MATHEMATICS OF COMPUTATION, VOLUME 29, NUMBER 130
APRIL 1975, PAGES 620–647

New Primality Criteria and Factorizations of $2^m \pm 1$

By John Brillhart, D. H. Lehmer and J. L. Selfridge

Abstract. A collection of theorems is developed for testing a given integer N for primality. The first type of theorem considered is based on the converse of Fermat's theorem and uses factors of $N - 1$. The second type is based on divisibility properties of Lucas sequences and uses factors of $N + 1$. The third type uses factors of both $N - 1$ and $N + 1$ and provides a more effective, yet more complicated, primality test. The search bound for factors of $N \pm 1$ and properties of the hyperbola $N = x^2 - y^2$ are utilized in the theory for the first time.

A collection of 133 new complete factorizations of $2^m \pm 1$ and associated numbers is included, along with two status lists: one for the complete factorizations of $2^m \pm 1$; the other for the original Mersenne numbers.

1. Introduction. The theory of testing a given odd integer N for primality by some converse of Fermat's theorem, or by its generalization in Lucas sequences, was begun in 1876 by Lucas ([9], [10, p. 302]).

Since that time, this theory has gradually been developed by various writers (Proth [15], Lucas [11], Pocklington [14], Lehmer [6], [7], [8], Robinson [18], Brillhart and Selfridge [4], Williams and Zarnke [21], Riesel [17]) in the direction of reducing the amount of calculation needed to complete a primality test on N.

In Sections 2 through 7 of the present paper, this purpose is carried considerably further. The contents of these sections are the following:

Section 2 contains two theorems in which $N - 1$ is completely factored. Theorem 1 was given earlier in [4]. Theorem 2, which is somewhat unfamiliar, is an improvement on Theorem 1 (see Kraitchik [5]). In the latter theorem, the condition $a^{(N-1)/2} \equiv -1 \pmod N$ is used (see [18]) rather than the usual test that N is a "pseudoprime base a."

Section 3 contains five theorems and three corollaries which use only partial factorizations of $N - 1$. Theorem 3 is a strengthening of a theorem of Proth [15]. Theorem 4 and Corollary 1 are familiar. Theorem 5 is new and is an advance over the old theory in that the factored portion of $N - 1$ need only be about $N^{1/3}$ before the primality test can be completed. Corollary 3 brings the direct search bound for factors of $N - 1$ into the theory for the first time. Theorem 7 uses this bound to construct an improved version of Theorem 5. Ordinarily, representing N numerically as a difference of squares is used for

Received January 28, 1974.

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

Key words and phrases. Primality testing, factorization of $2^m \pm 1$, Lucas sequences, converse of Fermat's theorem.

the purpose of factoring a composite N. However, this representation is used in a new way to establish the primality test in Theorem 7. It also appears indirectly in the proofs of Theorems 5, 17, and 19.

Section 4 contains a resume of properties of Lucas sequences that are needed for the theoretical developments in Sections 5–7.

Sections 5 and 6 exactly parallel Sections 2 and 3 in that they contain comparable theorems in which factors of $N + 1$ are used instead of those of $N - 1$. That such a parallel development is possible rests on Theorem 16, which is due to Michael Morrison [12]. The discovery of this theorem came as a surprise, since, previously, it had been thought that the theory using the factors of $N + 1$ was considerably more complicated.

Section 7 contains two theorems and a corollary which utilize factorizations of both $N - 1$ and $N + 1$. A considerable advantage is gained thereby since the amount of factorization needed to test N for primality is substantially reduced. Theorem 21 is unusual in that it does not deal directly with the prime factors of $N \pm 1$, but rather with the primes dividing algebraic factors of these numbers.

The final section of the paper contains a discussion of numerical results, a listing of which is given in three tables. In particular, 133 complete factorizations of $2^m \pm 1$ and associated numbers are given, along with a status table showing which numbers of these forms have been completely factored. A current status table for the Mersenne numbers $2^p - 1$, $p \leqslant 257$, is also included.

It should be noted that many of the theorems in this paper are stated in more detail and generality than may be needed for some applications. In such applications, some of the variables can be set to their minimum values, and minor terms can often be dropped. The generality in the theorems may be of use in certain cases and has been given to delimit more carefully the theoretical results.

2. **Theorems Requiring a Complete Factorization of $N - 1$.** As it sometimes happens, a complete factorization of $N - 1$ can be found without difficulty. For example, if N has a special form such as $N = 3 \cdot 2^m + 1$, or if by chance $N - 1$ possesses only small prime factors which can be discovered almost immediately by direct search, the complete factorization is at hand. In these cases, because of the uncomplicated nature of the theorems in this section, as well as Theorem 3 in the next section, a simple program can be written to carry out the primality testing which does not require much memory space. Such a program, however, requires more running time than one based on later sections, but may be more suitable for use in small computers where memory space is limited (see Selfridge and Guy [20]).

By way of notation, the symbol N will denote an odd integer > 1, and p, q, and n (as well as p_i, q_i, and n_i) will denote primes throughout the rest of this paper. The expression "N is a psp base a" will be used for a number N which satisfies the congruence $a^{N-1} \equiv 1 \pmod{N}$, $1 < a < N - 1$, i.e., N is a "pseudoprime" base a. (Since a is chosen in advance, it is extremely rare that N is composite when it is found to be a psp base a.)

THEOREM 1. *Let $N - 1 = \Pi p_i^{\alpha_i}$. If for each p_i there exists an a_i such that N is a psp base a_i, but $a_i^{(N-1)/p_i} \not\equiv 1 \pmod{N}$, then N is prime.*

Proof. Let e_i be the order of $a_i \pmod{N}$. Since $e_i \mid N - 1$, but $e_i \nmid (N-1)/p_i$, then $p_i^{\alpha_i} \mid e_i$. But for each i, $e_i \mid \phi(N)$, so that $p_i^{\alpha_i} \mid \phi(N)$, which implies $N - 1 \mid \phi(N)$. Hence, N is prime. Q.E.D.

Remarks. 1. Theorem 1 indicates that if for any p_i a base a_i can be found for which both hypotheses are satisfied, then that p_i is settled once and for all. (See [4, p. 89].) This is in contrast to the somewhat less satisfactory situation in earlier theorems (see Lehmer [6] and Lucas [11]) where a single base a is used for which the hypotheses must be satisfied for *all* p_i.

2. The computations for each p_i can be done efficiently by calculating

$$a_i^{(N-1)/p_i} \equiv b_i \not\equiv 1 \pmod{N}, \quad \text{and then} \quad b_i^{p_i} \equiv 1 \pmod{N}. \tag{1}$$

3. In practice a good strategy for choosing the a_i is the following:

(i) Find a_1 by the quadratic reciprocity law so that $(a_1/N) = -1$.

(ii) Use a_1 for successive p_i as long as (1) is satisfied. (For each p_i for which the base is not changed, it is of course not necessary to compute the second part of (1).)

(iii) Whenever (1) is not satisfied, change the base according to (i), returning to a previous base, if possible, to avoid having to recompute the second part of (1).

The next theorem is an improvement over Theorem 1 in that slightly less calculation is required to complete the primality test.

THEOREM 2. *Let $N - 1 = \Pi p_i^{\alpha_i}$. If for each p_i there exists an a_i such that*

$$a_i^{(N-1)/2} \equiv -1 \pmod{N}, \tag{2}$$

but (for $p_i > 2$),

$$a_i^{(N-1)/2p_i} \not\equiv -1 \pmod{N}, \tag{3}$$

then N is prime.

Proof. Congruence (2) implies N is a psp for each base a_i. For each $p_i > 2$, if $a_i^{(N-1)/2p_i} \equiv b_i \pmod{N}$, then $a_i^{(N-1)/p_i} \equiv b_i^2 \not\equiv 1 \pmod{N}$; for, if $b_i^2 \equiv 1 \pmod{N}$ for some i, then, since p_i is odd, $-1 \equiv a_i^{(N-1)/2} \equiv b_i^{p_i} \equiv b_i \pmod{N}$, which contradicts (3). Hence, N is prime by Theorem 1. Q.E.D.

3. **Theorems in Which $N - 1$ is Partially Factored.** In the special case where a prime factor of $N - 1$ exceeds $\sqrt{N}/2 - 1$, the next theorem, which is a strengthening of a theorem of Proth [15], provides a primality test involving less computing than Theorem 2.

THEOREM 3. *Let $N - 1 = mp$, where p is an odd prime such that $2p + 1 > \sqrt{N}$.*

If there exists an a for which $a^{(N-1)/2} \equiv -1 \pmod N$, *but* $a^{m/2} \not\equiv -1 \pmod N$, *then N is prime.*

Proof. Let e be the order of $a \pmod N$. Then $e \mid N - 1$. But, using the same argument as in the proof of Theorem 2, $a^m \not\equiv 1 \pmod N$, so $e \nmid (N-1)/p$. Hence, $p \mid e$, and since $e \mid \phi(N)$, then $p \mid \phi(N)$. Also,

$$\phi(N) | N\Pi(n_i - 1) = (mp + 1)\Pi(n_i - 1),$$

so $p \mid \Pi(n_i - 1)$, or $p \mid n_i - 1$ for some i, say $i = 1$. Thus, $n_1 \equiv 1 \pmod{2p}$. But $N \equiv 1 \pmod{2p}$, which implies $N/n_1 \equiv 1 \pmod{2p}$. On the other hand, since $n_1 \geqslant 2p + 1 > \sqrt{N}$, then $1 \leqslant N/n_1 < \sqrt{N} < 2p + 1$. Therefore, the only possibility for N/n_1 is 1, so N is prime. Q.E.D.

Remark. This theorem reduces the amount of testing because the prime factors of m can be ignored. Also, note that p need not be the largest prime divisor of $N - 1$, as $N = 31$ and $p = 3$ shows.

Throughout the rest of this paper the notation $N - 1 = F_1 R_1$ will be used, where F_1 is the even factored portion of $N - 1$, R_1 is > 1, and $(F_1, R_1) = 1$.

THEOREM 4 (POCKLINGTON [14]). *If for each prime p_i dividing F_1 there exists an a_i such that N is a psp base a_i and* $(a_i^{(N-1)/p_i} - 1, N) = 1$, *then each prime divisor of N is* $\equiv 1 \pmod{F_1}$.

Proof. Let n be a prime divisor of N, and e_i be the order of $a_i \pmod n$. Then $e_i | n - 1$. Also, $a_i^{N-1} \equiv 1 \pmod n$, so $e_i \mid N - 1$. On the other hand, $(a_i^{(N-1)/p_i} - 1, n) = 1$, so $e_i \nmid (N-1)/p_i$, which implies $p_i^{\alpha_i} \mid e_i$, where $p_i^{\alpha_i} \| F_1$. Hence, for each i, $p_i^{\alpha_i} | n - 1$, so that $F_1 \mid n - 1$. Q.E.D.

Remark (R. DeVogelaere). In verifying the hypotheses of this theorem, only one GCD computation is necessary: First find an a_i such that $a_i^{(N-1)/p_i} - 1 \equiv b_i \not\equiv 0 \pmod N$ for each i; then calculate the product $\Pi\, b_i \equiv c \pmod N$; and finally, if $c \neq 0$, compute $d = (c, N)$.

If $d \neq 1$, then N is composite and a factor has been found. Also, if $c = 0$, then some b_i has a prime factor in common with N.

For convenience of reference put:

(I) *For each prime p_i dividing F_1 there exists an a_i such that N is a psp base a_i and* $(a_i^{(N-1)/p_i} - 1, N) = 1$.

