A NOTE ON THE PRIMALITY OF $6^{2^n} + 1$ AND $10^{2^n} + 1$

H. C. WILLIAMS*
University of Manitoba, Winnipeg, Manitoba, Canada R3T 2N2

(Submitted November 1986)

1. INTRODUCTION

In 1877, Lucas [3] presented the first practical test for the primality of the Fermat numbers $F_n = 2^{2^n} + 1$. We give a version of this test below, using the slightly modified form which Lucas used later in [5, p. 313] and with some minor errors corrected.

Test (T1.1) for the Primality of $F_n = 2^{2^n} + 1$ $(r = 2^n)$

Let $S_0 = 6$ and define $S_{i+1} = S_i^2 - 2$. F_n is a prime when $F_n | S_{r-1}$; F_n is composite if $F_n \nmid S_i$ for all $i \leqslant r - 1$. Finally, if t is the least subscript for which $F_n | S_t$, the prime divisors of F_n must have the form $2^{t+1}q + 1$.

Three weeks after Lucas' announcement of this test, Pepin [8] pointed out that the test was possibly not effective; that is, it might happen that a prime F_n would divide S_t, where t is too small for the primality of F_n to be proved. He provided the following effective primality test.

Test (T1.2) for the Primality of F_n

Let $S_0 = 5^2$ and define $S_{i+1} \equiv S_i^2 \pmod{F_n}$. F_n is a prime if and only if $S_{r-1} \equiv -1 \pmod{F_n}$.

Pepin also noted that his test would be valid with $S_0 = 10^2$.

Somewhat later, Proth [9], [10] gave, without a complete proof, another effective test for the primality of F_n. His test is essentially that of Pepin with $S_0 = 3^2$. The proof of Proth's test was completed by Lucas [7], who also noted [5, p. 313] that Pepin's test would be valid for $S_0 = a^2$ when the Jacobi symbol $(a/F_n) = -1$.

While effective tests for the primality of F_n have been known for almost 100 years, little seems to have been done concerning the development of effec-

Research supported by NSERC of Canada, Grant #A7649.

tive tests for the primality of other integers of the form $(2a)^{2^n}+1$. The two smallest values of a after 1 for which this form could possibly yield primes distinct from the Fermat numbers are $a=3$ and $a=5$. Riesel [11] denoted these numbers by $G_n = 6^{2^n}+1$ and $H_n = 10^{2^n}+1$; he also provided a small table of factors for some of these numbers. Now G_n is of the form $A3^r+1$ and H_n is of the form $2A5^r+1$. These are forms of integers for which Lucas [4], [5], [6] presented primality tests. These tests, which are given in a modified and corrected form (there are several errors in Lucas' statements of these tests) make use of the Fibonacci numbers $\{U_m\}$, where $U_0 = 0$, $U_1 = 1$, and $U_{k+1} = U_k + U_{k-1}$. Note that neither Test T1.3 nor Test T1.4 is an effective test for the primality of N.

Test (T1.3) for the Primality of $A3^r+1$

Let $N = A3^r+1$ with $N \equiv \pm 1 \pmod{10}$. Put $S_0 \equiv U_{3A}/U_A \pmod{N}$ and define

$$S_{k-1} \equiv S_k^3 - 3S_k^2 + 3 \pmod{N}. \tag{1.1}$$

N is a prime when $N \mid S_{r-1}$; if t is the least subscript such that $N \mid S_t$, the prime factors of N must be of the form $2q3^{t+1}+1$ or $2q3^{t+1}-1$.

