and none of $S_1, S_2, S_3, \ldots, S_n, S'_1, S'_2, S'_3, \ldots, S'_k$ is a divisor of N, then, if G is defined as above and (1) and (3) are both true, any prime of the first kind which divides N must exceed $S + K$. Thus, M_3 must exceed $S + K$; and this is usually an increase in the previous size of M_3 as determined by the methods of [10].

Other methods which utilize the tests (1), (2), (3), or (4) can also be devised for proving primality. Some of these will be discussed with respect to certain examples in a later section.

7. Some Computational Results. A computer program similar in design to that of Selfridge and Wunderlich [8] was written for an IBM/370-158 computer. This program incorporated the tests of [1], [10] and those of the present work (including the selection of G as presented in Section 6) as a means of proving a given number N prime. This program attempts to factor $N-1, N+1, N^2+1, N^2+N+1, N^2-N+1$ by utilizing, as test divisors, all the primes less than a certain factor bound B. The method described by Wunderlich and Selfridge [11] was used in this particular program segment.

If, after the factoring, sufficient information is available to prove N a prime, the required final tests are executed. If insufficient information is available, Pollard's [7] method is used to attempt to factor R_1, R_2, R_4. If this produces enough additional factors, the final tests are executed.

Should the computer still not have enough information to execute the final tests, the algorithm of [8] is used when either R_1 or R_2 is a pseudoprime. That is, the computer attempts to prove the pseudoprime a prime, or, failing that, attempts to increase the appropriate factor bound. (See [1, p. 627].)

This program was run on all the pseudoprimes listed in the factorization tables of l_n and f_n in [2]. Of the seventy-nine pseudoprimes, forty are easily found to be prime by using only the tests of [1] and $B = 5 \times 10^5$. Two of the remaining numbers (the pseudoprime divisors of f_{331} and f_{353}) have been discussed in [10]. The remaining thirty-seven are also all prime, and the techniques needed to demonstrate the primality of each one are described in Table 1.

In the first column of Table 1, we denote by N_n the large pseudoprime factor of l_n and by $\bar{N}_n$ the large pseudoprime factor of f_n. In the second column we give the number of digits of the pseudoprime in the first column; in the third column we give the value of B the program used. When no entry appears in this column, $B = 5 \times 10^5$. In the fourth column the final tests needed to prove N_n or $\bar{N}_n$ a prime are given. These are presented as [1] to indicate that only the tests of [1] were needed; [1], [10] to indicate that the tests of both [1] and [10] were needed; and [1], [10], PW to indicate that the tests of [1], [10] and those of the present work were needed. Finally, in the fifth column we give some appropriate remarks. When the letter P appears in this column, it indicates that one of R_1 or R_2 is a pseudoprime, even though this fact was not needed by the program to prove the corresponding N_n or $\bar{N}_n$ prime.

8. Some Special Cases. In this section we discuss some of the more interesting of the numbers of Table 1.

For $N = N_{368}$, the number in the introduction, we have (using the notation of [10])

$$M > 6 \times 10^{43}, \quad M_3 > 10^{24},$$

and consequently

$$N < \min(MM_3, M_3^3).$$

TABLE 1

N	No. of Digits	B	Tests	Remarks
N_{206}	38		[1],[10],PW	P
N_{208}	29		[1],[10]	P
N_{212}	36		[1],[10],PW	P
N_{218}	42		[1],[10]	Pollard's method found the factor 8570437 of N+1 .
$\bar{N}_{223}$	30		[1],[10]	
N_{229}	45		[1],[10],PW	Pollard's method found the factor 2948041 of N+1 .
N_{239}	44		[1],[10]	P
N_{241}	38		[1],[10]	P
N_{247}	31		[1],[10]	P
N_{259}	42		[1],[10]	P
N_{263}	40		[1],[10]	
$\bar{N}_{263}$	46		[1],[10],PW	P
N_{278}	53		[1],[10],PW	P
$\bar{N}_{281}$	46		[1],[10]	P
N_{289}	48	1.6×10^{7}	[1],[10],PW	
N_{293}	56		[1],[10]	
$\bar{N}_{299}$	56		[1],[10]	
N_{307}	62	3×10^{8}	[1],[10],PW	See discussion below.
N_{311}	61		[1],[10],PW	
$\bar{N}_{311}$	44		[1],[10],PW	P
N_{314}	57		[1],[10],PW	
N_{316}	60	1.1×10^{6}	[1],[10],PW	R_1 (53 digits) proved prime using [1],[7],PW (P), then N proved prime using [1].
N_{319}	50		[1],[10],PW	P
N_{321}	36		[1]	R_2 proved prime, then N proved prime.
$\bar{N}_{329}$	51	2.5×10^{6}	[1],[10],PW	
N_{332}	64	6×10^{7}	[1]	$N+1 = 2^3\cdot3\cdot7\cdot83\cdot59138939\cdot R2$. R_2 proved prime, then N proved prime.
N_{337}	58		[1]	Pollard's method found the factor 12815681 of N-1 .