COROLLARY 1. *Assume* (I). *If* $F_1 > \sqrt{N}$, *then N is prime.*

Remark. Corollary 1 is an improvement over Theorem 2 in that the primality test can be completed as soon as the factored part of $N - 1$ exceeds the unfactored part. This saving in time is offset only to a slight degree by the amount of computing needed to calculate the required GCD's. It will be the main goal of the rest of this paper to continue to reduce the amount of auxiliary factorization, as in this case, through the introduction of various conditions which require a small amount of computing time as compared to the factoring time eliminated. In this regard, the next theorem is a considerable improvement on Corollary 1, since $N - 1$ need only be factored to the point where $F_1 > (N/2)^{1/3}$ rather than $F_1 > \sqrt{N}$. A further reduction is possible if m is chosen to be > 1. The cost of this reduction is at most the time needed to calculate $(r^2 - 8s)^{1/2}$ and the trial division of $\lambda F_1 + 1$ into N for $m - 1$ values of λ.

THEOREM 5. *Assume* (I) *and let* m *be* $\geqslant 1$. *When* $m > 1$, *assume further that* $\lambda F_1 + 1 \nmid N$ *for* $1 \leqslant \lambda < m$. *If*

$$N < (mF_1 + 1)[2F_1^2 + (r - m)F_1 + 1], \tag{4}$$

where r *and* s *are defined by* $R_1 = (N - 1)/F_1 = 2F_1 s + r$, $1 \leqslant r < 2F_1$, *then* N *is prime if and only if* $s = 0$ *or* $r^2 - 8s \neq \square$. ($r \neq 0$ *since* R_1 *is odd.*)

Proof. The theorem will be proved in the equivalent form: N is composite if and only if $s \neq 0$ and $r^2 - 8s = \square$.

(i) ($\Rightarrow$). From Theorem 4 it follows that all factors of N are 1 (mod F_1). Thus, since N is composite,

$$N = (cF_1 + 1)(dF_1 + 1), \qquad c, d \geqslant m. \tag{5}$$

Also, R_1 is odd and F_1 is even, so the equation

$$R_1 = (N - 1)/F_1 = cdF_1 + c + d \tag{6}$$

implies that $c + d$ is odd, so cd is even. Hence, from

$$cdF_1 + c + d = R_1 = 2F_1 s + r \tag{7}$$

it follows that

$$c + d \equiv r \pmod{2F_1}, \tag{8}$$

where $c + d - r \geqslant 0$, since r is the least positive remainder (mod $2F_1$). On the other hand, $(c - m)(d - m) \geqslant 0$ implies $cd \geqslant m(c + d) - m^2$, so that

$$\begin{aligned}(mF_1 + 1)[2F_1^2 + (r - m)F_1 + 1] > N &= cdF_1^2 + (c + d)F_1 + 1 \\ &\geqslant [m(c + d) - m^2]F_1^2 + (c + d)F_1 + 1 \\ &= (mF_1 + 1)\{[(c + d) - m]F_1 + 1\}.\end{aligned}$$

Thus, $2F_1^2 + (r - m)F_1 + 1 > [(c + d) - m]F_1 + 1$, or $c + d - r < 2F_1$. Combining this result with (8) gives $c + d = r$. Thus, from (7) it follows that $2s = cd \neq 0$. Finally, $r^2 - 8s = (c + d)^2 - 4cd = (c - d)^2$.

(ii) ($\Leftarrow$). With $s \neq 0$ and, say, $r^2 - 8s = t^2$, then

$$\begin{aligned}N = F_1 R_1 + 1 = F_1(2F_1 s + r) + 1 &= [(r^2 - t^2)F_1^2/4] + rF_1 + 1 \\ &= \left[\left(\frac{r - t}{2}\right)F_1 + 1\right]\left[\left(\frac{r + t}{2}\right)F_1 + 1\right],\end{aligned}$$

where the factors on the right are > 1, since $s \neq 0$. Q.E.D.

Remarks. 1. In the factorization in (ii), if $m > 1$, the two factors are prime; for if $N = (cF_1 + 1)(dF_1 + 1)(eF_1 + 1)$, where $c, d, e \geqslant m \geqslant 2$, then (4) is contradicted.

To see this, it is sufficient to consider the smallest values of the coefficients, i.e., when $c = d = e = m$. Then

$$N = (mF_1 + 1)^3 = (mF_1 + 1)[m^2F_1^2 + 2mF_1 + 1] \geqslant (mF_1 + 1)[4F_1^2 + 2mF_1 + 1]$$

$$> (mF_1 + 1)[2F_1^2 + (r + 2m)F_1 + 1] > (mF_1 + 1)[2F_1^2 + (r - m)F_1 + 1].$$

This argument does not hold when $m = 1$.

2. Note that the right side of (4) is composite, so the inequality is sharp. (Cf. [18, Theorem 10], where $F_1 = 2^n$.)

3. The choice of m in the hypothesis is arbitrary. It would usually be chosen large enough to ensure that (4) is satisfied. Increasing the size of m for this purpose, of course, must be weighed against further factoring of $N - 1$ to try to increase the size of F_1. Differentiating the right side, $f(m)$, of (4) with respect to the real variable m (with F_1 and r constant) gives the critical value $m = F_1 + r/2$. Thus, $1 \leqslant m \leqslant F_1 + r/2$ and the largest N that can be tested by Theorem 5 is less than the integer $f(F_1 + r/2) = (F_1^2 + rF_1/2 + 1)^2$.

4. The coefficient 2 in (4) arises because 2 divides cd in (6). In general, if it can be shown that some odd integer g also divides cd, then the coefficient 2 in (4) can be replaced by $2g$. The 2 in the definition of r and s must also be replaced by $2g$. For example, if $N \equiv -1 \pmod 3$, then in (5) one of the factors, say $cF_1 + 1$, must be $\equiv 1 \pmod 3$. Thus, $3 \mid cF_1$, and since $3 \nmid F_1$, $3 \mid c$, i.e., $3 \mid cd$.

Also, if $N \equiv -1 \pmod 5$, and it is known that 5 is a quadratic residue of N, then since $5 \nmid F_1$, $5 \mid cd$. If $N \equiv -1 \pmod 8$, and 2 is a quadratic residue of N, then $8 \mid cdF_1$. But since $N - 1 \equiv -2 \pmod 8$, $2 \parallel F_1$, which implies $4 \mid cd$ (instead of 2 dividing cd). Similarly, if $N \equiv 3 \pmod 8$, and -2 is a quadratic residue of N, then $8 \mid cdF_1$, $2 \parallel F_1$, and $4 \mid cd$.

It should be observed that the above conditions, when they hold, can be combined to give a larger leading coefficient in (4). (These observations are due to Michael Morrison.)

THEOREM 6. *Let n be a prime divisor of N. If N is a psp base a, and*

$$(a^{F_1} - 1, N) = 1, \tag{9}$$

then $n \equiv 1 \pmod p$, where p is some prime divisor of R_1 depending on n.

Proof. Let e be the order of $a \pmod n$. Then $e \mid n - 1$. Also, since N is a psp base a, it follows that $e \mid N - 1 = F_1R_1$. But from (9), $a^{F_1} \not\equiv 1 \pmod n$, so $e \nmid F_1$. Hence, $(e, R_1) > 1$, i.e., there exists a prime p such that $p \mid e$ and $p \mid R_1$. Thus, $p \mid n - 1$. Q.E.D.

For convenience of reference put:

(II) *For some a, N is a psp base a and* $(a^{(N-1)/R_1} - 1, N) = 1$.

Remark. The exponent in (II) has the same form as the exponent in (I), so in a program, (I) and (II) can be treated as a single test by considering R_1 as the final "prime" factor of $N - 1$.

COROLLARY 2. *Assume* (I) *and* (II), *and let* n *be a prime divisor of* N. *Then* $n \equiv 1 \pmod{pF_1}$, *where* p *is some prime divisor of* R_1 *depending on* n.

Proof. Since $(F_1, R_1) = 1$, the corollary follows from Theorems 4 and 6. Q.E.D.

COROLLARY 3. *Assume* (I) *and* (II). *If all the prime factors of* R_1 *are* $\geqslant B_1$ *and* $B_1F_1 > \sqrt{N}$, *then* N *is prime.*

Proof. From Corollary 2, $n - 1 \geqslant pF_1 \geqslant B_1F_1 > \sqrt{N}$, which implies N is prime. Q.E.D.

Remark. The new feature on Corollary 3 is that B_1 appears in the inequality for N. The number B_1 is quite different from F_1, since F_1 contains the "discovered" factors of $N - 1$, while B_1 gives the information (not immediately verifiable) that the prime factors of R_1 are greater than or equal to B_1. (This latter assumes that no factor of $N - 1$ has been overlooked, as it might be if the computer were not working properly.)

The next theorem, which improves on Corollary 3, uses formulas relating to the hyperbola $x^2 - y^2 = N$, in a way similar to what was done implicitly in the proof of Theorem 5.

LEMMA 1. *If either* $0 < a \leqslant b \leqslant \sqrt{N}$ *or* $\sqrt{N} \leqslant b \leqslant a$, *then* $b + N/b \leqslant a + N/a$.

Proof. The conclusion follows from $(a^{-1} - b^{-1})(N - ab) \geqslant 0$. Q.E.D

THEOREM 7. *Assume* (I) *and* (II), *and also that the prime factors of* R_1 *are* $\geqslant B_1$. *If*

$$N < (B_1F_1 + 1)[2F_1^2 + (r - B_1)F_1 + 1], \tag{10}$$

where r *and* s *are defined by* $R_1 = 2F_1s + r$, $1 \leqslant r < 2F_1$, *then* N *is prime if and only if* $s = 0$ *or* $r^2 - 8s \neq \square$.

Proof. The theorem will be proved in the equivalent form: N is composite if and only if $s \neq 0$ and $r^2 - 8s = \square$.

(i) ($\Rightarrow$). From Theorem 4 all the factors of N are $1 \pmod{F_1}$. Since N is composite, it can be written as $N = nw = x^2 - y^2 = (x - y)(x + y) = (cF_1 + 1)(dF_1 + 1)$, $c, d \geqslant 1$, where n is the *smallest* prime factor of N and $w > 1$. Then $N = cdF_1^2 + (c + d)F_1 + 1$ and $2x = (c + d)F_1 + 2$. But $R_1 = cdF_1 + c + d$, and since R_1 is odd and F_1 is even, then $c + d$ is odd, so that cd is even, say $cd = 2g$. Then $N = 2gF_1^2 + 2x - 1$, so $2x = F_1R_1 + 2 - 2gF_1^2 = F_1(2F_1s + r) + 2 - 2gF_1^2 = (s - g)2F_1^2 + rF_1 + 2$. Let $\lambda = s - g$. Then from $rF_1 + 2 \leqslant F_1(2F_1 - 1) + 2 \leqslant 2F_1^2$ it follows, since $x > 0$, that $0 < 2x = 2\lambda F_1^2 + rF_1 + 2 \leqslant 2F_1^2(\lambda + 1)$, so that $\lambda \geqslant 0$. On the other hand, $2x = n + w = n + N/n$, and from Corollary 2, $n \equiv 1 \pmod{pF_1}$, so $n \geqslant pF_1 + 1 \geqslant B_1F_1 + 1$. Hence, using Lemma 1 and (10), $2\lambda F_1^2 + rF_1 + 2 = 2x = n + N/n \leqslant (B_1F_1 + 1) + N/(B_1F_1 + 1) < (B_1F_1 + 1) + 2F_1^2 + (r - B_1)F_1 + 1 = 2F_1^2 + rF_1 + 2$. Consequently, $\lambda < 1$. Thus, $\lambda = 0$ and $rF_1 + 2 = 2x = (c + d)F_1 + 2$, which implies $r = c + d$. Then $2F_1s + r = R_1 = cdF_1 + c + d$ gives $2s = cd \neq 0$.

