#A76 INTEGERS 22 (2022)

SOME PRIMALITY CONDITIONS FOR $N = 2p^n - 1$

E. L. Roettger
Department of General Education, Mount Royal University, Calgary, Alberta, Canada
eroettger@mtroyal.ca

H. C. Williams
Department of Mathematics and Statistics, University of Calgary, Calgary, Alberta, Canada
hwilliam@ucalgary.ca

Received: 2/15/22, Accepted: 7/19/22, Published: 8/3/22

Abstract

In 1876 Lucas published a primality test for numbers of the form $N_n = 2 \cdot 3^n - 1$. However, this test was only sufficient for the primality of N_n and required that $4 \nmid n$. In this paper we derive a necessary and sufficient test for the primality of $2p^n - 1$, where p is any prime. In the case where p is fixed and $p < 20$, we show that that this test is effective when $k \nmid n$, where k is a given fixed integer depending on p and greater than 10^{40}.

1. Introduction

In 1876 Lucas [5] introduced his test for the primality of the Mersenne numbers $M_n = 2^n - 1$. Although this test is not complete (it requires $n \equiv 3 \pmod 4$), it marked the beginning of a revolution in the theory of primality proving (see Williams [12, Chapters 3 and 5]) and led to the much-publicized Lucas-Lehmer test for the primality of M_n for any odd n. This latter test is both necessary and sufficient for the primality of M_n for any odd n. Although it is not so well-known, Lucas also proposed in [5] a primality test for the numbers of the form $N_n = 2 \cdot 3^n - 1$. (That there are primes of this form can be seen in the Table 2 of Williams and Zarnke [13].) However, this test is only a sufficiency test and is subject to the constraint that $n \equiv 2, 3 \pmod 4$. Since $5 \mid N_n$ when $n \equiv 1 \pmod 4$, this restriction could be replaced by $4 \nmid n$.

In this paper we will derive a necessary and sufficient criterion for the primality of N_n, which holds for all n such that some $k \nmid n$. Here k is a fixed integer of over 40 decimal digits. We next extend this approach to integers $N_n(p) = 2p^n - 1$, where p is any odd prime, and discuss in detail the resulting test for all $p < 20$. We also include a table of prime values of such $N_n(p)$ for all values of n less than a certain bound, depending on p.

2. Primality Testing of $Ap^n - 1$

In this section we will review several known results concerning the primality of $Ap^n - 1$, where A is an even integer. These ideas (see Roettger et al. [8]) owe their origin to the pioneering work of Lucas [6], but have since been somewhat refined.

We begin by defining the Lucas sequences (U_n) and (V_n). For coprime integers P and Q, put

$$U_n = U_n(P,Q) = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \quad V_n = V_n(P,Q) = \alpha^n + \beta^n,$$

where α, β are the zeros of $f(x) = x^2 - Px + Q$. We also designate the discriminant of $f(x)$ by $D = (\alpha - \beta)^2 = P^2 - 4Q$. The Lucas sequences have been the objects of considerable study (see, for example, [12, Chapter 4] for some of their properties). We note here that

$$V_n^2 - DU_n^2 = 4Q^n, \tag{1}$$

$$U_{2n} = U_nV_n, \quad V_{2n} = V_n^2 - 2Q^n. \tag{2}$$

Also, Lucas showed that if q is any prime such that $q \nmid Q$ and the Legendre symbol $(D/q) = -1$, then $q \mid U_{q+1}$ ([12, Theorem 4.3.1]).

It is often convenient when evaluating remote terms of (U_n) or (V_n) modulo some N [12, Section 4.4] to make use of

$$W_n = W_n(P,Q) \equiv V_{2n}(P,Q)Q^{-n} \pmod{N}, \tag{3}$$

when $\gcd(Q,N) = 1$. Note that $W_0 = 2$, $W_1 \equiv P^2Q^{-1} - 2 \pmod{N}$. Also,

$$W_{2n} \equiv W_n^2 - 2 \pmod{N}. \tag{4}$$

We have the following simple result.

Proposition 1. If q is any prime such that $q \nmid QD$, then for $n > 0$ we have

$$q \mid U_n \Leftrightarrow W_n \equiv 2 \pmod{q}.$$

Proof. Follows easily from (3), (1) and the last identity in (2). $\square$

On referring to [12, Section 4.2] (See also Stein and Williams [9]), we define polynomials $G_n(x)$ by

$$x^nG_n(x + x^{-1}) = \frac{x^{2n+1} - 1}{x - 1}.$$

We have $G_0(x) = 1$, $G_1(x) = x + 1$ and

$$G_{m+1}(x) = xG_m(x) - G_{m-1}(x) \quad (m \geq 1).$$

From (4.2.67) and (4.2.68) of [12], we have

$$U_{(2s+1)n} \equiv Q^{ns}U_nG_s(W_n), \quad V_{(2s+1)n} \equiv (-1)^sQ^{ns}V_nG_s(-W_n) \pmod N. \tag{5}$$

We also see by (3), (4) and the last congruence in (5) that

$$W_{(2s+1)n} \equiv (-1)^sW_nG_s(2 - W_n^2) \pmod N. \tag{6}$$

In what follows we will assume that N is given by

$$N = Ap^n - 1, \text{where } p \text{ is an odd prime, } n > 0,\ p \nmid A \text{ and } 2 \mid A. \tag{7}$$

The next result is Corollary 2.2 of [9].

Theorem 2. *Let N be given by (7) and $A < p^n$. If for some P, Q we have $\gcd(Q, N) = 1$ and*

$$G_s(W_{(N+1)/p}(P, Q)) \equiv 0 \pmod N,$$

where $s = (p - 1)/2$, then N is a prime.

Indeed, by using ideas which originate with the work of Lucas (see [8]), we can extend this theorem.

Theorem 3. *Let N be given by (7) and $A \leq 2p^{n-2\alpha+2}$, where $1 \leq \alpha \leq n$. If for some P, Q with $\gcd(Q, N) = 1$ we have*

$$G_s(W_{(N+1)/p^\alpha}(P, Q)) \equiv 0 \pmod N,$$

where $s = (p - 1)/2$, then N is a prime.

Proof. By Corollary 11.3.3 of [12], we know that if r is any prime divisor of N, then $r \equiv \pm 1 \pmod{p^k}$, where $p^k \mid\mid (N + 1)/p^{\alpha-1}$. Thus, since $p^\alpha \mid\mid N + 1$, we have $k = n - \alpha + 1$ and

$$r = hp^{n-\alpha+1} \pm 1.$$

Since r is a prime, we have $2 \mid h$ and $r \geq 2p^{n-\alpha+1} - 1$. Since $A \leq 2p^{n-2\alpha+2}$ and $p^{n-\alpha+1} > 2$, we have $r^2 > N$. It follows that N must be a prime. □

Suppose we put $T_0 \equiv W_A \pmod N$ and define

$$T_{i+1} \equiv (-1)^sT_iG_s(2 - T_i^2) \pmod N.$$

By (6) we see that

$$T_i \equiv W_{Ap^i} \pmod{N}. \tag{8}$$

Notice that if N is a prime, $\gcd(Q,N) = 1$ and $(D/N) = -1$, we must have $N \mid U_{N+1}$, which by Proposition 1 means that $W_{N+1} \equiv 2 \pmod{N}$. Thus from (8) we get

$$T_n \equiv 2 \pmod{N}.$$

In order to prove the main result of this section (Theorem 4) we need two simple observations.

Lemma 1. *If* $\gcd(U_A, N) = 1$, $\gcd(Q,N) = 1$ *and the Jacobi symbol* $(D/N) = -1$, *then* $T_0 = W_A \not\equiv 2 \pmod{N}$.

Proof. Suppose $W_A \equiv 2 \pmod{N}$. We have $V_{2A} \equiv 2Q^A \pmod{N}$ and $V_A^2 \equiv 4Q^A \pmod{N}$ by (2). Thus, from (1) we get

$$N \mid DU_A^2,$$

which is impossible. □

Lemma 2. *Suppose N is given by (7), N is a prime,* $\gcd(Q,N) = 1$, $(D/N) = -1$ *and $N \nmid U_A$. If m is the least positive integer such that* $T_m \equiv 2 \pmod{N}$, *then* $N \mid G_s(T_{m-1})$.

