SOME PRIMALITY TESTS CONSTRUCTED FROM A CUBIC EXTENSION OF THE LUCAS FUNCTIONS

E. L. ROETTGER AND H. C. WILLIAMS

ABSTRACT. The properties of a pair of integer valued sequences, similar to those of Lucas, are used to produce a sufficiency test for the primality of numbers N such that $N^2 + N + 1$ is divisible by a large power of a prime p. The test will run in $O((\log N)^3)$ time, provided that a small prime q ($\equiv 1 \pmod{p}$) is given such that N is a cubic nonresidue of q. It is also shown how this test can be converted to one that is necessary and sufficient. A short table of prime values of such N is also provided.

1. INTRODUCTION

In the 19th century, Ed. Lucas devised a number of primality tests that were derived from the properties of certain second order linear recurrence sequences, now called the Lucas sequences. These tests were for numbers N such that $N \pm 1$ could be mostly factored; in particular, he worked with values of N such that some large prime power p^n divides $N \pm 1$. Although he restricted the value of p to be 2, 3, or 5, it is possible to extend his tests to any prime p. This is discussed is some detail in Roettger, et al. [13], where it is also shown that a particular extension of the Lucas sequences can be used to test the primality of numbers N such that p^n divides $N^2 + 1$. For a brief history of primality testing and how the tests of Lucas fit into the broader history of primality testing, see [10].

As mentioned in [13], Lucas often speculated on the existence of higher order variants of his sequences, based on the roots of third or fourth degree polynomials, which might possess many of the features of his sequences to "arrive at important new properties of prime numbers." It is not clear what such new properties might have been, but likely they involved the places in the sequence where a prime might divide a particular term. It appears that Lucas never succeeded in finding such sequences, but in Müller, et al. [8] and the more detailed Roettger [11], it is argued that he could have discovered the sequences (C_n) and (W_n), which are the cubic analogues of his (quadratic) sequences. For the sequence (C_n), we know that if the corresponding polynomial $f(x)$ is irreducible modulo some prime r, then r must be a divisor of C_n, where $n = r^2 + r + 1$; this is a different condition from that of the Lucas sequence (u_n), where in the analogous situation, we would have $r \mid u_{r+1}$. In this paper, which should be regarded as a lengthy addendum to [13], we will use the properties of (C_n) and (W_n) to derive primality tests for numbers N such that some p^n divides $N^2 + N + 1$. Because such values of N tend to be different from those for which p^n divides $N^2 - 1$, these primality tests would be for numbers distinct from those to which Lucas' methods could be applied.

We begin with a brief characterization of these values of N. We first denote by $\lambda_n(p)$ and $\bar{\lambda}_n(p)$ the two solutions of the congruence

$$x^2 + x + 1 \equiv 0 \pmod{p^n} \quad (1 < x < p^n). \tag{1.1}$$

We will assume here that $\lambda_n(p) < \bar{\lambda}_n(p)$. Notice that for such solutions to exist with $n \geq 2$, it is necessary and sufficient that $p \equiv 1 \pmod 3$. We must also have

$$\lambda_n(p) + \bar{\lambda}_n(p) = p^n - 1. \tag{1.2}$$

Furthermore, $\lambda_n(p)^2 \equiv \bar{\lambda}_n(p) \pmod{p^n}$. Because by (1.2),

$$4((\lambda_n(p))^2 - \bar{\lambda}_n(p)) = [2\lambda_n(p) + 1]^2 + 3 - 4p^n > 3 - 4p^n,$$

we see that $(\lambda_n(p)^2 - \bar{\lambda}_n(p))/p^n > -1$. Hence,

$$((\lambda_n(p))^2 - \bar{\lambda}_n(p))/p^n \geq 0. \tag{1.3}$$

If we know a value of $\gamma_n(p) \in \{\lambda_n(p), \bar{\lambda}_n(p)\}$, we can find a solution of (1.1) when the modulus is p^{n+1} by the usual Hensel lifting process. We put $\kappa_n(p) = (\gamma_n(p)^2 + \gamma_n(p) + 1)/p^n$ and solve the linear congruence $\nu_n(p)(2\gamma_n(p) + 1) \equiv -\kappa_n(p) \pmod p$ for $\nu_n(p)$ with $0 \leq \nu_n(p) < p$. If we put $\gamma_{n+1}(p) = \gamma_n(p) + \nu_n(p)p^n$, then $\gamma_{n+1}(p)$ is a solution of (1.1) for the modulus p^{n+1}. Thus, if we select one of the two possible values for $\gamma_1(p)$, we can compute a fixed sequence $(\gamma_n(p))_{n\geq 1}$. Clearly, if p^n divides $N^2 + N + 1$, then N must have the form $A_n p^n + \gamma_n(p)$, where A_n is some integer and $\gamma_n(p) \in \{\lambda_n(p), \bar{\lambda}_n(p)\}$. In what follows, we will consider the primality of

$$N_n = Ap^n + \gamma_n(p), \tag{1.4}$$

where $n \geq 2$, A is some fixed positive integer, and $p \nmid A$. These forms of N are analogous to the forms $Ap^n \pm 1$ studied by Lucas. (See [13].) Notice that if we define $\bar{\gamma}_n(p) = p^n - 1 - \gamma_n(p)$, then $\bar{\gamma}_n(p)$ is the other solution to (1.1).

2. The C_n and W_n Functions

Let α, β, γ be the three roots of the cubic polynomial $f(x) = x^3 - Px^2 + Qx - R$, where P, Q, R are any integers. We restrict the roots of $f(x)$ to be distinct; hence, if

$$\delta = (\alpha - \beta)(\beta - \gamma)(\gamma - \alpha), \tag{2.1}$$

we have $\Delta = \delta^2 = P^2Q^2 - 4Q^3 - 4RP^3 + 18PQR - 27R^2$, and we see that $\delta \neq 0$. In [8], the functions that we will denote here by C_n or $C_n(P, Q, R)$ and W_n or $W_n(P, Q, R)$ are defined by

$$\begin{aligned} \delta C_n &= (\alpha^n - \beta^n)(\beta^n - \gamma^n)(\gamma^n - \alpha^n) \\ &= (\alpha^n\beta^{2n} + \beta^n\gamma^{2n} + \gamma^n\alpha^{2n}) - (\alpha^{2n}\beta^n + \beta^{2n}\gamma^n + \gamma^{2n}\alpha^n), \\ W_n &= (\alpha^n\beta^{2n} + \beta^n\gamma^{2n} + \gamma^n\alpha^{2n}) + (\alpha^{2n}\beta^n + \beta^{2n}\gamma^n + \gamma^{2n}\alpha^n). \end{aligned}$$

We have $C_0 = 0$, $C_1 = 1$, $C_2 = PQ - R$; $W_0 = 6$, $W_1 = PQ - 3R$, $W_2 = P^2Q^2 - 2Q^3 - 2P^3R + 4PQR - 3R^2$. Also, $C_{-n} = -R^{-2n}C_n$ and $W_{-n} = R^{-2n}W_n$. C_n and W_n are symmetric functions of α, β, γ and are therefore integers for all nonnegative values of n. It is these functions that we will use as our extensions of the Lucas functions. Observe that (C_n) is a divisibility sequence; also, both the sequences (C_n) and (W_n) satisfy the 6th order recurrence

$$X_{n+6} = A_1X_{n+5} - A_2X_{n+4} + A_3X_{n+3} - A_4X_{n+2} + A_5X_{n+1} - A_6X_n,$$

where $A_1 = PQ - 3R$, $A_2 = RP^3 + Q^3 - 5PQR + 6R^2$, $A_3 = R(P^2Q^2 - 2Q^3 - RP^3 + 4PQR - 7R^2)$, $A_4 = R^2A_2$, $A_5 = R^4A_1$, $A_6 = R^6$.

It is mentioned in [8] that Lucas was likely aware of the sequences (C_n) and (W_n) and it is shown there that the theory of them exactly parallels that of the Lucas sequences, even down

to the Euler criterion. There are addition formulas, multiplication formulas, and a number of identity relations. For example,

$$C_{2n} = C_n(W_n + 2R^n), \quad 2W_{2n} = \Delta C_n^2 + W_n^2 - 4R^n W_n$$

are the duplication formulas. What is particularly remarkable in this system is that, just as in the case of the Lucas sequences, only the two sequences (C_n) and (W_n) are required for its development. Furthermore, it is argued in [8] and [11] that Lucas had the mathematical knowledge and ability needed to discover these results.

