MATHEMATICS OF COMPUTATION, VOLUME 32, NUMBER 143
JULY 1978, PAGES 905–917

Some Observations on Primality Testing

By H. C. Williams and R. Holte

Abstract. Let N be an integer which is to be tested for primality. Previous methods of ascertaining the primality of N make use of factors of $N \pm 1$, $N^2 \pm N + 1$, and $N^2 + 1$ in order to increase the size of any possible prime divisor of N until it is impossible for N to be the product of two or more primes. These methods usually work as long as $N < K^2$, where K is 1/12 of the product of the known prime power factors of $N \pm 1$, $N^2 \pm N + 1$, and $N^2 + 1$. In this paper a technique is described which, when used in conjunction with these methods, will often determine the primality of N when $N < lK^3$ and l is small.

1. Introduction. Let N be an integer which is to be tested for primality. In Brillhart, Lehmer and Selfridge [1] and Williams and Judd [5], [6] several methods are presented for ascertaining the primality of N. These methods make use of the factors of $N \pm 1$, $N^2 + 1$, or $N^2 \pm N + 1$ in order to increase the size of the possible prime factors of N until it is impossible for N to be the product of two or more primes.

The combination of these various methods has proved quite successful for testing values of N up to 90 or more digits; however, it sometimes occurs that a much smaller number can be very troublesome. For example, consider the 76 digit value of N below:

$$N = 1242340672101622515322951453717640776208728774955230695528416715857159207729.$$

This number is the large pseudoprime divisor of the Lucas number l_{476}. Here

$$\begin{aligned} N - 1 &= 2^4 \cdot 7^2 \cdot 17 \cdot 773 \cdot R_1, \\ N + 1 &= 2 \cdot 3^4 \cdot 5 \cdot 199 \cdot 2571 \cdot R_2, \\ N^2 + N + 1 &= 73 \cdot R_3, \\ N^2 + 1 &= 1741 \cdot R_4, \\ N^2 - N + 1 &= 3 \cdot 13 \cdot 31 \cdot 37 \cdot R_6, \end{aligned}$$

where R_1, R_2, R_3, R_4, R_6 are all composite and have no prime divisor $< 5 \times 10^7$. With this information it is not possible to prove N a prime by using only the methods referred to above.

For a given N let

$$\begin{aligned} N - 1 &= F_1 R_1, \quad (\bar{F}_1 = F_1/2), \\ N + 1 &= F_2 R_2, \quad (\bar{F}_2 = F_2/2), \end{aligned}$$

Received July 7, 1977; revised November 14, 1977.
AMS (MOS) subject classifications (1970). Primary 10A25.

$$N^2 + N + 1 = F_3R_3, \quad (\bar{F}_3 = F_3/3 \text{ when } 3|F_3; \text{ otherwise } \bar{F}_3 = F_3),$$
$$N^2 + 1 = F_4R_4, \quad (\bar{F}_4 = F_4/2),$$
$$N^2 - N + 1 = F_6R_6, \quad (\bar{F}_6 = F_6/3 \text{ when } 3|F_6; \text{ otherwise } \bar{F}_6 = F_6),$$

where F_1, F_2, F_3, F_4, F_6 are completely factored and all prime divisors of any of the R_i $(i = 1, 2, 3, 4, 6)$ must exceed the factor bound B. We further assume that if p^α is a prime power divisor of any of the above polynomials in N and $p < B$, then p^α appears as a factor in the appropriate F_i. Put

$$K = F_1\bar{F}_2\bar{F}_3\bar{F}_4\bar{F}_6$$

and assume that $(N, 6) = 1$, $B > 3$. In this paper we present a technique which can often be used in conjunction with the tests of [1], [5] and [6] to determine whether or not N is a prime when $N < lK^3$ and l is small.

2. N the Product of Three Primes. If N is not too large (not over 100 digits), it is usually possible to use the methods of [6] to show that N cannot be the product of three or more primes. In this section we give another method which is sometimes useful for proving that N cannot be the product of three primes. We make use of the notation of [5], [6] and we assume that N has satisfied the appropriate tests of [1], [5], [6]. As we make extensive use of [5] and [6] in what follows, we will indicate, when relevant, those parts of these papers which we are referencing.

Assume $N = p_1p_2p_3$, where p_1, p_2, p_3 are primes and p_1 is a prime of the first kind [5, p. 167]. We have

$$p_1 \equiv 1 \pmod{q_1F_1},$$
$$p_1 \equiv -1 \pmod{q_2F_2},$$
$$p_1^2 \equiv -1 \pmod{q_4F_4},$$

where q_i is some prime divisor of R_i $(i = 1, 2, 4)$. Let Q be the largest prime divisor of $\bar{F}_4$ when $\bar{F}_4 > 1$; then

$$p_1 \equiv \lambda_1 \text{ or } \lambda_2 \pmod{C},$$

where $C = QF_1\bar{F}_2$, $\lambda_1 \equiv \lambda_2 \equiv 1 \pmod{F_1}$, $\lambda_1 \equiv \lambda_2 \equiv -1 \pmod{F_2}$, $\lambda_1 \equiv N \pmod{Q}$, $\lambda_2 \equiv -N \pmod{Q}$, and $0 \leqslant \lambda_1, \lambda_2 < C$. Now p_2 and p_3 must both be of the same kind [5, p. 167], and we first assume that they are of the second kind; hence, $p_2 \equiv p_3 \equiv \pm 1 \pmod{F_2}$. If we choose the positive sign here, we get

$$p_2 \equiv p_3 \equiv 1 \pmod{F_1\bar{F}_2} \quad \text{and} \quad p_2 > B^2F_1\bar{F}_2, \quad p_3 > B^2F_1\bar{F}_2.$$

If we verify by trial division that $\lambda_i + mC \nmid N$ for $i = 1, 2$ and $0 \leqslant m \leqslant T$, we cannot have $TCB^4F_1^2\bar{F}_2^2 > N$.