Proof. We have already seen that $T_n \equiv 2 \pmod{N}$ and by Lemma 1 we have $T_0 \not\equiv 2 \pmod{N}$. Thus, a value of m must exist. By Proposition 1, we have $N \mid U_{Ap^m}$. It follows from (5) and (8) that $N \mid U_{Ap^{m-1}} G_s(T_{m-1})$. If $N \mid U_{Ap^{m-1}}$, then by Proposition 1, we have $T_{m-1} \equiv 2 \pmod{N}$, which by Lemma 1 means that $m - 1 \geq 1$. However, this violates the definition of m, hence, $N \mid G_s(T_{m-1})$. □

Theorem 4. *Suppose we have P, Q such that* $\gcd(Q,N) = 1$, *the Jacobi symbol* $(D/N) = -1$ *and $N \nmid U_A(P,Q)$. Suppose further that m is the least positive integer such that $m \leq n$ and* $T_m \equiv 2 \pmod{N}$. *If no such m exists, then N is composite. If* $G_s(T_{m-1}) \not\equiv 0 \pmod{N}$, *then N is composite; if* $G_s(T_{m-1}) \equiv 0 \pmod{N}$ *and* $A \leq 2p^{2m-n}$, *then N is a prime.*

Proof. By Lemma 2 we know that m must exist if N is a prime. Thus, if $T_m \not\equiv 2 \pmod{N}$ for all m such that $1 \leq m \leq n$, then N is composite. If N is a prime, we know from Lemma 2 that $N \mid G_s(T_{m-1})$; thus, if $N \nmid G_s(T_{m-1})$, then N is composite. If $G_s(T_{m-1}) \equiv 0 \pmod{N}$, by Theorem 3 with $\alpha = n - m + 1$, we see that N must be a prime when $A \leq 2p^{2m-n}$. □

Notice that if $A = 2$ and $2m \geq n$, then $A \leq 2p^{2m-n}$. We now have the following sufficiency test for the primality of $N = 2p^n - 1$, when we are given P, Q such that $(D/N) = -1$ and $\gcd(PQ,N) = 1$ ($U_A = U_2 = P$).

Corollary 1. *For N, P, Q given as above*

1) Put

$$T_0 \equiv W_2 \pmod{N}, \quad s = (p-1)/2.$$

2) Define

$$T_{i+1} \equiv (-1)^s T_i G_s(2 - T_i^2) \pmod{N}.$$

3) Find the least positive m such that $m \leq n$, $T_m \equiv 0 \pmod{N}$ and $G_s(T_{m-1}) \equiv 0 \pmod{N}$. If no such m exists, N is composite. If such an m exists and $2m \geq n$, then N is a prime.

If $T_m \equiv 2 \pmod{N}$, $G_s(T_{m-1}) \equiv 0 \pmod{N}$ and $2m < n$, we cannot decide whether or not N is a prime. However, by results in Williams [11] (Theorem 2), we have, for a given Q and D, precisely $\phi(Ap^m)$ values of $P \pmod{N}$ are such that $G_s(T_{m-1}) \equiv 0 \pmod{N}$. Thus, there are at least $p^n - p^{\lfloor n/2 \rfloor}$ values of P for which $G_s(T_{m-1}) \equiv 0 \pmod{N}$ and $2m \geq n$. Thus, a selection of P such that $G_s(T_{m-1}) \equiv 0 \pmod{N}$ and $2m < n$ would be very unlikely. This makes Corollary 1 a very practical test for the primality of N given by (7). In the sequel we will tighten this up even further.

3. Lucas-Lehmer Type Tests for Primality

We begin this section by pointing out that results in Williams [10] can be used to prove the following theorem for N given by (7) and $p = 3$.

Theorem 5. *Let $N = A3^n - 1$ for $n > 0$, $2 \mid A$, $3 \nmid A$, and $A < 3^n$. Suppose q is some prime such that $q \equiv 1 \pmod{3}$, $N^{(q-1)/3} \not\equiv 1 \pmod{q}$ and $4q = t^2 + 27u^2$, where $t \equiv 1 \pmod{3}$. If $\gcd(N, qu) = 1$, $P = t$, $Q = q$, then N is a prime if and only if $W_{(N+1)/3}(P, Q) \equiv -1 \pmod{N}$.*

A proof that for any given prime $q \equiv 1 \pmod{3}$, values of t and u must always exist can be found in Section 6 of Chapter 9 of Ireland and Rosen [4] and Chapter 4 of Cox [3]. Also, the values of D here is $-27u^2$ and $(D/N) = (-3/N) = (N/3) = -1$. We should mention here that this result was improved by Berrizbeitia and Berry [1], who showed using a different approach that it will hold when $A/2 < 4 \cdot 3^n - 1$.

Corollary 2. *For N, P, Q given in the theorem*

1) Put

$$T_0 \equiv W_2 \pmod{N}.$$

2) Define

$$T_{i+1} \equiv T_i(T_i^2 - 3) \pmod{N} \quad (i > 0).$$

3) N is a prime if and only if $T_{n-1} \equiv -1 \pmod{N}$.

In the case of $N = 2 \cdot 3^n - 1$, it is shown in [12, Section 11.3], that if $P = 1$, $Q = 7$, Corollary 2 gives a necessary and sufficient test for the primality of N whenever $6 \nmid n$. This test falls into a category of tests defined in [7] as being of L-L or Lucas-Lehmer type. For a certain fixed $l \geq 1$ such tests satisfy the following 4 conditions:

1) The test is restricted to values of N given by an expression involving some base b and some exponent n, which belongs to a preselected congruence class and exceeds a given bound.

2) The test makes use of l sequences $(T_{i,k})_{k\geq 0}$, where $1 \leq i \leq l$. The values of $T_{i,0}$ $(i = 1, 2, \dots, l)$ (the seeds) can be calculated by a simple, deterministic process and values of terms in the sequence $(T_{i,k})_{k\geq 0}$ $(i = 1, 2, \dots, l)$ modulo N can be computed from $T_{i,j+1} \equiv g_i(T_{i,j}) \pmod{N}$, where each g_i $(i = 1, 2, \dots, l)$ is a fixed (independent of n and j) polynomial in l variables and with integer coefficients. This step terminates at a value for k determined from n.

3) There is a closing condition which declares N a prime if and only if it divides some fixed polynomial function(s) of some of the $T_{i,j}$ values computed in (2).

4) The entire test executes in time $O(nM(n))$.

Here $M(n)$ denotes the number of elementary bit operations needed to multiply two numbers of n bits. Notice that the Lucas-Lehmer test for the primality of M_n also fall into this class of tests for $l = 1$. In this paper we will show how to find L-L tests with $l = 1$ for $N = 2p^n - 1$.

We first review some results in [12, Chapter 11]. Let p, q be distinct odd primes such that $q \equiv 1 \pmod{p}$. There exist certain integers $C(i, p, q)$ for $i = 0, 1, 2, \dots, s-1$ $(s = (p-1)/2)$ which can be computed by a deterministic algorithm requiring at most $O((p + \log q)q) + O(p^3)$ arithmetic operations, where the numbers involved will not exceed $(2q)^{p/2}$ (see p.264 of [12, Section 11.1]). Suppose r is any prime such that $r \equiv -1 \pmod{p}$ and R be any one of the roots of $G_s(x) \equiv 0 \pmod{r}$ (there must be exactly s of these) and put $P = \sum_{i=0}^{s-1} C(i, p, q)R^i$, $Q = q^{r-2}$; then, if $r^{(q-1)/p} \not\equiv 1 \pmod{q}$ we must have ([12, p. 274])

$$r \nmid U_{(r+1)/p}(P, Q) \quad \text{and} \quad r \mid U_{r+1}.$$

By (5) we get the following theorem.

Theorem 6. *Let r be any prime such that $r \equiv -1 \pmod{p}$ and let R be any integer such that $G_s(R) \equiv 0 \pmod{r}$. If $r^{(q-1)/p} \not\equiv 1 \pmod{q}$ and*

$$P \equiv \sum_{i=0}^{s-1} C(i, p, q)R^i, \quad Q \equiv q^{p-2} \pmod{r},$$

then

$$G_s(W_{(r+1)/p}) \equiv 0 \pmod{r}.$$

By combining the results of Theorem 6 and Theorem 3, we get Theorem 7 (cf. Theorem 11.3.6 of [12]).