In Section 3 of Roettger and Williams [12], it is shown how to compute remote terms of (C_n) and (W_n) modulo any N such that $\gcd(N, R) = 1$. If $k = \log m$, this technique requires $12k$ modular multiplications to compute C_m and W_m modulo N. More specifically, if we define

$$X_n = W_n/(2R^n), \quad \tilde{D}_n = \Delta C_n^2/(4R^{2n}), \quad \text{and} \quad Y_{m,n} = C_{mn}/(C_n R^{mn-n})$$

for any positive integers n and m, then there exist polynomials $F_m, G_m \in \mathbb{Z}[x, y]$ such that

$$X_{mn} = F_m(X_n, \tilde{D}_n) \text{ and } Y_{m,n} = G_m(X_n, \tilde{D}_n).$$

We have $F_0(x, y) = 3$, $F_1(x, y) = x$, $F_2(x, y) = x^2 + y - 2x$,
$F_3(x, y) = x^3 + 3xy + 3y - 3x^2 + 3$ and $G_0(x, y) = 0$, $G_1(x, y) = 1$, $G_2(x, y) = 2x + 2$, $G_3(x, y) = 3x^2 + y$. Also, if we define the sextet $\mathcal{S}_m = \{F_m, F_{m+1}, F_{m+2}, G_m, G_{m+1}, G_{m+2}\}$, then given any $\mathcal{S}_m$, we can compute $\mathcal{S}_{2m+1}$ or $\mathcal{S}_{2m}$ in 12 multiplications by using the formulas in [12]. We remark here that there are some misprints in formulas (14) and (15) of [12]. For our case, they should read

$$F_{2m+3} = F_{m+1}(F_{m+2} - x) + yG_{m+1}(G_{m+2} + 1) + F_m,$$
$$G_{2m+3} = F_{m+1}(G_{m+2} - 1) + G_{m+1}(F_{m+2} + x) - G_m,$$

respectively. If $x \equiv X_n$ and $y \equiv \tilde{D}_n \pmod N$, this allows us to compute $X_{mn} \equiv F_m(x, y)$, $Y_{m,n} \equiv G_m(x, y) \pmod N$ in $12k$ modular multiplications modulo N, where $k = \lceil \log N \rceil$. Notice that $\tilde{D}_{nm} \equiv \tilde{D}_n G_m^2 \pmod N$.

Suppose for any positive integer n, we define

$$D_n = \gcd(C_n, W_n - 6R^n).$$

In [8], it is shown that the sequence (D_n) is a divisibility sequence. It is also proved that if m is any positive integer such that $\gcd(m, R) = 1$, then there exists a *rank of apparition* of m in (D_n); this is the least positive integer $\omega = \omega(m)$ such that $m \mid D_\omega$. Furthermore, if $m \mid D_n$, then $\omega \mid n$.

Now, let r be any prime. From results in Chapter 5 of [11], we know that if $r \nmid 6\Delta R$, then $\omega(r)$ must divide either $r - 1$, $r^2 - 1$, or $r^2 + r + 1$. If the Legendre symbol $(\Delta/r) = 1$, then $\omega(r) \mid r^2 + r + 1$ if and only if $f(x)$ is irreducible modulo r and $\omega(r) \mid r - 1$, otherwise. As in [8], we will call a prime r such that $f(x)$ is irreducible modulo r an I-prime w.r.t. $f(x)$. This brings us to the question of, given any prime r, how to construct a polynomial $f(x)$ that is irreducible modulo r? It is pointed out by Lehmer in [6] that if q $(\neq r)$ is a prime congruent to 1 modulo 3 and $r^{(q-1)/3} \not\equiv 1 \pmod q$, then the cubic polynomial $f_1(x) = x^3 - P_1x^2 + Q_1x - R_1$, where $P_1 = 0$, $Q_1 = -3q$, and $R_1 = qt$, is irreducible modulo r, whenever $r \nmid tu$. Here, the values of t and u are determined from the quadratic partition $4q = t^2 + 27u^2$, where $t \equiv 1 \pmod 3$. We can also put $\delta_1 = 27qu$. In what follows, we will assume that the primes r and q satisfy the above conditions.

From the theory of finite fields (see Lidl and Niederreiter [7]), we know that if $f(x)$ is an irreducible cubic modulo r, then in $\mathbb{F}_r[x]$, we have $f(x) \mid g(x)$, where $g(x) = x^{r^3} - 1$. Since the splitting field of $g(x)$ over $\mathbb{F}_r$ is $\mathbb{F}_{r^3}$, we see (as is well known) that the splitting field of

$f(x)$ must be $\mathbb{F}_{r^3}$. Because $|\mathbb{F}_{r^3}| = r^3$, we see that if α_1 is any root of $f_1(x)$ in $\mathbb{F}_{r^3}$ and α is any root of $f(x)$ over $\mathbb{F}_r$, there must exist a, b, $c \in \mathbb{F}_r$ such that

$$\alpha = a + b\alpha_1 + c\alpha_1^2. \tag{2.2}$$

Note that we cannot have $b = c = 0$ here, because $\alpha \notin \mathbb{F}_r$. Thus, if we put

$$\begin{aligned} &P = 3a - 2cQ_1, \quad Q = 3a^2 - 4acQ_1 + b^2Q_1 - 3bcR_1 + c^2Q_1^2, \\ &R = a^3 + b^3R_1 + c^3R_1^2 - 3abcR_1 + (ab^2 - 2a^2c)Q_1 + ac^2Q_1^2 + bc^2Q_1R_1, \end{aligned} \tag{2.3}$$

then $f(x) = x^3 - Px^2 + Qx - R$ must be irreducible modulo r, whenever $(b, c) \neq (0, 0)$ and $r \nmid R$; furthermore, if $f(x) = x^3 - Px^2 + Qx - R$ is irreducible modulo r, then there must exist a, b, $c \in \mathbb{F}_r$ with $(b, c) \neq (0, 0)$ such that P, Q, and R can be determined by (2.3). For P, Q, R given as above, it is easy to show, from (2.1), that

$$\delta = \delta_1(b^3 + bc^2Q_1 - c^3R_1) \in \mathbb{F}_r; \tag{2.4}$$

and $r \nmid \Delta$.

3. A Sufficiency Test for the Primality of N_n

In this section, we will develop a sufficiency test for the primality of numbers of the form (1.4). We begin with a useful lemma.

Lemma 3.1. *Let N be any positive integer such that $\gcd(N, 2R) = 1$ and n be any positive integer such that $\gcd(N, n) = 1$. If m is any positive integer such that $N \mid C_{mn}/C_m$, then $\gcd(N, D_m) = 1$.*

Proof. This is easy to show from the proof of Lemma 7.7 of [8]. □

We can now prove a theorem analogous to Theorem 2.4 of [13].

Theorem 3.2. *Let N be any positive integer such that $\gcd(N, 2R) = 1$. Suppose that n is any positive integer such that $\gcd(N, n) = 1$ and that for some positive integer m, we have $N \mid D_{mn}$ and $N \mid C_{mn}/C_m$. If t is any prime divisor of N, then $\omega(t) \mid mn$ and $\omega(t) \nmid m$.*

Proof. Clearly, we must have $\omega(t) \mid mn$, as $t \mid D_{mn}$. Also, by Lemma 3.1, we see that t cannot divide D_m; hence, $\omega(t) \nmid m$. □

We now turn our attention to the case of N, given as N_n of (1.4). We will assume that

(1) neither $\gamma_n(p)$ nor $\bar{\gamma}_n(p)$ is a divisor of N_n;
(2) $A \neq 4p^n - 4\gamma_n(p) + \kappa_n(p) - 4$, where $\kappa_n(p) = (\gamma_n(p)^2 + \gamma_n(p) + 1)/p^n$.

Because $\gamma_n(p)$ and $\bar{\gamma}_n(p)$ both exceed 1, (1) must hold if N_n is to be a prime. Also, if $A = 4p^n - 4\gamma_n(p) + \kappa_n(p) - 4$, then it is easy to see that $N_n = (p^n + \bar{\gamma}_n(p))^2$, which means that N_n cannot be a prime. Before proving the main result of this section, we need the following simple lemma.

Lemma 3.3. *If k is an integer such that $1 \leq k < n$, then*

$$N_n \neq (p^k + \bar{\gamma}_n(p))^2.$$

Proof. If $N_n = (p^k + \bar{\gamma}_n(p))^2$, then

$$p^n \mid (p^k - 1 - \gamma_n(p))^2 - \gamma_n(p),$$

which means that

$$p^n \mid p^{2k} - 2p^k(\gamma_n(p) + 1).$$

It follows that because p is odd and $n > k \geq 1$, we must have $p \mid \gamma_n(p) + 1$, because $p \mid \gamma_n(p)^2 + \gamma_n(p) + 1$, is impossible. □

We are now able to prove a sufficiency condition for the primality of N_n.