There are a number of puzzling aspects of this test. First, why did Lucas restrict himself to a test for numbers $N \equiv \pm 1 \pmod 5$? Of course, as we shall see below, it is necessary for $N \equiv \pm 1 \pmod 5$ in order to use the Fibonacci numbers in a primality test for N, but other Lucas sequences could also be used. For example, if $N \equiv -1 \pmod 4$, we could use $P = 4$, $Q = 1$; if $N \equiv 5 \pmod 8$, we could use $P = 10$, $Q = 1$; and if $N \equiv 1 \pmod 8$, we could use $P = 6$, $Q = 1$ (see Section 2). It may be that because of Lucas' great interest in Fibonacci numbers, he restricted his values of N to those that could be tested by making use of them. Also, why did Lucas give this test in a form which, unlike T1.1 and T1.4, does not allow for the inclusion of a test for the compositeness of N? Finally, to the author's knowledge, nowhere among the vast number of identities that Lucas developed for the Lucas functions does he mention the simple identity on which (1.1) is based.

Lucas also gave:

Test (T1.4) for the Primality of $N = 2A5^r+1$

Put $S_0 \equiv U_A \pmod{N}$ and define $S_{k+1} \equiv 25S_k^5 + 25S_k^3 + 5S_k \pmod{N}$. N is a prime when the first S_k divisible by N is S_r; if none of the S_i $(i \leqslant r)$ is divisible by N, N is composite; if t is the least subscript such that $N|S_t$, then the prime factors of N must be of the form $2q5^t+1$ or $2q5^t-1$.

The purpose of this paper is to derive tests for the primality of G_n and H_n, which are very much in the spirit of Lucas' test for the primality of F_n. We will do this by modifying tests T1.3 and T1.4. Further, like Pepin's test, our tests will be effective. In order to achieve this, we shall be guided by the methods developed by Williams [12], [13], and [14]. It should be mentioned here that the techniques we use here could also be applied, as in the manner of [14], to other numbers of the form Ar^n+1.

2. SOME PROPERTIES OF THE LUCAS FUNCTIONS

In order to develop primality tests for G_n and H_n, we will require some properties of the Lucas functions V_n and U_n. Most of these properties are well known and are included here for reference.

Let α, β be the zeros of x^2-Px+Q, where P, Q are coprime integers. We define

$$V_n=\alpha^n+\beta^n,\ U_n=(\alpha^n-\beta^n)/(\alpha-\beta), \tag{2.1}$$

and put $\Delta=(\alpha-\beta)^2=P^2-4Q$. The following identities can be found in [5] or verified by direct substitution from (2.1):

$$V_n^2-\Delta U_n^2=4Q^n, \tag{2.2}$$
$$V_{2n}=V_n^2-2Q^n, \tag{2.3}$$
$$U_{2n}=U_nV_n, \tag{2.4}$$
$$V_{3n}=V_n(V_n^2-3Q^n), \tag{2.5}$$
$$U_{3n}=U_n(\Delta U_n^2+3Q^n), \tag{2.6}$$
$$U_{3n}=U_n(V_n^2-Q^n), \tag{2.7}$$
$$V_{5n}=V_n(V_n^4-5Q^nU_n^2+5Q^{2n}), \tag{2.8}$$
$$U_{5n}=U_n(\Delta^2U_n^4+5Q^n\Delta U_n^2+5Q^{2n}), \tag{2.9}$$
$$U_{5n}=U_n(V_n^4-3Q^nV_n^2+Q^{2n}). \tag{2.10}$$

If we put $X_n=U_{3n}/U_n$, then

$$X_n=\Delta U_n^2+3Q^n, \tag{2.11}$$

by (2.6), and

$$X_{3n}=\Delta U_{3n}^2+3Q^{3n}=\Delta U_n^2X_n^2+3Q^{3n}=X_n^2(X_n-3Q^n)+3Q^{3n},$$

by (2.11). Hence,

$$X_{3n}=X_n^3-3Q^nX_n^2+3Q^{3n}; \tag{2.12}$$

also

$$X_{2n} = U_{6n}/U_{2n} = (U_{3n}/U_n)(V_{3n}/V_n) = X_n(X_n - 2Q^n),$$

by (2.4), (2.5), and (2.2). Hence, by (2.12), we get

$$X_{6n} = X_n^3(X_n - 2Q^n)^3 - 3Q^{2n}X_n^2(X_n - 2Q^n)^2 + 3Q^{6n}. \tag{2.13}$$