Theorem 7. *Let $N = Ap^n - 1$, $s = (p-1)/2$, where p is an odd prime, $A < p^n$ and $2 \mid A$. Let q be any prime such that $q \equiv 1 \pmod{p}$ and $N^{(q-1)/p} \not\equiv 0, 1 \pmod{p}$. If R satisfies the congruence*

$$G_s(R) \equiv 0 \pmod{N}$$

and

$$P \equiv \sum_{i=0}^{s-1} C(i, p, q) R^i, \quad Q \equiv q^{p-2} \pmod{r},$$

then N is a prime if and only if $G_s(T_{n-1}) \equiv 0 \pmod{N}$, where $T_0 \equiv W_A \pmod{N}$ and

$$T_{i+1} \equiv (-1)^s G_s(2 - T_i^2) \pmod{N} \quad (i = 0, 1, 2, \dots).$$

By combining Theorem 4 and Theorem 7 it is possible to devise a Lucas-Lehmer test for the primality of $N = Ap^n - 1$ (cf. Algorithm 11.3.7 of [12]).

Algorithm 8. Test for the primality of $N = Ap^n - 1$, where $A < p^n$, p an odd prime, and $2 \mid A$. We assume we are given P, Q, q such that $(D/N) = -1$, $N \nmid U_A$ and $N^{(q-1)/p} \not\equiv -1 \pmod{q}$,

1) Put $S_0 \equiv W_A(P, Q) \pmod{N}$ and compute $S_1, S_2, \dots$ by

$$S_{i+1} \equiv (-1)^s S_i G_s(2 - S_i^2) \pmod{N}.$$

until we find the least positive $m \leq n$ such that

$$S_m \equiv 2 \pmod{N}.$$

If no such m exists, then N is composite and the algorithm terminates. Put $R \equiv S_{m-1} \pmod{N}$. If $G_s(R) \not\equiv 0 \pmod{N}$, then N is composite and the algorithm terminates. If $A < 2p^{2m-n}$, then N is a prime and the algorithm terminates.

2) If $A \geq 2p^{2m-n}$, put

$$P' \equiv \sum_{i=0}^{s-1} C(i, p, q) R^i, \quad Q' \equiv q^{p-2}, \quad T_0 \equiv W_A(P', Q') \pmod{N}.$$

3) Compute T_{n-1} by using

$$T_{i+1} \equiv (-1)^s T_i G_s(2 - T_i^2) \pmod{N}.$$

4) N is a prime if and only if $N \mid G_s(T_{n-1})$.

Notice here that we execute step (1), and if we are unsuccessful in determining whether N is composite or prime, we nevertheless obtain a piece of information, namely a value for R, which can be used in steps (2)-(4) and is guaranteed to resolve the issue of whether N is a prime. If we know values for P, Q, q, the complexity of Algorithm 8 is $O(nM(n))$. Also, as noted in Section 2, in practice we almost always prove N a prime in step (1).

The difficulty in applying Algorithm 8 is that it is not effective; that is, it does not provide a means of finding, for a given N, suitable values of P, Q such that $N \nmid U_A(P,Q)$, $(D/N) = -1$, and a prime q such that $q \equiv 1 \pmod{p}$ and $N^{(q-1)/p} \not\equiv 1 \pmod{q}$. For certain special values of N it is often possible to do this, but in general this seems to be a difficult problem. In the next section we will address this problem in the special case of $A = 2$.

4. Determination of Suitable P, Q and q

In this section we will consider the question of how to find values for P, Q, q which will be applicable to Algorithm 8 when N is given by (7). We first observe that for N given by (7), we have $N \equiv 1 \pmod{4}$. Thus, if we have some prime r such that the Legendre symbol $(N/r) = -1$, then on putting $P = 2$, $Q = 1 - r$, we get $D = 4r$ and

$$(D/N) = (4r/N) = (r/N) = (N/r) = -1.$$

In the case of $p \equiv -1 \pmod{4}$, we have

$$(N/p) = (-1/p) = -1;$$

thus, we can put $r = p$ in this case. However, in the case where $p \equiv 1 \pmod{4}$, there is no obvious value for r. In either case, we see that since $U_A = U_2 = P = 2$, we have $N \nmid U_A$. Indeed, for any A and a fixed p, we see that since $2^{A-1}(\sqrt{r})^{A-1} > U_A(2, 1-r) > 0$, we find that for all sufficiently large values of n we have $N_n > U_A = U_A(2, 1-r)$. That is, there exists a fixed bound $B(p, r, A)$ whose value depends only on p, r, and A such that if $n > B(p, r, A)$, then $N_n > U_A$ and therefore $N_n \nmid U_A$. Thus, our object in this section is that of finding a prime r such that $(N/r) = -1$ when $p \equiv 1 \pmod{4}$ and a prime q such that $q \equiv 1 \pmod{p}$ and $N^{(p-1)/q} \equiv 1 \pmod{q}$. We will leave the first problem in abeyance and deal with the second problem first.

For some fixed prime p, let $\mathscr{C} = \{q_1, q_2, \ldots, q_j\}$ be a set of j primes such that $q_i \equiv 1 \pmod{p}$ $(i = 1, 2, \ldots, j)$. We say (see [12, Section 16.4] or [9, Section 4]) that $\mathscr{C}$ is a p^{th} power nonresidue covering set for (N_n) if for any $n \geq 0$, there must exist some $q \in \mathscr{C}$ such that

$$N_n^{(q-1)/p} \not\equiv 1 \pmod{q}. \tag{9}$$

For example, if $N_n = 4 \cdot 3^n - 1$, it is easy to establish that $\mathscr{C} = \{7, 13\}$ is a cubic nonresidue covering set for (N_n). As discussed in [12, Section 16.4] and in the particular instance of $A = p - 1$ in [9], it is often the case that such a covering set will exist for most (N_n) defined in (7) except those for which $A = p^{pk} - x^p$ $(x = \pm 1)$. When $k = 0$ and $x = -1$, we get $A = 2$, which excludes those N_n where $A = 2$. Indeed, when $N_n = 2p^n - 1$, we have $N_0 = 1$, and consequently there cannot exist any p^{th} power nonresidue covering set for (N_n). Thus, for a fixed p, the best that we might hope to have is some small finite set $\mathscr{T}$ of primes such that for some $q \in \mathscr{T}$, we have (9) unless $n = 0$. However, it is easy to see that such a $\mathscr{T}$ cannot exist. For since $\mathscr{T}$ is finite, there must exist some integer h such that $p^h \equiv 1 \pmod{q}$ for all $q \in \mathscr{T}$. In this case $N_{ht} \equiv 1 \pmod{q}$ for any integer t and all $q \in \mathscr{T}$. It follows that (9) cannot be true whenever $h \mid n$. We should instead search for a small set $\mathscr{T}$ and a large integer k such that

$$N_n^{(q-1)/p} \not\equiv 1 \pmod{q} \text{ for some } q \in \mathscr{T} \text{ when } k \nmid n. \tag{10}$$

As a simple example, we remind the reader that when $p = 3$, we can put $\mathscr{T} = \{7\}$ and $k = 6$.

To realize this objective, we first consider any prime q and let g be a primitive root of q. If we define $i_q = \text{ind}_g p$, $\sigma_q = \gcd(i_q, q-1)$ and $\omega_q = (q-1)/\sigma_q$, then ω_q is the order of p modulo q. If $q \nmid N_n$, $q \equiv 1 \pmod{p}$ and (9) is not true, then

$$N_n^{(q-1)/p} \equiv 1, t, t^2, \ldots, t^{j-1} \pmod{q},$$

where $t \equiv g^p \pmod{q}$ and $j = (q-1)/p$. Thus, since $N_n = 2p^n - 1$, we get

$$p^n \equiv \frac{q+1}{2}(1 + t^i) \pmod{q}$$

for some i such that $0 \le i \le j - 1$. Now set

$$\mathscr{R}_q = \left\{ \frac{q+1}{2}(1 + t^i) \pmod{q} : i = 0, 1, \ldots, j-1 \right\}.$$

We need

$$p^n \equiv u \pmod{q}, \tag{11}$$

where $u \in \mathscr{R}_q$. This means that $\sigma_q \mid \text{ind}_g u$. Put

$$\mathscr{Y}_q = \{ y \in \mathscr{R}_q : \sigma_q \mid \text{ind}_g y \}$$

and

$$\mathscr{W}_q = \left\{ w : w \equiv (i_q/\sigma_q)^{-1} (\text{ind}_g y)/\sigma_q \pmod{\omega_q}, y \in \mathscr{Y}_q \right\}.$$

Thus, we see by (11) that

$$N_n^{(q-1)/p} \equiv 1 \pmod{q}, \tag{12}$$

if and only if $n \pmod{\omega_q} \in \mathscr{W}_q$.