Now suppose $p_2 \equiv p_3 \equiv -1 \pmod{F_2}$. Since $p_2^2 \equiv p_3^2 \equiv 1 \pmod{F_4}$, we see that

$$p_2 \equiv \nu_1, \nu_2 \pmod{C} \quad \text{and} \quad p_3 \equiv \nu_1, \nu_2 \pmod{C},$$

where $\nu_1 \equiv \nu_2 \equiv 1 \pmod{F_1}$, $\nu_1 \equiv \nu_2 \equiv -1 \pmod{F_2}$, $\nu_1 \equiv 1 \pmod{Q}$, $\nu_2 \equiv -1 \pmod{Q}$, and $0 \leqslant \nu_1, \nu_2 < C$. Let $p_i \equiv r_i \pmod{C}$ $(i = 1, 2, 3)$, where $0 < r_i < C$.

There are only three possible values for $r_1r_2r_3$; these are $\lambda_1\nu_1^2$, $\lambda_1\nu_2^2$, $\lambda_2\nu_1\nu_2$. Let V_1, V_2, V_3 be the three possible values of $(N - r_1r_2r_3)/C$. Since N is of the form

$$N = (m_1C + r_1)(m_2C + r_2)(m_3C + r_3),$$

we see that

$$V_i \equiv m_1r_3r_2 + m_2r_3r_1 + m_3r_1r_2 \pmod{C}.$$

It follows that $m_1 + m_2 + m_3 \geqslant \overline{V}_i \pmod{F_1\overline{F}_2}$, where $\overline{V}_i \equiv V_i \pmod{F_1\overline{F}_2}$, $0 \leqslant \overline{V}_i < F_1\overline{F}_2$. Let $\overline{V} = \min(\overline{V}_1, \overline{V}_2, \overline{V}_3)$ and verify that $mC + \nu_i \nmid N$ for $i = 1, 2$ and all $m \leqslant T$. Since one of m_1, m_2, m_3 must exceed $\overline{V}/3$, we see that if $T^2\overline{V}C^3/3 > N$, we have a contradiction.

When p_1, p_2, p_3 are all of the first kind,

$$N = (m_1C + r_1)(m_2C + r_2)(m_3C + r_3),$$

where $r_1r_2r_3$ can only be $\lambda_1^2\lambda_2$ or λ_2^3. Let $\overline{V}_4$ and $\overline{V}_5$ be the two possible values of $(N - r_1r_2r_3)/C$ modulo $F_1\overline{F}_2$ $(0 \leqslant \overline{V}_4, \overline{V}_5 < F_1\overline{F}_2)$. We can use the same reasoning as that above to show that $m_1 + m_2 + m_3 \geqslant \overline{V}_i$ $(i = 4, 5)$. Thus, if

$$V = \min(\overline{V}_1, \overline{V}_2, \overline{V}_3, \overline{V}_4, \overline{V}_5) \quad \text{and} \quad N < \min(T^2\overline{V}C^3/3, TCB^4F_1^2F_2^2),$$

then N cannot be the product of three primes.

If this method fails because one of the inequalities above is not satisfied, another method of proceeding is to find a lower bound B_1 on a prime of the first kind which divides N by using the method of [6, p. 878] to first find all the possible positive remainders $S_1, S_2, S_3, \ldots, S_k \pmod{K}$ of a prime factor of the first kind of N. We then verify that for each S_i, $S_i + mK \nmid N$ for $m = 0, 1, 2, \ldots, T$, and put $B_1 = (T + 1)K$.

If p is a prime divisor of N of the second kind, we must have either

$$\begin{aligned} p^2 &\equiv 1 \pmod{q_1F_1}, \\ p^2 &\equiv 1 \pmod{q_2F_2}, \\ p^2 &\equiv 1 \pmod{q_3F_3}, \\ p^2 &\equiv 1 \pmod{q_4F_4}, \\ p^2 &\equiv 1 \pmod{q_6F_6}, \end{aligned}$$

and $p > \sqrt{B^5K}$ or

$$(*) \qquad \begin{cases} p \equiv 1 \pmod{F_1}, \\ p \equiv \delta \pmod{F_2} \quad (|\delta| = 1), \\ p^2 + p + 1 \equiv 0 \pmod{F_3}, \\ p^2 \equiv 1 \pmod{F_4}, \\ p^2 + \epsilon p + 1 \equiv 0 \pmod{F_6} \quad (|\epsilon| = 1), \end{cases}$$

where we cannot have $\delta = \epsilon = -1$. If the system of congruences $(*)$ has no positive solution which divides N and is also less than B_1 and if $B^5K > B_1^2$, then N cannot be the product of three primes when $B_1^3 > N$.

