Journal of Integer Sequences, Vol. 23 (2020),
Article 20.4.8

A Sextic Extension of the Lucas Functions

E. L. Roettger
Department of General Education
Mount Royal University
4825 Mount Royal Gate SW
Calgary, AB T3E 6K6
Canada
eroettger@mtroyal.ca

H. C. Williams
Department of Mathematics and Statistics
University of Calgary
2500 University Drive NW
Calgary, AB T2N 1N4
Canada
williams@math.ucalgary.ca

Abstract

We develop a necessary and sufficient primality test for integers N such that N^6-1 is divisible by a large power of 7, based on the properties of two linear recurrence sequences of order 6. These two sequences are analogous to the well-known Lucas sequences. In addition, we provide tables from which it is easy to compute the characteristic polynomial of the sequences.

1 Introduction

Consider the sequence (G_n), where $G_0 = 0$, $G_1 = 1$ and $G_{n+1} = G_n - 7G_{n-1}$ for all $n \geq 1$. In Table 1 below we tabulate the first few terms of (G_n), together with their prime factorizations.

n	G_n	n	G_n
0	0	13	-93911
1	1	14	$146329 = 41 \cdot 43 \cdot 83$
2	1	15	$803706 = 2 \cdot 3 \cdot 29 \cdot 31 \cdot 149$
3	$-6 = -2 \cdot 3$	16	$-220597 = -13 \cdot 71 \cdot 239$
4	-13	17	-5846539
5	29	18	$-4302360 = -2^3 \cdot 3^2 \cdot 5 \cdot 19 \cdot 629$
6	$120 = 2^3 \cdot 3 \cdot 5$	19	$36623413 = 113 \cdot 324101$
7	-83	20	$66739933 = 13 \cdot 29 \cdot 211 \cdot 839$
8	$-923 = -13 \cdot 71$	21	$-189623958 = -2 \cdot 3 \cdot 83 \cdot 503 \cdot 757$
9	$-342 = -2 \cdot 3^2 \cdot 19$	22	$-656803489 = -8513 \cdot 77153$
10	$6119 = 29 \cdot 211$	23	$670564217 = 139 \cdot 4824203$
11	8513	24	$5268188640 = 2^5 \cdot 3 \cdot 5 \cdot 11 \cdot 13 \cdot 23 \cdot 47 \cdot 71$
12	$-34320 = -2^4 \cdot 3 \cdot 5 \cdot 11 \cdot 13$	25	$574239121 = 29 \cdot 449 \cdot 44101$

Table 1: First few values of the sequence (G_n) and their factorizations.

Notice that the terms with subscript divisible by 3 tend to have a lot of small prime factors belonging to no particular residue classes, but the other terms seem only to be divisible by primes that are congruent to ± 1 modulo 14. In fact, it can be shown that this is always the case for (G_n). This explains why terms with index a multiple of 3 will tend to be highly composite; for all the primes $\not\equiv \pm 1 \pmod{14}$, two thirds of them must wait until 3 divides n in order to divide some G_n.

If we let q be a prime such that $q \equiv 1 \pmod 3$, it is well known that there exist integers x and y such that $4q = x^2 + 27y^2$. See, for example, Ireland and Rosen [7, §6 of Chapter 9] or Cox [5, Chapter 4]. Put $Q = q$ and $P = x$ and define the Lucas sequence (U_n) by $U_0 = 0$, $U_1 = 1$ and $U_{n+1} = PU_n - QU_{n-1}$ for $n \geq 0$. By a special case ($p = 3$) of Williams [20, Corollary 11.2.4] we have the following result:

Theorem 1. *Let q be a prime such that $q \equiv 1 \pmod 3$. Put $P = x$ and $Q = q$, where $4q = x^2 + 27y^2$. If r is a prime such that $r \nmid 3qy$, $r \mid U_n$ and $3 \nmid n$, then r must be a cubic residue of q.*

We see, then, that for $q = 7$ ($x = 1$ and $y = 1$), it follows that $(U_n) = (G_n)$ and every prime divisor r of G_n when $3 \nmid n$ must be a cubic residue of 7. Since the only cubic residues of 7 are ± 1, we must have $r \equiv \pm 1 \pmod{14}$.

