LUCAS-LEHMER PRIMALITY TESTS FOR CERTAIN PRIME CURIOS

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

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

Received: 4/10/21, Revised: 10/6/21, Accepted: 11/5/21, Published: 11/19/21

Abstract

Prime numbers of the form $N_d(n,m) = 10^{2n+m} - d10^n - 1$ are of interest to the recreational mathematics community. In this paper we derive two different algorithms for testing the primality of $N_d(n,m)$. Both of these tests are similar in many respects to the well-known Lucas-Lehmer test for the primality of $2^n - 1$. We also present the results of a computer implementation of these algorithms.

– *Dedicated to the memory of Harvey Dubner* $(1928 - 2019)$.

1. Introduction

It has long been recognized that play is an essential component of all human endeavours, even mathematics. When mathematical practitioners play with mathematics, the result is often called recreational mathematics, a study in which more professional mathematicians delight than are perhaps willing to admit. While recreational mathematics is often regarded as the precinct of amateurs and enthusiasts, it can be a source of very interesting and often challenging problems. Because of this or just the simple desire for fun, serious theoreticians often indulge in this pastime. Of particular interest to number theory recreationists are prime numbers with unconventional properties; lately, it seems to have become fashionable to call such integers prime curios.

There appears to be no formal definition of a prime curio; however, some idea of the enormous variety of such numbers and what makes them curios can be found, for example, in sources like Caldwell and Honaker [6], Pyne [12] or in the extensive companion website of [6]. The term *prime curio* itself seems to have originated in

the 1954 book of Friend [8, p. 45]. Frequently, such numbers are primes which have a peculiar digit pattern in their base 10 or decimal expression. For example, the number $(10^{19}-1)/9$ is a prime consisting of 19 ones in its decimal representation and appears in the website associated to [6]. This is an example of what is called a *repunit* prime, a prime number which consists only of 1-digits in its decimal representation. Unfortunately, such numbers are very hard to find and are extremely difficult to prove prime. However, if we loosen the above restriction to the idea of a *near-repdigit prime* (see [6, p. 259]), a prime with all the same digits except for one of them, we discover that such numbers are much easier to identify. Indeed, we can even ask that the number be palindromic as well. As an example, we point out that the number $N = 99999199999$, a number that also appears in [6], is a near-repdigit palindromic prime.

More generally, numbers like N can be represented as $N_d(n) = 10^{2n+1} - d10^n - 1$ $(1 \le d \le 9)$. That is, if $g = 9 - d$, then the decimal representation of N is

$$N = 999\ldots9g999\ldots9, \tag{1}$$

where $999\ldots9$ denotes n consecutive nines. Of course, if N is to be a prime, then d cannot be divisible by 3. Thus, $d \in A$, where A denotes the set of admissible values of d, i.e., $A = \{1, 2, 4, 5, 7, 8\}$. Several primes of type (1) were discovered by the late Harvey Dubner in 1989 and can be found on the website [6]; for example, $N_7(2874)$ occurs under the contributor Dobb. More recently, $N_8(157363)$ and some others have been identified as primes by Darren Bedwell. Dubner generalized N to what we will denote by $N_d(n, m)$, where

$$N_d(n, m) = 10^{2n+m} - d10^n - 1. \tag{2}$$

Here d is now a number of m digits. This N has the base-10 representation given by (2), where now g is the base-10 representation of $10^m - d - 1$. If N is to be palindromic, then g must also be palindromic, which means that d must be a palindrome. Note, then, that if m is even, then 11 must divide N, and therefore N cannot be a prime. If we wish this N to have only two distinct decimal digits, we put $d = f(10^{m-1} + 1)$, where $m \ge 3$ and $f \in A$. If, in this case we put $g = 9 - f$, we find that $N_d(n, m)$ has the decimal representation

$$N_d(n, m) = 999\ldots9g999\ldots9g999\ldots9,$$

where the first and last group of nines is of length n and the middle group of nines is of length $m - 2$.

We next examine the question of how to ascertain which values of $N_d(n, m)$ are prime. This means that we must now provide a brief discussion of the problem of primality testing. A much more detailed account of this problem can be found in the books of Crandall and Pomerance [7] and Williams [17]. The first of these is both

theoretically and computationally oriented, whereas the latter is more historical in its focus. The simplest way of approaching the problem of testing a given odd N for primality is to select some base b relatively prime to N and evaluate $b^{N-1} \pmod N$; if this is not 1, then N cannot be a prime by Euler's Theorem. This very naïve technique will most often settle the problem when N is not a prime; furthermore, the process for executing the algorithm requires time (number of elementary bit operations) of order $O(nM(n))$, where n is the number of bits of N and $M(n)$ is number of elementary bit operations needed to multiply two numbers of n bits. It is clear that $M(n) = O(n^2)$, but recently Harvey and van der Hoeven [10] have shown that $M(n) = O(n \log n)$. A brief sketch of the subject of algorithmic complexity can be found in Chapter 1 of [17].

We can modify the above test if we know a value for b such that the value of the Jacobi symbol (b/N) is 1. In this case, if N is a prime, then $b^{(N-1)/2} \equiv 1 \pmod N$ or $b^{(N+1)/2} \equiv b \pmod N$. If, in addition, we know that $N \equiv -1 \pmod 4$, then we must have

$$\left(b^{(N+1)/4}\right)^2 \equiv b \pmod N. \tag{3}$$

Thus, if (3) is not satisfied by $N \equiv -1 \pmod 4$, then N cannot be a prime. Since most arbitrarily selected values for N will be composite, it makes sense to execute this simple test before doing anything else. However, if N passes this test, then something else must be done because many composite values for N can satisfy $(b^{(N+1)/4})^2 \equiv b \pmod N$ when $(b/N) = 1$. In what follows, we will devise two tests very much like the famous Lucas-Lehmer test for the primality of Mersenne numbers; either of these can be used to establish rigorously the prime character of certain $N_d(n, m)$. The first of these works when $N_d(n, m)$ satisfies (3) for $N = N_d(n, m)$ and $b = 5$, but the second does not rely on (3).

2. The Lucas-Lehmer Test for Primality

The well-known Lucas-Lehmer test for the primality of numbers of the form $M_n = 2^n - 1$ (Mersenne numbers) is as follows:

> *Let $N = M_n$, where $n > 2$ and n is odd. If we put $T_0 = 4$ and define*
>
> $$T_{i+1} \equiv T_i^2 - 2 \pmod N \quad (i \geq 0),$$
>
> *then N is a prime if and only if $N \mid T_{n-2}$.*

This very elegant and efficient test has been used to establish the primality of Mersenne numbers since the latter part of the 19^{th} century. At the time of this writing 51 Mersenne primes have been identified; all of these can be found at the GIMPS (Great International Mersenne Prime Search) website [9]. The 51^{st} of these

is $M_{82589933}$, a number of over 24 million decimal digits and the largest prime known. Indeed, since 1955 the largest currently known prime has always been generated by using this test.

To derive his test Lucas made use of the properties of what today are called the Lucas sequences. Let P and Q be be complex numbers and α, β be the roots of the quadratic polynomial $f(x) = x^2 - Px + Q$ with $\delta = \alpha - \beta$. When P and Q are both integers, Lucas[1] defined his sequences (U_n) and (V_n) by using the functions:

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

Put $\Delta = \delta^2 = P^2 - 4Q$. The means by which Lucas discovered his (and other tests) is discussed is some detail in Chapters 3 and 5 of Williams [17]. Note that $U_{2n} = U_n V_n$.

While the many attributes of the Lucas sequences have been described in a number of sources, we will find it convenient for our purposes to refer to [17] for the properties that we will require. The following lemmas are well known (see, for example, [17, Section 4.3]).

Lemma 1. *Let p by any odd prime such that $p \nmid Q$. If ϵ_p is the value of the Legendre symbol (Δ/p), then $p \mid U_{p-\epsilon_p}$.*

From this result we see that if p is any odd prime such that $p \nmid Q$, there must exist a minimal integer $\omega(= \omega(p)) > 0$ such that $p \mid U_\omega$.

Lemma 2. *If p is any odd prime such that $p \nmid Q$, then $p \mid U_n$ $(n > 0)$ if and only if $\omega(p) \mid n$.*

Proof. Follows from [17, Theorem 4.3.4] and the fact that (U_n) is a divisibility sequence. □

We now also confine our attention to the (V_n) sequence. We observe that $V_2 = P^2 - 2Q$ and if we define $W_n = V_{2n}/Q^n$, it follows immediately that

$$W_1 = P^2 Q^{-1} - 2. \tag{4}$$

Also, it is easy to see from (4.2.7) of [17] that

$$W_{2n} = W_n^2 - 2. \tag{5}$$

We also have the following result.

Lemma 3. *If p an odd prime and $p \nmid Q$, then $p \mid V_{\frac{p-\epsilon_p}{2}}$ when $(Q/p) = -1$.*

[1]Lucas stipulated that P, Q be coprime integers, but this restriction will not be necessary in much of what follows because we will be concerned with results modulo N where $\gcd(Q, N) = 1$.

Proof. This is [17, Theorem 4.3.1]. □

Lehmer [11] generalized the Lucas-Lehmer test to numbers of the form $N = A2^n - 1$,

Theorem 1. *Let $N = A2^n - 1$, where $n > 1$, A is odd and $A < 2^n$. If the Jacobi symbols $(\Delta/N) = (Q/N) = -1$, then N is a prime if and only if $N \mid V_{(N+1)/2}$.*

Proof. If N is a prime, then $\epsilon_N = -1$ and $N \mid V_{\frac{N+1}{2}}$ by Lemma 3. Suppose next that N is composite and p $(< N)$ is any prime divisor of N. Since $p \mid V_{\frac{N+1}{2}}$, we have $p \mid U_{N+1}$. Since p is odd and $p \nmid Q$, we see by [17, (4.36)] that $p \nmid U_{\frac{N+1}{2}}$. Thus, by Lemma 2 we have $\omega(p) \mid A2^n$ and $\omega(p) \nmid A2^{n-1}$; it follows that $2^n \mid \omega(p)$. Thus, by Lemmas 1 and 2 we get $\omega(p) \mid p - \epsilon_p$ which means that $p = 2^n k \pm 1$ for some positive integer k. Since $A \leq 2^n - 1$, we cannot have $p = 2^n - 1$ unless $A = 1$, which means that $N = p$, a contradiction. Thus, $p \geq 2^n + 1 > \sqrt{N}$, which is impossible when N is composite. □

That this is a generalization of the Lucas-Lehmer test is not immediately obvious; however, if we have $A = 1$, $n \geq 3$ and n odd, then $N = M_n$, $N \equiv -1 \pmod 8$ and $N \equiv 1 \pmod 3$. Thus, if we put $P = 2$ and $Q = -2$, then $\Delta = 12$ and $(\Delta/N) = (3/N) = -1$. Also, $(Q/N) = (-2/N) = -1$. From (4) we get $W_1 = -4 = -T_0$, and by (5) we find that $T_i \equiv W_{2^i} \pmod N$, where $i > 0$. Hence, $T_{n-2} \equiv V_{(N+1)/2}/Q^{(N+1)/4} \pmod{\text{N}}$, and therefore $N \mid T_{n-2}$ if and only if $N \mid V_{(N+1)/2}$.