3. N **a Product of Two Primes.** If N has satisfied the tests of [1], [5] and [6] and if N must be the product of at most two primes, then $N = p_1p_2$, where p_1 is a prime of the first kind and p_2 is a prime of the second kind. There are six possible cases ([5, pp. 167–168], [6, pp. 877–878]). For all of these cases we have

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

For two of these cases we have

$$p_1 \equiv \pm N \pmod{q_4F_4}, \quad p_2 \equiv \pm 1 \pmod{q_4F_4},$$
$$p_1 \equiv N \pmod{q_3F_3}, \quad p_2 \equiv 1 \pmod{q_3F_3},$$
$$p_1 \equiv N \pmod{q_6F_6}, \quad p_2 \equiv 1 \pmod{q_6F_6},$$

where q_i is some prime divisor of R_i. Thus, if $s_1 \equiv s_2 \equiv 1 \pmod{F_1}$, $s_1 \equiv s_2 \equiv -1 \pmod{F_2}$, $s_1 \equiv s_2 \equiv N \pmod{\bar{F}_3\bar{F}_6}$, $s_1 \equiv N \pmod{F_4}$, $s_2 \equiv -N \pmod{F_4}$, $0 < s_1, s_2 < K$, and $Km + s_1, Km + s_2 \nmid N$ for $m = 0, 1, 2, \ldots, T$, then neither of these cases can hold if $TB^4KF_1\bar{F}_2\bar{F}_3\bar{F}_6 > N$. Since, in most cases, this inequality can be satisfied when we are dealing with a value for N that is not too large, we will devote the rest of this paper to a discussion of the four remaining cases.

For another pair of cases we have

$$p_1 \equiv \pm N \pmod{q_4F_4}, \quad p_2 \equiv \pm 1 \pmod{q_4F_4},$$
$$p_1 \equiv 1 \pmod{q_3F_3}, \quad p_2 \equiv N \pmod{q_3F_3},$$
$$p_1 \equiv -1 \pmod{q_6F_6}, \quad p_2 \equiv -N \pmod{q_6F_6},$$

and we put $E = \bar{F}_2$. In the last pair of cases we have

$$p_1 \equiv \pm N \pmod{q_4F_4}, \quad p_2 \equiv \pm 1 \pmod{q_4F_4},$$
$$p_1 \equiv -N - 1 \pmod{F_3}, \quad p_2 \equiv -N - 1 \pmod{F_3},$$
$$p_1 \equiv -N + 1 \pmod{F_6}, \quad p_2 \equiv N - 1 \pmod{F_6},$$

and we put $E = \bar{F}_2\bar{F}_6$. For all of these cases we see that

$$p_1 \equiv -p_2 \pmod{E}^*$$

and in each of them we can find r_1, r_2 such that $p_1 \equiv r_1, p_2 \equiv r_2 \pmod{K}$ and $0 < r_1, r_2 < K$. Thus, if N is composite,

$$N = (m_1K + r_1)(m_2K + r_2)$$

for some nonnegative integers m_1 and m_2.

We will assume that $m_1 \geqslant m_2$. We have

$$M = (N - r_1r_2)/K = m_1m_2K + r_1m_2 + r_2m_1;$$

* An analogous theory to that given below can also be developed for $E = \bar{F}_1$ in the second pair of cases and $E = \bar{F}_1\bar{F}_3$ in the last pair of cases.

hence, $r_1 m_2 + r_2 m_1 \equiv M \pmod{K}$. Since $m_1 \geqslant m_2$, we get $m_1 - m_2 = M_1 + sE$, where $s \geqslant 0$, $M_1 \equiv r_2^{-1} M \pmod{E}$ and $0 \leqslant M_1 < E$. It follows that $m_1 m_2 > m_2 sE$. Since $p_1 p_2 > m_1 m_2 K^2$ and $N < lK^3$, we see that if $m_2 sE > lK$, we have a contradiction.

We attempt to show that $m_2 sE > lK$. This can usually be done on a fast computer as long as $lK/E < 10^{20}$. We do this by first finding G a factor of K/E such that $(G, E) = 1$ and $EG > lK/L$, where L is some preselected integer such that $L^3 > lK/E > N/EK^2$. We use three algorithms to show that $m_2 sE > lK$. The first algorithm determines that either $m_2 > L$ or N is composite, the second algorithm determines that $s > L$ or N is composite, and the third algorithm determines that either s or $m_2 \geqslant G$ or N is composite.

Once these algorithms have been employed we know that N is composite or that m_1 cannot exceed or equal m_2. If the latter occurs, we interchange the values of r_1 and r_2 and use the algorithms again. This will show that N is either composite or m_2 cannot exceed or equal m_1. If this latter case occurs, we see that

$$N \neq (Km_1 + r_1)(Km_2 + r_2).$$

We repeat this entire procedure for each of the four possible pairs (r_1, r_2). After this has all been done, we will know whether or not N is a prime.

4. Algorithm to Show that s and m_2 Exceed L. We first verify that $Km_2 + r_2 \nmid N$ for all m_2 such that $0 \leqslant m_2 \leqslant [l]$.** Then, since $m_1 m_2 < lK$, we have $m_1 < K$. Since

$$m_1 r_2 + m_2 r_1 \equiv M \pmod{K},$$

we have $m_1 = A_1 m_2 + A_2 - \nu K$, where

$$A_1 \equiv -r_2^{-1} r_1 \pmod{K} \quad (0 \leqslant A_1 < K),$$
$$A_2 \equiv M r_2^{-1} \pmod{K} \quad (0 \leqslant A_2 < K).$$

Put

$$\nu_1 = [(A_1 + A_2)/K], \qquad \mu_1 = A_1 + A_2 - \nu_1 K,$$

and define

$$\mu_{k+1} = \mu_k + A_1 - \epsilon_k K, \qquad \nu_{k+1} = \nu_k + \epsilon_k,$$

where

$$\epsilon_k = \begin{cases} 0 & \text{when } \mu_k < K - A_1, \\ 1 & \text{when } \mu_k \geqslant K - A_1. \end{cases}$$

If $k = m_2$, then $\nu_k = \nu$ and $\mu_k = m_1$.