Finally, $r^2 - 8s = (c + d)^2 - 4cd = (c - d)^2$.

(ii) ($\Leftarrow$). The proof is the same as Theorem 5(ii). Q.E.D.

Remark. If it happens that R_1 is a pseudoprime but B_1 is not large enough for (10) to be satisfied, then a primality investigation can be carried out on R_1 itself (see Brillhart [3, p. 448]). If it can be shown that R_1 is prime, then the theorems of Section 2 can be used to show N is prime. If, however, it is difficult to show that R_1 is prime, Theorem 4 can at least be used (with the factors of $R_1 - 1$) to establish a lower bound for the prime factors of R_1, which, if it exceeds B_1, can replace B_1 in Theorem 7.

4. Lucas Sequences. The primality theory which was established in the preceding sections was based on factoring $N - 1$. In this section and the two that follow, a primality theory is developed which depends on factoring $N + 1$.

Central to the $N + 1$ theory are the divisibility properties of certain second order recurring sequences known as *Lucas* sequences. These properties, which contain Fermat's theorem as a special case, will be reviewed here along with several other results that apply to the later development. Some of the more familiar results will be given without proof (see Lucas [10]).

The Lucas sequences $\{U_k\}$ and $\{V_k\}$ are defined recursively by the formulas:

$$U_{k+2} = PU_{k+1} - QU_k, \quad k \geqslant 0, \quad U_0 = 0, \quad U_1 = 1,$$

$$V_{k+2} = PV_{k+1} - QV_k, \quad k \geqslant 0, \quad V_0 = 2, \quad V_1 = P,$$

where P and Q are integers such that $D = P^2 - 4Q \neq 0$. (In case several sequences, defined by P_i and Q_i, are used, the notation $\{U_k^{(i)}\}$ and $\{V_k^{(i)}\}$ will be employed.)

If α and β are the (unequal) roots of $x^2 - Px + Q = 0$, then the members of these sequences can be expressed in terms of α and β by the equations:

$$U_k = (\alpha^k - \beta^k)/(\alpha - \beta) \quad \text{and} \quad V_k = \alpha^k + \beta^k, \qquad k \geqslant 0.$$

From these formulas four useful identities can be derived:

$$U_{2k} = U_k V_k, \tag{11}$$

$$DU_k^2 = V_{2k} - 2Q^k, \tag{12}$$

$$V_k^2 - DU_k^2 = 4Q^k, \tag{13}$$

$$2V_{r+s} = V_r V_s + DU_r U_s. \tag{14}$$

In what follows the notation ϵ_t will be used for the value of the Jacobi symbol (D/t).

The main divisibility properties of these sequences are contained in the theorems and corollaries which follow.

THEOREM 8. (a) *If* $p \nmid 2Q$, *then* $U_{p-\epsilon_p} \equiv 0 \pmod p$.

(b) *If* $p \nmid 2QD$, *then* $V_{p-\epsilon_p} \equiv 2Q^{(1-\epsilon_p)/2} \pmod p$.

Remark. Theorem 8(a) is the generalization of Fermat's theorem mentioned earlier. As such, it could also be used as a test for compositeness: If $N \nmid Q$ and $N \nmid U_{N-\epsilon_N}$, then N is composite. (Fermat's theorem can be obtained from Theorem 8(a) in the following way: Let p be an odd prime such that $p \nmid a(a-1)$. Consider the Lucas sequence with $\alpha = a$ and $\beta = 1$, so $D = (a-1)^2$. Then $\epsilon_p = 1$ and $a^{p-1} - 1 = (a-1)U_{p-1} \equiv 0 \pmod p$.)

THEOREM 9. *If $p \nmid 2QD$, then $p \mid U_{(p-\epsilon_p)/2}$ if and only if $(Q/p) = 1$.*

Proof. Identity (12), Theorem 8(b), and Euler's criterion give

$$DU^2_{(p-\epsilon_p)/2} = V_{p-\epsilon_p} - 2Q^{(p-\epsilon_p)/2} \equiv 2Q^{(1-\epsilon_p)/2} - 2(Q/p)Q^{(1-\epsilon_p)/2}$$

$$= 2Q^{(1-\epsilon_p)/2}\{1 - (Q/p)\} \pmod p,$$

from which the theorem immediately follows. Q.E.D.

COROLLARY 4. *If $p \nmid 2QD$, then $p \mid V_{(p-\epsilon_p)/2}$ if and only if $(Q/p) = -1$.*

Proof. This follows from Theorem 8, (11), Theorem 9, and (13). Q.E.D.

From Corollary 4 a test for compositeness can also be obtained.

COROLLARY 5. *Suppose $N \nmid QD$ and that $(Q/N) = -1$. If $N \nmid V_{(N-\epsilon_N)/2}$, then N is composite.*

Remark. The residues of U_m and $V_m \pmod N$, which must be computed in these theorems, can be computed with about triple the work of computing a power $\pmod N$. An efficient method for calculating $V_m \pmod N$ is discussed in detail in Lehmer [8, p. 129]. To compute $U_m \pmod N$ one can use the formulas: $U_{2k} = U_k V_k$ and $V_{2k} = V_k^2 - 2Q^k$ for doubling the subscript, and $U_{2k+1} = (PU_{2k} + V_{2k})/2$ and $V_{2k+1} = (DU_{2k} + PV_{2k})/2$ for a "side-step" of 1. The sequence of doublings and side-steps to be followed is easily obtained from the binary expansion of m.

Theorem 8 shows that an odd prime p, not dividing Q, will divide at least one term of $\{U_k\}$, namely $U_{p-\epsilon_p}$. The least positive k such that $p \mid U_k$ is called the "rank of apparition" of p (or just "rank") and is denoted here by $\rho(p)$. (If several Lucas sequences $\{U_k^{(i)}\}$ are being employed, then $\rho_i(p)$ will denote rank in $\{U_k^{(i)}\}$.) This notation will also designate the rank of a composite number.

THEOREM 10. *Suppose $p \nmid 2Q$ and that $p^\alpha \| U_{\rho(p)}$, $\alpha \geqslant 1$. Then $p^{\alpha+\beta} \| U_{m\rho(p)}$ if and only if $p^\beta \| m$.*

Remark. If a prime p divides Q but does not divide P, then $p \nmid U_k$, $k \geqslant 1$.

When $(N, Q) = 1$, the following formula for $\rho(N)$ can be obtained from Theorems 8(a) and 10:

$$\rho(N) = \operatorname*{LCM}_{1 \leqslant i \leqslant s} [\rho(n_i) n_i^{\max(\gamma_i - \alpha_i, 0)}],$$

where $N = \prod_{i=1}^s n_i^{\gamma_i}$ and $n_i^{\alpha_i} \| U_{\rho(n_i)}$.

THEOREM 11. *Suppose $(N, Q) = 1$. Then*

(a) *$\rho(N)$ exists.*

(b) $N \mid U_k$ *if and only if* $\rho(N) \mid k$.

It will be convenient to introduce a function, similar to the Euler ϕ function, which will be of use in deriving the primality theorems.

Definition. If $(N, D) = 1$ and $N = \Pi_{i=1}^{s} n_i^{\gamma_i}$, let

$$\psi(N, D) = 2^{1-s} \prod_{i=1}^{s} (n_i - \epsilon_{n_i}) n_i^{\gamma_i - 1}.$$

(This function is not a generalization of the Euler function, because of the power of 2 in front of the product.)

THEOREM 12. *If* $(N, D) = 1$, *then* $\psi(N, D) = N - \epsilon_N$ *if and only if* N *is prime.*

Proof. ($\Leftarrow$). Clear from the definition of ψ.

($\Rightarrow$). The statement will be proved in the equivalent form:

If N is composite, then $\psi(N, D) \neq N - \epsilon_N$.

Case 1. $s = 1$, i.e., $N = n^\gamma$, $\gamma \geqslant 2$. *Then*

$$\psi(N, D) = (n - \epsilon_n) n^{\gamma - 1} = N - N\epsilon_n/n \neq N - \epsilon_N.$$

Case 2. $s \geqslant 2$. In this case

$$\psi(N, D) = 2 \prod_{i=1}^{s} \tfrac{1}{2}(n_i - \epsilon_{n_i}) n_i^{\gamma_i - 1} \leqslant 2 \prod_{i=1}^{s} \tfrac{1}{2}(n_i + 1) n_i^{\gamma_i - 1}$$

$$= 2N \prod_{i=1}^{s} \tfrac{1}{2}\left(1 + \frac{1}{n_i}\right) \leqslant 2N\left(\frac{2}{3}\right)\left(\frac{3}{5}\right) \cdots \leqslant \frac{4N}{5} < N - 1. \qquad \text{Q.E.D.}$$

COROLLARY 6. *If* $(N, D) = 1$, *then* $N - \epsilon_N \mid \psi(N, D)$ *implies that* N *is prime.*

Proof. If N is composite, then $\psi(N, D) < N - 1$ in Case 2 of the above proof. In Case 1, $N - \epsilon_N \mid N - N\epsilon_n/n$ implies $\epsilon_n = -1$. However, in that case $n^\gamma \pm 1 \mid n^\gamma + n^{\gamma-1}$, which is impossible when $\gamma \geqslant 2$. Q.E.D.

COROLLARY 7. *If* $(N, QD) = 1$, *then* $\rho(N) \mid \psi(N, D)$.

Proof. The condition $(N, QD) = 1$ implies N has a rank. Thus

$$\rho(N) = \underset{1 \leqslant i \leqslant s}{\mathrm{LCM}} \left[\rho(n_i) n_i^{\max(\gamma_i - \alpha_i, 0)}\right]$$

which divides

$$\underset{1 \leqslant i \leqslant s}{\mathrm{LCM}} \left[(n_i - \epsilon_{n_i}) n_i^{\gamma_i - 1}\right] = 2 \underset{1 \leqslant i \leqslant s}{\mathrm{LCM}} \left[\tfrac{1}{2}(n_i - \epsilon_{n_i}) n_i^{\gamma_i - 1}\right],$$

which divides

$$2 \prod_{i=1}^{s} \tfrac{1}{2}(n_i - \epsilon_{n_i}) n_i^{\gamma_i - 1} = \psi(N, D). \qquad \text{Q.E.D.}$$

5. **Theorems Requiring a Complete Factorization of** $N + 1$. With the preparation in the last section it is now possible to prove a collection of theorems based on the factorization of $N + 1$. These theorems, which are proved in this and the next section, exactly parallel Theorems 1–7.

LEMMA 2. *Let* $\{U_k\}$ *be a Lucas sequence for which* $(D/N) = -1$ *and* $N \mid U_{N+1}$.

Then $(N, QD) = 1$, $\psi(N, D)$ *is defined, and* N *has a rank which divides* $N + 1$.

Proof. Since the Jacobi symbol $(D/N) \neq 0$, it follows that $(N, D) = 1$. If there were a prime n dividing both N and Q, it would follow from $D = P^2 - 4Q$ that $n \nmid P$, since $n \nmid D$. But then the remark following Theorem 10 would imply n, and therefore N, has no rank, contrary to the fact that $N \mid U_{N+1}$. Therefore, $(N, Q) = 1$. The remainder of the conclusion follows from the definition of $\psi(N, D)$ and Theorem 11. Q.E.D.