TABLE 1 (*continued*)

N	No. of Digits	B	Tests	Remarks
N_{341}	50		[1], [10]	P
N_{343}	46		[1]	Here $R_2-1 = F_1'R_1'$. R_1', then R_2, then N proved prime.
N_{356}	69		[1], [10],PW	See discussion below.
N_{357}	41		[1], [10]	Pollard's method found the factor 106929516613 of N^2+1 .
N_{368}	62	1.8×10^6	[1],[10],PW	See discussion below.
$\bar{N}_{371}$	61	5×10^7	[1],[10],PW	See discussion below.
N_{372},	47		[1], [10],PW	P
N_{373}	75		[1], [10],PW	P
$\bar{N}_{373}$	58		[1], [10]	P
N_{381}	43		[1], [10],PW	

Thus, $N = p_1p_2$, where p_1 and p_2 are primes,

$$p_1 \equiv 762385150126634192052929 \pmod{F_1\bar{F}_2\bar{F}_4}, \qquad p_2 > 10^{24},$$

and $(C^2 - 16D \mid p_1) = -1$, $(D \mid p_1) = -1$. By verifying (3) and using (b) for p_1, it was shown by actual division that any possible value of p_1 less than $F_1\bar{F}_2\bar{F}_4\bar{F}_6$ is not a divisor of N. Hence

$$p_1 > 9 \times 10^{23} \times 2.7 \times 10^{13} > 2.4 \times 10^{37} \quad \text{and} \quad p_1p_2 > 2.4 \times 10^{61} > N.$$

Thus N must be a prime.

For

$$N_{356} = 565768471959285714079262248889509474547974219027885983055827845016103$$

and $B = 5 \times 10^5$, we get

$$F_1 = 2 \cdot 3 \cdot 659 \cdot 1567, \qquad F_2 = 2^3 \cdot 53 \cdot 89, \qquad F_4 = 2 \cdot 5,$$

$$F_3 = 3 \cdot 7 \cdot 2659, \qquad F_6 = 241 \cdot 7759.$$

This is not enough to prove N_{356} a prime. However, R_1 and R_2 are both pseudoprime. The larger of these (R_2) is easier to prove prime than R_1. In fact, if

$$N' = R_2 = 14992804535702928611386004051555794852341907436609232114050981689$$

(65 digits) and $B = 3 \times 10^6$, we get

$$F_1' = 2^3 \cdot 3 \cdot 67 \cdot 7411 \cdot 51169, \qquad F_2' = 2 \cdot 5 \cdot 31 \cdot 23039,$$

$$F_4' = 2 \cdot 17^2 \cdot 37, \quad F_3' = 3 \cdot 7 \cdot 13 \cdot 43 \cdot 61 \cdot 1087 \cdot 5119 \cdot 10501, \quad F_6' = 2221.$$

By using the tests of [1], [10] and PW (neither R_1' nor R_2' is a pseudoprime), N' can be shown to be a prime. It is then a simple matter to prove N_{356} a prime.

For

$$N = \overline{N}_{371} = 10668914543306923609111184699154927702112864025685324579661 13$$

and $B = 5 \times 10^7$, we get

$$F_1 = 2^5 \cdot 29, \quad F_2 = 2 \cdot 3 \cdot 7 \cdot 11 \cdot 53 \cdot 11239 > 2 \cdot 7 \times 10^8,$$

$$F_4 = 2 \cdot 5 \cdot 165041, \quad F_3 = 1431907, \quad F_6 = 3 \cdot 13 \cdot 19,$$

and R_1 and R_2 are both composite. With this information it is possible to demonstrate with the computer program that either N is a prime or it is the product of two primes p_1 and p_2. Further, if $N = p_1p_2$, p_1 is a prime of the first kind; and p_2 is a prime of the second kind.