Now suppose we have some positive integer k and a corresponding set $\mathscr{T}$ such that (10) is true. Our objective will be to find for a given positive integer $\hbar$ such that $\hbar \nmid k$, a set $\mathscr{T}' \supseteq \mathscr{T}$ of primes q ($\equiv 1 \pmod{p}$) such that (10) holds when k is replaced by k' and $k' = \text{lcm}[\hbar, k]$. For example, consider the case of $N_n = 2 \cdot 3^n - 1$, $\mathscr{T} = \{7\}$ and $k = 6$. Select $\hbar = 9$ and $q = 19$. We have $\omega_q = 18$ and

$$\mathscr{W}_{19} \equiv \{0, 8, 10, 13, 14\} \pmod{18}.$$

Since $6 \mid 18$ the only possible entry in $\mathscr{W}_{19}$ for (12) to hold is 0 for $\mathscr{T}' = \{7, 19\}$. Thus, we can guarantee (10) with k replaced by 18 and $\mathscr{T}$ replaced by $\mathscr{T}'$.

In order to implement this idea in general, we let B be some convenient (for the computational environment) bound and put

$$\mathbb{Q}_p = \{q : q \text{ is prime}, q \equiv 1 \pmod{p}, q < B\}$$

when $N_n = 2p^n - 1$. We will require $\hbar \mid \omega_q$, which means that $q \equiv 1 \pmod{\hbar}$. We now define

$$\mathbb{Q}(l) = \{q : q \in \mathbb{Q}_p, \hbar \mid \omega_q\}.$$

Let $q \in \mathbb{Q}(\hbar)$, put $k_q = \gcd(\omega_q, k)$ and

$$\mathfrak{X}_q \equiv \{w \in \mathscr{W}_q : w \equiv 0 \pmod{k_q}\} \pmod{w_q}.$$

If we have a set of primes $\mathscr{T}^* \subseteq \mathbb{Q}(\hbar)$ such that

$$\bigcap_{q \in \mathscr{T}^*} \mathfrak{X}_q \equiv \{0\} \pmod{\hbar}, \tag{13}$$

then (9) holds for some prime in $\mathscr{T} \cup \mathscr{T}^*$ when $k \nmid n$ and $\hbar \nmid n$. Thus, we can replace $\mathscr{T}$ by $\mathscr{T} \cup \mathscr{T}^*$ and k by $k' = \text{lcm}[k, \hbar]$.

Under the not unreasonable assumption that elements in the set $\mathfrak{X}_q \pmod{l}$ are somewhat randomly distributed, we would expect that (13) would occur for a small value of $\#\mathscr{T}^*$. For example, consider once again $N_n = 2 \cdot 3^n - 1$. For $\mathscr{T} = \{7, 19\}$ we have $k = 18$. Suppose that we select $\hbar = 11$. For $q = 67$, we get $\omega_{67} = 22$ and $k_{67} = 2$. Thus, $\mathfrak{X}_{67} \equiv \{0, 4, 10\} \pmod{22} \equiv \{0, 4, 10\} \pmod{11}$. If $q = 397$, we get $\omega_{397} = 198$, $k_{397} = 18$, $\mathfrak{X}_{397} \equiv \{0, 108, 162\} \pmod{198} \equiv \{0, 9, 8\} \pmod{11}$. Since $\mathfrak{X}_{67} \cap \mathfrak{X}_{397} \equiv \{0\} \pmod{11}$, we can replace $\mathscr{T}$ by $\{7, 19, 67, 397\}$ and k by $11 \cdot 18 = 198$.

We now turn our attention to the problem of finding a prime r when $p \equiv 1 \pmod{4}$. It is easy to see that the technique just described can be used, but instead of $\mathscr{W}_q$, we deal with

$$\mathscr{W}_r' = \{n : (N_n/r) = 1; n = 0, 1, 2, \ldots, \omega_r - 1\}.$$

Also, to compute $\mathscr{W}_r'$, we can use the simple recurrence formula

$$N_{i+1} \equiv pN_i + p - 1 \pmod r \quad (j \geq 0),$$

where $N_0 = 1$. We use the method above to find a set of primes $\mathscr{T}$ and an integer k such that $(N_n/r) = -1$ for some $r \in \mathscr{T}$ whenever $k \nmid n$. For example, suppose $p = 17$ and $r = 5$; we get $\omega_5 = 4$ and

$$\mathscr{W}_5' \equiv \{0\} \pmod 4.$$

Thus, if $\mathscr{T} = \{5\}$, we can use $k = 4$. If we next select $l = 3$ and put $r = 7$, the $\omega_7 = 6$ and

$$\mathscr{W}_7' \equiv \{0, 3, 5\} \pmod 6.$$

Putting $k_7 = \gcd(\omega_7, k) = \gcd(6, 4) = 2$, we get the corresponding

$$\mathscr{X}_7 \equiv \{0\} \pmod 3.$$

Thus, we can put $\mathscr{T} = \{5, 7\}$ and $k = 12$.

5. Computational Results

To test the effectiveness of the procedures of the previous section, we implemented them on a computer. We coded using Maple and ran the programs on a iMac with an Apple M1 chip and 16 GB of memory. After a given initial value for $\hbar$, the computer program selected values for $\hbar = t^\alpha$, where t is a prime < 100 and $\hbar < 1000$.

In the case of $N_n = 2 \cdot 3^n - 1$, we were able to produce Table 1 when $B = 10000$. To have some indication of run time we note here that to find the starting step where $q = 7$ in the table below, the computer took 1825.20 seconds to search up to the bound $B = 10000$. However, if we stop the search after a set is found i.e., $\{0\}$ when $q = 7$, the program executes in only takes 0.82 seconds. We then continue using the methods described in Section 4; we choose a value for $\hbar$ and use the program to find q values that allow us to increase our value for k. For instance in the table below, to search all potential q (up to our bound) in the second row where $\hbar = 9$ takes 439.65 seconds. We note that as our k increases in size the search time decreases significantly as it produces fewer potential useful primes.

q	ω_q	k_q	$\mathscr{X}_q \pmod{\hbar}$	$\hbar$	k
7	6		$\{0\}$	6	$2 \cdot 3$
19	18	6	$\{0\}$	9	$2 \cdot 3^2$
61	10	2	$\{0\}$	5	$2 \cdot 3^2 \cdot 5$
421	105	15	$\{0\}$	7	$2 \cdot 3^2 \cdot 5 \cdot 7$