Theorem 1, unfortunately, is not effective in that it does not provide an explicit recipe for finding the values of P and Q which can be used. However, In the case where $3 \nmid AN$, it is, as we have just seen, a simple matter to show that when $n \geq 3$, we can always use $P = 2$ and $Q = -2$, but when $3 \mid A$, the problem of finding suitable values for P and Q becomes more difficult; however, in [3] Bosma showed how to produce such P and Q as long as $A \neq 4^m - 1$. Recently, these results have been improved via the more general approach of Deng and Huang [5]. Once P and Q have been determined, we can convert Theorem 1 into a necessary and sufficient primality test for N:

1) Put $W_1 \equiv P^2Q^{-1} - 2 \pmod N$.

2) Compute $W_A \pmod N$ by using, say, the technique of [17, Section 4.4].

3) Put $T_0 = W_A$ and use

$$T_{i+1} \equiv T_i^2 - 2 \pmod N$$

to compute $T_{n-2}(\equiv W_{2^{n-2}A}) \pmod N$.

4) N is prime if and only if $T_{n-2} \equiv 0 \pmod N$.

Unfortunately, step (2) above is rather inelegant when A is large; however, in Williams [15] it was shown how to replace this algorithm with a more streamlined version for some $N = A2^{2n} + B2^n - 1$. Indeed, this technique can be applied to certain $N = Ab^{2n} + Bb^n - 1$ for a fixed base b. In what follows we will extend the ideas in [15] to $N = N_d(n, m)$, where $b = 10$.

We can also approach this problem by using the next lemma.

Lemma 4. *Let p be a prime such that $p \equiv -1 \pmod 4$. There exist P, Q such that $(\Delta/p) = (Q/p) = -1$ if and only if $Q \equiv a^2 + b^2$, $P \equiv 2a \pmod p$, where a and b are integers such that $((a^2 + b^2)/p) = -1$.*

Proof. Suppose $Q \equiv a^2 + b^2$, $P \equiv 2a \pmod p$ and $((a^2 + b^2)/p) = -1$. We have $(Q/p) = -1$ and $p \nmid b$. Since $\Delta \equiv -4b^2 \pmod p$, we have $(\Delta/p) = -1$. Next, suppose that $(\Delta/p) = (Q/p) = -1$. We have $((4Q - P^2)/p) = 1$; hence, there must exist some c such that $c^2 \equiv 4Q - P^2 \pmod p$ and as a consequence we have $Q \equiv (2^{-1}P)^2 + (2^{-1}c)^2 \pmod p$; the result follows on putting $a \equiv 2^{-1}P$, $b \equiv 2^{-1}c \pmod p$. □

We can combine the results of Theorem 1 and Lemma 4 to produce the following test:

Theorem 2. *Let $N = A2^n - 1$, where $n > 1$, A is odd and $A < 2^n$. Let q be a prime such that $q \equiv 1 \pmod 4$ and $(N/q) = -1$. If a and b are integers such that $q = a^2 + b^2$ and we put $P = 2a$, $Q = q$, then N is a prime if and only if $N \mid V_{(N+1)/2}$.*

If the q in this theorem is small, we can find a and b by trial, but if it is large, Brillhart's [4] modification of Hermite's algorithm can be used to find them very efficiently. Unfortunately, we are still left with the problem of finding an appropriate value for q, but in most cases some small value of q usually suffices. For example, if $N = 9 \cdot 2^n - 1$, then $q \in \{5, 17\}$ or $q \in \{5, 13, 241\}$.

As noted in [15], it is possible to place the Lucas-Lehmer test into a more general class of primality criteria. In [5] it is shown that this class can be extended even further. We will specialize this to a family characterized, for a certain $l \geq 1$, by the following 4 properties:

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 $T_{i,0}$ $(i = 1, 2, \ldots, l)$ (the seeds) can be calculated by a simple, deterministic process and values of terms in the sequence $(T_{i,k})_{k\geq 0}$ $(i = 1, 2, \ldots, l)$ modulo N can be computed from $T_{i,j+1} \equiv g_i(T_{i,j}) \pmod N$, where each g_i $(i = 1, 2, \ldots, l)$

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 $O(nM(n))$.

We will say that any primality test for N which satisfies all of the above four conditions for a particular value of l is of L-L or Lucas-Lehmer type. Notice that the Lucas-Lehmer test itself is an instance with $l = 1$ of this more general class. In what follows we will show that the primality of many $N_d(n, m)$ can be determined by a test of L-L type.

3. The (W_n) Sequence

We begin by summarizing some further results concerning (W_n). From (4.2.8), (4.2.10) and (4.2.50) of [17] we find that

$$W_{n+m} + W_{n-m} = W_n W_m, \tag{6}$$
$$W_{n+m} W_{n-m} = W_{2n} + W_{2m}, \tag{7}$$
$$W_{5n} = W_n(W_n^4 - 5W_n^2 + 5). \tag{8}$$

More generally, if we define the polynomials $C_m(x)$ $(m = 1, 2, 3, \dots)$ by $C_0(x) = 2$, $C_1(x) = x$ and

$$C_k(x) = xC_{k-1}(x) - C_{k-2}(x) \quad (k \geq 2), \tag{9}$$

then

$$W_{mn} = C_m(W_n). \tag{10}$$

We also note that we can write

$$C_{m+n}(x) = C_n(x)C_m(x) - C_{n-m}(x), \tag{11}$$
$$C_m(C_n(x)) = C_{mn}(x), \tag{12}$$

and by (4.2.33) in [17], we have

$$C_k(x) = \sum_{i=0}^{\lfloor k/2 \rfloor} \frac{k}{k-i} \binom{k-i}{i} (-1)^i x^{k-2i} \quad (k > 0).$$

Now let

$$G_2(x) = x^2 + x - 1 = (x - \tau_1)(x - \tau_2),$$

where $\tau_1 + \tau_2 = -1$ and $\tau_1\tau_2 = -1$. We see that

$$\begin{aligned} G_2(x)G_2(y) &= (x-\tau_1)(x-\tau_2)(y-\tau_1)(y-\tau_2) \\ &= (xy - \tau_1(x+y) + \tau_1^2)(xy - \tau_2(x+y) + \tau_2^2) \\ &= (xy + 1 - \tau_1(x+y+1))(xy + 1 - \tau_2(x+y+1)). \end{aligned}$$

Hence,

$$G_2(x)G_2(y) = (xy+1)^2 + (x+y+1)(xy+1) - (x+y+1)^2, \tag{13}$$
$$G_2(-x)G_2(-y) = (xy+1)^2 - (x+y-1)(xy+1) - (x+y-1)^2. \tag{14}$$

Also,

$$G_2(x^2-2) = G_2(-x)G_2(x). \tag{15}$$

If we put $x = W_{n+m}$, $y = W_{n-m}$, we have

$$x + y + 1 = W_nW_m + 1 \quad \text{and} \quad xy + 1 = W_{2n} + W_{2m} + 1,$$

by (6) and (7), respectively. From (5) we get $xy + 1 = W_n^2 + W_m^2 - 3$. Thus,

$$G_2(W_{n+m})G_2(W_{n-m}) = K(W_n, W_m), \tag{16}$$

where

$$\begin{aligned} K(x,y) &= (x^2+y^2-3)^2 + (xy+1)(x^2+y^2-3) - (xy+1)^2 \\ &= x^4 + y^4 + xy(x^2+y^2) + x^2y^2 - 5(x^2+y^2) - 5xy + 5. \end{aligned} \tag{17}$$

We next suppose that p is a prime such that $p \equiv -1 \pmod 5$ and q is a prime ($\equiv 1 \pmod 5$) such that

$$p^{(q-1)/5} \not\equiv 0, 1 \pmod q.$$

As a special case of the proof of Theorem 11.3.4 of [17], we know that if R satisfies

$$G_2(R) \equiv 0 \pmod p,$$

then when

$$P = C(0,5,q) + C(1,5,q)R, \quad Q = q^3, \tag{18}$$

we have

$$G_2(W_{(p+1)/5}) \equiv 0 \pmod p. \tag{19}$$

The values of the coefficients $C(0,5,q)$, $C(1,5,q)$ are discussed in Section 11.3 of [17] and exhibited for all $q \le 1601$ in Table 11.3.1. For example, when $q = 11$, we have $C(0,5,11) = -57$, $C(1,5,11) = -25$. A more extensive table of these numbers ($q \le 9941$) can be found in [16, Table 4].

4. A Lucas-Lehmer Test for the Primality of $N_d(n, m)$

The main ingredient required for establishing Lucas' tests for the primality of a certain N is the determination of the possible forms of prime divisors of N. Indeed, it is often possible to proceed when we know that N has at least one prime divisor of a particular form. For suppose $N = N_d(n, m)$ where $3 \nmid d$; in this case $d^2 + 4 \cdot 10^m \equiv 2 \pmod 3$ and cannot be a square. Thus, by Lemma 8 of [15], we have the following simple result.

Theorem 3. *If $N_d(n, m)$ has a prime divisor p such that $p \equiv \epsilon \pmod{5^n}$, where $\epsilon \in \{1, -1\}$, then $N_d(n, m)$ must be a prime when*

$$5^n > 2^{2n-3} \cdot 10^m + d2^{n-2}. \tag{20}$$

Notice that if $m = 1$ and $1 \le d \le 8$, then (20) holds whenever $n \ge 3$. Of course, for any fixed m, (20) will hold for n sufficiently large.

The following result (Corollary 11.3.3 of [17]) will be useful in what follows.

Theorem 4. *Suppose* $\gcd(N, 5Q) = 1$. *If*

$$G_2(W_t) \equiv 0 \pmod N \tag{21}$$

and p is any prime divisor of N, then $p \equiv \epsilon \pmod{5^n}$, where $\epsilon \in \{1, -1\}$ and $5^n \mid\mid 5t$.

Thus, if $N = N_d(n, m)$ and we have some t such that $5^n \mid\mid 5t$ and (21) holds, then N must be a prime when (20) is satisfied.

In order to advance any further, we need to be able to solve

$$G_2(x) \equiv 0 \pmod N, \tag{22}$$

when $N = N_d(n, m)$ is a prime. To this end we put $S_0 = 5^{25}$ and define

$$S_{k+1} \equiv S_k^{10} \pmod N.$$

We have

$$S_t \equiv 5^{25 \cdot 10^t} \pmod N.$$

Lemma 5. *If $N = N_d(n, m)$ is a prime, then*

$$R \equiv 2^{-1}(-1 + S_{2n+m-2} S_{n-2}^{-d}) \pmod N$$

is a solution of (22).