Theorem 3.4. *Let N_n be given by (1.4) such that conditions (1) and (2) hold. Put $m = p^{h-1}(N_n^2 + N_n + 1)/p^n$, where $1 \leq h \leq n$. If $\gcd(N_n, \Delta R) = 1$, Δ is a perfect integral square, $N_n \mid D_{pm}$, and $N_n \mid C_{pm}/C_m$, then N_n is a prime, when $A < 2p^{2h-n}$.*

Proof. Suppose that N_n is composite; then if t is any prime divisor of N_n and $N_n = tT$, we must have $T > 1$. By Theorem 3.2, we must have $\omega(t) \mid pm$ and $\omega(t) \nmid m$. Hence, $p^h \mid \omega(t)$. Because $(\Delta/t) = 1$, we know that $\omega(t)$ is a divisor of $t - 1$ or of $t^2 + t + 1$. Thus, we must have $t \equiv 1 \pmod{p^h}$ or $t \equiv \gamma_n(p)$ or $\bar{\gamma}_n(p) \pmod{p^h}$. In the first case, we get $t = u_1 p^h + 1$, where u_1 must be even and greater than 0. Also, because $N_n = tT$, we must have $T \equiv \gamma_n(p) \pmod{p^h}$ and therefore, $T = u_2 p^h + \gamma_n(p)$, where $u_2 \geq 1$. It follows that because

$$N_n = Ap^n + \gamma_n(p) = (u_1 p^h + 1)(u_2 p^h + \gamma_n(p)),$$

we get $p^n A > u_1 u_2 p^{2h}$, which means that $A > 2p^{2h-n}$, a contradiction.

We must now address the case of $t \equiv \gamma_n(p)$ or $\bar{\gamma}_n(p) \pmod{p^h}$. In the first case, we have $t = u_1 p^h + \gamma_n(p)$, where $u_1 \geq 1$. Also, because $T\gamma_n(p) \equiv \gamma_n(p) \pmod{p^h}$, we get $T \equiv 1 \pmod{p^h}$ and because T must be odd, we find, as above, that $A > 2p^{2h-n}$, a contradiction. If $t \equiv \bar{\gamma}_n(p) \pmod{p^h}$, then $T\bar{\gamma}_n(p) \equiv \gamma_n(p) \pmod{p^h}$, which means that $T \equiv \bar{\gamma}_n(p) \pmod{p^h}$. Hence,

$$t = u_1 p^h + \bar{\gamma}_n(p), \quad T = u_2 p^h + \bar{\gamma}_n(p),$$

where $u_1, u_2 \geq 1$. If $u_1 = u_2 = 1$, then $N_n = (p^h + \bar{\gamma}_n(p))^2$, a case that is excluded by Lemma 3.3 unless $h = n$, but if $h = n$, we get a contradiction to condition (2). It follows that we must have

$$N_n = Ap^n + \gamma_n(p) = (u_1 p^h + \bar{\gamma}_n(p))(u_2 p^h + \bar{\gamma}_n(p)),$$

where at least one of u_1, u_2 must exceed or equal 2. From the above equality, we see that

$$A = u_1 u_2 p^{2h-n} + \bar{\gamma}_n(p) p^{h-n}(u_1 + u_2) + (\bar{\gamma}_n(p)^2 - \gamma_n(p))/p^n > u_1 u_2 p^{2h-n},$$

by (1.3). Because $u_1 u_2 \geq 2$, we once again get $A > 2p^{2h-n}$, a contradiction. □

Notice that if N_n is a prime, q ($\neq N_n$) is a prime congruent to 1 modulo 3 such that $N_n^{(q-1)/3} \not\equiv 1 \pmod{q}$ and P, Q, R are selected using (2.3), then we must have that Δ a perfect integral square by (2.4) and, furthermore, $N_n \mid D_m$, where $m = N_n^2 + N_n + 1$.

Now, suppose that r is any I-prime w.r.t. $f(x)$. We must have $r \mid D_{r^2+r+1}$. If p is some prime such that $p^n \mid r^2 + r + 1$, put

$$w = (r^2 + r + 1)/p^n$$

and suppose that $r \nmid D_w$; there must exist some minimal h such that $1 \leq h \leq n$ and $r \mid D_{wp^h}$. If we put $m = p^{h-1}w$, we have $r \mid D_{pm}$ and $r \nmid D_m$. We next need the following result.

Theorem 3.5. *If r is an I-prime w.r.t. $f(x)$, then $r \mid C_n$ if and only if $r \mid D_n$.*

Proof. This is Theorem 5.7 of [11]. □

We see, then, that if $r \nmid D_m$, then $r \nmid C_m$ and because $r \mid D_{pm}$, we must have $r \mid C_{pm}/C_m$.

For r given as above, we will need an algorithm to determine h. We first observe that by the definition of X and Y, we have

$$X_{p^i w} \equiv W_{p^i w}/(2R^{p^i w}), \quad Y_{p,p^{i-1}w} \equiv C_{p^i w}/(C_{p^{i-1}w} R^{p^i w - p^{i-1} w}) \pmod{r}.$$

It follows that h is the least value of i such that $0 \le i \le n$, $X_{p^i w} \equiv 3$, and $Y_{p,p^{i-1}w} \equiv 0 \pmod r$.

Algorithm 3.6. *For the prime r defined as above, this algorithm determines h, the least value of i, if it exists, such that $1 \le i \le n$, $X_{p^i w} \equiv 3$, and $Y_{p,p^{i-1}w} \equiv 0 \pmod r$.*

(i) Put $X_1 \equiv W_1/(2R)$, $d_1 = \delta/(2R)$, $\tilde{D}_1 \equiv d_1^2 \pmod r$, and $w = (r^2 + r + 1)/p^n$.
(ii) Use the technique mentioned in the previous section to compute X_w, $Y_{w,1}$, $d_w \equiv d_1 Y_{w,1}$, and $\tilde{D}_w \equiv d_w^2 \pmod r$.
(iii) If $X_w \equiv 3$ and $Y_{w,1} \equiv 0 \pmod r$, then h cannot exist and the algorithm terminates.
(iv) Initialize i to 1.
(v) Compute

$$X_{p^i w} \equiv F_p(X_{p^{i-1}w}, \tilde{D}_{p^{i-1}w}), \quad Y_{p,p^{i-1}w} \equiv G_p(X_{p^{i-1}w}, \tilde{D}_{p^{i-1}w}) \pmod r.$$

(vi) If $X_{p^i w} \equiv 3$ and $Y_{p,p^{i-1}w} \equiv 0 \pmod r$, put $h = i$ and terminate the algorithm.
(vii) If $i < n$, put $d_{p^i w} \equiv d_{p^{i-1}w} Y_{p,p^{i-1}w}$ and $\tilde{D}_{p^i w} \equiv (d_{p^i w})^2 \pmod r$. Replace the value of i by $i + 1$ and go back to step (v).

From this material, we are now able to formulate the following test for the primality of certain odd N_n given by (1.4).

Test 3.7. *This algorithm tests the primality of odd N_n of form (1.4), where $n \ge 2$ and A is some fixed positive integer such that $p \nmid A$ and $A < 2p^n$.*

(i) We first check that conditions (1) and (2) hold. If this is not the case, then N_n is not a prime and we are finished.
(ii) Select some prime q such that q is congruent to 1 modulo 3 and $N_n^{(q-1)/3} \not\equiv 1 \pmod q$.
(iii) Select some triple of integers (a, b, c) such that $(b, c) \not\equiv (0, 0) \pmod{N_n}$ and use (2.3) to compute P, Q, R.
(iv) Check that $\gcd(N_n, \Delta R) = 1$. If not, then N_n is not a prime and we terminate the test.
(v) Put $w = (N_n^2 + N_n + 1)/p^n$. If $X_w \equiv 3$ and $Y_{w,1} \equiv 0 \pmod{N_n}$, then terminate the test and output: "Indeterminate, Circumstance 1" and include the values of a, b, c.
(vi) Use Algorithm 3.6, with r replaced by N_n, to find the least value of h such that $1 \le h \le n$, $X_{p^h w} \equiv 3$, and $Y_{p,p^{h-1}w} \equiv 0 \pmod{N_n}$. If no such h exists, then N_n cannot be a prime.
(vii) If $A < 2p^{2h-n}$, then N_n is a prime. If $A \ge 2p^{2h-n}$, then terminate the algorithm and output: "Indeterminate, Circumstance 2".