The Lucas sequences are examples of linear recurrence sequences of order 2; the purpose of this paper is to find extensions of Lucas' sequences of order greater than 2, which possess properties analogous to those that we have observed in (G_n). We then use these sequences to develop primality tests for certain numbers of special form.

2 The Lucas sequences and their extensions

Let P and Q be coprime integers and α, β be the roots of the quadratic polynomial $f(x) = x^2 - Px + Q$ with $\delta = \alpha - \beta$ and $D = \delta^2 = P^2 - 4Q$. We define the Lucas sequences (U_n) and (V_n) as follows:

$$U_n = (\alpha^n - \beta^n)/\delta, \qquad\qquad V_n = \alpha^n + \beta^n.$$

Since both U_n and V_n are symmetric functions of the roots of a polynomial with integer coefficients they must both be integers for all non-negative integral values of n. Also, both (U_n) and (V_n) satisfy the following second-order linear recurrence:

$$X_{n+1} = PX_n - QX_{n-1},$$

with $U_0 = 0$, $U_1 = 1$ and $V_0 = 2$, $V_1 = P$. The Lucas sequences have many interesting properties that have been applied to many problems; some books that include one or several sections devoted to these sequence, particularly as they apply to primality testing, are Bressoud and Wagon [3], Crandall and Pomerance [6], Ribenboim [11] and Williams [20].

Lucas first applied these sequences to the problem of primality testing of Mersenne numbers; see [20, §5.1 and 5.4]. Indeed, he was actually able to prove the well-known Lucas-Lehmer criterion for the primality of $M_n = 2^n - 1$. This test is both a necessary and sufficient condition for M_n to be a prime number. Lucas also considered, for a fixed value of A, the more general $N_n = A2^n - 1$, and provided a sufficiency test for N_n to be a prime. For some commentary on this work, see Roettger, Williams and Guy [15]. It was Lehmer [8] who essentially proved the following result:

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

This result can be modified slightly, as follows.

Theorem 3. *Let $N_n = A2^n - 1$, where $n > 1$, A is odd and $A < 2^n$. Let q be a prime such that $q \equiv 1 \pmod 4$ and the Legendre symbol $(N_n/q) = -1$. If x and y are integers such that $q = x^2 + y^2$, put $P = 2x$, $Q = q$; then N_n is a prime if and only if $N_n \mid V_{(N_n+1)/2}$.*

In the case that $N_n = A3^n - 1$, results in Williams [19] can be used to prove the following analogue of Theorem 3.

Theorem 4. *Let $N_n = A3^n - 1$, where $n > 1$, $3 \nmid A$ and $A < 3^n$. Suppose q is a prime congruent to 1 modulo 3 such that $N_n^{(q-1)/3} \not\equiv 1 \pmod q$ and $4q = x^2 + 27y^2$. Put $P = x$ and $Q = q$. If $\gcd(N_n, qy) = 1$, then N_n is a prime if and only if $V_{2\theta} \equiv -Q^\theta \pmod{N_n}$, where $\theta = (N_n + 1)/3$.*

We say that a sequence of integers (X_n) is a *divisibility sequence* if whenever $X_n \neq 0$, we have $X_n \mid X_{mn}$ for all non-negative integers n and m. For example, (n) is trivially a divisibility sequence, but so are (G_n) and the Mersenne sequence (M_n). Lucas made much use of the fact that (U_n) is always a divisibility sequence.

Let the sequence (X_n) be determined by an initial set of h integer values

$$X_0, X_1, X_2, \ldots, X_{h-1} \tag{1}$$

and the h^{th} order linear recurrence

$$X_{n+h} = P_1 X_{n+h-1} - P_2 X_{n+h-2} + \cdots + (-1)^{h-1} P_h X_n, \tag{2}$$

where P_1, P_2,..., P_h are given fixed integers. Notice that the values for X_n for all $n \geq 0$ are completely determined by (1) and (2). We define the *characteristic polynomial* $f(x)$ of the *linear recurrence sequence* (X_n) to be

$$f(x) = x^h - P_1 x^{h-1} + P_2 x^{h-2} - \cdots + (-1)^h P_h. \tag{3}$$

Lucas speculated that his sequences might be extended to those that satisfy a linear recurrence sequence of order greater than 2. Indeed, it is argued in Roettger, Williams and Guy [14] that the Lucas sequences are characterized by five basic properties:

(1) There are two sequences of integers (when $n \geq 0$).