To obtain a result analogous to (2.12) for $Y_n = U_{5n}/U_n$, we note that

$$Y_n = \Delta^2U_n^4 + 5Q^n\Delta U_n^2 + 5Q^{2n},$$

by (2.9); thus,

$$\begin{aligned} Y_{5n} &= \Delta^2U_n^4Y_n^4 + 5Q^{5n}\Delta U_n^2Y_n^2 + 5Q^{10n} \\ &= Y_n^4(Y_n - 5Q^n\Delta U_n^2 - 5Q^{2n}) + 5Q^{5n}\Delta U_n^2Y_n^2 + 5Q^{10n}. \end{aligned}$$

We get

$$Y_{5n} = Y_n^5 + 5Q^n(Q^n - \Delta U_n^2)Y_n^4 + 5Q^{5n}\Delta U_n^2Y_n^2 + 5Q^{10n}. \tag{2.14}$$

For the development of one of our tests, it will be convenient to define

$$W_n \equiv V_{2n}Q^{-n} \pmod{N}. \tag{2.15}$$

Here the modulus N is assumed to be coprime to Q. From (2.8) and (2.2), we get

$$W_{10n} \equiv W_n^2(W_n^3 - 5W_n^2 + 5)^2 - 2 \pmod{N}. \tag{2.16}$$

Also, by (2.10), we have

$$(U_{10n}/U_{2n})Q^{-4n} \equiv W_n^4 - 3W_n^2 + 1 \pmod{N}. \tag{2.17}$$

We will also require some standard number-theoretic properties of the Lucas functions. We list these as a collection of theorems together with appropriate references. We let p be an odd prime and put

$$\varepsilon = (\Delta/p),\ \eta = (Q/p),$$

where $(\cdot/p)$ is the Legendre symbol.

Theorem 2.1 (Carmichael [1], Lehmer [2]): If $p \nmid \Delta Q$, then $p \mid U_{p-\varepsilon}$. □

Theorem 2.2 (Lehmer [2]): If $p \nmid \Delta Q$, then $p \mid U_{(p-\varepsilon)/2}$ if and only if $\eta = 1$. □

Theorem 2.3 (Carmichael [1], p. 51): The g.c.d. of U_{pn}/U_n and U_n divides p. (This result is true as well for $p = 2$.) □

Theorem 2.4: Let g.c.d.$(N, 2pQ) = 1$. If $p \mid m$, $N \mid U_m$, and g.c.d.$(U_{m/p}, N) = 1$, then the prime factors of N must be of the form $kp^\nu \pm 1$, where ν is the highest power to which p occurs as a factor of m ($p^\nu \| m$). □

By combining Theorem 2.4 with Theorem 2.3, we get the following

Corollary: If g.c.d.$(N, 2pQ) = 1$ and

$$U_{pn}/U_n \equiv 0 \pmod{N},$$

then the prime factors of N must be of the form $kp^\nu \pm 1$, where $p^{\nu-1} \| m$.

If we put $p = 2$, we have $U_{pk}/U_k = V_k$; hence, $N = F_n$ is a prime if for some P, Q we have $V_{(N-1)/2} \equiv 0 \pmod{N}$. On the other hand, if $N = F_n$ is a prime, we must have $V_{(N-1)/2} \equiv 0 \pmod{N}$ if $N \nmid \Delta Q$, $(\Delta/N) = 1$, and $(Q/N) = -1$. This will certainly be the case if we put $P = a + 1$, $Q = a$ $(\alpha = a, \beta = 1)$, where $(a/N) = -1$. Thus, $N = F_n$ is a prime if and only if $V_{(N-1)/2} \equiv 0 \pmod{N}$ when $P = a + 1$, $Q = a$, and $(a/N) = -1$. This, of course, is the Pepin ($a = 5, 10$) or the Proth ($a = 3$) test for the primality of F_n.