It follows by using the results of Section 6 that

$$p_1 = r_1, r_1', r_1'' \pmod K, \quad p_2 \equiv r_2, r_2', r_2'' \pmod K,$$

where r_1, r_2 are obtained by using the first case of (a) and (b), r_1', r_2' by the second case of (a), (b), and r_1'', r_2'' by the third case of (a), (b).

Now $K = F_1\overline{F}_2\overline{F}_3\overline{F}_4\overline{F}_6 > 3 \cdot 7 \times 10^{25}$ and if

$$p_1 = r_1 + t_2K, \quad p_2 = r_2 + t_2K,$$

then

$$N = r_1r_2 + (t_1r_2 + t_2r_1)K + t_1t_2K^2.$$

We now make use of an extension of an idea introduced in [1]. For if

$$(N - r_1r_2)/K \equiv T \pmod{F_2},$$

where $|T| < \overline{F}_2$, then, recalling that $r_1 \equiv -1 \pmod{F_2}$, $r_2 \equiv 1 \pmod{F_2}$, we get

$$t_1 - t_2 \equiv T \pmod{F_2}.$$

If $t_1 - t_2 \neq T$, then $|t_1 - t_2| > \overline{F}_2$; and consequently, t_1 or $t_2 > \overline{F}_2 > 1.37 \times 10^8$. It is possible to verify on the computer that

$$p_1 \nmid N, p_2 \nmid N \quad \text{for } 0 \leqslant t_1, t_2 \leqslant 6;$$

hence

$$p_1p_2 > 6 \times 1.37 \times (3.7)^2 \times 10^{58} > N.$$

If $t_1 - t_2 = T$, we must have

$$A = (r_1 - r_2 + KT)^2 + 4N$$

a perfect integer square. It is easy to use the computer to find a small prime $\pi \nmid K$ such that $(A \mid \pi) = -1$. In a similar manner we can dispose of the other two cases:

$p_1 \equiv r_1'$, $p_2 \equiv r_2'$ and $p_1 \equiv r_1''$, $p_2 \equiv r_2''$ (mod K). By using this strategy the number N was proved prime.

For

$$N = N_{307} = 11739610117429203651282768407085324070169775523763828726810201$$

and $B = 3 \times 10^8$, we get

$$F_1 = 2^3 \cdot 5^2 \cdot 7 \cdot 307, \quad F_2 = 2 \cdot 3 \cdot 431 \cdot 6911 > 1.78 \times 10^7,$$

$$F_4 = 2, \quad F_3 = 737497, \quad F_6 = 3 \cdot 229;$$

and R_1, R_2 are both composite. None of the other numbers considered in Table 1 presented as much difficulty in proving primality as this one. The strategy used to prove N prime is a refinement of that used in demonstrating the primality of $\bar{N}_{371}$. In this particular example use was made of tests (1), (2), (3), and (4) as well as all the tests (I, II, III, IV) of [1] and the test (β) of [10].

We have $M = 1 + B^3 F_1 \bar{F}_2 \bar{F}_4 > 10^{38}$. In order to show that N is the product of at most two primes, we must obtain a large ($> 1.2 \times 10^{23}$) lower bound on any prime of the first kind p which divides N. We have

$$p \equiv 1 \quad (q_1 F_1), \qquad p \equiv -1 \quad (q_2 F_2),$$

and if $(p \mid P)_3 = 1$,

$$p \equiv 1 \quad (q_3 F_3), \qquad p \equiv -1 \quad (q_6 F_6),$$

where q_i is some prime divisor of R_i ($q_i > B$). In this case we have $p > 1 + B^2 F_1 \bar{F}_3 = 2.5 \times 10^{28} > 1.2 \times 10^{23}$. Since $\bar{F}_3$ and $\bar{F}_6$ are both primes, there are four possibilities for p modulo K ($= F_1 \bar{F}_2 \bar{F}_3 \bar{F}_6 > 6.48 \times 10^{20}$) when $(p \mid P)_3 \neq 1$. These are given by

$$\begin{cases} p \equiv N & (\text{mod } \bar{F}_3), \\ p \equiv N & (\text{mod } \bar{F}_6), \end{cases} \qquad \begin{cases} p \equiv -N - 1 & (\text{mod } \bar{F}_3), \\ p \equiv N & (\text{mod } \bar{F}_6). \end{cases}$$

$$\begin{cases} p \equiv N & (\text{mod } \bar{F}_3), \\ p \equiv -N + 1 & (\text{mod } \bar{F}_6), \end{cases} \qquad \begin{cases} p \equiv -N - 1 & (\text{mod } \bar{F}_3), \\ p \equiv -N + 1 & (\text{mod } \bar{F}_6). \end{cases}$$