(2) Both sequences satisfy the same linear recurrence relation.

(3) One of the two sequences is a divisibility sequence.

(4) There are addition formulas for the terms of the sequences.

(5) There are multiplication formulas for the terms of the sequences.

Given what we know about Lucas' unsuccessful attempt to generalize his sequences, it seems that every sequence that he might have found acceptable as a proper generalization of (U_n) and (V_n) should possess these five properties.

In [14] the authors proposed generalizing Lucas' sequence to

$$U_n = \lambda^{n-1} \prod_{i=1}^{k} (1 - \gamma_i^n)/(1 - \gamma_i) \qquad \text{and} \qquad V_n = \lambda^n \prod_{i=1}^{k} (1 + \gamma_i^n), \tag{4}$$

where λ and $\gamma_1, \gamma_2, \ldots, \gamma_k$ are simply constrained to be distinct non- zero algebraic numbers such that $V_1 \neq 0$ and both (U_n), (V_n) are sequences of integers for $n \geq 0$. Notice that, just as in the case of the Lucas sequences, we have $V_n = U_{2n}/U_n$.

Under the above constraints it is easy to prove that if $k = 1$, $P = \lambda(\gamma_1 + 1)$, $Q = \lambda^2 \gamma_1$, then both P and Q must be integers because $V_1 = \lambda(\gamma_1 + 1)$, $V_2 = \lambda^2(1 + \gamma_1^2)$, $U_3 = \lambda^2(1 + \gamma_1 + \gamma_1^2)$

are all integers. In this case, we see that in (4) $U_n = U_n(P,Q)$, $V_n = V_n(P,Q)$, where $\alpha = \lambda$ and $\beta = \lambda\gamma_1$. Thus, (4) represents a generalization of the Lucas functions.

For a fixed value of k, conditions on λ and $\gamma_1, \gamma_2, \ldots, \gamma_k$ were derived in [14] to ensure that both (U_n) and (V_n) are sequences of integers that satisfy the same linear recurrence. For example, one of these conditions is that $Q = \lambda^2\gamma_1\gamma_2\cdots\gamma_k$ be a rational integer. It is also shown that under these same conditions (U_n) is a divisibility sequence. In the case that $k = 2$, we must have T_1, T_2 and Q integers, where

$$T_1 = \lambda(1+\gamma_1)(1+\gamma_2), \qquad T_2 = \lambda^2(\gamma_1+\gamma_2)(1+\gamma_1\gamma_2) + 2\lambda^2\gamma_1\gamma_2, \qquad Q = \lambda^2\gamma_1\gamma_2.$$

Thus, if we put $P_1 = T_1$ and $P_2 + 2Q = T_2$, we must have P_1, P_2 and Q integers. In this case we find that both (U_n) and (V_n) satisfy the same fourth-order linear recurrence:

$$X_{n+4} = P_1X_{n+3} - (P_2+2Q)X_{n+2} + P_1QX_{n+1} - Q^2X_n, \tag{5}$$

with initial conditions $U_0 = 0$, $U_1 = 1$, $U_2 = P_1$, $U_3 = P_1^2 - P_2 - 3Q$, $V_0 = 4$, $V_1 = P_1$, $V_2 = P_1^2 - 2P_2 - 4Q$, $V_3 = P_1(P_1^2 - 3P_2 - 3Q)$. Indeed, it has been shown by Abrate et al. [1] that if (X_n) is a linear recurrence sequence of order four that is nondegenerate (no quotient of any two of the roots of the characteristic polynomial is a root of unity) and a divisibility sequence, then (X_n) must satisfy a linear recurrence of the form (5) for some integers P_1, P_2 and Q.

The above sequences, denoted here by (U_n) and (V_n), were discussed in some detail by Williams and Guy in [21] and in greater detail in [15]. Suffice it to say here that they possess the five properties of the Lucas sequences mentioned above; furthermore, they also enjoy many of the arithmetic properties of the Lucas sequences. Thus, these are evidently the fourth-order analogs of the Lucas sequences.