241	120	30	$\{0\}$	8	$2^3 \cdot 3^2 \cdot 5 \cdot 7$
379	378	126	$\{0\}$	27	$2^3 \cdot 3^3 \cdot 5 \cdot 7$
1201	300	60	$\{0\}$	25	$2^3 \cdot 3^3 \cdot 5^2 \cdot 7$
751	750	150	$\{0\}$	125	$2^3 \cdot 3^3 \cdot 5^3 \cdot 7$
1471	294	42	$\{0, 42\}$	49	$2^3 \cdot 3^3 \cdot 5^3 \cdot 7$
2647	2646	378	$\{0, 14\}$	49	$2^3 \cdot 3^3 \cdot 5^3 \cdot 7^2$
67	22	2	$\{0, 4, 10\}$	11	$2^3 \cdot 3^3 \cdot 5^3 \cdot 7^2$
397	198	18	$\{0, 8, 9\}$	11	$2^3 \cdot 3^3 \cdot 5^3 \cdot 7^2 \cdot 11$
2731	2730	210	$\{0, 5, 10\}$	13	$2^3 \cdot 3^3 \cdot 5^3 \cdot 7^2 \cdot 11$
2887	78	6	$\{0, 2, 9\}$	13	$2^3 \cdot 3^3 \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 13$
103	34	2	$\{0, 12, 13\}$	17	$2^3 \cdot 3^3 \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 13$
409	204	12	$\{0, 1, 5, 115\}$	17	$2^3 \cdot 3^3 \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17$
1597	19	1	$\{0, 1, 5, 7, 8, 10, 16, 18\}$	19	$2^3 \cdot 3^3 \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17$
2053	1026	54	$\{0, 3, 6, 9, 14, 15\}$	19	$2^3 \cdot 3^3 \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19$
139	138	6	$\{0, 2, 3, 7, 12, 15, 16, 19\}$	23	$2^3 \cdot 3^3 \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19$
691	690	30	$\{0, 4, 5, 6, 10, 13, 14, 20\}$	23	$2^3 \cdot 3^3 \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23$
4177	232	8	$\{0, 13, 19, 28\}$	29	$2^3 \cdot 3^3 \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23$
5743	522	18	$\{0, 3, 11, 21, 27\}$	29	$2^3 \cdot 3^3 \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29$
1303	434	14	$\{0, 6, 8, 10, 13, 16, 18, 24, 29\}$	31	$2^3 \cdot 3^3 \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29$
5581	2790	90	$\{0, 7, 11, 14, 22, 26, 30\}$	31	$2^3 \cdot 3^3 \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31$
6661	1665	45	$\{0, 5, 6, 7, 8, 9, 16, 17, 21, 23, 35\}$	37	$2^3 \cdot 3^3 \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31$
7993	1998	54	$\{0, 14, 15, 18, 20, 24, 29, 30, 32, 36\}$	37	$2^3 \cdot 3^3 \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37$
2707	2706	66	$\{0, 3, 5, 11, 15, 17, 26, 27, 29, 30, 33, 35, 37\}$	41	$2^3 \cdot 3^3 \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37$
2953	738	18	$\{0, 4, 10, 12, 14, 19, 20, 21, 25, 36, 38\}$	41	$2^3 \cdot 3^3 \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 41$
97	48	24	$\{0\}$	16	$2^4 \cdot 3^3 \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 41$
2689	1344	336	$\{0\}$	64	$2^6 \cdot 3^3 \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot$

					41
4051	810	270	$\{0\}$	81	$2^6\cdot 3^4\cdot 5^3\cdot 7^2\cdot 11\cdot 13\cdot 17\cdot 19\cdot 23\cdot 29\cdot 31\cdot 37\cdot 41$
487	486	162	$\{0\}$	243	$2^6\cdot 3^5\cdot 5^3\cdot 7^2\cdot 11\cdot 13\cdot 17\cdot 19\cdot 23\cdot 29\cdot 31\cdot 37\cdot 41$
1459	1458	486	$\{0\}$	729	$2^6\cdot 3^6\cdot 5^3\cdot 7^2\cdot 11\cdot 13\cdot 17\cdot 19\cdot 23\cdot 29\cdot 31\cdot 37\cdot 41$
3613	1806	42	$\{0,5,9,17,32,34,35,36,37,40,42\}$	43	$2^6\cdot 3^6\cdot 5^3\cdot 7^2\cdot 11\cdot 13\cdot 17\cdot 19\cdot 23\cdot 29\cdot 31\cdot 37\cdot 41$
4129	129	3	$\{0,2,5,6,12,14,23,26,27,28,29,33,35,36,38\}$	43	$2^6\cdot 3^6\cdot 5^3\cdot 7^2\cdot 11\cdot 13\cdot 17\cdot 19\cdot 23\cdot 29\cdot 31\cdot 37\cdot 41$
6451	6450	150	$\{0,4,11,14,20,21,22,24,25,30,31,32,39,41\}$	43	$2^6\cdot 3^6\cdot 5^3\cdot 7^2\cdot 11\cdot 13\cdot 17\cdot 19\cdot 23\cdot 29\cdot 31\cdot 37\cdot 41\cdot 43$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
1747	1746	18	$\{0,3,4,5,8,10,11,13,14,20,22,24,27,33,34,35,36,37,39,40,41,45,51,58,62,69,71,79,81,82,84,85,89,91,93,96\}$	97	$2^6\cdot 3^6\cdot 5^3\cdot 7^2\cdot 11\cdot 13\cdot 17\cdot 19\cdot 23\cdot 29\cdot 31\cdot 37\cdot 41\cdot 43\cdot 47\cdot 53\cdot 59\cdot 61\cdot 67\cdot 71\cdot 73\cdot 79\cdot 89$
4657	2328	24	$\{0,2,4,5,6,8,9,10,12,16,26,31,34,35,53,54,56,59,66,67,70,72,75,78,79,80,81,83,88,90,91,92,94\}$	97	$2^6\cdot 3^6\cdot 5^3\cdot 7^2\cdot 11\cdot 13\cdot 17\cdot 19\cdot 23\cdot 29\cdot 31\cdot 37\cdot 41\cdot 43\cdot 47\cdot 53\cdot 59\cdot 61\cdot 67\cdot 71\cdot 73\cdot 79\cdot 89$
5821	1455	15	$\{0,4,6,7,11,13,16,17,27,28,31,35,38,39,40,47,48,49,53,55,57,60,63,68,69,71,73,74,75,81,84,92,93,95\}$	97	$2^6\cdot 3^6\cdot 5^3\cdot 7^2\cdot 11\cdot 13\cdot 17\cdot 19\cdot 23\cdot 29\cdot 31\cdot 37\cdot 41\cdot 43\cdot 47\cdot 53\cdot 59\cdot 61\cdot 67\cdot 71\cdot 73\cdot 79\cdot 89$
8731	8730	90	$\{0,5,6,15,18,19,20,23,27,29,30,34,39,43,44,45,52,54,57,58,59,62,76,79,82,83,91,92\}$	97	$2^6\cdot 3^6\cdot 5^3\cdot 7^2\cdot 11\cdot 13\cdot 17\cdot 19\cdot 23\cdot 29\cdot 31\cdot 37\cdot 41\cdot 43\cdot 47\cdot 53\cdot 59\cdot 61\cdot 67\cdot 71\cdot 73\cdot 79\cdot 89\cdot 97$

Table 1: $N_n(3) = 2\cdot 3^n - 1$, $\mathfrak{X}_q \equiv \{x \in \mathscr{W}_q : x \equiv 0 \pmod{k_q}\}$ $(q < 10000)$

For the sake of brevity we have not included the complete Table 1. The missing rows are for all the prime values of k such that $47 \le k \le 89$ with the exception of

$\hbar = 83$, which the computer could not handle with $B = 10000$. By increasing B somewhat, we were able to deal with the case of $\hbar = 83$.

q	ω_q	k_q	$\mathcal{X}_q \pmod{\hbar}$	$\hbar$	k
4483	1494	18	$\{0, 1, 3, 5, 10, 11, 12, 13, 14, 15, 18, 19, 23, 28, 29, 31, 32, 38, 44, 45, 46, 48, 54, 62, 63, 73, 74, 75, 82\}$	83	$2^6 \cdot 3^6 \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 41 \cdot 43 \cdot 47 \cdot 53 \cdot 59 \cdot 61 \cdot 67 \cdot 71 \cdot 73 \cdot 79$
9463	9462	114	$\{0, 17, 28, 31, 32, 37, 44, 47, 48, 53, 55, 56, 61, 65, 72, 73, 79, 82\}$	83	$2^6 \cdot 3^6 \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 41 \cdot 43 \cdot 47 \cdot 53 \cdot 59 \cdot 61 \cdot 67 \cdot 71 \cdot 73 \cdot 79$
11953	2988	36	$\{0, 2, 3, 5, 6, 11, 12, 14, 15, 17, 18, 20, 21, 22, 23, 24, 26, 29, 33, 36, 38, 46, 47, 50, 53, 59, 62, 63, 67, 71, 72, 75, 80, 81\}$	83	$2^6 \cdot 3^6 \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 41 \cdot 43 \cdot 47 \cdot 53 \cdot 59 \cdot 61 \cdot 67 \cdot 71 \cdot 73 \cdot 79 \cdot 83$