To extend these ideas to the G_n and the H_n numbers, we must find a result analogous to Theorem 2.2 for $U_{(p-\varepsilon)/3}$ and $U_{(p-\varepsilon)/5}$ when $\varepsilon = 1$. This can be done by using a simple modification of an idea developed in Williams [12] and [13]. We describe this briefly here and refer the reader to [13] for more details. (In [13] we deal with the case $p \equiv -q \equiv 1 \pmod{r}$ only.)

We let p, q, and r be odd primes such that $p \equiv q \equiv 1 \pmod{r}$ and let $K = GF(p^{q-1})$. Write $t = \text{ind } m$, where $m \equiv g^t \pmod{q}$ $(0 \leqslant t \leqslant q - 2)$ and g is a fixed primitive root of q. We consider the Gauss sum

$$(\xi, \omega) = \sum_{1}^{q-1} \xi^{\text{ind}\,k} \omega^k,$$

where ξ and ω are, respectively, primitive r^{th} and q^{th} roots of 1 in K. If, as in [13], we let $j = \text{ind } p$,

$$q\alpha = (\xi, \omega)^r, \quad q\beta = (\xi^{-1}, \omega)^r,$$

then $\alpha + \beta$, $\alpha\beta \in GF(p)$, and in K,

$$(q\alpha)^{(p-1)/r} = (\xi, \omega)^{p-1} = (\xi, \omega)^{-1}(\xi, \omega\ ) = \xi^{-j}.$$

Thus, if $P \equiv \alpha + \beta \pmod{p}$ and $Q \equiv \alpha\beta \pmod{p}$, then $U_{p-1} \equiv 0 \pmod{p}$. Also

$$U_{(p-1)/r} \not\equiv 0 \pmod{p},$$

if $\qquad p^{(q-1)/r} \not\equiv 0, 1 \pmod{q}$.

This result is analogous to Theorem 2.2; however, in order for it to be useful, we must be able to compute values for $\alpha + \beta$ and $\alpha\beta$. The value of $\alpha\beta$ is simply q^{r-2}, but $\alpha + \beta$ is rather more complicated. It can be written as

$$\alpha + \beta \equiv \sum_{i=0}^{(r-3)/2} C(i, r, q)R^i \pmod{p}, \tag{2.18}$$

where the coefficients $C(i, r, q)$ are independent of p, and R can be any solution of a certain polynomial congruence (modulo p). In the case of $r = 3$, R does not occur in (2.18); in the case of $r = 5$, R can be any solution of

$$x^2 + x - 1 \equiv 0 \pmod{p}.$$

For more details on R and tables of $C(i, r, q)$, we refer the reader to [12] and [14]. Here, it is sufficient to note that $C(0, 3, 7) = 1$, $C(0, 5, 11) = -57$, and $C(1, 5, 11) = -25$.

3. THE PRIMALITY TESTS

It is evident from the results in Section 2 that it is a very simple matter to develop a sufficiency test for the primality of numbers like G_n and H_n. One need only select some integer a such that g.c.d.$(a, N) = 1$, put $P = a + 1$, $Q = a$, and determine whether

$$U_{N-1}/U_{(N-1)/r} \equiv 0 \pmod{N}. \tag{3.1}$$

Here, $r = 3$ for $N = G_n$ and $r = 5$ for $N = H_n$. If (3.1) holds, N is a prime; however, if (3.1) does not hold, we have no information about N and must select another value for a. In practical tests for the primality of these numbers we would use, instead of (3.1), the two conditions

$$\text{g.c.d.}(a^{(N-1)/r} - 1, N) = 1 \tag{3.2a}$$

and

$$a^{N-1} \equiv 1 \pmod{N}. \tag{3.2b}$$

In this case, if (3.2a) and (3.2b) hold, then (3.1) holds; if (3.2b) does not hold, N is composite. Also, if N is a prime, the first value of a selected (by trial) usually causes both (3.2a) and (3.2b) to hold. Nevertheless, this test is not effective, in that we cannot give *a priori* a value for a such that, if N is a prime, (3.2a) and (3.2b) must hold.