THEOREM 13. *Let* $N + 1 = \Pi q_i^{\beta_i}$, *and consider the set* $\mathfrak{U}$ *of Lucas sequences* $\{U_k^{(i)}\}$ *with the given discriminant* D *for which the Jacobi symbol* $(D/N) = -1$. *If for each* q_i *there exists a Lucas sequence in* $\mathfrak{U}$ *such that* $N \mid U_{N+1}^{(i)}$, *but* $N \nmid U_{(N+1)/q_i}^{(i)}$, *then* N *is prime.*

Proof. It is clear from Lemma 2 that $\rho_i(N) \mid N + 1$. But $\rho_i(N) \nmid (N + 1)/q_i$, so $q_i^{\beta_i} \mid \rho_i(N)$. By Corollary 7, $\rho_i(N) \mid \psi(N, D)$ for all i. This implies $q_i^{\beta_i} \mid \psi(N, D)$. Thus, $N + 1 \mid \psi(N, D)$, so N is prime by Corollary 6. Q.E.D.

Remarks. 1. This theorem corresponds to Theorem 1 in that it allows for a change to another sequence with the same discriminant if $N \mid U_{(N+1)/q_i}^{(i)}$ for some q_i. As such, it constitutes an improvement over the earlier theorem in which a single sequence with $P = 1$ was employed (see [8, p. 128]).

2. From one Lucas sequence with P_1, Q_1, and D, another with the same D can be obtained by setting $P_2 = P_1 + 2$ and $Q_2 = P_1 + Q_1 + 1$. (It is necessary to check that $(N, Q_i) = 1$.)

The next theorem improves on Theorem 13 in that only V's (with smaller subscripts) are calculated in the primality test (see the remark following Corollary 5), (also see Theorem 3, p. 128 in [8]).

THEOREM 14. *Let* $N + 1 = \Pi q_i^{\beta_i}$ *and consider the set* $\mathfrak{V}$ *of Lucas sequences* $\{V_k^{(i)}\}$ *with the given discriminant* D *for which the Jacobi symbol* $(D/N) = -1$. *If for each* q_i *there exists a sequence in* $\mathfrak{V}$ *such that*

$$N \mid V_{(N+1)/2}^{(i)}, \tag{15}$$

but (for $q_i > 2$*)*

$$N \nmid V_{(N+1)/2q_i}^{(i)}, \tag{16}$$

then N *is prime.*

Proof. From (11) and (15) it follows for each i that $N \mid U_{N+1}^{(i)}$, so $\rho_i(N)$ exists and $\rho_i(N) \mid N + 1$ by Theorem 11(b). Also, for each $q_i > 2$, $N \nmid U_{(N+1)/q_i}^{(i)}$; for, if $N \mid U_{(N+1)/q_i}^{(i)}$ for some i, then from Theorem 11(b),

$$N \mid U_{s(N+1)/q_i}^{(i)}, \tag{17}$$

where $s = (q_i - 1)/2$. But then, using (15), (14), and (17), it follows that

$$0 \equiv 2V^{(i)}_{(N+1)/2} = 2V^{(i)}_{[s(N+1)/q_i + (N+1)/2q_i]}$$

$$= V^{(i)}_{s(N+1)/q_i} V^{(i)}_{(N+1)/2q_i} + DU^{(i)}_{s(N+1)/q_i} U^{(i)}_{(N+1)/2q_i}$$

$$\equiv V^{(i)}_{s(N+1)/q_i} V^{(i)}_{(N+1)/2q_i} \pmod{N}.$$

Now, $(N, V^{(i)}_{s(N+1)/q_i}) = 1$; for, if a prime divided both numbers, it would divide $U^{(i)}_{s(N+1)/q_i}$ by (17), and so by (13) would divide Q. But by Lemma 2, $(N, Q) = 1$. Hence, $N \mid V^{(i)}_{(N+1)/2q_i}$, which contradicts (16). Thus, N is prime by Theorem 13. Q.E.D.

6. Theorems in Which $N + 1$ is Partially Factored.

THEOREM 15. *Let $N + 1 = mq$, where q is an odd prime such that $2q - 1 > \sqrt{N}$. If there exists a Lucas sequence $\{V_k\}$ of discriminant D with $(D/N) = -1$ for which $N \mid V_{(N+1)/2}$, but $N \nmid V_{m/2}$, then N is prime.*

Proof. From (11) it follows that $N \mid U_{N+1}$, so $\rho(N)$ exists and $\rho(N) \mid N + 1$ by Theorem 11(b). Also, using the same argument as in the proof of Theorem 14, $N \nmid U_{(N+1)/q}$, so $\rho(N) \nmid (N + 1)/q$. Hence, $q \mid \rho(N)$, and since $\rho(N) \mid \psi(N, D)$ by Corollary 7, $q \mid \psi(N, D)$. But

$$\psi(N, D) \mid N \prod_{i=1}^{s} (n_i - \epsilon_{n_i}) = (mq - 1) \prod_{i=1}^{s} (n_i - \epsilon_{n_i}),$$

so $q \mid \prod_{i=1}^{s} (n_i - \epsilon_{n_i})$, or $q \mid n_i - \epsilon_{n_i}$ for some i, say $i = 1$. Thus $n_1 \equiv \epsilon_{n_1} \pmod{2q}$. Also, $N \equiv -1 \pmod{2q}$, so $N/n_1 \equiv -\epsilon_{n_1} \pmod{2q}$. But $n_1 \geqslant 2q - 1 > \sqrt{N}$, which implies $1 \leqslant N/n_1 < \sqrt{N} < 2q - 1$. Thus, the only possibility in the interval $[1, 2q - 1)$ is that $N/n_1 = 1$, i.e., N is prime. Q.E.D.

Throughout this section the notation $N + 1 = F_2R_2$ will be used, where F_2 is the even factored portion of $N + 1$, R_2 is > 1, and $(F_2, R_2) = 1$.

THEOREM 16 (MORRISON [12]). *Consider the set $\mathcal{U}$ of Lucus sequences $\{U^{(i)}_n\}$ with the given discriminant D for which $(D/N) = -1$. If for each prime q_i dividing F_2 there exists a Lucas sequence in $\mathcal{U}$ such that $N \mid U^{(i)}_{N+1}$ and $(U^{(i)}_{(N+1)/q_i}, N) = 1$, then each prime divisor n of N is $\equiv \epsilon_n \pmod{F_2}$.*

Proof. It is clear from Lemma 2 that $\rho_i(N) \mid N + 1$, which implies $\rho_i(n) \mid N + 1$. Since $n \nmid U^{(i)}_{(N+1)/q_i}$, Theorem 11(b) implies $\rho_i(n) \nmid (N + 1)/q_i$. Thus, $q_i^{\beta_i} \mid \rho_i(n)$, where $q_i^{\beta_i} \parallel F_2$. Also, $\rho_i(n) \mid n - \epsilon_n$, so $q_i^{\beta_i} \mid n - \epsilon_n$ for all i, that is, $F_2 \mid n - \epsilon_n$. Q.E.D.

For convenience of reference put:

(III) *For each prime q_i dividing F_2 there exists a Lucas sequence $\{U^{(i)}_k\}$ with discriminant D for which $(D/N) = -1$, $N \mid U^{(i)}_{N+1}$, and $(U^{(i)}_{(N+1)/q_i}, N) = 1$.*

COROLLARY 8. *Assume* (III). *If $F_2 > \sqrt{N} + 1$, then N is prime.*

Proof. $n + 1 \geqslant n - \epsilon_n \geqslant F_2 > \sqrt{N} + 1$, which implies N is prime. Q.E.D.

In what follows the notation $\overline{F}_1 = F_1/2$ and $\overline{F}_2 = F_2/2$ will be used.

THEOREM 17. *Assume* (III) *and let m be $\geqslant 1$. When $m > 1$, then assume further* *that* $\lambda F_2 \pm 1 \nmid N$, $1 \leqslant \lambda < m$. *If*

$$N < (mF_2 - 1)[2F_2^2 + (m - |r|)F_2 + 1],$$

where r *and* s *are defined by* $R_2 = 2F_2 s + r$, $|r| < F_2$, *then* N *is prime if and only if* $s = 0$ *or* $r^2 + 8s \neq \square$.

Proof. The theorem will be proved in the equivalent form: N is composite if and only if $s \neq 0$ and $r^2 + 8s = \square$.

(i) $(\Rightarrow)$. Since $N \equiv -1 \pmod{F_2}$, it follows from Theorem 16 that $N = (cF_2 - 1)(dF_2 + 1)$, $c, d \geqslant m$. Also, R_2 is odd and F_2 is even, so the equation $R_2 = (N + 1)/F_2 = cdF_2 + c - d$ implies that $c - d$ is odd, so cd is even. Hence, from

$$cdF_2 + c - d = R_2 = 2F_2 s + r \tag{18}$$

it follows that

$$c - d \equiv r \pmod{2F_2}. \tag{19}$$

On the other hand, $(c - m)(d + m) \geqslant 0$ implies that $cd \geqslant (d - c)m + m^2$, so that

$$(mF_2 - 1)[2F_2^2 + (m - r)F_2 + 1] \geqslant (mF_2 - 1)[2F_2^2 + (m - |r|)F_2 + 1]$$

$$> N = cdF_2^2 + (c - d)F_2 - 1 \geqslant [(d - c)m + m^2]F_2^2$$

$$+ (c - d)F_2 - 1 = (mF_2 - 1)[(d - c + m)F_2 + 1].$$

Thus, $2F_2^2 + (m - r)F_2 + 1 > (d - c + m)F_2 + 1$, or

$$-2F_2 + r < c - d. \tag{20}$$

Also, $(c + m)(d - m) \geqslant 0$ implies $cd \geqslant (c - d)m + m^2$, so that

$$(mF_2 + 1)[2F_2^2 + (m + r)F_2 - 1] \geqslant (mF_2 - 1)[2F_2^2 + (m - |r|)F_2 + 1]$$

$$> N = cdF_2^2 + (c - d)F_2 - 1 \geqslant [(c - d)m + m^2]F_2^2 + (c - d)F_2 - 1$$

$$= (mF_2 + 1)[(c - d + m)F_2 - 1].$$

Thus, $2F_2^2 + (m + r)F_2 - 1 > (c - d + m)F_2 - 1$, or $c - d < r + 2F_2$.

Combining this result with (19) and (20) gives $c - d = r$.

Thus, from (18) it follows that $2s = cd \neq 0$. Finally, $r^2 + 8s = (c - d)^2 + 4cd = (c + d)^2$.

(ii) $(\Leftarrow)$. With $s \neq 0$ and, say, $r^2 + 8s = t^2$, then

$$N = F_2 R_2 - 1 = F_2(2F_2 s + r) - 1$$

$$= [(t - r)\bar{F}_2 + 1]\,[(t + r)\bar{F}_2 - 1],$$

where the factors on the right are > 1, since $s \neq 0$. Q.E.D.

Remark. The value of r in Theorem 17 is chosen to be the absolutely least remainder because $c - d$ may well be negative.

THEOREM 18. *Let n be a prime divisor of N. If for some Lucas sequence* $\{U_k\}$ *for which* $(D/N) = -1, N \mid U_{N+1}$ *and*

$$(U_{F_2}, N) = 1, \tag{21}$$

then $n \equiv \epsilon_n \pmod q$, *where q is some prime divisor of* R_2 *depending on n.*

Proof. By Lemma 2 and Theorem 8(a), $\rho(n) \mid n - \epsilon_n$ and $\rho(n) \mid N + 1 = F_2 R_2$. But (21) implies $\rho(n) \nmid F_2$, so $(\rho(n), R_2) > 1$, i.e., there exists a prime q such that $q \mid \rho(n)$ and $q \mid R_2$. Hence, $q \mid n - \epsilon_n$. Q.E.D.