Proof. Since $n \ge 2$, we have $N \equiv -1 \pmod 4$ and $N \equiv -1 \pmod 5$. Hence, the Legendre symbol $(5/N) = 1$; thus, as mentioned in Section 1,

$$\left(5^{(N+1)/4}\right)^2 \equiv 5 \cdot 5^{(N-1)/2} \equiv 5 \pmod N. \tag{23}$$

Also,

$$\frac{N+1}{4} = 25 \cdot 10^{2n+m-2} - 25 \cdot d \cdot 10^{n-2}. \tag{24}$$

It follows that since N is a prime, then by (23) and (24) we get

$$S_{2n+m-2}^2 \equiv 5S_{n-2}^{2d} \pmod{N}. \tag{25}$$

If

$$R \equiv 2^{-1}(-1 + S_{2n+m-2}S_{n-2}^{-d}) \pmod{N},$$

by (25) it is easy to see that

$$4G_2(R) \equiv 0 \pmod{N},$$

which, since N is odd, means that $G_2(R) \equiv 0 \pmod{N}$. □

We next suppose that we have some prime q such that $q \equiv 1 \pmod 5$ and

$$N^{(q-1)/5} \not\equiv 0, 1 \pmod{q}. \tag{26}$$

When $N = N_d(n, 1)$ and $d \in A$, this will be the case for $q = 11$ when neither $d = 1$ and $2 \nmid n$ nor $d = 8$ and $2 \mid n$ hold. We emphasize here that the process of finding an appropriate q, just as in the case of Theorem 2 of Section 2, is not in general deterministic because we can only use a limited number of candidates for q and none of those may be successful. This obstruction is discussed at some length in Section 16.4 of [17], and it seems in most cases that it is not a difficult problem, in practice, to find an appropriate q for most values of N. Certainly, we can easily specify an infinitude of possible values of $N_d(n, m)$ for which it is easy to find a satisfactory value for q. As we have already seen, $q = 11$ works for all $N_d(n, 1)$, when $d = 2$, 4, 5, 7 (mod 11). This is discussed in more detail in Section 8 below.

Assuming we have q, we can use the extended Euclidean algorithm, a simple deterministic process requiring time $O(nM(n))$, to compute M such that

$$2q^2S_{n-2}^d M \equiv 1 \pmod{N}. \tag{27}$$

If we put $A = 2C(0, 5, q) - C(1, 5, q)$, $B = C(1, 5, q)$ and

$$T_0 \equiv qM^2(AS_{n-2}^d + BS_{2n+m-2})^2 - 2 \pmod{N}, \tag{28}$$

then by (4) and (27) we have $T_0 \equiv W_1 \pmod N$ when P, Q satisfy (18). If N is a prime, we must have $G_2(W_{(N+1)/5}) \equiv 0 \pmod N$ by Lemma 5 and the last observation in the previous section. If we compute

$$T_{i+1} \equiv (T_i(T_i^4 - 5T_i^2 + 5))^2 - 2 \pmod{N}, \tag{29}$$

then by (5) and (8), we see that

$$T_k \equiv W_{10^k} \pmod{N}. \tag{30}$$

Now define the polynomial

$$J_d(x, y) = K(x^2 - 2, C_d(y)^2 - 2).$$

We have the following result.

Lemma 6. *Suppose $N = N_d(n, m)$ and put $r = 2 \cdot 10^{2n+m-1}$, $s = 2d10^{n-1}$. We have*

$$J_d(T_{2n+m-1}, T_{n-1}) \equiv G_2(W_{r+s})G_2(W_{r-s}) \pmod{N}. \tag{31}$$

Proof. Since

$$r - s = \frac{N+1}{5},$$

by (5) and (10) we get

$$W_r \equiv T_{2n+m-1}^2 - 2 \pmod{N}, \quad W_s \equiv C_d(T_{n-1})^2 - 2 \pmod{N}.$$

Thus, by (16) we get

$$J_d(T_{2n+m-1}, T_{n-1}) \equiv G_2(W_{r+s})G_2(W_{r-s}) \pmod{N}.$$

□

If we define T_i $(i = 0, 1, 2, 3, \dots)$ as above, we are now able to prove a result analogous to Theorem 2 for $N = N_d(n, m)$.

Theorem 5. *Let $N = N_d(n, m)$ and suppose that (20) holds; then N is a prime if and only if $N \mid J_d(T_{2n+m-1}, T_{n-1})$.*

Proof. Let r and s be defined as in Lemma 6. If N is a prime, then $G_2(W_{r-s}) \equiv 0 \pmod{N}$ by (19). Thus, by Lemma 6 we have $N \mid J_d(T_{2n+m-1}, T_{n-1})$. If $N \mid J_d(T_{2n+m-1}, T_{n-1})$, then by (31), there must exist a prime divisor p of N such that $p \mid G_2(W_{r+s})$ or $p \mid G_2(W_{r-s})$. Since $5^n \mid 5(r + s)$ and $5^n \mid 5(r - s)$, we see by Theorem 4 and Theorem 3 that N must be a prime. □

We can now state our $l = 1$ version of an L-L test for the primality of $N = N_d(n, m)$ when (20) holds and we have a prime q $(\equiv 1 \pmod 5)$ satisfying (26). We give this as a Corollary to Theorem 5.

Corollary 1. *Let $N = N_d(n, m)$. Suppose q is a prime such that $q \equiv 1 \pmod 5$ and (26) holds. If (20) holds, the following test is both necessary and sufficient for the primality of N.*

1) Compute S_{2n+m-2} and S^d_{n-2}. If (25) does not hold, then N is composite.

2) If (25) holds, compute M, satisfying (27), and T_0 by (28).

3) Use (29) to compute T_{n-1} and T_{2n+m-1} (mod N).

4) Then N is a prime if and only if $N \mid J_d(T_{2n+m-1}, T_{n-1})$.

This test is somewhat awkward because of the process required to find T_0. We can avoid this problem if we make use of the fourth order analogues of the Lucas sequences. These were introduced in [18] and investigated further in [14]. In the next sections we will use them to develop other versions of Theorem 5, but in order to do this we first need to derive some results concerning these extended Lucas functions (U_n), (V_n) and their companion sequences (X_n), (Y_n) defined in Williams and Guy [18], [19].

5. Some Results Concerning the Extended Lucas Sequences

As in [18] we let P_1, P_2, Q be integers and ρ_1, ρ_2 be the roots of

$$x^2 - P_1 x + P_2 = 0.$$

We put $\delta^2 = \Delta = (\rho_1 - \rho_2)^2 = P_1^2 - 4P_2$. For a given integer Q, let α_i, β_i $(i = 1, 2)$ be the roots of

$$x^2 - \rho_i x + Q = 0 \quad (i = 1, 2),$$

and put

$$E = (\alpha_1 - \beta_1)^2(\alpha_2 - \beta_2)^2 = (P_2 + 4Q)^2 - 4QP_1^2. \tag{32}$$

Note that

$$\Delta P_1^2 + 4E = (P_1^2 - 2P_2 - 8Q)^2. \tag{33}$$

The α_i, β_i $(i = 1, 2)$ are the four roots of $F(x)$ where

$$F(x) = x^4 - P_1 x^3 + (P_2 + 2Q)x^2 - P_1 Q x + Q^2$$

and the discriminant D of $F(x)$ is given by

$$D = E\Delta^2 Q^2.$$

In what follows we assume that $D \neq 0$.

We define the integer sequences (W_n), (U_n), (X_n), (Y_n) for $n \geq 0$ by

$$W_n + \rho_i U_n = \alpha_i^n + \beta_i^n, \quad X_n + \rho_i Y_n = \frac{\alpha_i^n - \beta_i^n}{\alpha_i - \beta_i}.$$

In [16, Section 10.1] the symbols $V_{0,n}$, $V_{1,n}$, $U_{0,n}$, $U_{1,n}$ were used to denote W_n, U_n, X_n, Y_n, respectively. Each of these sequences satisfies the fourth order linear recurrence

$$T_{n+4} = P_1 T_{n+3} - (P_2 + 2Q)T_{n+2} + P_1 Q T_{n+1} - Q^2 T_n \tag{34}$$

with initial conditions

$$\begin{array}{llll} W_0 = 2, & W_1 = 0, & W_2 = -P_2 - 2Q, & W_3 = -P_1 P_2; \\ U_0 = 0, & U_1 = 1, & U_2 = P_1, & U_3 = P_1^2 - P_2 - 3Q; \\ X_0 = 0, & X_1 = 1, & X_2 = 0, & X_3 = -P_2 - Q; \\ Y_0 = 0, & Y_1 = 0, & Y_2 = 1, & Y_3 = P_1. \end{array}$$

Let p denote any prime such that $p \nmid 2Q$. In what follows we will present a sequence of Lemmas each of which determines some ψ $(= \psi(p)) > 0$ such that $p \mid X_\psi$ and $p \mid Y_\psi$.

Lemma 7. *If $p \mid P_1$, then*

$$X_\psi \equiv Y_\psi \equiv 0 \pmod{p},$$

where

$$\psi = \begin{cases} p - \gamma, & \text{when } \gamma \neq 0; \\ 2p, & \text{when } \gamma = 0, \end{cases}$$

and γ is the value of the Legendre symbol $((P_2^2 + 4QP_2)/p)$.

Proof. Since $p \mid P_1$, we can use (34), the initial conditions for (X_n), and (Y_n) and mathematical induction to establish that

$$X_{2n} \equiv 0, \quad X_{2n+1} \equiv \bar{U}_n(-P_2, Q), \quad Y_{2n} \equiv \bar{U}_{2n}(-P_2, Q), \quad Y_{2n+1} \equiv 0 \pmod{p}, \tag{35}$$

where $\bar{U}_n(r, q)$ is the Lehmer function defined in the first section of [19]. Since $-P_2 - 4Q$ is the discriminant for $(\bar{U}_n(-P_2, Q))$, we know (see Theorem 1.9 of Lehmer [11]) that

$$p \mid \bar{U}_\psi(-P_2, Q).$$

Since $2 \mid \psi$, it follows from (35) that $X_\psi \equiv Y_\psi \equiv 0 \pmod{p}$. □

Lemma 8. *If $p \nmid P_1 \Delta$ and $p \mid E$, then*

$$X_\psi \equiv Y_\psi \equiv 0 \pmod{p},$$

where $\psi = p(p - \lambda)$ and λ is the value of the Legendre symbol $((P_1^2 - 2P_2 - 8Q)/p)$.

Proof. Since $p \mid E$ and $p \nmid P_1\Delta$, we must have $(\Delta/p) = 1$ by (33). By using the reasoning of Case 8 (b) in [18], we deduce that

$$X_\psi \equiv Y_\psi \equiv 0 \pmod{p}.$$

□

Lemma 9. *If $p \nmid P_1\Delta E$, then*

$$X_\psi \equiv Y_\psi \equiv 0 \pmod{p},$$

where

$$\psi = \begin{cases} p - \eta, & \text{when } (\Delta/p) = (E/p) = 1; \\ p^2 + 1, & \text{when } (\Delta/p) = (E/p) = -1. \end{cases}$$

Here η is the value of the Legendre symbol $((P_1^2 + \Delta - 16Q + 2P_1d)/p)$, where $d^2 \equiv \Delta \pmod{p}$.