We can obtain positive integers A_1, A_2, A_3, A_4 such that $p \equiv A_i$ (mod K) for some $i \leqslant 4$ ($A_i < K$). It was shown by machine that $A_i + t_i K \nmid N$ for $0 \leqslant t_i \leqslant 186$ and $1 \leqslant i \leqslant 4$; hence, if p is a prime of the second kind and $p \mid N$, then

$$p > 186 \times 6.48 \times 10^{20} = 1.2 \times 10^{23}.$$

We have $M_3^3 > N$ and $M_3 M > N$; it follows that N is prime or $N = p_1 p_2$, where p_1 is a prime of the first kind and p_2 is a prime of the second kind. We suppose that

N is the product of two primes and deal with the three possible cases.

Case 1. $(p_2 \mid P)_3 = 1$. We have

$$p_2 \equiv 1 \quad (q_1F_1), \qquad p_2 \equiv 1 \quad (q_2F_2), \qquad p_2 \equiv 1 \quad (q_3F_3), \qquad p_2 \equiv 1 \quad (q_6F_6);$$

hence,

$$p_2 > 1 + B^4K > 4 \times 10^{54} \quad \text{and} \quad p_1p_2 > N.$$

Case 2. $(p_1 \mid P)_3 = 1$. We have

$$p_1 \equiv 1 \quad (q_1F_1), \qquad p_2 \equiv 1 \quad (q_1q_2F_1\bar{F}_2), \qquad p_1 \equiv 1 \quad (q_3F_3);$$

thus,

$$p_1 > 1 + B^2F_1\bar{F}_3 > 2.85 \times 10^{28}, \qquad p_2 > 1 + B^2F_1\bar{F}_2 > 3.45 \times 10^{29}.$$

We also have

$$\begin{cases} p_1 \equiv -1 \pmod{F_2}, \\ p_1 \equiv -1 \pmod{F_6}, \end{cases} \qquad \begin{cases} p_2 \equiv N \pmod{F_3}, \\ p_2 \equiv -N \pmod{F_6}. \end{cases}$$

Hence, we can determine integers r_1, r_2 such that

$$p_1 \equiv r_1 \pmod{K}, \qquad p_2 \equiv r_2 \pmod{K}.$$

If we use the argument employed in the discussion of $\bar{N}_{371}$, we see that for some k we must have

$$A(k) = (r_1 - r_2 + KT + kKF_2)^2 + 4N$$

a perfect square, where

$$T \equiv (N - r_1r_2)/K \pmod{F_2}, \qquad |T| < \bar{F}_2,$$

$$p_1 = r_1 + t_1K, \qquad p_2 = r_2 + t_2K, \qquad t_1 - t_2 = T + kF_2.$$

Let Π be the set of all primes, which do not divide K and are less than 100. It was easily verified by using a sieve process that

$$(A(k) \mid \pi) = -1 \quad \text{for some } \pi \in \Pi$$

for each k such that $0 \leqslant |k| \leqslant 3.6 \times 10^4$. Thus, since $\min(p_1, p_2) > 2.85 \times 10^{28}$, and one of t_1, t_2 must exceed $(|k| - 1/2)F_2$, we have

$$p_1p_2 > 2.85 \times 10^{28} \times 6.48 \times 10^{20} \times 1.78 \times 10^7 \times 3.6 \times 10^4 > N.$$

Case 3. $(p_1 \mid P)_3 \neq 1$, $(p_2 \mid P)_3 \neq 1$. We have

$$-N - 1 \equiv p_1 \equiv p_2 \pmod{\bar{F}_3}, \qquad -N + 1 \equiv p_1 \equiv -p_2 \pmod{\bar{F}_6}.$$