As in [15, §7], let q be a prime such that $q \equiv 1 \pmod 5$ and define in (5)

$$P_1 = P(1,5,q), \qquad P_2 = P(2,5,q), \qquad Q = q^3, \tag{6}$$

where the rational integers $P(i,5,q)$ are defined in [20, (11.1.5)]. As indicated by the notation, the values of P_1, P_2 and Q here depend only on the value of q. Notice that when $k = 2$ in [20, §10.1], the functions denoted by symbols C_n and $V_{1,n}$ there are the same except possibly for sign; also $U_n = V_{1,n} = \pm C_n$. If we let D here denote the discriminant of the characteristic polynomial of (U_n), we have the following consequence of [20, Corollary 11.2.5]:

Theorem 5. *Suppose P_1, P_2 and Q are given by (6). If r is a prime such that $r \nmid 5qD$, $r \mid U_n$ and $5 \nmid n$, then r must be a quintic residue of q.*

This result is for the extended Lucas sequence (U_n) above exactly analogous to the case of the Lucas sequence of Theorem 1. In the case of $q = 11$, we have $P_1 = P(1,5,q) = -89$, $P_2 = P(2,5,q) = 1199$. The prime factorizations of the values of the corresponding U_n for $n = 0, 1, \ldots, 30$ are provided in [20, Table 11.2.1]. The behaviour of these factorizations

is similar to the corresponding case of (G_n), but more extreme because only two of the 10 nonzero residues of 11 are quintic resides of 11.

Let $\eta = \pm 1$. If a is an odd integer, define $m(a)$ by $m(a) = (a-\eta)/5$ when $a \equiv \eta \pmod 5$; otherwise put $m(a) = (a^2+1)/5$. Also, as in [15], let $\gamma_n(5)$ denote the odd solution x of $x^2 + 1 \equiv 0 \pmod{5^n}$ such that $0 < x < 5^n$. Set

$$N_n = A5^n + \eta \qquad \text{or} \qquad N_n = A5^n + \eta\gamma_n(5). \tag{7}$$

By using the methods of [15, §7] it is possible to prove the following analogue of Theorem 4.

Theorem 6. *Let N_n be given by (7), where A is even, $\gamma_n(5) \nmid A$, and $A < 2 \cdot 5^n$. Suppose that q is a prime congruent to 1 modulo 5 such that $N_n^{(q-1)/5} \not\equiv 1 \pmod q$ and let P_1, P_2, and Q be given by (6), $\Delta = P_1^2 - 4P_2$, and $m = m(N_n)$. If $\gcd(N_n, qD) = 1$, then N_n is a prime if and only if*

$$V_m \equiv -Q^{m/2} \pmod{N_n} \qquad \textit{and} \qquad \Delta U_m^2 \equiv 5Q^m \pmod{N_n}.$$

3 Some sixth-order divisibility sequences

We say that a linear recurring sequence of order k that is also a divisibility sequence is a *linear divisibility sequence* (LDS) of order k. We have already discussed some properties of certain LDSs of order 2 and 4. In this section we discuss some sixth-order LDSs that can be derived from (4). Much more concerning this can be found in [14].

When $k = 3$, the situation in (4) is somewhat more complicated than in the cases of $k = 1$, 2 because the corresponding (U_n) and (V_n) sequences satisfy a linear recurrence of order 8, given in [14, Theorem 5.3]. A difficulty arises when we try to develop the addition and multiplication formulas because it becomes necessary to introduce a third sequence in order to do this; thus, the sequences when $k = 3$ cannot in general satisfy the five conditions given earlier. This, of course is also likely the case for $k > 3$. Nevertheless, there is a special case when $k = 3$ that does allow us to require only two sequences; this is the case when $\gamma_1\gamma_2\gamma_3 = 1$. Here we must have λ an integer, denoted by R, and the resulting sequences (U_n) and $(V_n - 2R^n)$ satisfy the same linear recurrence of order 6:

$$X_{n+6} = S_1X_{n+5} - (S_2 + 3R^2)X_{n+4} + (S_3 + 2R^2S_1)X_{n+3} - R^2(S_2 + 3R^2)X_{n+2} + R^4S_1X_{n+1} - R^6X_n, \tag{8}$$