We do not learn anything about the primality of N_n when either Circumstance 1 or 2 holds. In what follows, we will address this possibility.

4. Gaussian Periods

We first focus on the likelihood that Circumstance 1 holds. When N_n is a prime, we require the following lemma.

Lemma 4.1. *Let r be any prime such that $r \nmid 2R\Delta$ and let $\mathbb{K}$ be the splitting field of $f(x)$ over $\mathbb{F}_r$. If α, β, γ are the roots of $f(x)$ in $\mathbb{K}$, then $r \mid D_n$ if and only if $\alpha^n = \beta^n = \gamma^n$ in $\mathbb{K}$.*

Proof. This is proved as Lemma 5.4 in [11]. □

Next, suppose r is an I-prime w.r.t. $f(x)$; then the splitting field $\mathbb{K}$ of $f(x) \in \mathbb{F}_r[x]$ is $\mathbb{F}_{r^3}$. Also, in $\mathbb{K}$, the three roots α, β, γ of $f(x)$ satisfy:

$$\beta = \alpha^r,\ \gamma = \beta^r,\ \alpha = \gamma^r. \tag{4.1}$$

We now have a simple condition for $r \mid D_n$.

Theorem 4.2. *If r is an I-prime w.r.t. $f(x)$, then $r \mid D_n$ if and only if $\alpha^{(r-1)n} = 1$ in $\mathbb{K}$. Here, α denotes any of the three roots of $f(x)$ in $\mathbb{K}$.*

Proof. If $r \mid D_n$, then in $\mathbb{K}$, we have $\alpha^n = \gamma^n$ by Lemma 4.1. Hence $\alpha^{rn} = \gamma^{rn}$, which means, by (4.1), that $\alpha^{rn} = \gamma^{rn} = \alpha^n$, and therefore, $\alpha^{(r-1)n} = 1$.

If $\alpha^{(r-1)n} = 1$ in $\mathbb{K}$, then $\alpha^n = \alpha^{rn}$, which by (4.1) means that $\alpha^n = \beta^n$. By raising both sides of this equality to the power r, we get $\alpha^{rn} = \beta^{rn}$. By (4.1), we have $\gamma^n = \alpha^n$; hence, $r \mid D_n$, by Lemma 4.1. □

If G is any finite cyclic group of order m, it is well known that if $n \mid m$, there are exactly n elements x in G that satisfy $x^n = 1$. Furthermore, the number of elements of order n in G is $\phi(n)$, where ϕ is Euler's totient function. Let p be any prime such that $p^n \mid r^2 + r + 1$ $(n \geq 1)$. Because $\mathbb{F}^*_{r^3}$ is a finite cyclic group, this means that there are exactly $(r-1)w$ elements α of $\mathbb{F}^*_{r^3}$ such that $\alpha^{(r-1)w} = 1$, where $w = (r^2 + r + 1)/p^n$. Thus, for a randomly selected admissible triple of integers (a, b, c) with $0 \leq a, b, c < r$ such that $(b, c) \neq (0, 0)$, we expect, for $f(x)$ determined by using (2.3) and α a root of $f(x)$ in $\mathbb{F}^*_{r^3}$, that $\alpha^{(r-1)w} = 1$ with probability $(r-1)w/|\mathbb{F}^*_{r^3}| = 1/p^n$. It follows from Theorem 4.2 that if p^n is large, it would be unlikely that $r \mid D_w$, when P, Q, R are determined by (2.3).

If N_n is composite and Circumstance 1 holds for many or all admissible (a, b, c), then N_n would be a sort of pseudoprime with respect to the sequence $(D_k)_{k \geq 0}$. As pseudoprimes tend to be rarer than primes, it seems that Circumstance 1 would be an infrequent occurrence for composite N_n, but as shown in Section 7, such values of N_n, although unusual, do exist.

We next focus on the possibility that Circumstance 2 does not hold; that is

$$A < 2p^{2h-n}. \tag{4.2}$$

Notice that if $h = n$, then (4.2) holds by selection of A. Also, if N_n is a prime, we expect that for a randomly selected $f(x)$, we would have $h = n$ with probability $\phi(N_n^3 - 1)/(N_n^3 - 1)$, a quantity that is mostly close to 1. (see Section 18.4 of Hardy and Wright [4]) Thus, if N_n is a prime, then Test 3.7 will likely establish that this is so, but we will try to eliminate some of the probabilistic aspects of the test.

Let f be some fixed integer and p be any prime such that $p = 1 + ef$. Also, let g be any primitive root of p and ζ_p be any primitive pth root of unity. We define the e Gaussian periods η_i for $i = 0, 1, 2, \ldots, e-1$ by

$$\eta_i = \sum_{j=0}^{f-1} \zeta_p^{g^{ej+i}}.$$

It has been known since Gauss that the e Gaussian periods are the roots of the Gaussian period equation $H(x) = 0$, where $H(x) \in \mathbb{Z}[x]$ and is of degree e.

Now, consider the case of $f = 3$. If we put $s = g^e$, then $p \mid s^2 + s + 1$ and the e Gaussian periods are given by

$$\eta_i = \zeta_p^{g^i} + \zeta_p^{sg^i} + \zeta_p^{s^2 g^i} \quad (i = 0, 1, 2, \ldots, e-1). \tag{4.3}$$

By making use of $\zeta_p^p = 1$, it is easy to see, for example, that in the case of $p = 7$, we have $H(x) = x^2 + x + 2$ and in the case of $p = 13$, we have $H(x) = x^4 + x^3 + 2x^2 - 4x + 3$. More

information concerning this polynomial can be found in Lehmer and Lehmer [5]. If we put $f = 6$, the resulting Gaussian periods are the roots of $H^*(x)$, where $H^*(x) \in \mathbb{Z}[x]$ and is of degree $(p-1)/6$. For example, $H^*(x) = x + 1$ for $p = 7$; $H^*(x) = x^2 + x - 3$ for $p = 13$; $H^*(x) = x^3 + x^2 - 6x - 7$ for $p = 19$.

Consider r to be an I-prime w.r.t. $f(x)$. There must exist some nonzero $\lambda \in \mathbb{F}_{r^3}$ such that $\mathbb{F}^*_{r^3} =< \lambda >$; and if we put $\zeta_p = \lambda^{(r^3-1)/p}$, then $\zeta_p^p = 1$ and $\zeta_p^m \neq 1$, when $p \nmid m$. It follows that if $\mu \in \mathbb{F}_{r^3}$ and $\mu^p = 1$, then $\mu = \zeta_p^i$ for some nonnegative integer i $(< p)$. We can use (4.3) to define the Gaussian periods in $\mathbb{F}_{p^r}$, where $s = r$ or $s = r^2$. Note that by (4.3), we have $\eta_i^r = \eta_i$ and therefore, $\eta_i \in \mathbb{F}_r$. Furthermore, we also observe that

$$G_j = \zeta_p^j + \zeta_p^{js} + \zeta_p^{js^2} \tag{4.4}$$

must be a Gaussian period $(f = 3)$ when $p \nmid j$; thus, $G_j \in \mathbb{F}_r$. Furthermore, it is not difficult to see that $G_j + G_{-j}$ must be a solution of $H^*(x) \equiv 0 \pmod r$. If we put $\nu_1 = \zeta_p^j$, $\nu_2 = \zeta_p^{js}$, $\nu_3 = \zeta_p^{js^2}$, we have $G_j = \nu_1 + \nu_2 + \nu_3$, $G_{-j} = \nu_1\nu_2 + \nu_2\nu_3 + \nu_3\nu_1$, and $\nu_1\nu_2\nu_3 = 1$. Thus, for $k \geq 3$, we have

$$G_{kj} = G_j G_{(k-1)j} - G_{-j} G_{(k-2)j} + G_{(k-3)j}$$

with $G_0 = 3$ and $G_{2j} = G_j^2 - 2G_{-j}$. For any nonnegative integer k, define the two variable polynomial $K_k(x, y)$ $(\in \mathbb{Z}[x, y])$ by $K_0(x, y) = 3$, $K_1(x, y) = x$, $K_2(x, y) = x^2 - 2y$, $K_3(x, y) = x^3 - 3xy + 3$ and for $k \geq 3$,

$$K_k(x, y) = xK_{k-1}(x, y) - yK_{k-2}(x, y) + K_{k-3}(x, y).$$

Notice that $K_k(x, y)$ is of degree k, its coefficients depend only on k, and that $G_{kj} = K_k(G_j, G_{-j})$.

Next, we have a theorem that allows us to find some pair G_j, $G_{-j} \in \mathbb{F}_r$.