Now since $M = m_1 m_2 K + r_1 m_2 + r_2 m_1$, we have

$$(M - A_2 r_2)/K = A_1 m_2^2 + m_2(A_2 + (A_1 r_2 + r_1)/K) - \nu(m_2 K + r_2).$$

**We use the notation $[\alpha]$ to denote the largest integer which is less than or equal to α.

Let Π be a set of about 30 small primes such that if $\pi \in \Pi$, then $\pi \nmid K$. For each of these $\pi_i \in \Pi$ put

$$a_i \equiv K^{-1}A_1 \pmod{\pi_i},$$
$$b_i \equiv K^{-1}(A_2 + (A_1r_2 + r_1)/K) \pmod{\pi_i},$$
$$c_i \equiv -K^{-1}(M - A_2r_2)/K \pmod{\pi_i},$$
$$d_i \equiv K^{-1}r_2 \pmod{\pi_i},$$

where $0 \leqslant a_i, b_i, c_i, d_i < \pi_i$. Tabulate modulo π_i the values of

$$f_{i,k} \equiv (a_ik^2 + b_ik + c_i)(k + d_i)^{-1} \pmod{\pi_i}$$

for all values of $k \pmod{\pi_i}$ except $k \equiv -d_i \pmod{\pi_i}$. We note that if $m_2 \equiv k \pmod{\pi_i}$, then $\nu \equiv f_{i,k} \pmod{\pi_i}$.

To determine that $m_2 > L$ we simply calculate each ν_k for $k = 1, 2, 3, \ldots, L$, and find some π_i such that $\nu_k \not\equiv f_{i,k} \pmod{\pi_i}$. If, for some value of k, $\nu_k \equiv f_{i,k} \pmod{\pi_i}$ for each $\pi_i \in \Pi$, trial divide N by $r_2 + kK$. If $r_2 + kK$ divides N, N is composite.

In order to show that $s > L$ we use the result

$$m_1 = M_1 + m_2 + sE$$

together with

$$N = K^2m_1m_2 + Kr_2m_1 + Kr_1m_2 + r_1r_2.$$

If we put $X = Km_2$ and substitute for m_1 in the formula for N, we get

$$N = X^2 + X(KM_1 + KEs + r_1 + r_2) + KM_1r_2 + KEr_2s + r_1r_2.$$

Since X is an integer, we must have

$$h(s) = (KM_1 + KEs + r_1 + r_2)^2 - 4(KM_1r_2 + KEr_2s + r_1r_2 - N)$$
$$= (KM_1 + r_1 - r_2 + KEs)^2 + 4N,$$

a perfect integer square.

In order to show that $h(s)$ is not a perfect square for any nonnegative $s \leqslant L$, we select $\pi \in \Pi$ and find those values of $s \pmod{\pi}$ such that $(h(s)|\pi) = -1$ (Legendre symbol) and then eliminate all such $s \leqslant L$. We then take another prime from Π and eliminate more s values. We continue sieving in this way until all values of $s \leqslant L$ have been eliminated. If there are still some s values left over after all the $\pi \in \Pi$ have been used, then some further primes can be used. If after this there is still a value of s which is not eliminated, $h(s)$ may be a perfect square. Find $Y = \sqrt{h(s)}$. If Y is an integer, then since $KM_1 + KEs + r_1 - r_2 < N$, we must have $Y - KM_1 + r_2 - r_1 - KEs > 2$, and N is composite.

5. Some Results Concerning m_2. We must now devise a technique to show that $s \geqslant G$ or $m_2 \geqslant G$. In order to do this we require some preliminary results, which we will develop in this section.

We first find λ, κ such that $0 \leqslant \lambda, \kappa < G$ and $s \equiv \lambda m_2 + \kappa \pmod{G}$. Since $m_1 r_2 + m_2 r_1 \equiv M \pmod{G}$ and $m_1 = M_1 + m_2 + sE$, we have

$$\lambda \equiv -(r_2 E)^{-1}(r_1 + r_2) \pmod{G},$$
$$\kappa \equiv (r_2 E)^{-1}(M - r_2 M_1) \pmod{G}.$$

Select a factor H of K/EG such that $(H, G) = 1$ $(H^2 \approx G)$ and then determine α, β such that $0 \leqslant \alpha, \beta < H$ and $u = \alpha m_2 + \beta \pmod{H}$, where $s = \lambda m_2 + \kappa - uG$. By using the formulas above, we get

$$\alpha \equiv (r_2 EG)^{-1}(r_1 + r_2 + r_2 E\lambda) \pmod{H},$$
$$\beta \equiv (r_2 EG)^{-1}(r_2 E\kappa + r_2 M_1 - M) \pmod{H}.$$

Our method of showing that either $s \geqslant G$ or $m_2 \geqslant G$ consists of assuming that s, $m_2 < G$ and determining that this cannot be so. Under our assumption we have $0 \leqslant L < \lambda m_2 + \kappa - Gu < G$ and $u = \alpha m_2 + \beta - vH$; consequently, $\rho m_2 + \sigma < v < \rho m_2 + \sigma + 1/H$, where $\rho = (G\alpha - \lambda)/GH$, $\sigma = (G\beta - \kappa)/GH$. It follows that if $H \geqslant 2$, then $v = [\rho m_2 + \sigma] + 1$. Denoting by $\{\gamma\}$ the value of $\gamma - [\gamma]$, we must have $1 > \{\rho m_2 + \sigma\} > 1 - 1/H$.