Proof. From the results of Section 7 of [18], we have

$$W_\psi^2 - 4Q^\psi \equiv U_\psi \equiv 0 \pmod{p},$$

Since

$$(\alpha_i^n + \beta_i^n)^2 - (\alpha_i - \beta_i)^2 \left(\frac{\alpha_i^n - \beta_i^n}{\alpha_i - \beta_i}\right)^2 = 4Q^n$$

and

$$(\alpha_i - \beta_i)^2 = \rho_i^2 - 4Q = P_1\rho_i - P_2 - 4Q,$$

we can easily deduce that since $\rho_1 \neq \rho_2$ ($\Delta \neq 0$):

$$W_n^2 - P_2U_n^2 + (P_2 + 4Q)X_n^2 + 2P_1P_2X_nY_n + P_2(P_1^2 - P_2 - 4Q)Y_n^2 = 4Q^n,$$
$$2W_nU_n + P_1U_n^2 - P_1X_n^2 - 2(P_1^2 - P_2 - 4Q)X_nY_n - P_1(P_1^2 - 2P_2 - 4Q)Y_n^2 = 0.$$

It follows that if

$$W_n^2 - 4Q^n \equiv U_n \equiv 0 \pmod{p},$$

then

$$(P_2 + 4Q)X_n^2 + 2P_1P_2X_nY_n + P_2(P_1^2 - P_2 - 4Q)Y_n^2 \equiv 0 \pmod{p}, \tag{36}$$
$$P_1X_n^2 + 2(P_1^2 - P_2 - 4Q)X_nY_n + P_1(P_1^2 - 2P_2 - 4Q)Y_n^2 \equiv 0 \pmod{p}. \tag{37}$$

By multiplying (36) by P_1, (37) by $(P_2 + 4Q)$ and subtracting we find that

$$2EX_nY_n + P_1EY_n^2 \equiv 0 \pmod{p}$$

by (32). Thus since $p \nmid E$, we get $p \mid Y_n(2X_n + P_1Y_n)$. If $p \mid Y_n$, then it is easy to show from (36) and (37) that $p \mid X_n$; if $p \mid 2X_n + P_1Y_n$, it is also easy to show from (36) and (37) that $p \mid X_n$ and $p \mid Y_n$ when $p \nmid \Delta$. Thus, since $p \nmid E\Delta$, we have $X_\psi \equiv Y_\psi \equiv 0 \pmod{p}$. □

In summary, we have the following theorem.

Theorem 6. *If γ, λ, η are defined as above and*

$$\psi = \psi(p) = \begin{cases} p - \gamma, & \text{when } p \mid P_1 \text{ and } \gamma \neq 0; \\ 2p, & \text{when } p \mid P_1 \text{ and } \gamma = 0; \\ p(p - \lambda), & \text{when } p \nmid P_1\Delta \text{ and } p \mid E; \\ p - \eta, & \text{when } (\Delta/p) = (E/p) = 1; \\ p^2 + 1, & \text{when } (\Delta/p) = (E/p) = -1, \end{cases}$$

we have

$$X_\psi \equiv Y_\psi \equiv 0 \pmod{p}. \tag{38}$$

There remains the case of $p \nmid P_1$ and $p \mid \Delta$. In this case we are unable to find ψ (> 0) such that (38) holds; however, we do have the following result.

Lemma 10. *If $p \nmid P_1$ and $p \mid \Delta$, then*

$$X_\psi + (P_1/2)Y_\psi \equiv 0 \pmod{p}$$

where $\psi = p - \epsilon$ and ϵ is the value of the Legendre symbol $(((P_1/2)^2 - 4Q)/p)$.

Proof. We can again use the initial conditions for (X_n) and (Y_n) and (34) with $P_2 \equiv P_1^2/4 \pmod{p}$ to prove by induction that

$$X_n + (P_1/2)Y_n \equiv U_n(P_1/2, Q) \pmod{p}.$$

By Lemma 2, we have

$$X_\psi + (P_1/2)Y_\psi \equiv 0 \pmod{p}.$$

□

6. Some Results in $\mathbb{K}$

We observe that since ρ_1, ρ_2 are the roots of a monic quadratic polynomial with integer coefficients, we have $\rho_i \in \mathcal{O}$ $(i = 1, 2)$, where $\mathcal{O}$ is the order of $\mathbb{K}$ with discriminant Δ. We have $\mathcal{O} = \mathbb{Z} + \omega\mathbb{Z}$, where $\omega = \frac{\Delta+\delta}{2}$ and $\mathbb{Z}$ denotes the set of all rational integers. We can put

$$\rho_i = (P_1 + \epsilon_i\delta)/2 \quad (i = 1, 2),$$

where $\epsilon_i \in \{1, -1\}$ and $\epsilon_1 = -\epsilon_2$. Note that $\rho_i \in \mathcal{O}$ $(i = 1, 2)$.

We define

$$u_n(\rho_i, Q) = \frac{\alpha_i^n - \beta_i^n}{\alpha_i - \beta_i}, \quad v_n(\rho_i, Q) = \alpha_i^n + \beta_i^n \quad (i = 1, 2) \tag{39}$$

and we see that both sequences $(u_n(\rho_i, Q))$ and $(v_n(\rho_i, Q))$ satisfy the recurrence formula

$$T_n = \rho_i T_{n-1} - QT_{n-2} \quad (i = 1, 2). \tag{40}$$

Since $u_0(\rho_i, Q) = 0$, $u_1(\rho_i, Q) = 1$, $v_0(\rho_i, Q) = 2$, $v_1(\rho_i, Q) = \rho_i$, it is clear by using induction on (40) that

$$u_n(\rho_i, Q), v_n(\rho_i, Q) \in \mathcal{O} \quad (i = 1, 2)$$

for $n \geq 0$.

It is easy to use the formulas in (39) to verify the identities:

$$v_n^2(\rho_i, Q) - (\alpha_i - \beta_i)^2 u_n^2(\rho_i, Q) = 4Q^n; \tag{41}$$

$$2u_{n+m}(\rho_i, Q) = u_n(\rho_i, Q)v_m(\rho_i, Q) + v_n(\rho_i, Q)u_m(\rho_i, Q); \tag{42}$$

$$v_{2n}(\rho_i, Q) = v_n^2(\rho_i, Q) - 2Q^n, \quad u_{2n}(\rho_i, Q) = u_n(\rho_i, Q)v_n(\rho_i, Q); \tag{43}$$

and

$$u_{5n}(\rho_i, Q) = Q^{2n} G_2(v_{2n}(\rho_i, Q)/Q^n) u_n(\rho_i, Q); \tag{44}$$

$$v_{5n}(\rho_i, Q) = Q^{2n} G_2(-v_{2n}(\rho_i, Q)/Q^n) v_n(\rho_i, Q), \tag{45}$$

with the latter two results following from (4.2.67) and (4.2.68) of [17], respectively. Furthermore, since (4.2.37) and (4.2.39) of [17] hold for any values of P, Q, we see that

$$u_{mn}(\rho_i, Q)/u_n(\rho_i, Q) \in \mathcal{O} \quad (i = 1, 2).$$

Thus, $u_n(\rho_i, Q) \mid u_{mn}(\rho_i, Q)$ in $\mathcal{O}$; that is, $(u_k(\rho_i, Q))_{k \geq 1}$ is a divisibility sequence in $\mathcal{O}$.

Let p be any rational prime and let $\mathfrak{p}$ denote any prime $\mathcal{O}$-ideal divisor of p. We define $\omega_i(\mathfrak{p})$ to be the least positive value of n (if it exists) such that

$$\mathfrak{p} \mid u_n(\rho_i, Q).$$

We can now deduce the following important result.

Theorem 7. *Suppose p is a prime such that $p \nmid 2Q$. If $\mathfrak{p} \mid p$ and $\mathfrak{p} \mid u_n(\rho_i, Q)$ for some $n \geq 1$, then $\omega_i(\mathfrak{p})$ exists and $\omega_i(\mathfrak{p}) \mid n$.*

Proof. Put $\omega = \omega_i(\mathfrak{p})$ and let $n = q\omega + r$, where $0 \leq r < \omega$. If $r = 0$, we are done. Suppose $r > 0$. By (42) we have

$$2u_n(\rho_i, Q) = u_{q\omega}(\rho_i, Q)v_r(\rho_i, Q) + v_{q\omega}(\rho_i, Q)u_r(\rho_i, Q).$$

Since $(u_k(\rho_i, Q))$ is a divisibility sequence, we have $\mathfrak{p} \mid u_{q\omega}(\rho_i, Q)$ and since $\mathfrak{p} \mid u_n(\rho_i, Q)$, we get

$$\mathfrak{p} \mid v_{q\omega}(\rho_i, Q)u_r(\rho_i, Q).$$

By (41) we cannot have $\mathfrak{p} \mid v_{q\omega}(\rho_i, Q)$; thus, $\mathfrak{p} \mid u_r(\rho_i, Q)$, but since $1 \leq r < \omega$, this contradicts the definition of ω. □

We point out that

$$2v_n(\rho_i, Q) = 2W_n + P_1U_n + \epsilon_i\delta U_n, \quad 2u_n(\rho_i, Q) = 2X_n + P_1Y_n + \epsilon_i\delta Y_n. \tag{46}$$

Thus, if $p \mid Y_n$ and $p \mid X_n$, then $2u_n(\rho_i, Q) \equiv 0 \pmod{p}$. Now let p be any prime such that $p \nmid 2Q$ and $(\Delta E/p) \neq -1$. The question of the existence of $\omega_i(\mathfrak{p})$ is addressed in the next theorem.

Theorem 8. *Let p by any prime such that $p \nmid 2Q$ and $(\Delta E/p) \neq -1$. If $\mathfrak{p} \mid p$ and ψ is defined as in Theorem 6 or Lemma 10, then*

$$\mathfrak{p} \mid u_\psi(\rho_i, Q).$$

Furthermore, $\omega_i(\mathfrak{p})$ exists and $\omega_i(\mathfrak{p}) \mid \psi(p)$.