Theorem 4.3. *Suppose that r and p are as above. If $p \mid n$, $r \mid D_n$, and $r \nmid D_m$, where $m = n/p$, then for some i such that $p \nmid i$, we have that $G_i = (W_m + \delta C_m)/(2R^m)$ and $G_{-i} = (W_m - \delta C_m)/(2R^m)$ are Gaussian periods for $f = 3$ in $\mathbb{F}_r$.*

Proof. Because $r \mid D_n$, we know, by Lemma 4.1, that $\alpha^n = \beta^n = \gamma^n$ in $\mathbb{K}$. Because $C_m \neq 0$, we can only have

$$\alpha^m = \zeta_p^i \beta^m, \;\; \beta^m = \zeta_p^j \gamma^m, \;\; \gamma^m = \zeta_p^k \alpha^m, \tag{4.5}$$

where $p \nmid ijk$. However, because by multiplying the above expressions, we get $R^m = \zeta_p^{i+j+k} R^m$ and $R \neq 0$, we must have $p \mid i + j + k$. Also, because $\alpha^m - \beta^m = \beta^m(\zeta_p^i - 1)$ and $\alpha^m + \beta^m = \beta^m(\zeta_p^i + 1)$ with similar results for $\beta^m \pm \gamma^m$ and $\gamma^m \pm \alpha^m$, we get

$$\begin{aligned}
\delta C_m &= R^m(\zeta_p^i - 1)(\zeta_p^j - 1)(\zeta_p^k - 1) \\
&= R^m(\zeta_p^i + \zeta_p^j + \zeta_p^k - \zeta_p^{i+j} - \zeta_p^{j+k} - \zeta_p^{k+i}), \\
W_m &= R^m(\zeta_p^i + 1)(\zeta_p^j + 1)(\zeta_p^k + 1) - 2R^m \\
&= R^m(\zeta_p^i + \zeta_p^j + \zeta_p^k + \zeta_p^{i+j} + \zeta_p^{j+k} + \zeta_p^{k+i}).
\end{aligned}$$

By (4.5), we have $\alpha^{rm} = \zeta_p^{ir}\beta^{rm}$ and by (4.1), $\beta^m = \zeta_p^{ir}\gamma^m$; similarly $\gamma^m = \zeta_p^{ir^2}\alpha^m$. It follows, from (4.5), that $j = ir$ and $k = ir^2$. Because $r + 1 = -r^2$, $r^2 + 1 = -r$, and $r^2 + r = -1$, we get, for $s = r$ that

$$\delta C_m = R^m(G_i - G_{-i}) \;\text{ and }\; W_m = R^m(G_i + G_{-i}).$$

□

If we return to Algorithm 3.6 and put $m = p^{h-1}w$, we have $W_m/(2R^m) \equiv X_m$, $C_m/(2R^m) \equiv d_m \pmod{r}$; thus, in this case, we have, for some j, that $G_j = X_m + d_m$ and $G_{-j} = X_m - d_m$ are both Gaussian periods for $f = 3$ in $\mathbb{F}_r$. We can now replace Step (vii) in Test 3.7 by:

(vii)′ *If $A < 2p^{2h-n}$, then N_n is a prime; if $A \geq 2p^{2h-n}$, put $G \equiv X_m + d_m \pmod{N_n}$ and $\bar{G} \equiv X_m - d_m \pmod{N_n}$. If $H(G) \not\equiv 0$ or $H(\bar{G}) \not\equiv 0 \pmod{N_n}$, then N_n is not a prime. If $H^*(G + \bar{G}) \not\equiv 0 \pmod{N_n}$, then N_n is not a prime.*

Thus, if h exists, the resulting algorithm will establish whether or not N_n is a prime or, for $f = 3$, find two particular solutions G and $\bar{G}$ to $H(x) \equiv 0 \pmod{N_n}$ such that $H^*(G+\bar{G}) \equiv 0 \pmod{N_n}$. In the next section, we will show how, given such solutions of $H(x) \equiv 0 \pmod{N_n}$, we can find some $f(x)$ such that $h = n$, when N_n is a prime.

5. Some Results Concerning Gaussian Sums

As before, we consider three distinct primes p, q, r, where $p \equiv 1 \pmod 3$, $q \equiv 1 \pmod p$, and $p \mid r^2 + r + 1$. Let χ denote a primitive character of order p. If t is a primitive root of q, we can define χ by $\chi(t^j) = \zeta_p^j$. It is well known (see Chapter 11 of Williams [14] or Berndt, et al. [2]), that if $\tau(\chi)$ denotes the Gaussian sum

$$\tau(\chi) = \sum_{j=1}^{q-1} \chi(j)\zeta_q^j,$$

where ζ_q is a primitive qth root of unity, then

$$\tau(\chi)\tau(\chi^{-1}) = q. \tag{5.1}$$

It follows that, if z is any complex number and we denote by $\bar{z}$ the complex conjugate of z, then $\chi^{-1} = \bar{\chi}$.

We also know that $(\tau(\chi))^p/q$ can be written as the sum $\sum_{i=0}^{p-2} b_i\zeta_p^i$, where $b_i \in \mathbb{Z}$ for $i = 0, 1, 2, \ldots, p-2$. We can write

$$(\tau(\chi^j))^p/q = \sum_{i=0}^{p-2} b_i\zeta_p^{ij}, \quad (j = 1, 2, \ldots, p-2). \tag{5.2}$$

This is a consequence of

$$\tau(\chi_1)\tau(\chi_2) = J(\chi_1, \chi_2)\tau(\chi_1\chi_2), \tag{5.3}$$

where $J(\chi_1, \chi_2)$ is the Jacobi sum. (For more information on Jacobi sums, see [2].) It is sufficient here to note that

$$J(\chi, \chi^j) = \sum_{i=0}^{p-1} B(i, j)\zeta_p^i, \tag{5.4}$$

where $B(i, j)$ is a nonnegative integer for $0 \leq i, j \leq p-1$. By using (5.4) and

$$(\tau(\chi))^p = q\prod_{i=1}^{p-2} J(\chi, \chi^i),$$

a consequence of (5.3) and (5.1), all $p-2$ values of the integers b_i in (5.2) can be computed in $O(p^3)$ arithmetic operations. Notice that the values of these integers depend only on the values of p and q.

Now, suppose s is a solution of $x^2+x+1\equiv 0 \pmod p$. For a fixed value of j, put $\alpha_j=(\tau(\chi^j))^p/q$, $\beta_j=(\tau(\chi^{sj}))^p/q$, $\gamma_j=(\tau(\chi^{s^2j}))^p/q$. By (4.4) and (5.2), we see that

$$S_1=\alpha_j+\beta_j+\gamma_j=\sum_{i=1}^{p-2}b_iG_{ij}=\sum_{i=1}^{p-2}b_iK_i(G_j,G_{-j}). \tag{5.5}$$

Also, we can use (4.4) and (5.2) and $\zeta_p^p=1$ to compute $c_i\in\mathbb{Z}$ $(i=1,2,\dots,p-2)$ such that $\alpha_j^2=\sum_{i=1}^{p-2}c_i\zeta_p^{ij}$; we then have $\beta_j^2=\sum_{i=1}^{p-2}c_i\zeta_p^{sij}$, $\gamma_j^2=\sum_{i=1}^{p-2}c_i\zeta_p^{s^2ij}$, and

$$S_2=\alpha_j^2+\beta_j^2+\gamma_j^2=\sum_{i=1}^{p-2}c_iG_{ij}=\sum_{i=1}^{p-2}c_iK_i(G_j,G_{-j}). \tag{5.6}$$

We can also compute integers m_i $(i=1,2,\dots,p-2)$ such that $\alpha_j^3=\sum_{i=1}^{p-2}m_i\zeta_p^{ij}$, $\beta_j^3=\sum_{i=1}^{p-2}m_i\zeta_p^{sij}$, and $\gamma_j^3=\sum_{i=1}^{p-2}m_i\zeta_p^{s^2ij}$ and we get

$$S_3=\alpha_j^3+\beta_j^3+\gamma_j^3=\sum_{i=1}^{p-2}m_iG_{ij}=\sum_{i=1}^{p-2}m_iK_i(G_j,G_{-j}). \tag{5.7}$$

Putting $P_j=\alpha_j+\beta_j+\gamma_j$, $Q_j=\alpha_j\beta_j+\beta_j\gamma_j+\gamma_j\alpha_j$, $R_j=\alpha_j\beta_j\gamma_j$, we have, by Newton's identities, $P_j=S_1$, $2Q_j=P_j^2-S_2$, $3R_j=S_3-P_j^3+3P_jQ_j$, and it follows that P_j, Q_j, $R_j\in\mathbb{F}_r$. If we put $f_j(x)=x^3-P_jx^2+Q_jx-R_j$, then $f_j(x)\in\mathbb{F}_r[x]$.