We will now give effective tests for the primality of G_n and H_n. We first note that, since $(\Delta/G_n) = (5/G_n) = (2/5) = -1$, we cannot use the Fibonacci numbers in a test for the primality of G_n. However, we can still give a very simple test like Test T1.2 for the primality of G_n.

Let $N = G_n$. By the results at the end of the last section we know that if $P = 1$ and $Q = 7$ then, since $N^2 \not\equiv 0, 1 \pmod{7}$, we must have

$$U_{N-1}/U_{(N-1)/3} \equiv 0 \pmod{N}$$

when N is a prime. Also, under the assumption that N is a prime,

$$(Q/N) = (7/N) = (N/7) = (2/7) = 1 \quad \text{and} \quad U_{(N-1)/2} \equiv 0 \pmod{N}$$

by Theorem 2.2. Further, since $U_{(N-1)/3} \not\equiv 0 \pmod{N}$, we cannot have $U_{(N-1)/6} \equiv 0 \pmod{N}$ by (2.4); hence,

$$U_{(N-1)/2}/U_{(N-1)/6} \equiv 0 \pmod{N}. \tag{3.3}$$

If we define $Z_m \equiv (U_{3m}/U_m)Q^{-m} = X_m Q^{-m} \pmod{N}$, then by (2.13) we have

$$Z_{6m} \equiv Z_m^3(Z_m - 2)^3 - 3Z_m^2(Z_m - 2)^2 + 3 \pmod{N}.$$

by putting $S \equiv Z_{6^k} \pmod{N}$, we have

$$S_{k+1} \equiv S_k^3(S_k - 2)^3 - 3S_k^2(S_k - 2)^2 + 3 \pmod{N}. \tag{3.4}$$

If $r = 2^n$, then

$$S_{r-1} \equiv (U_{(N-1)/2}/U_{(N-1)/6})Q^{-(N-1)/6} \pmod{N}. \tag{3.5}$$

It follows that, if $S_r \equiv 0 \pmod{N}$, then any prime factor of N must have the form $k3^{2^n} \pm 1$. Since $(2 \cdot 3^{2^n} - 1)^2 > N$, we see that N must be a prime.

Now,

$$S_0 = Z_1 \equiv (U_3/U_1)Q^{-1} \pmod{N} \quad \text{and} \quad U_3/U_1 = P^2 - Q;$$

hence,

$$S_0 \equiv P^2Q^{-1} - 1 \equiv 7^{-1} - 1 \equiv 3(N - 2)/7 \pmod{N}. \tag{3.6}$$

Thus, by combining the results (3.6), (3.4), (3.5), (3,3), and the theorems of Section 2, we get the following necessary and sufficient primality test for G_n:

<u>Primality Test (T3.1) for $N = 6^{2^n} + 1$ ($r = 2^n$)</u>

1. Put $S_0 = 3(N - 2)/7$ and define

$$S_{k+1} \equiv S_k^3(S_k - 2)^3 - 3S_k^2(S_k - 2)^2 + 3 \pmod{N}.$$

2. N is a prime if and only if

$$S_{r-1} \equiv 0 \pmod{N}.$$

Unfortunately, because of the difficulty in finding R, the primality test which we shall develop for H_n is not as simple or elegant as T3.1. Also, the formula (2.14) for Y_{5n} is not as simple as (2.12); that is, we cannot express Y_{5n} in terms of a simple polynomial in Y_n and Q^n only. However, in this case, we can directly integrate Lucas' Test T1.4 into an effective test for the primality of H_n.