If $m_2 = h + kH$, then $k \leqslant [G/H]$ and $0 \leqslant h < H$. Also, $\{\rho m_2 + \sigma\} = \{\{\rho h + \sigma\} + 1 - \{\lambda k/G\}\}$. We now have two cases.

Case 1. $\{\rho k + \sigma\} \geqslant \{\lambda k/G\}$. In this case we have

$$\{\rho m_2 + \sigma\} = \{\rho h + \sigma\} - \{\lambda k/G\}.$$

If $\{\rho h + \sigma\} \leqslant 1 - 1/H$, then so is $\{\rho m_2 + \sigma\}$. If $\{\rho h + \sigma\} > 1 - 1/H$ and $\{\rho m_2 + \sigma\} > 1 - 1/H$, we must have $\{k\lambda/G\} < 1/H$. If we find all pairs (h, k) such that $0 \leqslant h < H$, $\{\rho h + \sigma\} > 1 - 1/H$, $0 \leqslant k \leqslant [G/H]$, and $\{k\lambda/G\} < 1/H$ and verify for each such pair that $Km_2 + r_2 \nmid N$ for $m_2 = h + kH$, we will see that Case 1 cannot occur.

Case 2. $\{\rho h + \sigma\} < \{\lambda k/\sigma\}$. Here we have

$$\{\rho m_2 + \sigma\} = \{\rho h + \sigma\} - \{k\lambda/G\} + 1;$$

thus, if $\{\rho m_2 + \sigma\} > 1 - 1/H$, we find that

$$\{\rho h + \sigma\} < \{k\lambda/G\} < \{\rho h + \sigma\} + 1/H.$$

If we find all pairs (h, k) such that this is so and verify that $Km_2 + r_2 \nmid N$ for $m_2 = h + Hk$, we will see that Case 2 cannot occur.

In order to eliminate Case 1 or Case 2, we must begin by sorting the lists $\{\rho h + \sigma\}$ $h = 0, 1, 2, 3, \ldots, H-1$, and $\{k\lambda/G\}$, $k = 0, 1, 2, 3, \ldots, [G/H]$. We make use of the following theorem (see, for example, Slater [3]).

THEOREM. *If the list* $\{k\theta\}$, *where* $0 < \theta < 1$, $k = 1, 2, 3, \ldots, n$, *is sorted in ascending order, the interval* $[0, 1]$ *is partitioned into only three distinct lengths. These are given by* $x = \{a\theta\}$, $y = 1 - \{b\theta\}$, $z = x + y$, *where* $\{a\theta\}$ *is the minimum element of the list and* $\{b\theta\}$ *is the maximum.*

We call the integers a, $-b$, $a - b$ the *integers corresponding* to x, y, z, respectively In [3] a fast and simple algorithm, which uses continued fractions, is given for calculating a and b when θ is rational or irrational.

6. An Algorithm to Show that m_2 or $s \geqslant G$. Find, by searching the list $\{\rho h + \sigma\}$, $h = 0, 1, 2, \ldots, H-1$, that integer η such that $\{\rho\eta + \sigma\}$ is the least element of the list. Let P be the positive remainder on dividing $(G\alpha - \lambda)\eta + G\beta - \kappa$ by GH: then $\{\rho\eta + \sigma\} = P/GH$. Let the three lengths for $\theta = \rho$, $n = H$ be x_1, y_1, z_1 with corresponding integers $a_1, -b_1, a_1 - b_1$. If t is any of these lengths, we can write it as Γ/GH for an integer Γ; for, if γ is the integer corresponding to t, Γ is the positive remainder on dividing $\gamma(G\alpha - \lambda)$ by GH when $\gamma > 0$ and Γ is GH decreased by the remainder on dividing $|\gamma|(G\alpha - \lambda)$ by GH when $\gamma < 0$. Arrange the three possible Γ's into ascending order $\Gamma_1, \Gamma_2, \Gamma_3$ with corresponding integers $\gamma_1, \gamma_2, \gamma_3$.

Let the lengths for $\theta = \lambda/G$, $n = [G/H]$ be x_2, y_2, z_2 with corresponding integers $a_2, -b_2, a_2 - b_2$. As before, we can represent any length t as Δ/G, where Δ is an integer. Arrange the possible Δ's into ascending order $\Delta_1, \Delta_2, \Delta_3$ with corresponding integers $\delta_1, \delta_2, \delta_3$.

Let

$$\{\rho h + \sigma\} = C_h/GH \quad (0 < C_h < GH),$$
$$\{k\lambda/G\} = D_k/GH \quad (0 < D_k < GH).$$

For Case 1 we wish (h, k) such that $C_h/GH > 1 - 1/H$ and $D_k/GH < 1/H$, i.e. $C_h > GH - G$, $D_k < G$. In Case 2 we wish (h, k) such that $C_h < D_k < G + C_h$.

We put $h_0 = \eta$, $C_{h_0} = P$ and define

$$h_{i+1} = h_i + \gamma_l, \qquad C_{h_{i+1}} = C_{h_i} + \Gamma_l,$$

where l is the least of 1, 2, 3 such that $0 < h_{i+1} < H$. We also put $k_0 = a_2$, $D_{k_0} = DH$ and define

$$k_{j+1} = k_j + \delta_l, \qquad D_{k_{j+1}} = D_{k_j} + H\Delta_l,$$

where l is the least of 1, 2, 3 such that $0 < k_{j+1} \leqslant [G/H]$ and D is the remainder on dividing $a_2\lambda$ by G. We see that the list

$$C_{h_i}/GH, \qquad i = 0, 1, 2, \ldots, H-1,$$

is the same as the list $\{\rho h + \sigma\}$, $h = 0, 1, 2, \ldots, H-1$, arranged in ascending order; also, the list

$$D_{k_i}/GH, \qquad i = 0, 1, 2, \ldots, [G/H] - 1,$$

is the list $\{k\lambda/G\}$, $k = 1, 2, 3, \ldots, [G/H]$, arranged in ascending order.