As a further abbreviation put:

(IV) *For some Lucas sequence* $\{U_k\}$ *for which* $(D/N) = -1$, $N \mid U_{N+1}$ *and* $(U_{(N+1)/R_2}, N) = 1$.

Remark. As in (II), the subscript of U is written to suggest (III) and (IV) can be computed together, R_2 being treated as the final "prime" factor of $N + 1$.

COROLLARY 9. *Assume* (III) *and* (IV), *and let n be a prime divisor of N. Then* $n \equiv \epsilon_n \pmod{qF_2}$, *where q is some prime divisor of* R_2 *depending on n.*

Proof. Since $(F_2, R_2) = 1$, the corollary follows from Theorems 16 and 18. Q.E.D.

COROLLARY 10. *Assume* (III) *and* (IV). *If all the prime factors of* R_2 *are* $\geqslant B_2$ *and* $B_2 F_2 > \sqrt{N} + 1$, *then N is prime.*

Proof. $n + 1 \geqslant n - \epsilon_n \geqslant qF_2 \geqslant B_2 F_2 > \sqrt{N} + 1$, which implies N is prime. Q.E.D.

THEOREM 19. *Assume* (III) *and* (IV), *and also that the prime factors of* R_2 *are* $\geqslant B_2$. *If*

$$N < (B_2 F_2 - 1)[2F_2^2 + (B_2 - |r|)F_2 + 1], \tag{22}$$

where r and s are defined by $R_2 = 2F_2 s + r$, $|r| < F_2$, *then N is prime if and only if* $s = 0$ *or* $r^2 + 8s \neq \square$.

Proof. The theorem will be proved in the equivalent form: N is composite if and only if $s \neq 0$ and $r^2 + 8s = \square$.

(i) $(\Rightarrow)$. Let n be a prime factor of N, and write $N = nw$, $w > 1$. Then from Corollary 9, $n \equiv \epsilon_n \pmod{qF_2}$, and since $N \equiv -1 \pmod{qF_2}$, $w \equiv -\epsilon_n \pmod{qF_2}$. Then $N = (cF_2 + \epsilon_n)(dF_2 - \epsilon_n)$, where $c, d \geqslant B_2$. Also, R_2 is odd and F_2 is even, so

$$R_2 = (N + 1)/F_2 = cdF_2 + \epsilon_n(d - c),$$

implies $d - c$ is odd, so cd is even. Hence, from

$$cdF_2 + \epsilon_n(d - c) = R_2 = 2F_2 s + r \tag{23}$$

it follows that

$$\epsilon_n(d - c) \equiv r \pmod{2F_2}.$$

On the other hand,

$$(c - B_2)(d + B_2) \geqslant 0 \quad \text{implies } cd \geqslant (d - c)B_2 + B_2^2$$

and

$$(c + B_2)(d - B_2) \geqslant 0 \quad \text{implies } cd \geqslant (c - d)B_2 + B_2^2.$$

These together imply $cd \geqslant \pm \epsilon_n(d - c)B_2 + B_2^2$. Now using (22),

$$\begin{aligned}(B_2F_2 - 1)&[2F_2^2 + (B_2 - r)F_2 + 1] \\ &\geqslant (B_2F_2 - 1)[2F_2^2 + (B_2 - |r|)F_2 + 1] \\ &> N = cdF_2^2 + \epsilon_n(d - c)F_2 - 1 \\ &\geqslant [-\epsilon_n(d - c)B_2 + B_2^2]F_2^2 + \epsilon_n(d - c)F_2 - 1 \\ &= (B_2F_2 - 1)\{[-\epsilon_n(d - c) + B_2]F_2 + 1\}.\end{aligned}$$

Therefore,

$$2F_2 + B_2 - r > -\epsilon_n(d - c) + B_2, \quad \text{or} \quad -2F_2 + r < \epsilon_n(d - c).$$

Also,

$$\begin{aligned}(B_2F_2 + 1)&[2F_2^2 + (B_2 + r)F_2 - 1] \\ &\geqslant (B_2F_2 - 1)[2F_2^2 + (B_2 - |r|)F_2 + 1] \\ &> N = cdF_2^2 + \epsilon_n(d - c)F_2 - 1 \\ &\geqslant [\epsilon_n(d - c)B_2 + B_2^2]F_2^2 + \epsilon_n(d - c)F_2 - 1 \\ &= (B_2F_2 + 1)\{[\epsilon_n(d - c) + B_2]F_2 - 1\}.\end{aligned}$$

Thus,

$$2F_2 + B_2 + r > \epsilon_n(d - c) + B_2, \quad \text{or} \quad 2F_2 + r > \epsilon_n(d - c).$$

Hence, $r = \epsilon_n(d - c)$ and from (23), $2s = cd \neq 0$. Also,

$$r^2 + 8s = (d - c)^2 + 4cd = (c + d)^2.$$

(ii) ($\Leftarrow$). Same as Theorem 17(ii). Q.E.D.

7. Combined Theorems. As was mentioned in the introduction, a considerable advantage is gained by combining the information obtained from factoring both $N - 1$ and $N + 1$. This advantage lies as usual in reducing the total amount of factoring time by a trade-off with less time-consuming, nontentative tests (such as a GCD) (see [8]).

Of the two theorems given here, Theorem 20 and its corollary have proven to be quite useful when other primality tests could not be applied. Theorem 21 treats the case in which $N \pm 1$ can be factored algebraically into possibly rather large pieces, each of which has been factored to a certain extent (see [6, p. 329]).

THEOREM 20. *Assume* (I)–(IV), *and suppose the prime factors of* R_1 *and* R_2 *are respectively* $\geqslant B_1$ *and* B_2. *Define* r *and* s *by* $R_1 = \bar{F}_2 s + r$, $0 \leqslant r < \bar{F}_2$, *and let*

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

Further, in the case that $G = mF_1\bar{F}_2 + rF_1 + 1$, *assume* $(\lambda F_1\bar{F}_2 + rF_1 + 1) \nmid N$, $\delta_0^r \leqslant \lambda < m$, *where* δ_0^r *is the Kronecker delta.* (*Note*: *When* $r = 0$ *and* $m = 1$, *the* λ *interval is empty.*)

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

Proof (*by contradiction*). Assume N is composite, say $N = nw$, n prime and $w > 1$. Then Corollary 2 gives

$$n \equiv 1 \pmod{pF_1}, \tag{24}$$

where $p \mid R_1$, and $w \equiv nw = N = F_1R_1 + 1 \equiv 1 \pmod{pF_1}$. Thus,

$$w \geqslant pF_1 + 1 \geqslant B_1F_1 + 1. \tag{25}$$

Similarly, Corollary 9 gives

$$n \equiv \epsilon_n \pmod{qF_2}, \tag{26}$$

where $q \mid R_2$, and $w \equiv wn\epsilon_n = N\epsilon_n = (F_2R_2 - 1)\epsilon_n \equiv -\epsilon_n \pmod{qF_2}$. Also,

$$nw = N = F_1R_1 + 1 = F_1(s\bar{F}_2 + r) + 1 \equiv rF_1 + 1 \pmod{F_1\bar{F}_2}, \tag{27}$$

where $rF_1 + 1 < F_1\bar{F}_2 + 1$, or more sharply, $rF_1 + 1 \leqslant F_1\bar{F}_2 - 1$, i.e., $rF_1 + 1$ is the least positive remainder $\pmod{F_1\bar{F}_2}$.

Case 1. $\epsilon_n = 1$. Combining (24) and (26) gives

$$n \equiv 1 \pmod{pqF_1\bar{F}_2}, \tag{28}$$

since $(F_1, F_2) = 2$. Hence,

$$n \geqslant pqF_1\bar{F}_2 + 1 \geqslant B_1B_2F_1\bar{F}_2 + 1.$$

Also, $n \equiv 1 \pmod{F_1\bar{F}_2}$ from (28). Combining this with (27) gives $w \equiv nw \equiv rF_1 + 1 \pmod{F_1\bar{F}_2}$, which implies $w \geqslant mF_1\bar{F}_2 + rF_1 + 1$. On the other hand, $w \equiv -1 \pmod{qF_2}$ implies

$$w \geqslant qF_2 - 1 \geqslant B_2F_2 - 1.$$

These results with (25) give $w \geqslant G$. Thus finally, $N = wn \geqslant G(B_1B_2F_1\bar{F}_2 + 1)$, which is a contradiction. Hence, N is prime.

Case 2. $\epsilon_n = -1$. This case is the same as Case 1 with the roles of n and w reversed and (25) changed to read: $n \geqslant B_1F_1 + 1$. Q.E.D.

Remarks. 1. In practice $N - 1$ and $N + 1$ can be factored simultaneously; for if a trial divisor d for $N + 1$ leaves a remainder $t \neq 0$, then d will divide $N - 1$ if and only if $t = 2$.

2. Usually $B_1 = B_2$ when the factoring of $N - 1$ and $N + 1$ is done by the method of Remark 1. These factoring bounds may be different, however, if the form of N permits algebraic factorization, and the algebraic factors are investigated separately.

3. If the main inequality of the hypothesis is not satisfied at some point in the factorization of $N \pm 1$, there are three ways to increase the size of the product on the right of the inequality: increase B_1 and B_2; find more factors of $N \pm 1$ (thereby increasing F_1 or F_2); increase the size of m. What strategy is adopted will, of course, depend on the amount of incrêase needed to satisfy the inequality. An excellent example of the use of this theorem will be found in the next section where the factorizations of three Mersenne numbers M_{167}, M_{197}, and M_{241} are shown to be complete. From these examples, it becomes clear that none of the other hypotheses of Theorem 20 need to be verified until the inequality on N has been satisfied, i.e., the auxiliary testing, which is needed to complete the primality test, is done only after enough factoring data have been obtained. (This, of course, is true for the other theorems in this paper.) Thus, conditions (I)–(IV) are usually referred to as "final tests."

4. The special case when $r = 0$ occurs when $\bar{F}_2 | R_1$, which implies $\bar{F}_2$ is odd. Also, $\bar{F}_2 | N - 1$, and since $\bar{F}_2 | N + 1$, then $\bar{F}_2 | 2$. Thus, $\bar{F}_2 = 1$. This case will occur if and only if $N = 4k + 1$ and $N + 1$ has no "small" odd prime factors.

COROLLARY 11. *Assume* (I)–(IV) *and that the prime factors of both R_1 and R_2 are $\geqslant B = B_1 = B_2$.*

(a) *If $B > (N/F_1^2\bar{F}_2)^{1/3}$, then N is prime.*

(b) *If $B > (N/\bar{F}_1F_2^2)^{1/3}$, then N is prime.*

Proof. (a) $N < B^3F_1^2\bar{F}_2 < BF_1(B^2F_1\bar{F}_2 + 1) < G(B^2F_1\bar{F}_2 + 1)$. (Note here that only the first argument in the definition of G is used. Since the third argument in this definition is not used at all in this theorem, no divisibility testing is needed in the hypothesis of the corollary.)