Let $N = H_n$. Since $N^2 \not\equiv 0, 1 \pmod{11}$, by the results at the end of Section 2 we know that, if N is a prime, then

$$U_{N-1}/U_{(N-1)/5} \equiv 0 \pmod{N} \tag{3.7}$$

when $P \equiv -57 - 25R \pmod{N}$, $Q = 11^3 = 1331$, and

$$R^2 + R - 1 \equiv 0 \pmod{N}. \tag{3.8}$$

If we put $T_k \equiv W_{10^k} \pmod{N}$, by (2.16) we get

$$T_{k+1} \equiv T_k^2(T_k^4 - 5T_k^2 + 5)^2 - 2 \pmod{N}. \tag{3.9}$$

Hence, if $r = 2^n$, we also get

$$T_{r-1} \equiv W_{(N-1)/10} \equiv V_{(N-1)/5}Q^{-(N-1)/10} \pmod{N}.$$

It follows from (2.17) that (3.7) holds if and only if

$$T_{r-1}^4 - 3T_{r-1}^2 + 1 \equiv 0 \pmod{N}. \tag{3.10}$$

As mentioned above, the difficulty in using this as a test for the primality of H_n resides in the fact that we do not usually know *a priori* a value for R. We can, however, apply the noneffective Test T1.4 of Lucas. If this succeeds, we need not use the result above; but, even if it fails, it will provide us with a value for R and then we can use a test that we know is effective.

We note that in Lucas' test we have $P = 1$, $Q = -1$. Hence,

$$\varepsilon = (\Delta/N) = (5/N) = 1, \quad \eta = (Q/N) = 1,$$

and

$$U_{(N-1)/2} \equiv 0 \pmod{N} \tag{3.11}$$

when N is a prime.

Define

$$X_i \equiv V_{2^i} \pmod{N}$$
$$Y_i \equiv U_{2^i} \pmod{N} \quad (i \geqslant 1).$$

By (2.3) and (2.4), we have

$$Y_{i+1} \equiv Y_i X_i, \quad X_{i+1} \equiv X_i^2 - 2 \pmod{N}. \tag{3.12}$$

Also, by (2.2),

$$X_i^2 - 5Y_i^2 \equiv 4 \pmod{N}. \tag{3.13}$$

If we put $H_n = 2A5^r + 1$ ($r = 2^n$), then $A = 2^{r-1}$ and

$$U_A \equiv Y_{r-1} \equiv \prod_{i=0}^{r-2} X_i \pmod{N} \tag{3.14}$$

by (2.4). Thus, if N is a prime and $N|U_A$, we must have

$$X_m \equiv 0 \pmod{N} \tag{3.15}$$

for some $1 < m \leqslant r - 2$ ($X_1 = V_2 = 3$). Hence, by using (3.15) and (3.13), we see that

$$R \equiv 25(2 + 5 \cdot 10^{r/2}Y_m)10^{r-2} \pmod{N} \tag{3.16}$$

is a solution of (3.8).

Put

$$S_0 \equiv Y_{r-1} \pmod{N} \tag{3.17}$$

and define

$$S_{k+1} \equiv 25S_k^5 + 25S_k^3 + 5S_k \pmod{N}. \tag{3.18}$$

Using (2.9) we see that $S_k \equiv U_{A5^k} \pmod{N}$. If N is a prime, by (3.11) we must have $S_r \equiv 0 \pmod{N}$. If $S_0 \not\equiv 0 \pmod{N}$, then, for some $t < r$, we have

$$S_t \not\equiv 0 \pmod{N} \quad \text{and} \quad S_{t+1} \equiv 0 \pmod{N}.$$

By (3.18) we find that

$$R \equiv 5S_t^2 + 2 \pmod{N} \tag{3.19}$$

is a solution of (3.8). Also, if $(2 \cdot 5^{t+1} - 1)^2 > N$, then, by the Corollary of Theorem 2.4, we know that N is a prime.

We are now able to assemble this information and use (3.12), (3.16)-(3.19), (3.9) and (3.10) to develop the following test.