Hence, we can find r_1, r_2 (different from the preceding r_1, r_2) such that

$$p_1 = r_1 + t_1K, \qquad p_2 = r_2 + t_2K.$$

Using reasoning similar to the above, we get

$$t_1 + t_2 \equiv T \equiv r_1^{-1}(N - r_1 r_2)/K \pmod{F_1 \bar{F}_3},$$

where $|T| < \bar{F}_1 \bar{F}_3$. We verified that

$$A(k) = (r_1 + r_2 + KT + kKF_1\bar{F}_3)^2 - 4N$$

cannot be a perfect square for any k such that $0 \leqslant k \leqslant 8.6 \times 10^4$, and we also verified that $r_1 + t_1 K \nmid N$ for $0 \leqslant t_1 \leqslant 1040$.

Let

$$t_1 + t_2 = 2a > (k - 1/2)F_1\bar{F}_3 > 2.7 \times 10^{16}.$$

Since $p_2 > 3.45 \times 10^{29}$, it follows that $t_1 < t_2$; hence,

$$t_1 = a - b, \qquad t_2 = a + b,$$

where $0 \leqslant b \leqslant a$.

If $b > .999a$, then $t_2 > (1.999)a > 2.698 \times 10^{16}$ and

$$p_1 p_2 > 1040 \times 6.48 \times 10^{20} \times 2.698 \times 10^{16} \times 6.48 \times 10^{20} > N.$$

If $b \leqslant .999a$, then

$$t_1 \geqslant (.001)a > 1.35 \times 10^{13}, \qquad t_2 \geqslant a > 1.35 \times 10^{16},$$

and $p_1 p_2 > N$.

Since N cannot be the product of two or more primes, it must be prime.

In conclusion, we remark that had we wished to use factors of $(N^5 - 1)/(N - 1)$ or $(N^5 + 1)/(N + 1)$ to prove the primality of N_{307}, we would find with $B = 10^6$ that

$$(N^5 - 1)/(N - 1) = 5 \cdot 11 \cdot 821 \cdot R_5,$$
$$(N^5 + 1)/(N + 1) = 241 \cdot 9311 \cdot 9851 \cdot 35461 \cdot 151381 \cdot R_{10}.$$

The unfortunate aspect of investigating factors of higher cyclotomic functions of N is the very rapid proliferation of possible residue classes to which suspected prime divisors of N could belong. For very large N the creation of all the residue classes becomes so tedious and the resulting test divisions become so numerous that any advantage obtained by knowing a large collection of congruences that a suspected prime divisor must satisfy appears to be destroyed.

9. Acknowledgements. The authors gratefully acknowledge several suggestions from Professors John Brillhart and D. H. Lehmer. They also thank D. H. Lehmer for making available his notes [4] on primality testing.

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, "The economics of number theoretic computation," *Computers in Number Theory*, Academic Press, London and New York, 1971, pp. 1–9. MR 47 #3285.

4. D. H. LEHMER, "Use of Pierce functions for a primality test." (Unpublished notes.)

5. EMMA LEHMER, "Criteria for cubic and quartic residuacity," *Mathematika*, v. 5, 1958, pp. 20–29. MR 20 #1668.

6 T. A. PIERCE, "The numerical factors of the arithmetic forms $\Pi^n(1 \pm \alpha_i^m)$," *Ann. of Math.* (2), v. 18, 1916, pp. 53–64.

7. J. M. POLLARD, "Theorems on factorization and primality testing," *Proc. Cambridge Philos. Soc.*, v. 76, 1974, pp. 521–528. MR 50 #6992.

8. J. L. SELFRIDGE & M. C. WUNDERLICH, "An efficient algorithm for testing large numbers for primality," *Proc. Fourth Manitoba Conf. on Numerical Math.* (Winnipeg, Man.,1974), Congr. Numer., No. 12, Utilitas Math., Winnipeg, Man., 1975, pp. 109–120. MR 51 #5461.

9. H. C. WILLIAMS, "A generalization of Lehmer's functions," *Acta Arith.*, v. 29, 1976, pp. 315–341.

10. 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.

11. M. C. WUNDERLICH & J. L. SELFRIDGE, "A design for a number theory package with an optimized trial division routine," *Comm. ACM*, v. 17, 1974, pp. 272–276.