Proof. Suppose $p \nmid P_1$ and $p \mid \Delta$. By Lemma 10, we have

$$2X_\psi + P_1Y_\psi \equiv 0 \pmod{p}.$$

Since $p \mid \Delta$, we have $\mathfrak{p} \mid \delta$ and therefore by (46) we have

$$2u_\psi(\rho_i, Q) \equiv 0 \pmod{\mathfrak{p}}.$$

If $p \mid P_1$ or $p \nmid \Delta$, we have

$$2u_\psi(\rho_i, Q) \equiv 0 \pmod{\mathfrak{p}}$$

by Theorem 6, (38) and (46). Thus, by Theorem 7 $\omega_i(\mathfrak{p})$ must exist and $\omega_i(\mathfrak{p}) \mid \psi(p)$. □

Put $V_n = 2W_n + P_1U_n$ and define

$$Z_n = \frac{V_{2n}}{2Q^n}, \quad R_n = \frac{U_{2n}}{2Q^n}. \tag{47}$$

By the initial conditions for (U_n) and (V_n), we have $V_1 = P_1$, $U_1 = 1$, $V_2 = P_1^2 - 2P_2 - 4Q$, $U_2 = P_1$. Hence

$$Z_1 = \frac{P_1^2}{2Q} - \frac{P_1}{Q} - 2, \quad R_1 = \frac{P_1}{2Q}. \tag{48}$$

Also, since $2V_{2n} = V_n^2 + \Delta U_n^2 - 8Q^n$ and $U_{2n} = U_n V_n$, we find that

$$Z_{2n} = Z_n^2 + \Delta R_n^2 - 2, \quad R_{2n} = 2Z_n R_n. \tag{49}$$

If we define $w_n(\rho_i, Q)$ to be $v_{2n}(\rho_i, Q)/Q^n$, then by (46) and (47) we have

$$w_n(\rho_i, Q) := v_{2n}(\rho_i, Q)/Q^n = Z_n + \epsilon_i \delta R_n. \tag{50}$$

From (43) we get

$$w_{2n}(\rho_i, Q) = w_n^2(\rho_i, Q) - 2;$$

thus, by (15) we find that

$$G_2(w_n(\rho_i, Q))G_2(-w_n(\rho_i, Q)) = G_2(w_{2n}(\rho_i, Q)). \tag{51}$$

We are now able to prove the following theorem.

Theorem 9. *Let N be an integer such that $\gcd(N, 10Q) = 1$ and $(\Delta E/p) \neq -1$. If $G_2(w_n(\rho_i, Q)) \equiv 0 \pmod{\mathfrak{p}}$, where $\mathfrak{p} \mid p$ and p is any prime divisor of N, then $\psi(p) \equiv 0 \pmod{5^k}$, where $5^k \mid\mid 5n$.*

Proof. By (44) we have $\mathfrak{p} \mid u_{5n}(\rho_i, Q)$, where $\mathfrak{p}$ is any prime ideal divisor of p. If $\mathfrak{p} \mid u_n(\rho_i, Q)$, then $\mathfrak{p} \mid u_{2n}(\rho_i, Q)$ and by (41)

$$v_{2n}^2(\rho_i, Q) \equiv 4Q^{2n} \pmod{\mathfrak{p}}.$$

It follows that

$$w_n(\rho_i, Q) \equiv \pm 2 \pmod{\mathfrak{p}}.$$

Since $G_2(2) = 5$ and $G_2(-2) = 1$, we find that $\mathfrak{p} \nmid G_2(w_n(\rho_i, Q))$; hence, $\mathfrak{p} \nmid u_n(\rho_i, Q)$. It follows that $\omega_i(\mathfrak{p}) \mid 5n$ and $\omega_i(\mathfrak{p}) \nmid n$. Thus, $5^k \mid \omega_i(\mathfrak{p})$ and by Theorem 8, we must have $\psi(p) \equiv 0 \pmod{5^k}$. □

We also have a companion result to Theorem 9.

Theorem 10. *Let N be an integer such that $\gcd(N, 10Q) = 1$. If $G_2(-w_n(\rho_i, Q)) \equiv 0 \pmod{\mathfrak{p}}$, where $\mathfrak{p} \mid p$ and p is any prime divisor of N such that $(\Delta E/p) \neq -1$, then $\psi(p) \equiv 0 \pmod{2^h 5^k}$, where $5^k \mid\mid 5n$ and $2^h \mid\mid 2n$.*

Proof. By (45), we have $\mathfrak{p} \mid v_{5n}(\rho_i, Q)$. It follows that $\mathfrak{p} \mid u_{10n}(\rho_i, Q)$ and $\mathfrak{p} \nmid u_{5n}(\rho_i, Q)$ by (41). Since $\omega_i(p) \mid 10n$ and $\omega_i(p) \nmid 5n$ we have $2^h \mid \omega_i(p)$ and $2^h \mid \psi(p)$. If $\mathfrak{p} \mid u_{2n}(\rho_i, Q)$, then $v_{2n}^2(\rho_i, Q) \equiv 4Q^{2n} \pmod{\mathfrak{p}} \Rightarrow \mathfrak{p} \nmid G_2(-w_n(\rho_i, Q))$, a contradiction. Thus, $5^k \mid \omega_i(p)$ and $2^h 5^k \mid \psi(p)$. □

Corollary 2. *Under the conditions of the theorem, we must have $p \equiv \pm 1 \pmod{2^h 5^k}$ when $h \geq 2$.*

Proof. If $h \geq 2$, we cannot have $2^h \mid p^2+1$ or $2^h \mid 2p$. Thus $\psi(p)$ can only be $p \pm 1$ or $p(p \pm 1)$. □

Let p, q be odd primes such that $p \equiv -1 \pmod 5$, $q \equiv 1 \pmod 5$ and

$$p^{(q-1)/5} \not\equiv 0, 1 \pmod q.$$

Let $Q = q^3$, $P_1 = P(1,5,q)$, $P_2 = P(2,5,q)$ as defined in Section 11.1 of [17]. In this case we have $\Delta = P_1^2 - 4P_2 = 5C^2(1,5,q)$. Indeed, since

$$\rho_i = C(0,5,q) + C(1,5,q)\tau_i \quad (i = 1,2),$$

we get

$$\begin{aligned} P(1,5,q) &= 2C(0,5,q) - C(1,5,q), \\ P(2,5,q) &= C^2(0,5,q) - C(0,5,q)C(1,5,q) - C^2(1,5,q). \end{aligned}$$

Furthermore, since

$$\alpha_i = \tau(\chi^i)^5/q \quad \beta_i = \tau(\chi^{-i})^5/q \quad (i = 1,2)$$

are the roots of $F(x)$, it is easy to show from (11.1.1) in [17] that

$$E = (\alpha_1 - \beta_1)^2(\alpha_2 - \beta_2)^2 = 5e^2,$$

where e is an integer. Thus, ΔE is a perfect integral square.

By Theorem 11.2.2 of [17], we must have $p \nmid \Delta E$. By (11.2.2) of [17] we have in $\mathbb{F}_{p^2}$ that

$$q^\theta v_\theta(\rho_i, Q) = \tau q,$$

where $\tau^2 + \tau - 1 = 0$. Since $1 - \frac{p+1}{5} = \frac{3(p+1)}{10} - \frac{p-1}{2}$ we get

$$w_{\theta/2}(\rho_i, Q) = \frac{v_\theta(\rho_i, Q)}{Q^{\theta/2}} = \tau(Q/p).$$

Thus, $G_2((Q/p)w_{\theta/2}(\rho_i, Q)) = 0$ in $\mathbb{F}_p$. By (51) we get

$$G_2(w_\theta(\rho_i, Q)) \equiv 0 \pmod p. \tag{52}$$

Also,

$$G_2(-w_{\theta/2}(\rho_i, Q)) \equiv 0 \pmod p \tag{53}$$

when $(Q/p) = -1$.

7. Another Lucas-Lehmer Test for the Primality of $N_d(n, m)$

Suppose $N \equiv -1 \pmod{4 \cdot 5^n}$ (this is the case when $N = N_d(n, m)$ with $n \geq 2$) and suppose further that N has a prime divisor p such that $\psi(p) \equiv 0 \pmod{5^n}$. If $p \equiv \pm 1 \pmod{5^n}$, we have by Theorem 3 that $N_d(n, m)$ is a prime when (20) holds. Indeed, if $\psi(p) \equiv 0 \pmod{10^n}$ for $n \geq 2$, we can show from Lemma 8 of [15] that $N_d(n, m)$ must be a prime whenever $n > m$. We now need to examine the case of $p^2 \equiv -1 \pmod{5^n}$.

Let γ_n denote the unique odd value x such that

$$x^2 \equiv -1 \pmod{5^n} \tag{54}$$

and $0 < x < 5^n$. It is easy to compute γ_n by the usual Hensel lifting process as described, for example, in Section 6 of [14]. Also, since 1 and $5^n - 1$ are not solutions to (54), we must have

$$3 \leq \gamma_n \leq 5^n - 2 < N. \tag{55}$$

Since γ_n is odd, we have

$$\gamma_n^2 \equiv -1 \pmod{2 \cdot 5^n};$$

thus, $(N - \gamma_n^2)/(2 \cdot 5^n)$ is an integer.

For some $\epsilon \in \{1, -1\}$, compute t such that

$$t \equiv -\epsilon\gamma_n \left(\frac{N - \gamma_n^2}{2 \cdot 5^n} \right) \pmod{2 \cdot 5^n} \qquad (-5^n < t \leq 5^n). \tag{56}$$

We have

$$t\epsilon\gamma_n \equiv \frac{N - \gamma_n^2}{2 \cdot 5^n} \pmod{2 \cdot 5^n}.$$

We are now able to show that if $\gamma_n \nmid N$ and

$$t^2 - 4 \left(\frac{N - \gamma_n^2}{2 \cdot 5^n} - t\epsilon\gamma_n \right) / (2 \cdot 5^n) = u^2, \tag{57}$$

where u is an integer, then N is composite. Given (57), this follows from the simple identity

$$N = \left(2 \cdot 5^n \frac{t + u}{2} + \epsilon\gamma_n \right) \left(2 \cdot 5^n \frac{t - u}{2} + \epsilon\gamma_n \right).$$

We now restrict our attention to values N ($\equiv -1 \pmod{4 \cdot 5^n}$) such that

(i) $\gamma_n \nmid N$

(ii) (57) does not hold for $\epsilon = 1$ or $\epsilon = -1$ and t satisfying (56).

It is easy to verify whether or not (57) holds because we can certainly detect deterministically whether or not a positive integer M is a perfect square in time $O(nM(n))$, where n is the number of bits of the binary representation of M. (See Bach and Sorenson [1] and Bernstein [2] for an extensive discussion of this problem and better complexity results.) Indeed, it is usually the case that (57) does not hold, and this can be easily and quickly verified by finding some small prime r such that the left-hand side of (57) is not a quadratic residue of r, but this process is not in general deterministic.

We have seen that values of N which do not satisfy either (i) or (ii) are composite. We can now prove the result below.