By (5.3), we have $\tau(\chi^j)\tau(\chi^{sj})=J(\chi^j,\chi^{sj})\tau(\chi^{(s+1)j})$; thus, because $s^2\equiv -s-1 \pmod p$, we see, by (5.1), that

$$\tau(\chi^j)\tau(\chi^{sj})\tau(\chi^{s^2j})=qJ(\chi^j,\chi^{sj}). \tag{5.8}$$

Now, suppose that $n=(q-1)(p-1)$ and $\mathbb{K}=\mathbb{F}_{r^n}\supset\mathbb{F}_{r^3}$. Because $\mathbb{K}^*$ is a cyclic group with generator μ, we can put $\zeta_p=\mu^{(r^n-1)/p}$, $\zeta_q=\mu^{(r^n-1)/q}$ and repeat the above arguments in $\mathbb{K}$. From (5.4), we find that in $\mathbb{K}$,

$$J(\chi^j,\chi^{sj})^r=J(\chi^{rj},\chi^{rsj}),$$

which means that $J(\chi^j,\chi^{sj})\in\mathbb{F}_r$. Because $r^2+r+1\equiv 0 \pmod p$, we can put $s=r$ and we get

$$J(\chi^j,\chi^{rj})^r=J(\chi^{rj},\chi^{r^2j})=J(\chi^j,\chi^{rj})=J(\chi^{r^2j},\chi^j) \tag{5.9}$$

by Theorem 2.1.5 of [2]. If we put $\iota=\mathrm{ind}_t r$, then $p\nmid\iota$ if and only if $r^{(q-1)/p}\not\equiv 1 \pmod q$. Also, from the definition of $\tau(\chi^j)$, we get $\tau(\chi^j)^r=\sum_{i=0}^{q-1}\chi^{rj}(i)\zeta_p^{ri}=\zeta_p^{-\iota rj}\tau(\chi^{rj})$ and $\tau(\chi^j)^{r^2}=\zeta_p^{-2\iota r^2j}\tau(\chi^{r^2j})$. It follows that if $m=(r^2+r+1)/p$, then

$$\tau(\chi^j)^{pm}=q\zeta_p^{\iota(r+2)j}J(\chi^j,\chi^{rj})$$

by (5.8). By the definition of α_j, β_j, γ_j, with $s=r$, we get

$$\begin{aligned}\alpha_j^m&=q^{1-m}\zeta_p^{\iota(r+2)j}J(\chi^j,\chi^{rj}),\\ \beta_j^m&=q^{1-m}\zeta_p^{\iota r(r+2)j}J(\chi^{rj},\chi^{r^2j}),\\ \gamma_j^m&=q^{1-m}\zeta_p^{\iota r^2(r+2)j}J(\chi^{r^2j},\chi^j).\end{aligned} \tag{5.10}$$

From (5.10) and (5.9), it follows that $\alpha_j^{pm}=\beta_j^{pm}=\gamma_j^{pm}$; furthermore, if $p\nmid\iota$, then $\alpha_j^m\neq\beta_j^m$, $\beta_j^m\neq\gamma_j^m$, $\gamma_j^m\neq\alpha_j^m$. We have proved the following theorem.

Theorem 5.1. *Let p, q, r be primes such that $p \equiv 1 \pmod 3$, $q \equiv 1 \pmod p$, and $p \mid r^2+r+1$ and put $f(x) = f_j(x)$ for any j such that $p \nmid j$. If $r^{(q-1)/p} \not\equiv 1 \pmod q$, then $r \mid D_{pm}$ and $r \mid C_{pm}/C_m$, where $m = (r^2+r+1)/p$.*

6. A Necessary and Sufficient Test for the Primality of N_n

We can now make use of Theorem 5.1 to produce a necessary test for the primality of N_n.

Test 6.1. *This algorithm provides a necessary test for the primality of odd N_n of the form (1.4), where $n \geq 2$ and A is some fixed positive integer such that $p \nmid A$ and $A < 2p^n$.*

(i) For the case of $f = 3$, find two particular solutions G and $\bar{G}$ to $H(x) \equiv 0 \pmod{N_n}$ such that $H^*(G + \bar{G}) \equiv 0 \pmod{N_n}$.
(ii) Find a prime $q \equiv 1 \pmod p$ such that $q \nmid N_n$ and $N_n^{(q-1)/p} \not\equiv 1 \pmod q$.
(iii) Put $G_j = G$ and $G_{-j} = \bar{G}$. Compute P_j, Q_j, R_j as above after evaluating S_1, S_2, S_3 by formulas (5.5), (5.6), and (5.7), respectively.
(iv) For $f(x) = f_j(x)$ and $m = (N_n^2 + N_n + 1)/p$, compute $Y_{p,m}$ and $X_{pm} \pmod{N_n}$.
(v) If N_n is a prime, then we must have $X_{pm} \equiv 3$ and $Y_{p,m} \equiv 0 \pmod{N_n}$.

We now observe that we can combine the results of Theorem 5.1 and Theorem 3.4 to derive the following algorithm for the primality of odd N_n of the form (1.4), where $n \geq 2$ and A is some fixed positive integer such that $p \nmid A$ and $A < 2p^n$. We also assume that conditions (1) and (2) hold on N_n and that we know two particular solutions G and $\bar{G}$ to $H(x) \equiv 0 \pmod{N_n}$ such that $H^*(G + \bar{G}) \equiv 0 \pmod{N_n}$.

Algorithm 6.2. *Suppose N_n satisfies the conditions immediately above.*

(i) Find a prime $q \equiv 1 \pmod p$ such that $q \nmid N_n$ and $N_n^{(q-1)/p} \not\equiv 1 \pmod q$.
(ii) Put $G_j = G$ and $G_{-j} = \bar{G}$. Compute P_j, Q_j, R_j as above after evaluating S_1, S_2, S_3 by formulas (5.5), (5.6), and (5.7), respectively.
(iii) Check that $\gcd(N_n, \Delta_j R_j) = 1$. If not, then N_n is not a prime and we terminate the test.
(iv) For $f(x) = f_j(x)$ and $m = (N_n^2 + N_n + 1)/p$, compute $Y_{p,m}$ and $X_{pm} \pmod{N_n}$.
(v) N_n is a prime if and only if $X_{pm} \equiv 3$ and $Y_{p,m} \equiv 0 \pmod{N_n}$.

We can also combine some steps of Test 3.7, Step (vii)′ in Section 4, and the steps of Algorithm 6.2 to produce the following necessary and sufficient test for the primality of N_n.

Algorithm 6.3. *This algorithm provides a necessary and sufficient test for the primality of odd N_n of the form (1.4), where $n \geq 2$ and A is some fixed positive integer such that $p \nmid A$ and $A < 2p^n$.*

(i) Execute steps (i) to (vi) of Test 3.7.
(ii) If $A < 2p^{2h-n}$, then N_n is a prime; if $A \geq 2p^{2h-n}$, put $G \equiv X_m + d_m \pmod{N_n}$ and $\bar{G} \equiv X_m - d_m \pmod{N_n}$. If $H(G) \not\equiv 0$ or $H(\bar{G}) \not\equiv 0 \pmod{N_n}$, then N_n is not a prime. If $H^*(G + \bar{G}) \not\equiv 0 \pmod{N_n}$, then N_n is not a prime.
(iii) Execute steps (ii)–(iv) of Test 6.1.
(iv) If $X_{pm} \equiv 3$ and $Y_{p,m} \equiv 0 \pmod{N_n}$, then N_n is a prime; if these conditions do not hold, then N_n is not a prime.

We emphasize here that Algorithm 6.3 is not effective in that it does not completely specify how to find efficiently, values for some required parameters; in particular, these parameters are:

(a) A value q_1 for q in Step (ii) of Test 3.7;

(b) Values of a, b, c in Step (iii) of Test 3.7 such that h exists for that test;
(c) A value q_2 for q in Step (ii) of Test 6.1.