where S_1, S_2, and S_3 are integers such that

$$S_3 = RS_1^2 - 2RS_2 - 4R^3. \tag{9}$$

Let $G(x)$ be the characteristic polynomial of (8). In this case it turns out that ρ_1, ρ_2, ρ_3, where $\rho_i = R(\gamma_i + \gamma_i^{-1})$ $(i = 1, 2, 3)$, are the roots of the cubic polynomial

$$g(x) = x^3 - S_1x^2 + S_2x - S_3.$$

If we put $W_n = V_n - 2R^n$, it is shown in [14] that (U_n) is a divisibility sequence and the two sequences (U_n), (W_n) also possess the five properties mentioned in the previous section and we call them the extended Lucas sequences for $k = 3$.

We find that

$$\begin{gathered} U_0 = 0, U_1 = 1, U_2 = S_1 + 2R, U_3 = S_1^2 + RS_1 - S_2 - 3R^2; \\ W_0 = 6, W_1 = S_1, W_2 = S_1^2 - 2S_2 - 6R^2; \\ W_3 = S_1^3 - 3S_1S_2 + 3RS_1^2 - 6RS_2 - 3R^2S_1 - 12R^3. \end{gathered} \tag{10}$$

Furthermore, for every integer n we have

$$U_{-n} = -U_n/R^{2n} \qquad \text{and} \qquad W_{-n} = W_n/R^{2n}. \tag{11}$$

Suppose we are given integral values for S_1 ($\neq -2R$), S_2, and determine S_3 by (9). We know by [14, Theorem 7.2] that if (U_n), (W_n) satisfy the linear recurrence (8) with initial conditions given by (10) and subject to (11) for $n = 1$ and 2, then there must exist algebraic numbers γ_1, γ_2, γ_3 with $\gamma_1\gamma_2\gamma_3 = 1$ such that U_n and $V_n = W_n + 2R^n$ are given by (4).

Some examples of the sixth-order LDS (U_n) can be found in the *On-line Encyclopedia of Integer Sequences* (OEIS) [16]; in particular, we mention A180510 with $S_1 = -1$, $S_2 = -5$, $S_3 = 7$, $R = 1$, and A005120 with $S_1 = -3$, $S_2 = 2$, $S_3 = 1$, $R = 1$. Others are A001351, A001945 and A006235.

Many arithmetic properties of the extended Lucas sequences (U_n), (W_n) when $\gcd(S_1, S_2, R) = 1$ are provided in [14, 13]. These are very similar to corresponding results involving the standard Lucas sequences. If we put

$$\Delta = R^2(1-\gamma_1)^2(1-\gamma_2)^2(1-\gamma_3)^2,$$

we find that Δ is the discriminant of $g(x)$ and we can write

$$\Delta = S_1^2 - 4S_2 + 4RS_1 - 12R^2.$$

Also, if

$$\Gamma = R^4(\gamma_1-\gamma_2)^2(\gamma_2-\gamma_3)^2(\gamma_3-\gamma_1)^2, \tag{12}$$

we have

$$\Gamma = S_2^2 + 10RS_1S_2 - 4RS_1^3 - 11R^2S_1^2 + 12R^3S_1 + 24R^2S_2 + 36R^4.$$

Now assume that λ_i $(i = 1, 2, \ldots, 6)$ are distinct algebraic integers such that

$$\lambda_1\lambda_2 = \lambda_3\lambda_4 = \lambda_5\lambda_6 = R^2, \tag{13}$$

where R is a rational integer. Assume, in addition, that

$$\begin{aligned} &\lambda_1\lambda_3 = R\lambda_6, \quad &&\lambda_1\lambda_5 = R\lambda_4, \quad &&\lambda_2\lambda_4 = R\lambda_5, \\ &\lambda_2\lambda_6 = R\lambda_3, \quad &&\lambda_3\lambda_5 = R\lambda_2, \quad &&\lambda_4\lambda_6 = R\lambda_1. \end{aligned} \tag{14}$$