Theorem 11. *Suppose $N \equiv -1 \pmod{4 \cdot 5^n}$ and (i) and (ii) hold. If some prime divisor p of N satisfies $p \equiv \epsilon\gamma_n \pmod{5^n}$, where $\epsilon \in \{1, -1\}$, then N must be a prime when $2 \cdot 5^{3n} > N$.*

Proof. If N is composite, then $N = pT$, where $T > 1$. Since $\epsilon\gamma_n T \equiv \gamma_n^2 \pmod{5^n}$, we find that $T \equiv \epsilon\gamma_n \pmod{5^n}$. Since T and p are odd, we get

$$p = 2k_1 5^n + \epsilon\gamma_n, \quad T = 2k_2 5^n + \epsilon\gamma_n,$$

where k_1, $k_2 > 0$. Thus

$$N = 4k_1k_2 5^{2n} + 2\epsilon\gamma_n 5^n(k_1 + k_2) + \gamma_n^2. \tag{58}$$

Since t satisfies (56), we must have $k_1 + k_2 = 2 \cdot 5^n s + t$, where $s \geq 0$. If $s = 0$, then (57) must hold, which is impossible. Thus, $s \geq 1$. Also, since $k_1k_2 \geq k_1 + k_2 - 1$, we have

$$k_1k_2 \geq 2 \cdot 5^n s + t - 1. \tag{59}$$

By using (59), (56) and (55), it is a routine matter to deduce from (58) that

$$N > 2 \cdot 5^{3n}.$$

□

If $N = N_d(n, m)$ and

$$2 \cdot 5^n \geq 10^m 2^n, \tag{60}$$

then $N > 2 \cdot 5^{3n}$ and (20) also holds. Thus, if N satisfies conditions (i) and (ii) above, then N must be a prime if some prime divisor p of N satisfies $\psi(p) \equiv 0 \pmod{5^n}$.

We now require some results analogous to (16) in Section 3. Let $K(x, y)$ be defined as in (17) and $K'(x, y)$ be given as

$$K'(x, y) = x^4 + y^4 - xy(x^2 + y^2) + x^2y^2 - 5(x^2 + y^2) + 5xy + 5.$$

We next let (Z_n) and (R_n) be the sequences defined in (47). For a fixed n and m, put

$$\begin{aligned} I_1 &= Z_n^2 + Z_m^2 + \Delta(R_n^2 + R_m^2), \\ I_2 &= 2(R_n Z_n + R_m Z_m), \\ J_1 &= Z_n Z_m + \Delta R_n R_m, \\ J_2 &= R_n Z_m + R_m Z_n. \end{aligned}$$

Proposition 1. *If I_1, I_2, J_1, J_2 are defined as above we have*

$$\begin{aligned} &G_2(w_{n+m}(\rho_i, Q))G_2(w_{n-m}(\rho_i, Q)) = F_1 + \epsilon_i \delta F_2 \quad (i = 1, 2), \\ &G_2(-w_{n+m}(\rho_i, Q))G_2(-w_{n-m}(\rho_i, Q)) = F_1' + \epsilon_i \delta F_2' \quad (i = 1, 2), \end{aligned}$$

where

$$\begin{aligned} F_1 &= I_1^2 + \Delta I_2^2 + I_1 J_1 + \Delta I_2 J_2 - J_1^2 - \Delta J_2^2 - 5I_1 - 5J_1 + 5, \\ F_2 &= 2I_1 I_2 - 2J_1 J_2 + I_1 J_2 + I_2 J_1 - 5I_2 - 5J_2, \\ F_1' &= I_1^2 + \Delta I_2^2 - I_1 J_1 - \Delta I_2 J_2 - J_1^2 - \Delta J_2^2 - 5I_1 + 5J_1 + 5, \\ F_2' &= 2I_1 I_2 - 2J_1 J_2 - I_1 J_2 - I_2 J_1 - 5I_2 + 5J_2. \end{aligned}$$

Proof. Since both (6) and (7) hold when W_k is replaced by $w_k(\rho_i, Q)$, we find by (16) that

$$G_2(w_{n+m}(\rho_i, Q))G_2(w_{n-m}(\rho_i, Q)) = K(w_n(\rho_i, Q), w_m(\rho_i, Q)) \quad (i = 1, 2). \tag{61}$$

Also, by (14) and the reasoning in Section 3, we have

$$G_2(-w_{n+m}(\rho_i, Q))G_2(-w_{n-m}(\rho_i, Q)) = K'(w_n(\rho_i, Q), w_m(\rho_i, Q)) \quad (i = 1, 2). \tag{62}$$

From (50), we have

$$w_n(\rho_i, Q) = Z_n + \epsilon_i \delta R_n \quad \text{and} \quad w_m(\rho_i, Q) = Z_m + \epsilon_i \delta R_m.$$

Thus,

$$\begin{aligned} w_n^2(\rho_i, Q) + w_m^2(\rho_i, Q) &= (Z_n + \epsilon_i \delta R_n)^2 + (Z_m + \epsilon_i \delta R_m)^2 \\ &= I_1 + \epsilon_i \delta I_2, \end{aligned}$$

and

$$w_n(\rho_i, Q) w_m(\rho_i, Q) = J_1 + \epsilon_i \delta J_2.$$

By the definitions of $K(x, y)$ and $K'(x, y)$, we get

$$\begin{aligned} K(w_n(\rho_i, Q), w_m(\rho_i, Q)) &= F_1 + \epsilon \delta F_2, \\ K'(w_n(\rho_i, Q), w_m(\rho_i, Q)) &= F_1' + \epsilon \delta F_2'. \end{aligned}$$

The proposition now follows easily from (61) and (62). □

Clearly, F_1, F_1', F_2 and F_2' are polynomial functions of Z_n, R_n, Z_m, R_m and we can write

$$F_1 = F_1(Z_n, R_n, Z_m, R_m), \quad F_2 = F_2(Z_n, R_n, Z_m, R_m);$$
$$F_1' = F_1'(Z_n, R_n, Z_m, R_m), \quad F_2' = F_2'(Z_n, R_n, Z_m, R_m).$$

We now need results analogous to (29) and (30). From Section 4 of [14], we observe that if we put $H_0(x, y) = 1$, $H_1(x, y) = 3x + y - 3$ and use the recurrence formula

$$H_{k+1}(x, y) = (x + y - 2)H_k(x, y) + 2xH_k(y, x) - H_{k-1}(x, y),$$

we have

$$Z_{(2k+1)m} = Z_m H_k(\Delta R_m^2, Z_m^2), \quad R_{(2k+1)m} = R_m H_k(Z_m^2, \Delta R_m^2). \tag{63}$$

Note that

$$H_2(x, y) = 5x^2 + 10xy + y^2 - 5y - 15x + 5.$$

Thus, if we put

$$T_0 \equiv Z_2 \pmod N, \quad S_0 \equiv R_2 \pmod N$$

and compute

$$T_{i+1} \equiv T_i^2 H_2^2(\Delta S_i^2, T_i^2) + \Delta S_i^2 H_2^2(T_i^2, \Delta S_i^2) - 2 \pmod N, \tag{64}$$
$$S_{i+1} \equiv 2S_i T_i H_2(\Delta S_i^2, T_i^2) H_2(T_i^2, \Delta S_i^2) \pmod N, \tag{65}$$

then by (49) and (63)

$$T_k \equiv Z_{2\cdot 10^k}, \quad S_k \equiv R_{2\cdot 10^k} \pmod N.$$

Let $N = N_d(n, m)$ and q ($\equiv 1 \pmod 5$) be any prime such that $q \nmid N$ and (26) holds. As in Section 3, put $P_1 = P(1, 5, q)$, $P_2 = P(2, 5, q)$, $Q = q^3$. We can now provide a theorem similar to Theorem 5.

Theorem 12. *Let $N = N_d(n, m)$ satisfy the above requirements. Suppose that conditions (i) and (ii) hold and $2 \cdot 5^n \geq 10^m 2^n$. Put $r = 2 \cdot 10^{2n+m-1}$, $s = 2d10^{n-1}$. N is prime if and only if*

$$F_1(Z_r, R_r, Z_s, R_s) \equiv F_2(Z_r, R_r, Z_s, R_s) \equiv 0 \pmod N.$$

Proof. Suppose N is prime. By (52), we must have

$$G_2(w_\theta(\rho_i, Q)) \equiv 0 \pmod N \quad (i = 1, 2).$$

where $\theta = (N+1)/5$. Hence, by Proposition 1, we get

$$F_1(Z_r, R_r, Z_s, R_s) \equiv F_2(Z_r, R_r, Z_s, R_s) \equiv 0 \pmod{N} \tag{66}$$

for r, s defined in Section 4. On the other hand, if (66) holds for $N = N_d(n,m)$, then by Proposition 1 we have

$$N \mid G_2(w_{r+s}(\rho_i, Q))G_2(w_{r-s}(\rho_i, Q)).$$

Thus, if p is a prime divisor of N and $\mathfrak{p}$ is some prime ideal divisor p, then

$$\mathfrak{p} \mid G_2(w_{r+s}(\rho_i, Q)) \quad \text{or} \quad \mathfrak{p} \mid G_2(w_{r-s}(\rho_i, Q)).$$

In either case, by Theorem 9, we must have $\psi(p) \equiv 0 \pmod{5^n}$, which as noted above means that N must be a prime by Theorem 11. □

Now suppose that $N = N_d(n,m)$; conditions (i) and (ii) hold; and $2 \cdot 5^n \geq 10^m 2^n$. For such values of N we have the following ($l = 2$) L-L type test for N.

Corollary 3. *Let $N = N_d(n,m)$ and suppose N satisfies the conditions above. If q is a prime such that $q \equiv 1 \pmod 5$ and (26) holds, we have the following necessary and sufficient test for the primality of N:*

1) Put $P_1 = P(1,5,q)$, $P_2 = P(2,5,q)$, $Q = q^3$.

2) Let $N \equiv h \pmod{2q}$ and find j such that $jh \equiv -1 \pmod{2q}$. Put

$$\begin{aligned}
&M \equiv 4\left(\frac{jN+1}{2q}\right)^3 \pmod N \quad ((2Q)M \equiv 1 \pmod N),\\
&Z_1 \equiv MP_1^2 - 2MP_2 - 2, \quad R_1 \equiv MP_1 \pmod N,\\
&Z_2 \equiv Z_1^2 + \Delta R_1^2 - 2, \quad R_2 \equiv 2Z_1R_1 \pmod N,\\
&T_0 = Z_2, \quad S_0 = R_2.
\end{aligned}$$

3) By using (64) and (65) compute

$$T_{2n+m-1}, \quad S_{2n+m-1}, \quad T_{n-1}, \quad S_{n-1} \pmod N.$$

4) Put

$$Z_r \equiv T_{2n+m-1}, \quad R_r \equiv S_{2n+m-1}, \quad Z_t \equiv T_{n-1}, \quad R_t \equiv S_{n-1} \pmod N$$

and compute $Z_s(= Z_{dt})$, $R_s(= R_{dt}) \pmod N$ by using (49) and (63).

5) Then N is a prime if and only if

$$F_1(Z_r, R_r, Z_s, R_s) \equiv F_2(Z_r, R_r, Z_s, R_s) \equiv 0 \pmod N.$$

We can avoid testing conditions (i) and (ii) if we can find a prime q ($\equiv 1 \pmod 5$) such that N ($= N_d(n,m)$) satisfies (26) and $(Q/N) = (q/N) \equiv (-N)^{(q-1)/2} \equiv -1 \pmod q$. We now have the following companion result to Theorem 12.