(b) First observe in the proof of Theorem 20 that p and q are both $\geqslant B$, and since $p \neq q$, $pq \geqslant B(B + 2)$. Thus, the inequality following (28) can be written $n \geqslant B(B + 2)F_1\bar{F}_2 + 1$. Consequently, when $B = B_1 = B_2$, the inequality in the theorem can be strengthened to read $N < G[B(B + 2)F_1\bar{F}_2 + 1]$. Then

$$N < B^3\bar{F}_1F_2^2 < (BF_2 - 1)[B(B + 2)\bar{F}_1F_2 + 1]$$

$$\leqslant G[B(B + 2)F_1\bar{F}_2 + 1]. \qquad \text{Q.E.D.}$$

THEOREM 21. *Let $N - 1 = \prod_{i=1}^r R_i^{\alpha_i}$ and $N + 1 = \prod_{i=1}^s S_i^{\beta_i}$, where R_i and S_i are not necessarily prime, and $(R_i, R_j) = (S_i, S_j) = 1, i \neq j$. Suppose the prime factors of R_i and S_i are respectively greater than B_i and C_i. Let $B = \prod_{i=1}^r B_i^{\alpha_i}$ and $C = \prod_{i=1}^s C_i^{\beta_i}$. Assume* (II) *and* (IV) *are satisfied respectively for each R_i and S_i (where not necessarily the same base or Lucas sequence is used). Let $G = \max(B + 1, C - 1)$. If $N < G(BC/2 + 1)$, then N is prime.*

Proof. If N is not prime, then $N = nw$, where n is prime and $w > 1$. Let a_i be the base used for R_i in (II) and suppose the order of $a_i \pmod n$ is e_i. Then $e_i | N - 1$, but $e_i \nmid (N - 1)/R_i$. Hence, there is a prime divisor p_i of R_i which divides e_i to R_i's full power in $N - 1$; i.e., $p_i^{\alpha_i} | e_i$. But $e_i | n - 1$. Thus, since $(R_i, R_j) = 1$, $i \neq j$, $\prod_{i=1}^r p_i^{\alpha_i} | n - 1$. Also, $w \equiv nw = N \equiv 1 \pmod{\prod_{i=1}^r p_i^{\alpha_i}}$. On the other hand, if

$\{U_k^{(i)}\}$ is the sequence used for S_i in (IV) and $\rho_i(n)$ is the rank of n in $\{U_k^{(i)}\}$, then by Lemma 2, $\rho_i(n) | N + 1$, but $\rho_i(n) \nmid (N + 1)/S_i$. Thus there is a prime divisor q_i of S_i which divides $\rho_i(n)$ to S_i's full power in $N + 1$; i.e., $q_i^{\beta_i} | \rho_i(n)$. But $\rho_i(n) | n - \epsilon_n$, so since $(S_i, S_j) = 1$, $\Pi_{i=1}^s q_i^{\beta_i} | n - \epsilon_n$. Also,

$$w \equiv \epsilon_n nw = \epsilon_n N \equiv -\epsilon_n \quad \left(\text{mod } \prod_{i=1}^{s} q_i^{\beta_i}\right).$$

Case 1. $\epsilon_n = 1$. In this case

$$n \equiv 1 \quad \left(\text{mod } \prod_{i=1}^{s} q_i^{\beta_i}\right),$$

so since $(N - 1, N + 1) = 2$,

$$2n \equiv 2 \quad \left(\text{mod } \prod_{i=1}^{r} p_i^{\alpha_i} \prod_{i=1}^{s} q_i^{\beta_i}\right) \quad \text{and} \quad w \equiv 1 \quad \left(\text{mod } \prod_{i=1}^{r} p_i^{\alpha_i}\right).$$

(Note: p_i and q_i may be odd for all i.) Hence,

$$n \geqslant \frac{1}{2}\left(\prod_{i=1}^{r} p_i^{\alpha_i}\right)\prod_{i=1}^{s} q_i^{\beta_i} + 1 \geqslant \frac{1}{2}\left(\prod_{i=1}^{r} B_i^{\alpha_i}\right)\prod_{i=1}^{s} C_i^{\beta_i} + 1 = \frac{BC}{2} + 1$$

and

$$w \geqslant \prod_{i=1}^{r} p_i^{\alpha_i} + 1 > \prod_{i=1}^{r} B_i^{\alpha_i} + 1 = B + 1.$$

Also, $w \equiv -1 \pmod{\Pi_{i=1}^s q_i^{\beta_i}}$, so

$$w \geqslant \prod_{i=1}^{s} q_i^{\beta_i} - 1 \geqslant \prod_{i=1}^{s} C_i^{\beta_i} - 1 = C - 1.$$

Thus, $N = nw \geqslant (BC/2 + 1)\max(B + 1, C - 1) = G(BC/2 + 1)$, a contradiction.

Case 2. $\epsilon_n = -1$. This case is the same as Case 1 with the roles of n and w reversed. Q.E.D.

Remark. An example for which Theorem 21 might be of use is:

Let N be a pseudoprime of the form $(a^{128} + 1)/257$. Then

$$\begin{aligned} N - 1 &= (a^{128} - 256)/257 \\ &= (a^{16} - 2)(a^{16} + 2)(a^{16} - 2a^8 + 2)(a^{16} + 2a^8 + 2)(a^{64} + 16)/257; \end{aligned}$$

8. Numerical Results. The 131 complete factorizations given in Table 1 are the results obtained by the authors over the last seven years on numbers of the form $2^m \pm 1$, $2^{2r} \pm 2^r + 1$, and $2^{2r-1} \pm 2^r + 1$ (see [4, p. 87]). (Note that factorizations of both the primitive and algebraic parts of $2^{447} - 1$ and $2^{471} - 1$ appear in Table 1 and Section 9.)

In Table 1, all factors listed are prime. Those preceding a colon are algebraic; those following a colon are primitive. An asterisk indicates the factor was first discovered by R. M. Merson.

TABLE 1. *Complete Factorizations*

1.	$2^{94} + 2^{47} + 1$	= 7	: 4375578271·646675035253258729
2.	$2^{101} - 2^{51} + 1$	= 5	: 9491060093·53425037363873248657
3.	$2^{101} + 2^{51} + 1$	=	: 809·5218735279937·600503817460697
4.	$2^{102} - 2^{51} + 1$	= 3·19	: 123931·26159806891·27439122228481
5.	$2^{103} + 1$	= 3	: 415141630193·8142767081771726171
6.	$2^{104} - 2^{52} + 1$	= 241	: 84159375948762099254554456081
7.	$2^{106} - 2^{53} + 1$	= 3	: 6043·4475130366518102084427698737
8.	$2^{109} - 2^{55} + 1$	= 5	: 74323515777853·1746518852140345553
9.	$2^{112} - 2^{56} + 1$	= 97·673	: 2017·25629623713·1538595959564161
10.	$2^{114} - 2^{57} + 1$	= $3 \cdot 19^2$	: 19177458387940268116349766612211
11.	$2^{118} - 2^{59} + 1$	= 3	: 13099·4453762543897·1898685496465999273
12.	$2^{118} + 2^{59} + 1$	= 7	: 184081·27989941729·9213624084535989031
13.	$2^{119} + 1$	= 3·43·43691	: 823679683·143162553165560959297
14.	$2^{119} + 2^{60} + 1$	= 5·29·26317	: 9521·18292898984156916156396101
15.	$2^{120} - 2^{60} + 1$	= 433·38737	: 168692292721·469775495062434961
16.	$2^{121} - 2^{61} + 1$	= 2113	: 3389·91961·4036962584010807014809213
17.	$2^{121} + 1$	= 3·683	: 117371·11054184582797800455736061107
18.	$2^{121} + 2^{61} + 1$	= 5·397	: 1339272539833668386958920468400193
19.	$2^{122} - 2^{61} + 1$	= 3	: 1772303994379887829769795077302561451
20.	$2^{122} + 2^{61} + 1$	= 7	: 367·55633·37201708625305146303973352041
21.	$2^{124} + 1$	= 17	: 290657·3770202641·1141629180401976895873
22.	$2^{125} - 1$	= 31·601·1801	: 269089806001·4710883168879506001
23.	$2^{125} + 1$	= 3·11·251·4051	: 229668251·5519485418336288303251
24.	$2^{126} - 2^{63} + 1$	= 3·87211	: 379·119827·127391413339 ·56202143607667
25.	$2^{127} + 1$	= 3	: 56713727820156410577229101238628035243
26.	$2^{127} + 2^{64} + 1$	= 5	: 18797·72118729·2792688414613 ·8988357880501
27.	$2^{128} - 2^{64} + 1$	=	: 769·442499826945303593556473164314770689
28.	$2^{129} - 2^{65} + 1$	= 13·173·101653·500177	: ·5951631966296685834686149
29.	$2^{131} - 2^{66} + 1$	= 5	: 642811237·2745098189·308544695409769427309
30.	$2^{131} + 1$	= 3	: 1049·4744297*·182331128681207781784391813611

*Merson factor

TABLE 1 (*Continued*)

31.	$2^{131} + 2^{66} + 1 =$		: 269665073·810791440841·12450751815271172041
32.	$2^{133} - 2^{67} + 1 =$	5·29·229·457	: 1597·449329386292232535250647435097
33.	$2^{133} + 1 =$	3·43·174763	: 4523·106788290443848295284382097033
34.	$2^{133} + 2^{67} + 1 =$	113·525313	: 2129·126848469231149·679253585011429
35.	$2^{136} - 2^{68} + 1 =$	241	: 8161·40932193*·1467129352609·737539985835313
36.	$2^{136} + 1 =$	257·383521	: 2368179743873·373200722470799764577
37.	$2^{137} - 2^{69} + 1 =$		: 189061·921525707911840587390617330886362701
38.	$2^{137} + 1 =$	3	: 1097·15619·32127963626435681·105498212027592977
39.	$2^{138} - 2^{69} + 1 =$	3·19	: 6113142872404227834840443898241613032969
40.	$2^{138} + 2^{69} + 1 =$	73	: 79903·634569679·2232578641663·42166482463639
41.	$2^{139} - 2^{70} + 1 =$	5	: 1408349·15736774913·492717674609·12763660054721
42.	$2^{139} - 1 =$		: 5625767248687·123876132205208335762278423601
43.	$2^{139} + 1 =$	3	: 4506937*·51542639524661795300074174250365699
44.	$2^{139} + 2^{70} + 1 =$		: 557·1251163891299967635860272509229764287909
45.	$2^{140} + 1 =$	17·61681·15790321	: 84179842077657862011867889681
46.	$2^{141} + 2^{71} + 1 =$	13·140737471578113	: 5641·270097268484167653999069
47.	$2^{142} - 2^{71} + 1 =$	3	: 5113·17467·102241·203525545766301306933226271929
48.	$2^{143} - 2^{72} + 1 =$	53·157·2113	: 958673·661521349351105339668937661297
49.	$2^{143} - 1 =$	23·89·8191	: 724153·158822951431·5782172113400990737
50.	$2^{143} + 1 =$	3·683·2731	: 2003·6156182033·10425285443·15500487753323
51.	$2^{145} - 2^{73} + 1 =$	41·536903681	: 168781·12004541501954811085302214141
52.	$2^{145} - 1 =$	31·233·1103·2089	: 2679895157783862814690027494144991
53.	$2^{145} + 1 =$	3·11·59·3033169	: 7553921*·999802854724715300883845411
54.	$2^{145} + 2^{73} + 1 =$	5^2·107367629	: 17401·244716883381·3902095192430070721

*Merson factor

TABLE 1 (*Continued*)