Our algorithm is now easy to establish. Put $i = 0$ and find all D_{k_j} such that

$$(*) \qquad C_{h_i} < D_{k_j} < G + C_{h_i}.$$

At the same time save all k_t such that $D_{k_t} < G$ (include also 0 as a value for k_t). Store all the D_{k_j} and k_j values and verify that $K(h_i + Hk_j) + r_2 \nmid N$ (we will give in the next section a fast method for doing this). Next increase i by 1 and from among the stored D_{k_j} and newly created ones store only those D_{k_j} and k_j which satisfy (*) and verify that $K(h_i + Hk_j) + r_2 \nmid N$ for each pair (h_i, k_j). Continue this process until

$i > H - 1$. Store as well all h_q such that $C_{h_q} > GH - G$. Finally, determine for each pair (h_q, k_t) that $K(h_q + Hk_t) + r_2 \nmid N$ by trial division. This is not very time consuming as there are usually only a few of these pairs.

7. **A Method for Verifying that $K(h_i + Hk_j) + r_2 \nmid N$.** We give here a method which has proved to be very effective for determining that $K(h_i + Hk_j) + r_2 \nmid N$.

If $m_2 = h_i + Hk_j$ and $(m_2K + r_2)(m_1K + r_1) = N$, then, since $m_1 = M_1 + m_2 + sE$, $s = \lambda m_2 + \kappa - uG$, and $u = \alpha m_2 + \beta - vH$, we find

$$M - r_2M_1 - r_2E(\kappa - \beta G) = m_2(r_1 + KM_1 + KE(\kappa - \beta G) + r_2E(\lambda - G\alpha) + r_2) + m_2^2K(E(\lambda - G\alpha) + 1) + wm_2GEK + wr_2GE,$$

where $w = vH$. It follows that

$$w = ((G\alpha - \lambda)/G)m_2 - \frac{m_2}{GE} + \frac{\beta G - \kappa}{G} - \frac{r_1 + KM_1}{GEK} + \frac{M/GEK + r_1r_2/K^2GE}{m_2 + r_2/K}$$

$$= H(\rho m_2 + \sigma) - \frac{m_2}{GE} - \frac{r_1 + KM}{GEK} + \frac{M/GEK + r_1r_2/K^2GE}{m_2 + r_2/K}.$$

Since $v = [\rho m_2 + \sigma] + 1$ and $\{\rho m_2 + \sigma\} = \{\rho h + \sigma\} - \{\lambda k/\sigma\} + 1$, we see that

$$w - H(\rho m_2 + \sigma) = H(\{\lambda k/G\} - \{\rho h + \sigma\}) = D_{k_j}/G - C_{h_i}/G.$$

Thus,

$$D_{k_j} - C_{h_i} = -\frac{m_2}{E} - \frac{r_1 + KM_1}{EK} + \frac{M/EK + r_1r_2/K^2E}{m_2 + r_2/K}$$

$$= \left(\frac{M/EK}{m_2 + r_2/K} - \frac{m_2}{E}\right) - \frac{r_1}{EK} - \frac{M_1}{E} + \frac{r_1r_2}{K^2E(m_2 + r_2/K)}.$$

Now

$$0 < M_1/E \leqslant 1 - \frac{1}{E}, \quad 0 < \frac{r_1}{EK} < \frac{1}{E}, \quad 0 < \frac{r_1r_2}{K^2}\frac{1}{E(m_2 + r_2/K)} < \frac{r_1}{EK};$$

hence,

$$0 < \frac{M_1}{E} + \frac{r_1}{EK} - \frac{r_1r_2}{K^2E(m_2 + r_2/K)} < 1.$$

We must have

$$D_{k_j} - C_{h_i} = \left[\frac{M/EK}{m_2 + r_2/K} - \frac{m_2}{E}\right],$$

when $m_2 = h_i + k_jH$ and $Km_2 + r_2 \mid N$. To determine that $Km_2 + r_2 \nmid N$, compare $D_{k_j} - C_{h_i}$ to the computed value of $[(M/EK)/(m_2 + r_2/K) - m_2/E]$; only when they are a distance of 1 or less from each other do we need trial divide N by $Km_2 + r_2$. The advantage of this method is that M/EK is usually small enough to be stored on the computer as a double precision (or extended precision) floating point constant. Hence, these operations can be done using double (extended) precision arithmetic rather than multi-precise arithmetic.