Table 2: $N_n(3) = 2 \cdot 3^n - 1$, $\mathcal{X}_q \equiv \{x \in \mathscr{W}_q : x \equiv 0 \pmod{k_q}\}$ q unbounded

Put

$$\begin{aligned}\mathcal{T} =\{&7, 19, 61, 67, 97, 103, 139, 241, 379, 397, 409, 421, 487, 691, 751, 853, 877, 1201,\\ &1303, 1459, 1471, 1597, 1747, 1831, 2011, 2053, 2137, 2317, 2647, 2689, 2707, 2731,\\ &2887, 2953, 3217, 3319, 3499, 3541, 3613, 4027, 4051, 4129, 4177, 4231, 4261, 4273,\\ &4483, 4513, 4603, 4657, 5077, 5581, 5689, 5743, 5821, 6133, 6361, 6373, 6451, 6661,\\ &6997, 7639, 7669, 7993, 8011, 8419, 8731, 9199, 9463, 9613, 11953\}.\end{aligned}$$

Set $\kappa = 2 \cdot 3 \cdot 5 \cdots 97$, the product of all the distinct primes < 100. We have $\kappa = 2.3056 \times 10^{36}$. For $\mathcal{T}$ the set of all the primes in the first columns of Table 1, including those in the deleted rows, and Table 2, we see that $\#\mathcal{T} = 71$ and for some prime $q \in \mathcal{T}$

$$N_n^{(q-1)/3} \not\equiv 1 \pmod{q}$$

unless $k \mid n$, where $k = 2^5 \cdot 3^5 \cdot 5^2 \cdot 7 \cdot \kappa = 3.1375 \times 10^{42}$. Thus, we see that Corollary 2 is a Lucas-Lehmer test for the primality of $2 \cdot 3^n - 1$ whenever $n \not\equiv 0 \pmod{k}$.

We were also able to produce tables similar to Tables 1 and 2 for $N_n = 2p^n - 1$ and $p = 5, 7, 11, 13, 17, 19$. In Table 3, we give the sets $\mathcal{T}$ for $p = 5, 7, 11, 13, 17, 19$ and the corresponding k/κ. Again, we implemented the techniques of Section 4 to find a particular q for the given p and selected $\hbar$.

p	$\mathcal{T}$	$\#\mathcal{T}$	k
5	$\{31, 101, 211, 241, 271, 521, 541, 631, 811, 1021, 1061, 1151, 1291, 1471, 1831, 2011, 2131, 2371, 2441, 2671, 2791, 3001, 3191, 3331, 3541, 3691, 3881, 4021, 4231, 4261, 4421, 4441, 4481, 4621, 4651, 4691, 4721, 5531, 5591, 5741, 5981, 6571, 6581, 6791, 7151, 7411, 7541, 7681, 8011, 8521, 8731, 8761, 9011, 9151, 9491, 9791, 10271, 12451, 15331, 17431, 24071\}$	61	$2^7 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot \kappa$
7	$\{29, 43, 71, 197, 379, 449, 659, 701, 743, 967, 1093, 1303, 1429, 1877, 2437, 2591, 2633, 2689, 2969, 3011, 3389, 3613, 3739, 4019, 4271, 4523, 4649, 5279, 5531, 5741, 5783, 6133, 6217, 6637, 6763, 6833, 6959, 7687, 8009, 8233, 8443, 9199, 9241, 9941, 10739, 11621, 14323, 14939, 18691, 23087\}$	50	$2^5 \cdot 3^2 \cdot 5 \cdot 7^2 \cdot 11 \cdot \kappa$
11	$\{67, 89, 199, 353, 419, 683, 727, 1123, 1409, 1607, 1783, 2113, 2311, 2333, 2663, 2707, 2729, 2861, 2971, 3037, 3191, 3257, 3499, 3719, 3917, 4027, 4423, 5171, 5347, 5413, 5479, 5501, 5743, 6217, 6359, 6491, 6733, 7789, 8053, 8537, 9461, 9791, 9901, 10439, 10957, 11353, 12211, 12497, 13267, 15643, 17183, 19207, 19273\}$	53	$2^5 \cdot 3^4 \cdot 5 \cdot 11^2 \cdot 13 \cdot 17 \cdot \kappa$
13	$\{157, 313, 443, 547, 677, 859, 937, 1223, 1249, 1301, 1613, 1847, 1951, 2029, 2237, 2393, 2549, 2887, 3251, 3511, 3797, 4447, 4759, 4889, 5227, 5279, 5591, 6163, 6397, 6449, 8269, 9439, 9491, 10453, 10739, 11311, 12611, 12923, 13469, 13781, 15107, 15991, 16433, 19423, 22699, 23011, 31721, 50909, 64793\}$	49	$2^3 \cdot 3^2 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot \kappa$
17	$\{103, 409, 443, 647, 1667, 1871, 1973, 2347, 2551, 2687, 2789, 3163, 3299, 3469, 4013, 4591, 4999, 5101, 5407, 5849, 6053, 6359, 7243, 7549, 8059, 8161, 8467, 8501, 9011, 9181, 12037, 12547, 13159, 15131, 17579, 21727, 23087, 23971, 24889, 39509, 43283, 69497\}$	43	$2^3 \cdot 3^2 \cdot 5^2 \cdot 7 \cdot 17 \cdot \kappa$
19	$\{191, 419, 647, 1103, 1483, 1559, 1597, 1787, 1901, 2053, 2129, 2243, 2357, 2699, 3079, 3307, 4219, 4637, 4751, 4903, 6043, 7069,$	43	$2^3 \cdot 3^3 \cdot 5^2 \cdot \kappa$

	$7297, 7639, 7867, 8171, 8741, 8969, 9007, 9463, 11059, 12503, 15277, 15467, 18013, 18127, 22079, 22193, 24967, 27817, 71023, 73721, 84551\}$		

Table 3: Table of values q for each p

When $p \equiv 1 \pmod 4$ we need to produce a set of primes $\mathscr{T}$ and a corresponding value k such that $(N_n/r) = -1$ for some $r \in \mathscr{T}$ as long as $k \nmid n$. Our program executed in a similar way as our search for a value of q, except that for $p = 5$ and $p = 13$, there exist solutions of

$$2p^n - 1 = x^2 \tag{14}$$

for an integer x. By a result in Cohn [2], we know that the Diophantine equation

$$x^2 - 2y^n = -1 \quad (n > 2)$$

has only the solutions $(x, y, n) = (1, 1, n)$ and $(x, y, n) = (239, 13, 4)$. Thus if (14) does hold, then $n \leq 2$ or $n = 4$. When $p = 5$, we have $2 \cdot 5 - 1 = 3^2$ and $2 \cdot 5^2 - 1 = 7^2$ and there are no other solutions of (14) for $p = 5$. If we employ $r = 3$, we get $\omega_3 = 2$ and $\mathscr{W}_3' \equiv \{0\} \pmod 2$. Thus, in this case we can begin with $\mathscr{T} = \{3\}$ and $k = 2$. If we next consider $r = 7$, we have $\omega_7 = 6$ and $\mathscr{W}_7' \equiv \{0, 1, 3\} \pmod 6$; hence $\mathscr{X}_7 \equiv \{0\} \pmod 6$. At this point we can put $\mathscr{T} = \{3, 7\}$ and $k = 6$ and we proceed as earlier in spite of the global solutions of (14). For $p = 5$ and $B = 10000$ the computer found

$$\begin{aligned}\mathscr{T} =&\{3, 7, 19, 41, 47, 53, 61, 79, 83, 89, 101, 127, 149, 167, 173, 181, 197, 211, 223, 277,\\ &293, 367, 397, 401, 419, 439, 541, 659, 683, 691, 743, 821, 877, 971, 997, 1061, 1063,\\ &1123, 1163, 1291, 1303, 1373, 1423, 1459, 1471, 1553, 1607, 1621, 1747, 1787, 1831,\\ &1877, 2011, 2089, 2131, 2243, 2333, 2371, 2441, 2543, 2671, 2687, 2791, 2969, 3001,\\ &3011, 3083, 3319, 3359, 3631, 3701, 3739, 3881, 3917, 4013, 4219, 4357, 4451, 4463,\\ &4733, 5003, 5147, 5419, 5531, 5569, 5783, 6053, 6143, 6373, 6761, 6791, 6959, 7237,\\ &7243, 7639, 8011, 8179, 8233, 8419, 8521, 8663, 8713, 9127, 9431, 9521, 9871\}\end{aligned}$$

such that $\#\mathscr{T} = 106$ with corresponding $k = 2 \cdot 3^4 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13\kappa$.