55.	$2^{147} + 2^{74} + 1$	$= 13 \cdot 113 \cdot 1429 \cdot 4981857697937 : 17059410504738323992180849$
56.	$2^{149} + 1$	$= 3 : 1193 \cdot 650833 \cdot 38369587^{*} \cdot 7984559573504259856359124657$
57.	$2^{150} - 2^{75} + 1$	$= 3 \cdot 19 \cdot 18837001 : 4714696801 \cdot 281941472953710177758647201$
58.	$2^{153} + 2^{77} + 1$	$= 5 \cdot 109 \cdot 409 \cdot 3061 \cdot 13669 \cdot 26317 : 613 \cdot 318194713 \cdot 238495197879143209$
59.	$2^{154} - 2^{77} + 1$	$= 3 \cdot 67 \cdot 5419 \cdot 20857 : 14323 \cdot 7018079616527704034924570385 1057$
60.	$2^{154} + 2^{77} + 1$	$= 7^{2} \cdot 337 \cdot 599479 : 463 \cdot 49823976511782561513383022047 62057$
61.	$2^{155} - 2^{78} + 1$	$= 5^{2} \cdot 8681 \cdot 49477 : 37201 \cdot 87421 \cdot 52597081^{*} \cdot 2486589969383 4809641$
62.	$2^{155} + 1$	$= 3 \cdot 11 \cdot 715827883 : 11161 \cdot 5947603221397891 \cdot 29126056043168521$
63.	$2^{157} - 1$	$= \; : 852133201 \cdot 60726444167 \cdot 1654058017289 \cdot 2134387368610417$
64.	$2^{158} - 2^{79} + 1$	$= 3 : 647011 \cdot 13664473^{*} \cdot 137756946928984921847 44709216599873$
65.	$2^{159} - 2^{80} + 1$	$= 13 \cdot 15358129 \cdot 586477649 : 207973 \cdot 3000745925439318161801 2897$
66.	$2^{159} + 2^{80} + 1$	$= 5 \cdot 18014398241046 53 : 10177 \cdot 797186200486710330329346 2593$
67.	$2^{160} + 1$	$= 641 \cdot 6700417 : 3602561^{*} \cdot 94455684953484563055991838558081$
68.	$2^{161} - 2^{81} + 1$	$= 113 \cdot 277 \cdot 30269 : 3221 \cdot 169373 \cdot 209160253 \cdot 270370281184488 01270021$
69.	$2^{161} - 1$	$= 47 \cdot 127 \cdot 178481 : 1289 \cdot 3188767 \cdot 45076044553 \cdot 1480860771531 5782481$
70.	$2^{161} + 1$	$= 3 \cdot 43 \cdot 2796203 : 810346749275979232714980036156 4410265219$
71.	$2^{161} + 2^{81} + 1$	$= 5 \cdot 29 \cdot 1013 \cdot 1657 : 1933 \cdot 298817 \cdot 115927640417 \cdot 17935157473 6387915177$
72.	$2^{165} + 2^{83} + 1$	$= 13 \cdot 41 \cdot 61 \cdot 2113 \cdot 312709 \cdot 415878438361 : 391249826881 \cdot 13379250952981$
73.	$2^{167} - 1$	$= \; : 2349023 \cdot \text{prime}$
74.	$2^{167} + 1$	$= 3 : \text{prime}$
75.	$2^{168} - 2^{84} + 1$	$= 433 \cdot 38737 : 1009 \cdot 21169 \cdot 2627857^{*} \cdot 269389009 \cdot 1475204679190128571777$
76.	$2^{171} - 2^{86} + 1$	$= 5 \cdot 109 \cdot 229 \cdot 457 \cdot 275415303169 : 4598533^{*} \cdot 41435606371227835355919073$

*Merson factor

TABLE 1 (*Continued*)

77. $2^{174} + 2^{87} + 1 = 73 : \text{prime}$

78. $2^{175} - 2^{88} + 1 = 41 \cdot 101 \cdot 113 \cdot 8101 \cdot 7416361 : 701$
   $\cdot 2430065924693517198550322751963101$

79. $2^{175} + 1 = 3 \cdot 11 \cdot 43 \cdot 251 \cdot 281 \cdot 4051 \cdot 86171 : 1051 \cdot 110251$
   $\cdot 347833278451 \cdot 34010032331525251$

80. $2^{175} + 2^{88} + 1 = 5^3 \cdot 29 \cdot 268501 \cdot 47392381 :$
   $10382137934478419409082933558714 61401$

81. $2^{177} - 2^{89} + 1 = 13 \cdot 5521693 \cdot 104399276341 : 709 \cdot 12037$
   $\cdot 29952400871179090787359 42093$

82. $2^{177} + 2^{89} + 1 = 5 \cdot 1181 \cdot 3541 \cdot 157649 \cdot 174877 : 31153 \cdot 5397793^*$
   $\cdot 94789873 \cdot 20847858316750657$

83. $2^{183} - 2^{92} + 1 = 13 \cdot 3456749 \cdot 667055378149 : 5080081^*$
   $\cdot 4209508589941 \cdot 1912555651991 8081$

84. $2^{185} - 2^{93} + 1 = 41 \cdot 593 \cdot 231769777 : 1392776941$
   $\cdot 4964166554103541 \cdot 12587107251156 50761$

85. $2^{185} + 1 = 3 \cdot 11 \cdot 1777 \cdot 25781083 : 1481 \cdot 28136651^*$
   $\cdot 778429365397887608540618330873281$

86. $2^{189} - 2^{95} + 1 = 5 \cdot 29 \cdot 109 \cdot 14449 \cdot 246241 \cdot 40388473189 : 757$
   $\cdot 456376431053626339473533320957$

87. $2^{189} + 2^{95} + 1 = 13 \cdot 37 \cdot 113 \cdot 1429 \cdot 279073 \cdot 118750098349 :$
   $304832756195865229284807891468769$

88. $2^{190} - 2^{95} + 1 = 3 \cdot 331 \cdot 571 \cdot 160465489 : 1101811$
   $\cdot 1565399070589631354726923722004116936$

89. $2^{191} + 1 = 3 : \text{prime}$

90. $2^{195} - 2^{98} + 1 = 5 \cdot 521 \cdot 1321 \cdot 1613 \cdot 3121 \cdot 21841 \cdot 51481 \cdot 34110701 :$
   $2341 \cdot 723447661 \cdot 8925278993793241$

91. $2^{195} + 2^{98} + 1 = 13^2 \cdot 41 \cdot 53 \cdot 61 \cdot 157 \cdot 313 \cdot 1249 \cdot 108140989558681 :$
   $468781 \cdot 7204537724275184464 37641$

92. $2^{196} + 1 = 17 \cdot 15790321 : 7057 \cdot 273617 \cdot 1007441$
   $\cdot 375327457 \cdot 1405628248417 \cdot 364565561997841$

93. $2^{197} - 1 = \quad : 7487 \cdot \text{prime}$

94. $2^{199} + 1 = 3 : \text{prime}$

95. $2^{200} - 2^{100} + 1 = 241 \cdot 4562284561 : \text{prime}$

96. $2^{201} - 2^{101} + 1 = 13 \cdot 15152453 \cdot 9739278030221 : 3217 \cdot 192961$
   $\cdot 214473433 \cdot 71848008781 \cdot 175132692529$

97. $2^{201} + 2^{101} + 1 = 5 \cdot 269 \cdot 42875177 \cdot 2559066073 : 10453$
   $\cdot 132661 \cdot 157049009596512937742705213957 53$

98. $2^{203} - 1 = 127 \cdot 233 \cdot 1103 \cdot 2089 : 136417 \cdot 121793911$
   $\cdot 1134805558088327201109085605317536 1113$

99. $2^{205} + 1 = 3 \cdot 11 \cdot 83 \cdot 8831418697 : \text{prime}$

---

*Merson factor

TABLE 1 (*Continued*)

100.	$2^{205} + 2^{103} + 1$	=	41^2·181549·12112549 : 821·269896441 ·82777720757144341·758399801407611361
101.	$2^{207} - 2^{104} + 1$	=	13·37·277·30269·5415624023749 : 829 ·853669·267853371 49·49681708110915068592l
102.	$2^{207} + 2^{104} + 1$	=	5·109·1013·1657·70334392823809 : 3313 ·18217·318781·6542857·2539538214180546045 7
103.	$2^{213} - 2^{107} + 1$	=	5·569·148587949·5585522857 : 266677 ·1396429*·18369973*·40524027877 ·20111008087273
104.	$2^{213} + 2^{107} + 1$	=	13·4999465853·472287102421 : 853·189997 ·264618532848685412969316991139349
105.	$2^{215} + 2^{108} + 1$	=	5^2·1759217765581 : 370661·1952201* ·4538991421·260125854015641 ·1401345270171101
106.	$2^{217} - 2^{109} + 1$	=	113·5581·384773 : prime
107.	$2^{220} + 1$	=	17·353·61681·2931542417 : 109121·148721 ·3404676001·11035465708081 ·2546717317681681
108.	$2^{222} + 2^{111} + 1$	=	73 : 1999·10657·169831·1238761*·36085879* ·199381087·698962539799·4096460559560875111
109.	$2^{225} + 2^{113} + 1$	=	5^3·109·181·1321·54001·63901·268501·13334701 : 695701·307116398490301·6269989892198401
110.	$2^{231} - 2^{116} + 1$	=	13·113·1429·2113·8317·312709·76096559910757 : 3931002956111648245378728475226109181
111.	$2^{231} + 2^{116} + 1$	=	5·29·397·14449·4327489·869467061·3019242689 : 3652124453410972878264128383539559 21
112.	$2^{233} - 1$	=	: 1399·135607·622577·prime
113.	$2^{237} - 2^{119} + 1$	=	5·317·3813646118665073l7969 : 151681·prime
114.	$2^{239} - 1$	=	: 479·1913·5737·176383·134000609·prime
115.	$2^{241} - 1$	=	: 22000409·prime
116.	$2^{255} - 2^{128} + 1$	=	13·41·61·137·953·1326700741 ·7226904352843746841 : 51001·2949879781 ·611787251461·15455023589221
117.	$2^{255} + 1$	=	3^2·11·307·331·2857·6529·43691 ·2683142303606535261l : 12241 ·418562986357561·51366149455494753931
118.	$2^{255} + 2^{128} + 1$	=	5^2·409·1021·1321·3061·4421·13669·26317 ·550801·23650061 : 15571321 ·4251553088834471719044481725601
119.	$2^{272} - 2^{136} + 1$	=	97·673 : prime

*Merson factor

TABLE 1 (*Continued*)

120. $2^{273} + 2^{137} + 1 = 5 \cdot 29 \cdot 1093^2 \cdot 1613 \cdot 3121 \cdot 14449 \cdot 21841 \cdot 8861085190774909 : 1948129 \cdot 3194753987813988499397428643895659569$

121. $2^{283} - 2^{142} + 1 = 5$: prime

122. $2^{285} - 2^{143} + 1 = 5^2 \cdot 229 \cdot 457 \cdot 1321 \cdot 54721 \cdot 275415303169 \cdot 2766966312509537 41 : 185821 \cdot 247381 \cdot 3996146881 \cdot 2348041208209891332 6841$

123. $2^{298} + 2^{149} + 1 = 7$: prime

124. $2^{313} + 1 = 3$: prime

125. $2^{314} + 2^{157} + 1 = 7$: prime

126. $2^{315} + 2^{158} + 1 = 13 \cdot 37 \cdot 41 \cdot 61 \cdot 113 \cdot 1429 \cdot 7416361 \cdot 29247661 \cdot 118750098349 \cdot 1041815865690181 : 1711081 \cdot 430839361 \cdot 17369459529909057773233442461$

127. $2^{318} - 2^{159} + 1 = 3 \cdot 19$: prime

128. $2^{356} + 1 = 17$: prime

129. $2^{563} - 2^{282} + 1 = 5$: prime

130. $2^{613} - 2^{307} + 1 = 5$: prime

131. $2^{691} - 2^{346} + 1 = 5$: prime

TABLE 2. *Completed Factorizations*

$2^m - 1$, m odd: m = 1-167,171,175-183,189,195,197,201,203,207, 225,231,233,239,241,255,261,315,333,447,471,521,607,1279,2203, 2281,3217,4253,4423,9689,9941,11213,19937.