Given these parameters, the test will execute in $\tilde{O}((\log N_n)^2)$ bit operations. In practice, the determination of these parameters can usually be done in a few trials for q_1 and a, b, c. Thus, Algorithm 6.3 will likely execute in expected time complexity $\tilde{O}((\log N_n)^2)$. We could eliminate the need to find the parameters in (a) and (b) by using Algorithm 6.2, but for this we need to solve $H(x) \equiv 0 \pmod{N_n}$ for values for G and $\bar{G}$ such that $H^*(G+\bar{G}) \equiv 0 \pmod{N_n}$. Although there exist efficient algorithms for solving polynomial congruences (see Chapter 7 of Bach and Shallit [1]), they too are, in most cases, of probabilistic complexity. Consider the simplest case of $p = 7$; here, we have $H(x) = x^2 + x + 2$. If r is a prime such that the Legendre symbol $(-7/r) = 1$, then $H(x) \equiv 0 \pmod{r}$ has two solutions modulo r, and these can be computed readily from any solution of $x^2 \equiv -7 \pmod{r}$. There is lengthy literature on how to solve

$$x^2 \equiv a \pmod{r} \tag{6.1}$$

when $(a/r) = 1$, but, if no quadratic nonresidue n of r is known, the techniques are nondeterministic because they depend on finding (by trial) some n such that $(n/r) = -1$. For a discussion of some aspects of this problem and several references, see Müller [9]. If the extended Riemann hypothesis (ERH) is true, we must have some positive $n < 2(\log r)^2$, but this only renders the algorithm conditional on the ERH instead of being probabilistic. If $r \equiv -1 \pmod{4}$, then -1 is a quadratic nonresidue of r and $x \equiv a^{(r+1)/4} \pmod{r}$ is a solution of (6.1). Now when $p = 7$, we have $\lambda_n(7) \equiv 2$ or 4 and the Jacobi symbol $(-7/N_n) = (N_n/7) = 1$. Hence, in the case that $N_n \equiv -1 \pmod{4}$, there exists an efficient, deterministic algorithm that will find some x such that $H(x) \equiv 0 \pmod{N_n}$ or determine that N_n cannot be a prime.

In the case of $p = 13$, let j be any integer such that $13 \nmid j$; then G_j, G_{2j}, G_{-j}, and G_{-2j} are the four solutions of $H(x) \equiv 0 \pmod{r}$ and $G_1^* = G_j + G_{-j}$, $G_2^* = G_{2j} + G_{-2j}$ are the two solutions of $H^*(x) \equiv 0 \pmod{r}$. Because $H^*(x) = x^2 + x - 3$, we can find G_1^* and G_2^* by solving (6.1) with $a = 13$. Now, it is easy to show that for any p, we have

$$G_j G_{-j} = 3 + G_{(s-1)j} + G_{-(s-1)j}.$$

In our case, we have $s = 3$ or $s = 9$. With no loss of generality, suppose $s = 3$; we get $G_j G_{-j} = 3 + G_{2j} + G_{-2j}$ and $G_j G_{-j} = 3 + G_2^* = 2 - G_1^*$. Thus, G_j and G_{-j} are the two solutions of

$$x^2 - G_1^* x + 2 - G_1^* \equiv 0 \pmod{r}.$$

It follows that we can compute G_j and G_{-j} by solving (6.1) for $a = (G_1^*)^2 + 4G_1^* - 8$. This must be solvable because G_j, $G_{-j} \in \mathbb{F}_r$. For any p, similar techniques can be used to find G_j and $G_{-j} \pmod{r}$ from the solutions of $H^*(x) \equiv 0 \pmod{r}$.

We have seen, then, that there are certain values of N_n such that we can find values for G and $\bar{G}$ by a deterministic process, but, in general, we have to be content with a probabilistic procedure.

We also mention that, under the ERH, there exists an efficient, deterministic algorithm to solve (c), but given that the probability of any given value of $a \pmod{q}$ being a pth power residue of q is $1/p$, we would expect to find a suitable value of q_2 in only a few trials for q. This is certainly what happens in practice.

7. Computational Results

For a given integer r, we will say that a triple (a, b, c) is admissible if $0 \leq a, b, c < r$ and $(b, c) \neq (0, 0)$. The following tables (Tables 1–6) give the values of n for which N_n in (1.4) is a prime, when $1 \leq A \leq 60$ and $1 < n \leq 500$. These tables were computed by using Test 3.7 and the admissible triple $(a, b, c) = (0, 1, 0)$. In only a few instances was the test inconclusive because of Circumstances 1 or 2. These are indicated in the tables with the corresponding n value in round brackets (n) for Circumstance 1 or square brackets $[n]$ for Circumstance 2. In the latter case, the test was rerun with a different admissible triple with respect to N_n and was successful.

A	n	A	n	A	n
1	2, 62, 66	21		41	2, 3, 20, 113
2	118	22	17, 155, 263	42	
3	277, 361	23	45, 277, 360	43	2, 3, 11, 29
4	4, 5, 48, 134, 209, 460	24	6, 18, 276	44	6, 9, 13, 112, 160
5	3, 62	25	15, 40, 41, 42	45	65, 88, 107, 216, 226
6	7, 14, 18, 161	26	6	46	4, 17, 210
7		27	26, 166	47	2
8	51, 61	28		48	6, 9
9	10, 65, 216, 436	29	[2], 3, 34, 39, 133	49	
10	125, 160, 244	30	6, 9, 14, 18, 19, 47, 208, 285	50	4, 7, 194
11	2, 35, 143	31	2, 3, 12, 56, 182	51	113
12	7, 25, 322	32	369	52	5, 114, 162
13	3, 74, 262, 485	33	16, 26	53	3, 72
14		34	5, 17, 185, 459	54	24, 245
15	58	35		55	
16	4, 8, 86	36	7, 8, 61	56	
17	2, 11, 29, 34, 45, 52, 117	37	29, 33, 148	57	50
18	9, 201	38	5	58	4
19	(2), 3, 52, 455	39	188	59	38, 42, 77, 188, 324, 360
20		40		60	6, 31

Table 1. $p = 7$, $(a, b, c) = (0, 1, 0)$ and $\lambda_1(p) = 2$

A	n	A	n	A	n
1	2, (3), 16, 60, 130, 197	21		41	2, [3], 46, 71, 308
2	4, 203, 207, 231, 382	22	21	42	
3	56, 324	23	3, 22, 133, 392,431	43	[3], 79
4	4, 6, 7, 24, 141, 149, 176	24	7, 44, 55	44	73
5	2, 3, 29, 36, 80	25		45	
6	8, 47, 73, 271	26	4, 31, 211, 427	46	4, 7, 68, 121, 175, 270
7		27	10, 27, 36, 166, 323	47	3, 46, 72, 83
8	5, 8, 482	28		48	47
9	59, 288	29	[2], 58, 79, 170, 233	49	
10	4, 5, 6, 183	30	7, 24, 89, 140, 156, 393	50	17, 183
11	2, 15, 54, 196	31	3, 52, 260	51	36, 64
12	122, 129, 374	32	5, 86, 164, 198	52	4, 21, 47, 213, 251
13	16, 32, 35, 226	33	10, 58, 148, 182, 237	53	15, 22
14		34	6, 23, 219, 283	54	297
15	27, 168	35		55	2, 35, 405
16	28, 51, 206	36	9, 24, 86, 122	56	
17	3, 74, 77	37	2, 43	57	10, 27, 46, 181
18	18, 131, 202, 445	38	28, 44, 116, 201	58	5, 6, 13, 132, 160, 404, 440
19	33, 101, 117	39	35, 97	59	2, 78, 454, 481
20	17, 103, 210, 354, 381	40	326	60	6, 7, 235

TABLE 2. $p = 7$, $(a, b, c) = (0, 1, 0)$ and $\bar{\lambda}_1(p) = 4$

A	n	A	n	A	n
1	9, 13, 94	21	3, 8	41	[3], 16, 21, 115, 231
2	76	22	63	42	305
3	2, 18, 79, 411	23	3, 10	43	8, 9
4	393	24	36, 200	44	33
5	2, 9, 14	25		45	21, 410
6	82, 129	26		46	
7	5, 16	27	19	47	2, 6, 16, 52, 237
8	4, 26, 43, 47	28	11, 155	48	4, 77
9	[2], 6, 19, 179	29	16, 401	49	17, 110
10	58	30	54, 111	50	4, 43, 78, 102, 108
11	5, 7, 61, 186, 479	31	467	51	
12	45, 59, 80	32		52	
13		33	75	53	2
14	149	34	23, 126	54	4, 82, 314
15	6, 12, 79	35	39, 114	55	312
16	25, 26, 380	36	4, 23	56	11
17	[2], 14	37	5, 7, 206	57	6, 12, 74, 92
18	294	38	11	58	44, 71, 165
19	5, 64, 243	39		59	3
20	93, 104	40	222	60	23, 30, 34