When it is more desirable to use integer arithmetic, we note that

$$\frac{M/EK}{m_2 + r_2/K} = \frac{M/EK}{m_2}(1 + r_2/Km_2)^{-1} = \frac{M/EK}{m_2}\left(1 - \frac{r_2}{Km_2}\right) + \eta,$$

where $0 < \eta < Mr_2^2/EK^3m_2^3$. Since $m_2 > L$ and $L^3 > M/EK$, we see that $0 < \eta < 1$. Thus,

$$\frac{M/EK}{m_2 + r_2/K} - \frac{m_2}{E} - \frac{r_1}{EK} - \frac{M_1}{E} + \frac{r_1r_2}{K^2E(m_2 + r_2/K)}$$

$$= \left[\frac{[M/EK]}{m_2}\right] - \left[\frac{[Mr_2/EK^2]}{m_2^2}\right] - \left[\frac{m_2}{E}\right] + I,$$

where $|I| \leqslant 2$. We trial divide by $Km_2 + r_2$ only when $D_{k_i} - C_{h_i}$ is within 3 of

$$\left[\frac{[M/EK]}{m_2}\right] - \left[\frac{[Mr_2/EK^2]}{m_2^2}\right] - \left[\frac{m_2}{E}\right].$$

8. Some Examples. The above algorithms were implemented on an IBM/370-168 computer and run on 28 numbers supplied to the authors by John Brillhart. These numbers are pseudoprime divisors of various Lucas (l_n) and Fibonacci numbers (f_n). We give below some of the calculations performed on the number N given in Section 1.

Consider the case with N assumed to be p_1p_2 with

$$\begin{aligned}
p_1 &\equiv 1 \pmod{F_1}, & p_2 &\equiv 1 \pmod{F_1},\\
p_1 &\equiv -1 \pmod{F_2}, & p_2 &\equiv 1 \pmod{F_2},\\
p_1 &\equiv N \pmod{F_4}, & p_2 &\equiv 1 \pmod{F_4},\\
p_1 &\equiv 1 \pmod{F_3}, & p_2 &\equiv N \pmod{F_3},\\
p_1 &\equiv -1 \pmod{F_6}, & p_2 &\equiv -N \pmod{F_6},
\end{aligned}$$

$p_1 = m_1K + r_1$, $p_2 = m_2K + r_2$, $m_1 \geqslant m_2$. Here $E = 287804745$, and we selected $L = 1900000$, $l = 8$, $G = 77022424976$, $H = 253487$. With these values we found

$$\lambda = 17422150686,$$
$$\kappa = 45747446332,$$
$$\alpha = 86832,$$
$$\beta = 50918,$$
$$\eta = 226218,$$
$$P = 526817664872,$$

$$\Gamma_1 = 6149532242, \quad \Gamma_2 = 589944841356, \quad \Gamma_3 = 596094373598,$$
$$\gamma_1 = -30527, \quad \gamma_2 = 246350, \quad \gamma_3 = 215823,$$
$$\Delta_1 = 21636, \quad \Delta_2 = 300182, \quad \Delta_3 = 371818,$$
$$\delta_1 = -209354, \quad \delta_2 = 171493, \quad \delta_3 = -37861.$$

The computer was then able to verify in less than one minute that m_1 could not exceed or equal m_2. The other cases were also run and the number was found to be prime in about 35 minutes C.P.U. time.

Of the remaining 27 numbers the following 26 were proved prime. These are the large pseudoprime divisors of $f_{395}(60)$, $f_{401}(77)$, $f_{447}(58)$, $f_{463}(86)$, $f_{473}(88)$, $f_{475}(62)$, $f_{481}(72)$, $f_{487}(87)$, $f_{499}(89)$, $l_{387}(50)$, $l_{388}(65)$, $l_{392}(55)$, $l_{401}(71)$, $l_{403}(68)$, $l_{407}(54)$, $l_{416}(69)$, $l_{417}(55)$, $l_{436}(81)$, $l_{443}(85)$, $l_{446}(78)$, $l_{453}(50)$, $l_{458}(96)$, $l_{486}(68)$, $l_{487}(99)$, $l_{490}(56)$, $l_{494}(79)$. The numbers in the parentheses give the number of digits in the pseudoprime. Most of these were proved prime by using only the methods of [1], [5], and [6]; however, for the occasional number on which these methods did not suffice, the algorithms described above were used successfully.

Consider now the 121 digit number

$$N = 2^{400} - 593$$

$$= 258224987808690858965591917200301187432970579282922351283065936540647622016841194629645353280137831435903171972747492783.$$

With $B = 1.5 \times 10^8$ we have

$$F_1 = 2 \cdot 1384711,$$

$$F_2 = 2^4 \cdot 3^2 \cdot 3023 \cdot 23251093,$$

$$F_3 = 7 \cdot 2521 \cdot 2213647 \cdot 70792627,$$

$$F_4 = 2 \cdot 5 \cdot 13 \cdot 298013,$$

$$F_6 = 3 \cdot 19 \cdot 43.$$

In spite of the size of this number, the methods of [1], [5], [6] together with those given above suffice to demonstrate that N is a prime.

For the 65 digit pseudoprime divisor of l_{470}

$$N = 198099504767038917596358522238636063818278388463428292321898694 41,$$

we have with $B = 1.3 \times 10^9$

$$F_1 = 2^7 \cdot 5 \cdot 19 \cdot 37 \cdot 47 \cdot 139,$$

$$F_2 = 2 \cdot 3^3 \cdot 7,$$

$$F_3 = 13 \cdot 31 \cdot 73 \cdot 79,$$

$$F_4 = 2,$$

$$F_6 = 3.$$

For this number $l > N/K^3 \approx 9.2 \times 10^9$ is quite large. By using the methods described above it can be shown that N is either prime or at most the product of two primes p_1 and p_2 and that we have either

$$p_1 \equiv 1 \pmod{q_1F_1}, \quad p_2 \equiv 1 \pmod{q_1F_1},$$

$$p_1 \equiv 1 \pmod{q_3F_3}, \quad p_2 \equiv 1 \pmod{q_2F_2},$$

or

$$p_1 \equiv 1 \pmod{F_1}, \quad p_2 \equiv 1 \pmod{F_1},$$
$$p_1 \equiv -1 \pmod{F_2}, \quad p_2 \equiv 1 \pmod{F_2},$$
$$p_1 \equiv -N-1 \pmod{F_3}, \quad p_2 \equiv -N-1 \pmod{F_3}.$$

In the first case we see that

$$p_1 = 1 + m_1 q_1 q_3 F_1 \bar{F}_3, \quad p_2 = 1 + m_2 q_1 q_2 F_1 \bar{F}_2,$$

and one of m_1 or m_2 is even. For if m_1 and m_2 were both odd, then $2^8 \mid N-1$, which, since $2^7 \| N-1$, is impossible.*** Thus

$$N = p_1 p_2 > 2B^4 F_1^2 \bar{F}_2 \bar{F}_3 > N,$$

which is also not possible.