Where the procedure encountered some difficulty was when $p = 13$. In this case we have $2 \cdot 13 - 1 = 5^2$ and $2 \cdot 13^4 - 1 = 239^2$. If we begin with $r = 5$, we get $\omega_5 = 4$ and $\mathscr{W}_5' \equiv \{0\} \pmod 5$. We can therefore begin with $\mathscr{T} = \{5\}$ and $k = 4$. However, the program could not eliminate the entry 4 from the $\mathscr{W}_r'$ sets and the corresponding $\mathscr{X}_r$ $(= \{x \in \mathscr{W}_r' : x \equiv 0 \pmod{k_r}\})$ for $r > 5$ unless $r = 239$. In this case we have $\omega_{239} = 238 = 2 \cdot 7 \cdot 17$. If we put $\mathscr{T}_1 = \{239, 953, 1429, 4999, 9521\}$, we see that each element r of $\mathscr{T}_1$ is such that $238 \mid \omega_r$. Also,

$$\bigcap_{r \in \mathscr{T}_1} \mathscr{X}_r \equiv \{0, 42, 46, 56, 84, 92, 96, 118, 126, 160, 174, 184, 188, 198, 210, 212, 214\} \pmod{238}.$$

We have $34 \mid \omega_r$ when $r \in \mathcal{T}_2 = \{137, 409, 1021\}$ and $17 \mid \omega_r$ when $r \in \mathcal{T}_3 = \{103, 443\}$. Even though $238 \nmid \omega_r$ for these primes, we can produce $\mathfrak{X}'_r \equiv \mathfrak{X}_r \pmod{238}$ by padding $\mathfrak{X}_r$ with additional residues as follows:

$$\mathfrak{X}'_r = \{x + 34m : x \in \mathfrak{X}_r; r \in \mathcal{T}_2; m = 0, 1, 2, \ldots, 6\}$$
$$\mathfrak{X}'_r = \{x + 17m : x \in \mathfrak{X}_r; r \in \mathcal{T}_3; m = 0, 1, 2, \ldots, 13\}.$$

We find that

$$\bigcap_{r\in\mathcal{T}_1} \mathfrak{X}_r \bigcap_{r\in\mathcal{T}_2} \mathfrak{X}'_r \bigcap_{r\in\mathcal{T}_3} \mathfrak{X}'_r \equiv \{0, 84, 118, 174\} \pmod{238}$$
$$\equiv \{0, 6\} \pmod{14}.$$

This means that if $p = 13$, we have $(N_n/r) = -1$ for some $r \in \mathcal{T}_1 \cup \mathcal{T}_2 \cup \mathcal{T}_3$ whenever $n \notin \{0, 6\} \pmod{14}$. For $r = 29$, we have $\omega_{29} = 14$ and $\mathfrak{X}_{14} \equiv \{0, 2, 10, 12\} \pmod{14}$. Thus, if we put $\mathcal{T} = \{5, 29\} \cup \mathcal{T}_1 \cup \mathcal{T}_2 \cup \mathcal{T}_3$, then $(N_n/r) = -1$ for some $r \in \mathcal{T}$ and $k \nmid n$, where $k = 28$. From this point on the program executed smoothly with $B = 10000$ and produced

$$\begin{aligned}\mathcal{T} = \{&5, 19, 29, 79, 89, 103, 113, 137, 163, 167, 197, 239, 251, 257, 281, 307, 311, 317,\\ &353, 379, 389, 401, 409, 443, 449, 487, 499, 659, 673, 683, 743, 821, 929, 953, 977, 1021,\\ &1033, 1061, 1063, 1249, 1291, 1373, 1423, 1429, 1453, 1459, 1471, 1567, 1621, 1723,\\ &1747, 1753, 1877, 1993, 1999, 2011, 2029, 2221, 2441, 2551, 2591, 2671, 2687, 2699,\\ &2729, 2833, 2969, 3001, 3011, 3299, 3319, 3389, 3691, 3797, 3923, 4027, 4057, 4273,\\ &4861, 4999, 5113, 5531, 5569, 5783, 5987, 6143, 6257, 6299, 6761, 6959, 7243, 7321,\\ &7477, 7481, 7591, 7681, 7753, 8179, 8233, 8443, 8467, 8537, 8893, 9001, 9103, 9199,\\ &9521, 9613, 9871\}\end{aligned}$$

with $\#\mathcal{T} = 109$ and $k = 2^7 \cdot 3^4 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13\kappa$.

In the case of $p = 17$, there are no solutions of (14), and again with $B = 10000$, the computer found

$$\begin{aligned}\mathcal{T} =\{&5, 7, 19, 41, 79, 83, 89, 127, 167, 173, 197, 257, 271, 277, 283, 337, 367, 389, 401,\\ &409, 431, 439, 569, 641, 659, 677, 683, 733, 739, 743, 821, 997, 1061, 1069, 1123,\\ &1129, 1201, 1231, 1291, 1409, 1453, 1459, 1613, 1621, 1747, 1873, 1877, 1889, 1933,\\ &2029, 2221, 2243, 2281, 2377, 2441, 2657, 2671, 2729, 2789, 2833, 2843, 3001, 3067,\\ &3221, 3299, 3319, 3329, 3389, 3697, 3793, 3797, 3917, 4003, 4021, 4219, 4231, 4273,\\ &4289, 4441, 4691, 4733, 4817, 5101, 5113, 5147, 5531, 6163, 6661, 6689, 6791, 6959,\\ &7243, 7321, 7669, 7841, 7951, 8011, 8467, 8537, 9011, 9049, 9199, 9929\}\end{aligned}$$

such that $\#\mathcal{T} = 103$ and $k = 2^7 \cdot 3^4 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13\kappa$.

We conclude this section with tables of all prime values of $N_n(p) = 2p^n - 1$ for $p < 20$ and n bounded as indicated. These were determined by using Corollary 1 with $P = 2$ and $Q = 1 - r$. Notice here that, as expected, we always have $2m \geq n$.

n	m	r	n	m	r	n	m	r	n	m	r
1	1	3	27	25	3	387	387	3	9204	9204	3
2	2	3	35	34	3	579	578	3	12312	12311	3
3	2	3	56	56	3	644	644	3	18806	18806	3
7	7	3	62	62	3	1772	1771	3	21114	21114	3
8	8	3	68	68	3	3751	3751	3	49340	49340	3
12	12	3	131	131	3	5270	5270	3			
20	18	3	222	221	3	6335	6335	3			
23	23	3	384	383	3	8544	8544	3			

Table 4: Prime values of $N_n = 2 \cdot 3^n - 1$ with $1 \leq n \leq 100000$

n	m	r	n	m	r	n	m	r	n	m	r
4	4	7	30	30	17	274	273	7	4204	4203	7
6	6	17	54	54	11	1332	1332	53	17736	17736	17
16	16	7	96	96	19	2766	2766	17			
24	24	11	178	177	7	3060	3060	29			

Table 5: Prime values of $N_n = 2 \cdot 5^n - 1$ with $1 \leq n \leq 60000$

n	m	r	n	m	r	n	m	r	n	m	r
1	1	7	14	14	7	46	46	7	5180	5180	7
2	2	7	24	24	7	80	80	7	22581	22581	7
4	4	7	29	29	7	474	474	7			
5	5	7	36	36	7	1018	1018	7			

Table 6: Prime values of $N_n = 2 \cdot 7^n - 1$ with $1 \leq n \leq 30000$

n	m	r	n	m	r	n	m	r	n	m	r
2	2	11	248	247	11	2900	2899	11	24746	24746	11
8	8	11	2474	2473	11	6600	6600	11			