Theorem 13. *Let $N = N_d(n,m)$, where $n > m$ and let q satisfy the above conditions. Put $r = 10^{2n+m-1}$, $s = d10^{n-1}$. Then N is a prime if and only if*

$$F_1'(Z_r, R_r, Z_s, R_s) \equiv F_2'(Z_r, R_r, Z_s, R_s) \equiv 0 \pmod N.$$

Proof. Suppose N is a prime. By (53), we must have

$$G_2(-w_{\theta/2}(\rho_i, Q)) \equiv 0 \pmod N \quad (i = 1, 2),$$

where $\theta = (N+1)/5$. Thus, by Proposition 1 we get

$$F_1'(Z_r, R_r, Z_s, R_s) \equiv F_2'(Z_r, R_r, Z_s, R_s) \equiv 0 \pmod N. \tag{67}$$

If (67) holds, then by Proposition 1, we have

$$N \mid G_2(-w_{r+s}(\rho_i, Q))G_2(-w_{r-s}(\rho_i, Q)).$$

By Corollary 2 and our earlier reasoning, we must have $p \equiv \pm 1 \pmod{10^n}$ for any prime such that $p \mid N$. Thus, since $n > m$, N must be a prime. □

We now have another ($l = 2$) L-L type test for $N_d(n,m)$.

Corollary 4. *Let $N = N_d(n,m)$, where $n > m$. If q is a prime such that $q \equiv 1 \pmod 5$, (26) holds and $(-N)^{(q-1)/2} \equiv -1 \pmod q$, the following test is both necessary and sufficient for the primality of N.*

1) Put $P_1 = P(1,5,q)$, $P_2 = P(2,5,q)$, $Q = q^3$.

2) Let $N \equiv h \pmod{2q}$ and find j such that $jh \equiv -1 \pmod{2q}$. Put

$$M \equiv 4\left(\frac{jN+1}{2q}\right)^3 \pmod N \quad ((2Q)M \equiv 1 \pmod N),$$
$$Z_1 \equiv MP_1^2 - 2MP_2 - 2, \quad R_1 \equiv MP_1 \pmod N,$$
$$T_0 = Z_1, \quad S_0 = R_1.$$

3) By using (64) and (65) compute

$$T_{2n+m-1}, \quad S_{2n+m-1}, \quad T_{n-1}, \quad S_{n-1} \pmod N.$$

4) Put

$$Z_r \equiv T_{2n+m-1}, \quad R_r \equiv S_{2n+m-1}, \quad Z_t \equiv T_{n-1}, \quad R_t \equiv S_{n-1} \pmod N$$

and compute $Z_s (= Z_{dt})$, $R_s (= R_{dt}) \pmod N$ by using (49) and (63).

5) Then N is a prime if and only if

$$F_1'(Z_r, R_r, Z_s, R_s) \equiv F_2'(Z_r, R_r, Z_s, R_s) \equiv 0 \pmod N.$$

8. Computational Results

All of the above tests rely on finding for $N = N_d(n, m)$ a value of q such that (26) holds. In Table 1 below we show the results of a search for the smallest q such that this is the case for all $N = N_d(n, 1)$ and $3 \leq n \leq 11000$. The largest value of q needed was 191. In Table 2, we record the results of a search for the smallest q such that both (26) and the additional condition $(q/N) \equiv (-N)^{(q-1)/2} \equiv -1 \pmod{q}$ hold for all N in the same range. Here the largest value for q is 641. Notice that if $d = 5$, then q can always be 11; also, if $d = 2$ or 4, a value for q is in $\{11, 101\}$. In the case of $d = 7$, it can be shown that a value for q is always in T, where

$$T = \{11, 41, 61, 101, 211, 241, 271, 2161, 9901\}.$$

q	freq.	rel. freq.	q	freq.	rel. freq.	q	freq.	rel. freq.
11	49491	75.0000%	71	550	0.8335%	151	26	0.0394%
31	12099	18.3352%	101	53	0.0803%	181	7	0.0106%
41	2565	3.8871%	131	94	0.1425%	191	3	0.0045%
61	1100	1.6670%						

Table 1: Number of occurrences of each value for q used for testing for $3 \leq n \leq 11000$ here $(q/N) = \pm 1$

q	freq.	rel. freq.	q	freq.	rel. freq.	q	freq.	rel. freq.
11	21996	33.3333%	211	214	0.3243%	431	7	0.0106%
31	15395	23.3300%	241	262	0.3970%	461	4	0.0061%
41	6602	10.0048%	251	109	0.1652%	491	1	0.0015%
61	8616	13.0569%	271	7	0.0106%	521	1	0.0015%
71	4741	7.1846%	281	54	0.0818%	541	0	0%
101	2776	4.2068%	311	30	0.0455%	571	0	0%
131	2404	3.6431%	331	25	0.0379%	601	1	0.0015%
151	1374	2.0822%	401	28	0.0424%	631	0	0%
181	825	1.2502%	421	5	0.0076%	641	1	0.0015%
191	510	0.7729%						

Table 2: Number of occurrences of each value for q used for testing for $3 \leq n \leq 11000$ while ensuring $(q/N) = -1$

We conducted computer runs on both the $l = 1$ and $l = 2$ versions of the L-L tests for the primality of $N_d(n, 1)$ for $d \in A$. The results of these runs appears in Table 4 below. Although the primes in Table 4 are very likely known, we record them here for the convenience of the reader. In a comparison test of the run times for the $l = 1$ and $l = 2$ tests for $N_d(n, 1)$, we found that the $l = 1$ test (Corollary 1) is about 1.4 times faster than either of the $l = 2$ tests. This is understandable because

the cost of testing (25) together with that of calculating T_0 is still less than that of computing the additional set of values for $T_{2,k} \pmod N$ in the $l = 2$ algorithms. Also, since most of the values of $N_d(n, 1)$ are composite, we would expect the $l = 1$ test to be more efficient than the $l = 2$ test in a run over several values of n. For all the tables below the size of the prime being tested is always $2n + m$ decimal digits. The programs were written in Maple and executed on a Mac with a 3.3 GHz Quad-Core Intel Core i5 processor and 8 GB of RAM.

n	d	q_1	q_2	n	d	q_1	q_2	n	d	q_1	q_2
5	8	11	31	112	4	11	11	1246	1	11	31
8	7	11	41	118	2	11	31	1315	7	11	11
9	7	11	11	169	8	11	61	1579	8	11	71
13	8	11	41	181	8	11	31	1798	1	11	401
14	5	11	11	198	4	11	11	1918	7	11	31
22	5	11	11	352	7	11	101	2874	7	11	61
26	1	11	61	378	1	11	61	2917	1	31	151
36	5	11	11	530	7	11	71	4228	4	11	11
43	8	11	41	622	4	11	11	5876	7	11	31
88	4	11	11	697	7	11	11	6768	7	11	41
104	5	11	11	1136	5	11	11	10052	4	11	11

Table 3: Prime values of $N_d(n, 1)$ with $3 \le n \le 11000$ along with q_1, q_2 used for tests in Corollaries 3 and 4, respectively

n	d	$r.t.1$	$r.t.2$	n	d	$r.t.1$	$r.t.2$	n	d	$r.t.1$	$r.t.2$
5	8	2.91	5.20	112	4	2.91	4.97	1246	1	4.33	6.18
8	7	3.31	4.90	118	2	3.03	4.90	1315	7	4.28	5.83
9	7	3.01	4.69	169	8	3.05	4.92	1579	8	5.10	6.13
13	8	3.02	4.80	181	8	3.68	5.05	1798	1	5.35	6.42
14	5	3.05	4.77	198	4	3.29	4.64	1918	7	5.37	6.86
22	5	2.99	4.51	352	7	3.07	4.92	2874	7	10.12	11.97
26	1	3.05	4.87	378	1	3.72	4.93	2917	1	10.07	11.97
36	5	3.03	4.91	530	7	3.44	4.77	4228	4	18.81	21.07
43	8	3.09	4.87	622	4	3.61	5.02	5876	7	40.81	43.68
88	4	3.03	4.90	697	7	3.16	5.12	6768	7	53.82	56.82
104	5	3.25	4.92	1136	5	3.58	5.24	10052	4	133.10	139.64

Table 4: Prime values of $N_d(n, 1)$ with $3 \le n \le 11000$ along with run times ($r.t.1$ and $r.t.2$ measured in seconds) for tests in Corollaries 3 and 4, respectively

We also employed the L-L test for $l = 1$ on values of $N_d(n, m)$ $(m = 3, 5, 7, 9)$ when $d = f(10^{m-1} + 1)$ and $f \in A$. The prime values of these numbers are recorded in Tables 6, 8, 10 and 12 below.

n	d	q
28	101	11
48	101	11
48	808	11
56	202	11
72	808	11
74	808	11
83	404	11
90	808	11
92	707	11
214	101	11
283	808	11
284	707	11
317	808	11
333	505	11
363	505	11
370	707	11
442	808	11
462	707	11
662	707	11
798	101	11
933	505	11
1209	404	11
1443	505	11
1504	808	11
1610	202	11
2246	707	11
2572	808	11
3747	707	31
5839	707	31
6120	808	11
6265	808	11
6619	808	11
7446	707	11

Table 5: Prime values of $N_d(n, 3)$ with $28 \leq n \leq 8000$ along with q used for testing

n	d	$r.t.$
28	101	1.99
48	101	1.97
48	808	2.03
56	202	2.02
72	808	2.02
74	808	1.96
83	404	1.99
90	808	2.00
92	707	2.03
214	101	2.08
283	808	2.03
284	707	2.13
317	808	2.40
333	505	2.36
363	505	2.27
370	707	2.38
442	808	2.42
462	707	2.41
662	707	2.41
798	101	2.93
933	505	2.85
1209	404	3.45
1443	505	4.10
1504	808	4.53
1610	202	5.08
2246	707	7.68
2572	808	10.28
3747	707	21.02
5839	707	53.24
6120	808	59.17
6265	808	62.87
6619	808	70.35
7446	707	91.35

Table 6: Prime values of $N_d(n, 3)$ with $28 \leq n \leq 8000$ along with run time of the test ($r.t.$ measured in seconds)

n	d	q
69	50005	11
135	50005	11
201	70007	31
211	70007	31
274	70007	11
325	70007	31
404	70007	11
461	20002	11
622	80008	11
836	80008	11
1571	20002	11
1586	20002	11
2180	80008	11
3584	80008	11
3787	50005	11
4546	20002	11
5455	50005	11
6824	20002	11