Primality Test (T3.2) for $H_n = 10^{2^n} + 1$ $(r = 2^n)$

1. Put $X_1 = 3$, $Y_1 = 1$ and define

$$Y_{k+1} \equiv Y_k X_k \pmod{N},$$
$$X_{k+1} \equiv X_k^2 - 2 \pmod{N}.$$

2. If $X_m \equiv 0 \pmod{N}$ for some $m \leqslant r - 2$, put

$$R \equiv 25(2 + 5 \cdot 10^{r/2} Y_m)10^{r-2} \pmod{N}$$

and go directly to step 5; otherwise,

3. Put $S_0 \equiv Y_{r-1} \pmod{N}$ and define

$$S_{k+1} \equiv 25S_k^5 + 25S_k^3 + 5S_k \pmod{N}.$$

4. Find some $t < r$ such that

$$S_{t+1} \equiv 0 \pmod{N} \text{ and } S_t \not\equiv 0 \pmod{N}.$$

If no such t exists, then N is composite and our test ends. If

$$(2 \cdot 5^{t+1} - 1)^2 > N,$$

then N is a prime and our test ends. If

$$(2 \cdot 5^{t+1} - 1)^2 < N,$$

put

$$R \equiv 5S_t^2 + 2 \pmod{N}.$$

5. Put

$$T_0 \equiv (57 + 25R)^2((5N + 1)/11)^3 - 2 \pmod{N}$$

and define

$$T_{k+1} \equiv T_k^{10} - 10T_k^8 + 35T_k^6 - 50T_k^4 + 25T_k^2 - 2 \pmod{N}.$$

6. N is a prime if and only if

$$T_{r-}^4 - 3T_{r-1}^2 + 1 \equiv 0 \pmod{N}.$$

REFERENCES

1. R. D. Carmichael. "On the Numerical Factors of the Arithmetic Forms $\alpha^n \pm \beta^n$." *Annals of Math.* (2) ***15*** (1913-1914):30-70.
2. D. H. Lehmer. "An Extended Theory of Lucas' Functions." *Annals of Math.* (2) *31* (1930):419-448.
3. E. Lucas. "Sur la division de la circonference en parties égales." Académie des Sciences de Paris, *Comptes rendues* *85* (1877):136-139.
4. E. Lucas. "Considérations nouvelles sur la théorie des nombres premiers et sur la division géométrique de la circonference en parties égales." Assoc. Francaise pour l'Avancement des Sciences, *Comptes Rendues des Sessions*, 1877, pp. 159-167.
5. E. Lucas. "Theorie des functions numériques simplement périodiques." *Amer. J. Math.* *1* (1878):184-240, 289-321.
6. E. Lucas. "Sur la série récurrent de Fermat." *Bulletino di Bibliografia e di storia delle Scienze Mathematiche e Fisiche* ***11*** (1878):783-798.
7. E. Lucas. "Question 453." *Nouv. Corresp. Math.* **5** (1879):137.
8. P. Pepin. "Sur la formule $2^{2^n} + 1$." Académie des Sciences de Paris, *Comptes rendues* ***85*** (1877):329-331.
9. F. Proth. "Mémoires présentés." Académie des Sciences de Paris, *Comptes rendues* *87* (1878):374, see also p. 926.
10. F. Proth. "Extrait d'une lettre de M. Proth." *Nouv. Corresp. Math.* *4* (1878):210-211.
11. H. Riesel. "Some Factors of the Numbers $G_n = 6^{2^n} + 1$ and $H_n = 10^{2^n} + 1$." *Math. Comp.* *23* (1969):413-415; Corrigenda, *Math. Comp.* *24* (1970):243.
12. H. C. Williams. "An Algorithm for Determining Certain Large Primes." *Congressus Numerantium III, Proc. of the Second Louisiana Conf. on Combinatorics, Graph Theory and Computing*, Utilitas Mathematica, Winnipeg, 1971, pp. 533-556.
13. H. C. Williams. "A Class of Primality Tests for Trinomials Which Include the Lucas-Lehmer Test." *Pacific J. Math.* *98* (1982):477-494.
14. H. C. Williams. "Effective Primality Tests for Some Integers of the Forms $A5^n - 1$ and $A7^n - 1$." *Math. Comp.* (To appear.)

◆◇◆◇◆