Table 7: Prime values of $N_n = 2 \cdot 11^n - 1$ with $1 \leq n \leq 30000$

n	m	r
2	2	5
8	8	19
10	10	5
64	64	23
76	76	11

n	m	r	n	m	r	n	m	r
118	118	5	364	363	43	1607	1607	5
120	120	19	528	528	19	2091	2091	5
258	258	5	811	811	5	2572	2572	11
303	303	5	1270	1270	5	3596	3596	11
332	332	11	1362	1362	5	8190	8190	5

Table 8: Prime values of $N_n = 2 \cdot 13^n - 1$ with $1 \leq n \leq 30000$

n	m	r	n	m	r	n	m	r	n	m	r
2	2	5	74	74	5	386	386	5	630	630	5
30	30	5	122	121	5	476	476	7	20132	20132	7

Table 9: Prime values of $N_n = 2 \cdot 17^n - 1$ with $1 \leq n \leq 30000$

n	m	r	n	m	r	n	m	r	n	m	r
1	1	19	76	76	19	177	177	19	15592	15592	19
12	12	19	138	138	19	1997	1997	19	18947	18947	19
21	21	19	162	162	19	5370	5370	19			

Table 10: Prime values of $N_n = 2 \cdot 19^n - 1$ with $1 \leq n \leq 30000$

In order to provide a sense of the run time and the size of primes being tested, the following table provides this information for the largest primes found in each of the Tables 4–10.

p	n	$r.t.$ seconds	bits of $N = 2p^n - 1$
3	49340	525.39	78204
5	17736	131.82	41183
7	22581	348.78	63394
11	24746	799.67	85609
13	8190	65.87	30308
17	20132	806.02	82290
19	18947	775.13	80487

Table 11: Run time and size of largest prime found for each p

6. Conclusion

We have seen that for $N = 2p^n - 1$, p an odd prime and $p < 20$, we have an L-L test for the primality of N as long as $k \nmid n$, where k is some integer which depends for its value on p and is greater than 10^{40}. Undoubtedly, the above idea can be extended to any given prime p. Also, by going further, it should be possible to increase k for an increase in B and $\#\mathcal{T}$.

We can also apply these techniques to numbers of different forms than $Ap^n - 1$. In [7] the authors considered numbers of the form

$$M_d(n) = 10^{2n+1} - d10^n - 1,$$

where $d \in \mathcal{A} = \{1, 2, 4, 5, 7, 8\}$. They produced an L-L test for $M_d(n)$ for $d = 2, 4, 5, 7$ [7, Section 4], but where unable to do this when $d = 1$ or 8. What is required is a prime $q \equiv 1 \pmod 5$ such that $M_d(n)^{(q-1)/5} \not\equiv 1 \pmod q$. It is a simple matter to verify that is is always the case for $q = 11$ when $d \in \mathcal{A}$ and $d \neq 1,\ 8$. It is also easy to see why $d = 1$ and $d = 8$ are troublesome for any q; if we put $d = 8$, we have $M_d(n) \equiv 1 \pmod q$ when $n \equiv 0 \pmod{\omega_q}$ and if we put $d = 1$, we have $M_d(n) \equiv -1 \pmod q$ when $n \equiv -1 \pmod{\omega_q}$. Here ω_q denotes the multiplicative order of 10 modulo q. In either of these cases we get $M_d(n)^{(p-1)/5} \equiv 1 \pmod q$.

Thus, for $d = 1$ or $d = 8$ we need to deal with the problem of finding a set of primes $\mathcal{T} \subseteq \mathbb{Q}_5$ and corresponding k such that for some $q \in \mathcal{T}$, we must have

$$M_d(n)^{(q-1)/5} \not\equiv 1 \pmod q$$

unless $n \equiv e(d) \pmod k$, where

$$e(d) = \begin{cases} 0, & \text{if } d = 8; \\ -1, & \text{if } d = 1. \end{cases}$$

This can be managed by first letting g be a primitive root of $q \in \mathbb{Q}_5$ and computing $i_q = \mathrm{ind}_g 10$, $\sigma_q = \gcd(i_q, q-1)$, $\omega_q = (q-1)/\sigma_q$. For $t \equiv g^5 \pmod q$, we put

$$\mathcal{R}_q = \{1 + t^i \pmod q : i = 0, 1, 2, \ldots, j-1\},$$

where $j = (q-1)/5$. Now let

$$\mathcal{Y}_q = \{y : 10y^2 - dy \equiv u \pmod q, u \in \mathcal{R}_q, q \nmid u; \sigma_q \mid \mathrm{ind}_g y\}.$$

For this definition of the set $\mathcal{Y}_q$ we can define $\mathcal{W}_q$ as before and put $\mathcal{X}_q = \{x \in \mathcal{W}_q : x \equiv e(d) \pmod{k_q}\}$. We can now use the same approach as in Section 4 above, but we must modify the right hand side of (13) to $\{e(d)\}$.

When this process was implemented on the computer, we found

$$\begin{aligned}\mathcal{T} = \{&101, 151, 211, 241, 281, 311, 401, 491, 541, 661, 761, 941, 971, 991, 1021, 1231,\\ &1361, 1481, 1721, 1741, 2131, 2591, 2791, 2861, 3191, 5591, 6101, 6151, 7591,\\ &7951, 8461, 10601, 12391, 12421, 19471, 24851, 25621, 26701, 26801, 27011,\\ &29201, 29881, 31601, 32371, 32831, 50441, 60041, 77431\}\end{aligned}$$

with $\#\mathscr{T} = 48$, and $k = 2^2 \cdot 3^2 \cdot 5 \cdot 7\kappa$ for $d = 1$ and

$$\begin{aligned}\mathscr{T} =\{&11, 31, 61, 181, 191, 211, 281, 311, 401, 461, 571, 641, 661, 691, 751, 821, 971,\\ &1061, 1231, 1301, 1361, 1451, 1621, 1721, 1831, 1861, 2011, 2131, 2221, 2351,\\ &2371, 2441, 2671, 3011, 3691, 3701, 3881, 4021, 4231, 4241, 4261, 4451, 4651,\\ &4721, 5531, 6101, 6491, 6571, 6701, 6791, 7121, 7541, 7901, 8521, 9491, 12451,\\ &15331, 17431, 24071\}\end{aligned}$$

with $\#\mathscr{T} = 59$ and $k = 2^2 \cdot 3^2 \cdot 5^2\kappa$ for $d = 8$.

References

[1] P. Berrizbeitia and T. G. Berry, Cubic reciprocity and generalised Lucas-Lehmer tests for primality of $A3^n \pm 1$, *Proc. Amer. Math. Soc.* **127** (1999), 1923-1925.

[2] J. H. E. Cohn, Perfect Pell powers, *Glasgow Math. J.* **38** (1996), 19-20.

[3] D. A. Cox, *Primes of the Form $x^2 + ny^2$*, John Wiley and Sons, New York, 1989.

[4] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer-Verlag, New York, 1982.

[5] É. Lucas, Nouveaux théorèmes d'Arithmétique supérieure, *Comptes Rendus Acad. des Sciences, Paris* **83** (1876), 1286-1288.

[6] É. Lucas, Théorie des fonctions numériques simplement périodiques, *Amer. J. of Math.* **1** (1878), 184-240, 289-321.

[7] E. L. Roettger and H. C. Williams, Lucas-Lehmer tests for certain prime curios, *Integers* **21** (2021), #A109.

[8] E. L. Roettger and H. C. Williams and R. K. Guy, Some primality tests that eluded Lucas, *Des. Codes and Cryptog.* **77** (2015), 515-539.

[9] Andreas Stein and H. C. Williams, Explicit primality criteria for $(p-1)p^n - 1$, *Math. Comp.* **69** (2000), 1721-1734.

[10] H. C. Williams, The primality of $N = 2A3^n - 1$, *Can. Math. Bull* **15** (1972), 585-589.

[11] H. C. Williams, On numbers analogous to Carmichael numbers, *Can. Math. Bull* **20** (1977), 133-143.

[12] H. C. Williams, *Édouard Lucas and Primality Testing*, Wiley-Interscience, John Wiley and Sons, New York, 1998.

[13] H. C. Williams and C. R. Zarnke, Some prime numbers of the forms $2A3^n + 1$ and $2A3^n - 1$, *Math. Comp.* **26** (1972), no. 120, 995-998.