$2^m + 1$: m = 0-150,153-156,158-162,165-168,170,171,174, 175,177,178,180,182,183,185,186,189-192,194-196,198,199,201,202, 204-207,210,213,214,218,220,222,226,230,231,234,237,238,242,246, 250,252,254,255,258,262,266,270,278,282,285,286,290,294,300,306, 313,318,322,330,342,350,354,356,378,390,402,408,414,426,462,477, 510,566.

$2^m - 2^r + 1$, $m = 2r - 1$: m = 1-147,151-155,159,161,165,167,171, 175,177,183,185,189,195,201,207,213,217,231,237-241,255,283,285, 353,367,457,563,613,691.

$2^m + 2^r + 1$, $m = 2r - 1$: m = 1-135,139-147,153,157-165,171,175, 177,189,195,201,207,213,215,225,231,255,273,283,315,379.

TABLE 3. *Mersenne Status List*

$M_p = 2^p - 1, \quad p \text{ prime}, \quad p \le 257$

p	Character of $2^p - 1$
2,3,5,7,13,17,19,31,61,89,107,127	Prime
(All other p under 172), 179,181,197,233,239,241	Composite and completely factored
173,191,193,211,223,229,251	Cofactor is composite
199,227,257	Composite but no factor known

Table 2 shows which numbers of the above forms have been completely factored. (Also from Table 2 it is not difficult to discover that $2^{500} - 1$, $2^{600} - 1$, $2^{700} - 1$, $2^{816} - 1$, and $2^{1020} - 1$ have been completely factored.) Table 3 gives the present status of the "original" Mersenne numbers $M_p = 2^p - 1$, p a prime $\leqslant 257$. (The eight new factorizations of M_p are for $p = 137, 139, 149, 157, 167, 197, 239$, and 241.)

Several different methods were used to complete the factorization of those numbers in Table 1 whose cofactors were composite. Notable examples are:

(i) The cofactors of $2^{139} - 1$, $2^{205} + 2^{103} + 1$, and $2^{255} + 1$ were factored by a continued fraction method on the IBM 360/91 at the Campus Computing Network at UCLA (see Morrison and Brillhart [13]). The times required for these factorizations were 80, 15, and 12 minutes respectively.

(ii) $2^{101} + 2^{51} + 1$, $2^{109} - 2^{55} + 1$, $2^{136} + 1$, and $2^{137} + 1$ were factored by representing their composite cofactors as a difference of squares, using the delay-line sieve DLS 127 at UC, Berkeley. ($2^{136} + 1$ is particularly notable, having run on DLS 127 for 2600 hours (!) before it factored.)

(iii) $2^{102} - 2^{51} + 1$ was factored by expressing its cofactor as a sum of two squares in two different ways on DLS 127.

(iv) $2^{131} + 2^{66} + 1$, $2^{157} - 1$, and $2^{185} - 2^{93} + 1$ were completed on DLS 127 as in (ii) only after a new prime factor was found using idle time on the CDC 6400 at UC, Berkeley. Most surprising among these is the Mersenne number $2^{157} - 1$, which split unexpectedly into four factors.

Those numbers having a pseudoprime cofactor for some base $a > 2$ (see [4, p. 91]) were proved to be prime by some primality test (see Sections 2, 3, or 5). Of special interest are the Mersenne numbers M_{167}, M_{197}, M_{239}, and M_{241}, which were tested using Corollary 11.

To illustrate the use of this corollary, the details for M_{167} and M_{241} are given here.

(a) Let

$N = M_{167}/2349023 = 79638304766856507377778616296087448490695649$,
a number of 44 digits. N is a pseudoprime base 13. Also,

$$N - 1 = 2^5 \cdot 11 \cdot 37 \cdot 167 \cdot R_1,$$

where R_1 is composite with no factor $< 2 \cdot 10^6$. Further, $N + 1 = 2 \cdot 3^3 \cdot 5^2 \cdot 1381 \cdot 3167 \cdot R_2$, where R_2 is composite with no factor $< 2 \cdot 10^6$. Thus,

$$F_1 = 2^5 \cdot 11 \cdot 37 \cdot 167 = 2175008 > 2 \cdot 10^6,$$

so $\overline{F}_1 > 10^6$, and

$$F_2 = 2 \cdot 3^3 \cdot 5^2 \cdot 1381 \cdot 3167 = 5904396450 > 5 \cdot 10^9.$$

Hence, with $B = 2 \cdot 10^6$, the inequality in Corollary 11(b) is satisfied, since $B^3\overline{F}_1F_2^2 > (2 \cdot 10^6)^3 10^6 (5 \cdot 10^9)^2 > 10^{44} > N$.

The final tests (I)–(IV) required only a few seconds to show N was prime. The single Lucas sequence $P = 1$, $Q = 13$ was used in (III) and (IV).

(b) Let

$N = M_{241}/22000409$

$= 160619474372352289412737508720216839225805656328990879953332340439$,

a number of 66 digits. N is a pseudoprime base 13. Also, $N - 1 = 2 \cdot 241 \cdot 21221 \cdot R_1$ and $N + 1 = 2^3 \cdot 3^2 \cdot 5 \cdot 23 \cdot 643 \cdot 96763 \cdot 4975177 \cdot 17944799 \cdot R_2$. Then $F_1 = 10228522$ and $F_2 = 459936386170071464249859 60$. Hence, with $B = 21221$, N is prime by Corollary 11(b). One Lucas sequence with $P = 1$, $Q = 5$ was used in the final tests in (III) and (IV).

It is worth mentioning that the factorization of $2^{157} - 1$, along with the factorizations of $2^{109} \pm 1$ in [4], finish the 3 factorizations that were left incomplete in Robinson [19]; in fact, all numbers attempted there (except $F_8, F_9, \ldots$) have now been completely factored.

Several final comments are in order. The cofactors of F_9 and F_{10}, the ninth and tenth Fermat numbers, have been tested for pseudoprimality, and are both composite. The tests were run twice with complete agreement in the remainders.

In [4, p. 87], it was stated that "in general nothing but frustration can be expected to come from an attack on a number of 25 or more digits, even with the speeds available in modern computers." In view of the increase in speed of computers and the developments in factorization methodology (see [13]), a number of 40 digits can now be factored in about 50 minutes on, say, the IBM 360/91. Thus, the above quote should now be changed to read "50 or more digits."

9. Two Other Factorizations. The following "most wanted" Mersenne factorizations are due to R. Schroeppel at MIT (see [1]), who found them using essentially the continued fraction method discussed in [13].

$$2^{137} - 1 = 32032215596496435569 \cdot 5439042183600204290159,$$

$$2^{149} - 1 = 86656268566282183151 \cdot 8235109336690846723986161.$$

10. Acknowledgements. The authors would like to express their appreciation to Emma Lehmer, who has greatly assisted in obtaining the numerical results of this paper, and also to Michael Morrison, whose contributions to this paper have materially influenced the direction of its development and the character of its results. They would also like to thank Daniel Shanks for his valuable suggestions, Peter Weinberger and Alex Hurwitz for their programming and computing assistance, and Patrick Morton for his assistance in completing the manuscript. Finally, they would like to express their gratitude to the directors of the following computer centers, who made available the time to obtain the numerical results of this paper: Campus Computing Facility, UCLA (IBM 7094, IBM 360/91), Bell Telephone Laboratories, Holmdel, N. J. (IBM 7094), The Computer Center, UC, Berkeley (IBM 7094, CDC 6400).

Department of Mathematics
University of Arizona
Tucson, Arizona 85721

Department of Mathematics
University of California
Berkeley, California 94720

Department of Mathematics
Northern Illinois University
DeKalb, Illinois 60115

1. M. BEELER, R. W. GOSPER & R. SCHROEPPEL, *Artificial Intelligence Memo* 239, MIT, Artificial Intelligence Laboratory, 1972, p. 13.

2. J. BRILLHART, "Concerning the numbers $2^{2p} + 1$, p prime," *Math. Comp.*, v. 16, 1962, pp. 424–430. MR 26 #6100.

3. J. BRILLHART, "Some miscellaneous factorizations," *Math. Comp.*, v. 17, 1963, pp. 447–450.

4. J. BRILLHART & J. L. SELFRIDGE, "Some factorizations of $2^n \pm 1$ and related results," *Math Comp.*, v. 21, 1967, pp. 87–96; Corrigendum, *ibid.*, p. 751. MR 37 #131.

5. M. KRAITCHIK, *Théorie des Nombres*, vol. 2, Gauthier-Villars, Paris, 1926, p. 135.

6. D. H. LEHMER, "Tests for primality by the converse of Fermat's theorem," *Bull. Amer. Math. Soc.*, v. 33, 1927, pp. 327–340.

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

8. D. H. LEHMER, "Computer technology applied to the theory of numbers," *Studies in Number Theory*, MAA Studies in Math., vol. 6, Prentice-Hall, Englewood Cliffs, N. J., 1969, pp. 117–151. MR 40 #84.

9. E. LUCAS, "Considerations nouvelles sur la théorie des nombres premiers et sur la division géométrique de la circonference en parties égales," *Assoc. Franç. Avancement Sci. C. R.*, v. 6, 1877, p. 162.

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

11. E. LUCAS, "*Théorie des nombres*, Tome I: *Le Calcul des Nombres Entiers, le Calcul des Nombres Rationnels, la Divisibilité Arithmétique,* Librairie Scientifique et Technique, Albert Blanchard, Paris, 1961, pp. 423, 441. MR 23 #A828.

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

13. M. A. MORRISON & J. BRILLHART, "A method of factoring and the factorization of F_7," *Math. Comp.*, v. 29, 1975, pp. 183–205.

14. H. C. POCKLINGTON, "The determination of the prime or composite nature of large numbers by Fermat's theorem," *Proc. Cambridge Philos. Soc.*, v. 18, 1914–16, pp. 29–30.

15. E. PROTH, "Théorèmes sur les nombres premiers," *C.R. Acad. Sci. Paris*, v. 87, 1878, p. 926.

16. H. RIESEL, *En Bok om Primtal*, Studentlitteratur, Lund, Sweden, 1968, pp. 44–65. MR 42 #4507.

17. H. RIESEL, "Lucasian criteria for the primality of $N = h \cdot 2^n - 1$," *Math. Comp.*, v. 23, 1969, pp. 869–875. MR 41 #6773.

18. R. M. ROBINSON, "The converse of Fermat's theorem," *Amer. Math. Monthly*, v. 64, 1957, pp. 703–710. MR 20 #4520.

19. R. M. ROBINSON, "Some factorizations of numbers of the form $2^n \pm 1$," *MTAC*, v. 11, 1957, pp. 265–268. MR 20 #832.

20. J. L. SELFRIDGE & R. K. GUY, *Primality Testing with Applications to Small Machines*, Research Paper #121, Dept. of Math., Univ. of Calgary, Canada, 1971.

21. H. C. WILLIAMS & C. R. ZARNKE, "A report on prime numbers of the forms $M = (6a + 1)2^{2m-1} - 1$ and $M' = (6a - 1)2^{2m} - 1$," *Math. Comp.*, v. 22, 1968, pp. 420–422. MR 37 #2680.