Table 7: Prime values of $N_d(n, 5)$ with $69 \leq n \leq 7000$ along with q used for testing

n	d	$r.t.$	n	d	$r.t.$	n	d	$r.t.$
69	50005	2.34	404	70007	2.39	2180	80008	7.44
135	50005	2.69	461	20002	2.28	3584	80008	19.74
201	70007	2.30	622	80008	2.61	3787	50005	22.12
211	70007	2.52	836	80008	3.33	4546	20002	32.97
274	70007	2.28	1571	20002	5.06	5455	50005	44.41
325	70007	2.26	1586	20002	5.43	6824	20002	75.55

Table 8: Prime values of $N_d(n, 5)$ with $69 \leq n \leq 7000$ along with run time of the test ($r.t.$ measured in seconds)

n	d	q	n	d	q	n	d	q
67	5000005	11	197	4000004	11	1645	7000007	31
71	5000005	11	228	4000004	41	2215	4000004	11
74	4000004	31	243	5000005	11	2388	7000007	11
76	7000007	11	276	7000007	11	2460	2000002	11
82	8000008	11	291	4000004	11	2577	4000004	11
84	2000002	11	307	5000005	11	3448	7000007	11
104	4000004	31	324	7000007	11	3497	7000007	41
106	1000001	11	512	5000005	71	3862	2000002	11
109	5000005	11	670	1000001	11	6733	7000007	31

Table 9: Prime values of $N_d(n, 7)$ with $67 \leq n \leq 7000$ along with q used for testing

n	d	$r.t.$	n	d	$r.t.$	n	d	$r.t.$
67	5000005	2.34	197	4000004	2.52	1645	7000007	5.45
71	5000005	2.46	228	4000004	2.49	2215	4000004	8.45
74	4000004	2.55	243	5000005	2.55	2388	7000007	9.26
76	7000007	2.63	276	7000007	2.62	2460	2000002	9.98
82	8000008	2.58	291	4000004	2.85	2577	4000004	10.88
84	2000002	2.41	307	5000005	2.88	3448	7000007	18.78
104	4000004	2.49	324	7000007	2.90	3497	7000007	15.06
106	1000001	2.51	512	5000005	2.94	3862	2000002	21.20
109	5000005	2.47	670	1000001	3.02	6733	7000007	62.78

Table 10: Prime values of $N_d(n, 7)$ with $67 \leq n \leq 7000$ along with run time of the test ($r.t.$ measured in seconds)

n	d	q	n	d	q	n	d	q
87	400000004	11	498	100000001	11	1011	200000002	11
110	200000002	11	514	100000001	11	1395	700000007	31
111	400000004	11	564	700000007	11	1628	800000008	11
172	100000001	11	719	800000008	11	1760	700000007	11
186	700000007	11	846	700000007	11	1944	800000008	11
234	100000001	11	932	100000001	11	2486	100000001	11
398	800000008	11	938	100000001	11	3240	700000007	11
452	100000001	11	974	700000007	11	5663	800000008	11

Table 11: Prime values of $N_d(n, 9)$ with $87 \leq n \leq 7000$ along with q used for testing

n	d	$r.t.$	n	d	$r.t.$	n	d	$r.t.$
87	400000004	2.96	498	100000001	2.83	1011	200000002	4.18
110	200000002	3.27	514	100000001	3.27	1395	700000007	4.98
111	400000004	3.04	564	700000007	3.46	1628	800000008	5.39
172	100000001	3.32	719	800000008	3.09	1760	700000007	6.45
186	700000007	2.75	846	700000007	3.90	1944	800000008	7.32
234	100000001	2.79	932	100000001	3.82	2486	100000001	10.52
398	800000008	3.29	938	100000001	3.66	3240	700000007	16.42
452	100000001	3.34	974	700000007	3.86	5663	800000008	50.38

Table 12: Prime values of $N_d(n, 9)$ with $87 \leq n \leq 7000$ along with run time of the test ($r.t.$ measured in seconds)

In using the algorithm of Corollary 1 when $m > 1$, it was necessary to devise a fast method of computing both S_{n-1}^d and $C_d(T_{n-1}) \pmod N$. Since

$$S_{n-2}^{10^{m-1}} \equiv S_{n+m-3} \pmod N,$$

we can easily compute S_{n-1}^d from

$$S_{n-1}^d \equiv (S_{n+m-3}S_{n-1})^f \pmod N.$$

The value of S_{n+m-3} is computed on the way to computing S_{2n+m-2}; hence, we can save S_{n+m-3} for use in this computation.

The problem of computing $C_d(T_{n-1})$ is somewhat more complicated. We first observe from (12) that

$$C_d(T_{n-1}) = C_f(C_{10^{m-1}+1}(T_{n-1})).$$

Thus, the difficulty lies in the computation of

$$C_{10^{m-1}+1}(T_{n-1}) \pmod N.$$

To deal with this, we first introduce the polynomial $S_n(x)$, where $S_0(x) = 0$, $S_1(x) = 1$ and

$$S_n(x) = xS_{n-1}(x) - S_{n-2}(x). \tag{68}$$

This polynomial is discussed briefly in Section 4.2 of [17]. We have

$$C_{kn}(x) = C_k(C_n(x))$$

and

$$C_{kn+1}(x) = C_{n+1}(x)S_k(C_n(x)) - xS_{k-1}(C_n(x)). \tag{69}$$

We can prove (69) by induction on k. We first observe that (69) is true for $k = 1$ and $k = 2$. This is trivial for $k = 1$ and when $k = 2$ we have

$$C_{2n+1}(x) = C_{n+1}(x)C_n(x) - x$$

from (11). We also have

$$C_{(k+1)n+1}(x) = C_n(x)C_{kn+1}(x) - C_{(k-1)n+1}(x)$$

from (11); thus (69) can now be easily established by using (68). Since $C_{2n}(x) = C_n^2(x) - 2$ and $S_{2n}(x) = S_n(x)C_n(x)$, we see on putting $k = 10$ in (69) that

$$C_{10n+1}(x) = (C_{n+1}(x)C_n(x) - x)S_5(C_n^2(x) - 2) - xS_4(C_n^2(x) - 2). \tag{70}$$

The right-hand side of (70) can be considered as a polynomial in x, which we write as $h(C_{n+1}(x), C_n(x), x)$.

Since

$$C_{10n}(x) = C_n(C_{10}(x)),$$

we have

$$C_{10^j}(T_{n-1}) = C_{10^{j-1}}(C_{10}(T_{n-1})) = C_{10^{j-1}}(T_n);$$

hence

$$C_{10^j}(T_{n-1}) \equiv T_{n+j-1} \pmod{N}. \tag{71}$$

Also, by (70)

$$C_{10^j+1}(T_{n-1}) \equiv h(C_{10^{j-1}+1}(T_{n-1}), T_{n+j-2}, T_{n-1}) \pmod{N}. \tag{72}$$

Thus, we can compute

$$C_{10^{m-1}+1}(T_{n-1}) \pmod{N}$$

by iterating (72) $m-2$ times.

9. Conclusion

We have shown that it is possible to construct L-L type tests for the primality of numbers of the form $N_d(n,m)$, where either $d \in A$ or $d = f(10^{m-1}+1)$ and $f \in A$. The methods explained above can, of course, be extended to the development of rigorous primality testing algorithms for many other forms of numbers such as those mentioned in [15]. Indeed, if we consider numbers of the form

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

where d is an integer of m digits, then $M_d(n,m)$ is palindromic whenever d is. Notice that in this case $11 \mid M_d(n,m)$ whenever m is even. These numbers include the so-called Belphegor numbers (See A232448 and A232449 of Sloane [13]) when $m = 3$ and $d = 666$. In view of the different appearances of $N_d(n,m)$ and $M_d(n,m)$, it is remarkable that we can easily adapt the reasoning used to prove Corollary 4 (here, we use $\theta = (N-1)/5$, $r = 10^{2n+m-2}$, $s = 10^{n-1}$) to produce a L-L test for $M_d(n,m)$ with only a few modifications to the steps in Theorem 4: We need only change $(-N)^{(q-1)/2} \equiv -1 \pmod{q}$ to $N^{(q-1)/2} \equiv -1 \pmod{q}$ and replace the subscript $2n+m-1$ by $2n+m-2$ in Steps (3) and (4). Note that if m is odd, it is easy to see that $q = 11$ will work whenever $d \equiv 0, 5, 6 \pmod{11}$; this includes the Belphegor numbers.

Acknowledgment. We wish to thank an anonymous referee, whose careful reading of the original submission of this paper and thoughtful suggestions resulted in a substantial improvement in its exposition.

References

[1] E. Bach and J. Sorenson, Sieve algorithms for perfect power testing, *Algorithmica* **9** (1993), 313-328.

[2] D. J. Bernstein, Detecting perfect powers in essentially linear time, *Math. Comp.* **67** (1998), 1253-1283.

[3] Wieb Bosma, Explicit primality criteria for $h \cdot 2^k \pm 1$, *Math. Comp.* **61** (1993), 97-109.

[4] John Brillhart, Note on representing a prime as a sum of two squares, *Math. Comp.* **26** (1972), 1011-1013.

[5] Yingpu Deng and Dandan Huang, Explicit primality criteria for $h \cdot 2^n \pm 1$, *J. Théor. Nombres Bordeaux* **28** (2016), 55-74.

[6] Chris K. Caldwell and G. L. Honaker, *Prime Curios! The Dictionary of Prime Number Trivia*, CreateSpace, 2009. Companion website: `https://primes.utm.edu/curios/`.

[7] Richard Crandall and Carl Pomerance, *Prime Numbers A Computational Perspective*, Springer-Verlag, New York, 2001.

[8] Newton Friend, *Numbers: Fun and Facts*, Charles Scribner's Sons, New York, 1954.

[9] Great International Mersenne Prime Search. `https://mersenne.org`.

[10] David Harvey and Joris van der Hoeven, Integer multiplication in in time $O(n \log n)$. `https://hal.archives-ouvertes.fr/hal-02070778`

[11] D. H. Lehmer, An extended theory of Lucas' functions, *Ann. of Math.* **31** (1930), 419-448.

[12] Bruce Pyne, *Prime Recreations: An Olio of Curios about Prime Numbers*, Page Publishing, New York, 2018.

[13] N. J. A. Sloane et al., The On-Line Encyclopedia of Integer Sequences, 2021. Available at `https://oeis.org`.

[14] 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.

[15] H. C. Williams, A class of primality tests for trinomials which include the Lucas-Lehmer test, *Pacific J. Math.* **98** (1982), 477-494.

[16] H. C. Williams, Effective primality tests for some integers of the forms $A5^n - 1$ and $A7^n - 1$, *Math. Comp.* **48** (1987), 385-403.

[17] H. C. Williams, *Édouard Lucas and Primality Testing*, Wiley-Interscience, 1998.

[18] H. C. Williams and R. K. Guy, Some fourth-order linear divisibility sequences, *Int. J. Number Theory* **7** (2011),1255-1277.

[19] H. C. Williams and R. K. Guy, Odd and even linear divisibility sequences of order 4, *Integers* **15** (2015), A33.