The second case is more difficult. We first find r_1 and r_2 such that $p_1 = r_1 + m_1 K$ and $p_2 = r_2 + m_2 K$ and put $E = F_1 \bar{F}_3$. Then

$$m_1 + m_2 = M_1 + sE,$$

where $M_1 \equiv r_1^{-1} M \pmod{E}$, $0 < M_1 < E$, and $M = (N - r_1 r_2)/K$. Let $L = 1.9 \times 10^6$ and verify that $h'(s) = (KM_1 + r_1 + r_2 + KEs)^2 - 4N$ is not a perfect square for all nonnegative $s \leqslant L$. If $m_1 > m_2$, then $m_1 > \frac{1}{2}LE$ and $p_2 > B^2 F_1 \bar{F}_2$; consequently,

$$p_1 p_2 > (\tfrac{1}{2}LEK) B^2 F_1 \bar{F}_2 > N.$$

If we assume that $m_2 > m_1$, the size of l in this case does not permit us to use the algorithm of Section 4 to show that $m_1 > L$. However, by using the result that $m_2 = A_1' m_1 + A_2' - \nu K$, where

$$A_1' \equiv -r_1^{-1} r_2, \quad A_2' \equiv r_1^{-1} M \pmod{K} \ (0 < A_1', A_2' < K),$$

together with $M = K m_1 m_2 + r_1 m_2 + r_2 m_1$, we find that

$$\nu = (A_1'/K) m_1 + A_2'/K - \frac{M/K}{K m_1 + r_1} - \frac{r_1 r_2}{K^2 (K m_1 + r_1)} + \frac{r_2}{K^2}.$$

Since ν is an integer,

$$\nu = \left[(A_1'/K) m_1 + A_2'/K - \frac{M/K^2}{m_1 + r_1/K} \right] + 1.$$

This gives us another method of calculating the value of ν_n in Section 4. We first compute the value I_n of

$$\left[(A_1'/K) n + A_2'/K - \frac{M/K^2}{n + r_1/K} \right];$$

then $\nu_n = I_n + 1$. We can eliminate each possible value of ν_n for $n = 0, 1, 2, 3, \ldots, L$, by using the second part of the algorithm of Section 4.

Another method of proceeding is to first trial divide N by $K m_1 + r_1$ for $m_1 = 0, 1, 2, \ldots, L'$. If $L' < m_1 \leqslant L$, we have

*** The authors are indebted to John Brillhart for this suggestion.

$$\frac{A_1'(L'+1)}{K} - \frac{M/K^2}{L'+1} < \nu < \frac{A_1'L}{K} - \frac{M/K^2}{L+1} + 1.$$

Since $m_2 = A_1'm_1 + A_2' - \nu K$ and $N = (Km_1 + r_1)(Km_2 + r_2)$, we can substitute for m_2 as was done in the development of the second algorithm in Section 4 to find that the expression $(A_1'r_2 - r_1 - KA_2' + K^2\nu)^2 + 4A_1'N$ must be a perfect square. We can easily eliminate all the possible values of ν between the bounds above by using the sieve method described previously.

These tests were implemented and it was found that

$$p_1p_2 > K^2m_1m_2 > \tfrac{1}{2}L^2K^2E > N;$$

hence, N is a prime.

9. Conclusion. On comparing the above methods to those given in [1] or previously, it is evident that the stress here has moved from positive tests for primality to more negative processes such as searching, sieving, and trial division. However, the greatly increased power of these methods to some extent makes up for this somewhat undesirable shift in emphasis. For example, consider the large prime divisor N of l_{470}. At the authors' request D. H. Lehmer very kindly consented to use the ILLIAC IV in an attempt to find more factors of $N \pm 1, N^2 + 1, N^2 \pm N + 1$ than those given in Section 8. After using 4.75 hours of C.P.U. time, no additional factor was found with B increased to 38269275600. The techniques mentioned in this paper seem currently to be the only way of dealing with such stubborn numbers.

Probabilistic techniques such as those of Solovay and Strassen [4] run very quickly and have none of the negative aspects mentioned above; however, such methods do not prove primality but only support the likelihood of primality. Perhaps the best hope lies with ideas advanced by Miller [2]. When one of the algorithms discussed in [2] is combined with an as yet unpublished result of P. Weinberger, a fairly good test for primality can be obtained. Unfortunately, the proof of this algorithm requires the unproved Extended Riemann Hypothesis.

In any case it appears to the authors that the techniques of the present work have been pushed about as far as possible and any further advance in the problem of primality testing will probably have to be made in an entirely different direction.

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

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

3. NOEL B. SLATER, "Gaps and steps for the sequence $n\theta$ mod 1," *Proc. Cambridge Philos. Soc.*, v. 63, 1967, pp. 1115–1123.

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

5. 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.

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