TABLE 3. $p = 13$, $(a, b, c) = (0, 1, 0)$ and $\lambda_1(p) = 3$

A	n	A	n	A	n
1	2, 51	21	2, 8, 18, 60, 135, 424	41	7
2	38, 197, 339	22	4, 96, 177	42	
3	(2), 8	23		43	3
4		24	129	44	147
5	5	25	5, 6, 9, 10 135, 162	45	[3], 10, 13, 18
6	30, 36, 344	26		46	
7	12, 16, 19, 21, 65, 141, 235, 290	27		47	5, 7, 421, 457
8	30, 34, 38, 210	28	53	48	77, 105
9	2, 3, 6, 13, 401	29	295	49	9
10		30		50	147, 197
11	324	31	2, 3, 6, 338	51	2, 3, 37, 453
12		32	11, 128	52	
13		33	24, 37, 196	53	9, 13, 163, 221, 242, 468
14		34	55	54	4, 25, 93, 256
15	2, 48, 50, 79	35	139	55	10, 21
16	4	36	105	56	56, 356
17		37	52	57	46, 373
18	129, 400	38	101	58	120, 258
19	19	39		59	8
20	78, 183	40	38, 327, 353	60	40, 54, 134

TABLE 4. $p = 13$, $(a, b, c) = (0, 1, 0)$ and $\bar{\lambda}_1(p) = 9$

A	n	A	n	A	n
1	2, 7, 309	21	2, 56, 163, 256	41	18
2	21	22	23, 381	42	3, 72, 275, 328, 375
3	16	23	88, 125	43	5, 16, 134
4		24	20, 308	44	20, 26
5	435	25	7, 17, 66, 204	45	
6	3, 476	26	479	46	428
7	2, 167	27	2	47	37
8	21	28		48	20, 116, 341
9	2, 8, 10, 250	29	22, 74	49	2, 471
10	52, 246, 460	30	3, 107, 150	50	3
11		31	2, 89	51	8, 17, 386
12	20	32		52	14, 40, 63
13	5	33	121	53	55, 401
14	21	34		54	63, 136, 269
15	18	35	7, 10, 102, 114	55	[2], 38, 226, 469
16		36	93	56	190
17		37	[2], 32, 66, 118	57	
18	4	38		58	14
19		39	16, 82, 113	59	5, 6
20	3, 24, 190	40		60	63, 73

TABLE 5. $p = 19$, $(a, b, c) = (0, 1, 0)$ and $\lambda_1(p) = 7$

A	n	A	n	A	n
1	155, 362	21	2, 38, 43, 162	41	2, 6, 141
2		22	3, 336	42	
3	2	23	17, 283	43	6, 95, 145
4	24, 109	24	41, 101	44	110
5	2, 33, 50	25		45	57, 60
6	209	26		46	186
7	161	27		47	
8	67, 231	28	4, 11, 419	48	3, 19, 394
9		29		49	5, 32
10	4	30	3, 154	50	109
11	8	31	32	51	
12	41, 317	32	44	52	13
13	111	33	2	53	176
14	12, 45, 73	34	487	54	
15	2, 339, 489	35	2	55	7
16	3, 25	36	3, 63	56	9, 11
17		37	254	57	
18	44	38		58	3, 13, 42
19		39	16, 56	59	123
20	116, 361	40	4	60	52, 58

TABLE 6. $p = 19$, $(a, b, c) = (0, 1, 0)$ and $\bar{\lambda}_1(p) = 11$

In the few cases where Test 3.7 was unsuccessful because of Circumstance 1, the corresponding forms of N_n are: $19 \cdot 7^2 + 30$ $(q = 61)$, $7^3 + 18$ $(q = 61)$, $3 \cdot 13^2 + 22$ $(q = 73)$. These numbers are respectively: $961 (= 31^2)$, $361 (= 19^2)$, and $529 (= 23^2)$. That these numbers are all squares of a prime is no coincidence as we will now show. We begin with the following result.

Theorem 7.1. *If $r \nmid 6\Delta R$, r is an I-prime with respect to (D_n), and $r \mid D_m$, then $r^2 \mid D_m$.*

Proof. This is Theorem 5.7 of [8] or Theorem 4.9 of [11]. □

Theorem 7.2. *Let N_n be defined by (1.4). If $N_n = r^2$, where r is a prime such that $r \nmid 6\Delta R$, $r^{(q-1)/3} \not\equiv 1 \pmod{q}$, and $p \nmid r^2 + r + 1$, then $N_n \mid D_w$, where $w = (N_n^2 + N_n + 1)/p^n$.*

Proof. We first note the simple identity:

$$x^4 + x^2 + 1 = (x^2 + x + 1)(x^2 - x + 1).$$

It follows that

$$N_n^2 + N_n + 1 = (r^2 + r + 1)(r^2 - r + 1).$$

Because $p \mid N_n^2 + N_n + 1$ and $p \nmid r^2 + r + 1$, we must have $p \mid r^2 - r + 1$; hence, $r^2 + r + 1 \mid w$. Because $r^{(q-1)/3} \not\equiv 1 \pmod{q}$, r must be an I-prime with respect to (D_n), which means that $r \mid D_m$, where $m = r^2 + r + 1$. By Theorem 7.1, we find that $r^2 \mid D_m$, but because $m \mid w$, we must have $N_n \mid D_w$. □

Notice then that for all N_n given in the statement of Theorem 7.2, we must have $X_w \equiv 3$, $Y_{w,1} \equiv 0 \pmod{N_n}$, which is Circumstance 1. Thus, for such values of N_n, Circumstance 1 will always occur for any admissible triple (a, b, c) because the corresponding $f(x)$ is irreducible modulo r. It is easy to verify that each of the above three examples satisfies the conditions of Theorem 7.2.

8. Conclusion

We have shown that we can use the properties of the extended Lucas sequences discussed in [8] to produce a sufficiency test for the primality of numbers of the form (1.4) and that this test can also be extended to be necessary and sufficient. Certain of these results are analogous to some findings produced by Lucas for numbers of the form $Ap^n \pm 1$. Perhaps these were the kind of results that Lucas was hoping to produce by generalizing his sequences. The results exhibited here are the kind that Lucas might have found in that they come about from a study of particular divisibility sequences. A much more general approach, which does not rely on the properties of certain sequences, to the primality of the numbers addressed here and many others, can be found in Berrizbeitia, et al. [3].

References

[1] E. Bach and J. Shallit, *Algorithmic Number Theory*, MIT Proess, Cambridge MA, 1996.

[2] B. C. Berndt, R. J. Evans, and K. S. Williams, *Gauss and Jacobi Sums*, John Wiley and Sons, New York, 1998.

[3] P. Berrizbeitia, T. G. Berry, and J. T. Ayuso, *A generalization of Proth's Theorem*, Acta Arith., **110** (2003), 107–115.

[4] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Vol. 6, Oxford University Press, 2008.

[5] D. H. Lehmer and E. Lehmer, *Cyclotomy with short periods*, Math. Comp., **41** (1983), 743–758.

[6] E. Lehmer, *Criteria for cubic and quartic residuacity*, Mathematika, **5** (1958), 20–29.

[7] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and their Applications*, Cambridge University Press, 1994.

[8] S. Müller, H. G. Williams, and E. Roettger, *A cubic extension of the Lucas functions*, Ann. Sci. Math. Québec, **33.2** (2009), 185–224.
[9] S. Müller, *On the computation of square roots in finite fields*, Designs, Codes and Cryptography, **31** (2004), 301–312.
[10] C. Pomerance, *Primality testing: Variations on a theme of Lucas*, Congr. Numer., **201** (2010), 301–312.
[11] E. Roettger, *A Cubic Extension of the Lucas Functions*, PhD thesis, University of Calgary, 2009. available at `http://people.ucalgary.ca/~williams/`.
[12] E. L. Roettger and H. C. Williams, *Public-key cryptography based on a cubic extension of the Lucas functions*, Fundamenta Informaticae, **114** (2012), 325–344.
[13] E. L. Roettger, H. C. Williams, and R. K. Guy, *Some primality tests that eluded Lucas*, Designs, Codes and Cryptography, **77** (2015), 515–539.
[14] H. C. Williams, *Édouard Lucas and Primality Testing*, Wiley-Interscience, 1998.

MSC2020: 11Y11, 11B37, 11B50

Department of General Education, Mount Royal University, Calgary, Alberta, T3E 6K6, Canada
Email address: `eroettger@mtroyal.ca`

Department of Mathematics and Statistics, University of Calgary, Calgary, Alberta, T2N 1N4, Canada
Email address: `hwilliam@ucalgary.ca`