Proposition 7. *Suppose that λ_i $(i = 1, 2, \ldots, 6)$ satisfy the conditions (13) and (14). If we put $\rho_1 = \lambda_1 + \lambda_2$, $\rho_2 = \lambda_3 + \lambda_4$, $\rho_3 = \lambda_5 + \lambda_6$, then ρ_1, ρ_2, ρ_3 are the roots of a cubic $g(x) = x^3 - S_1x^2 + S_2x - S_3$ with integral coefficients satisfying (9) if and only if $\mu = \lambda_1 + \lambda_3 + \lambda_5$, $\nu = \lambda_2 + \lambda_4 + \lambda_6$ are the roots of a quadratic polynomial $x^2 - T_1x + T_2$ with integral coefficients.*

Proof. Follows easily from the following identities:

$$\rho_1 + \rho_2 + \rho_3 = \mu + \nu, \qquad \rho_1\rho_2 + \rho_2\rho_3 + \rho_3\rho_1 = R(\mu + \nu) + \mu\nu - 3R^2$$
$$\text{and} \qquad \rho_1\rho_2\rho_3 = R(\mu + \nu)^2 - 2R^2(\mu + \nu) - 2R\mu\nu + 2R^3.$$

The latter two of these can be easily verified by appealing to (13) and (14). □

We note that under the above conditions each λ_i $(i = 1, 2, \ldots, 6)$ is a root of

$$G(x) = x^6 - S_1x^5 + (S_2 + 3R^2)x^4 - (S_3 + 2R^2S_1)x^3 + R^2(S_2 + 3R^2)x^2 - R^4S_1x + R^6 = 0.$$

We next put $\mu_n = \lambda_1^n + \lambda_3^n + \lambda_5^n$, $\nu_n = \lambda_2^n + \lambda_4^n + \lambda_6^n$; since by (13) and (14) we find that $\lambda_1\lambda_3\lambda_5 = \lambda_2\lambda_4\lambda_6 = R^3$,

$$\begin{aligned}(\lambda_1^n - R^n)(\lambda_3^n - R^n)(\lambda_5^n - R^n) &= R^{2n}(\mu_n - \nu_n),\\ (\lambda_2^n - R^n)(\lambda_4^n - R^n)(\lambda_6^n - R^n) &= -R^{2n}(\mu_n - \nu_n).\end{aligned} \tag{15}$$

Note that if we put $\delta = \mu_1 - \nu_1$, then because the λ_i $(i = 1, 2, \ldots, 6)$ are all distinct, we conclude from (15) and (13) that $\delta \neq 0$. In fact, $\Delta = \delta^2$ is the discriminant of $g(x) = x^3 - S_1x^2 + S_2x - S_3$. We now define

$$U_n = (\mu_n - \nu_n)/(\mu_1 - \nu_1);$$

then

$$\begin{aligned}&U_0 = 0, U_1 = 1, U_2 = \mu_1 + \nu_1 + 2R = S_1 + 2R,\\ &U_3 = (\mu_1 + \nu_1)^2 - \mu_1\nu_1 = S_1^2 + RS_1 - S_2 - 3R^2.\end{aligned}$$

Also, it is easy to see from (13) that

$$\lambda_1^{-n} = \lambda_2^n/R^{2n}, \qquad \lambda_3^{-n} = \lambda_4^n/R^{2n}, \qquad \lambda_5^{-n} = \lambda_6^n/R^{2n};$$

hence, by (15) we get $U_{-n} = -U_n/R^{2n}$. It follows that (U_n) must be a sixth-order LDS with characteristic polynomial $G(x)$. If we put $\gamma_1 = \lambda_1/R$, $\gamma_2 = \lambda_3/R$, $\gamma_3 = \lambda_5/R$, then by (15) we get U_n and V_n $(= \mu_n + \nu_n + 2R^n)$ given by (4) with $\gamma_1\gamma_2\gamma_3 = 1$. Thus, if $W_n = V_n - 2R^n = \mu_n + \nu_n$, we see that (U_n) and (W_n) are the extended Lucas sequences when $k = 3$.

We conclude this section with some number-theoretic properties of the $k = 3$ extended Lucas sequence (U_n). Let m be an integer. We define the *ranks of apparition* ψ_1, ψ_2,... of m in (U_n) as follows: let ψ_1 (if it exists) be the least positive value of n such that $m \mid U_n$. For $i = 1, 2, \ldots$ define ψ_{i+1} (if it exists) to be the least positive integer such that $m \mid U_n$ for $n = \psi_{i+1}$ and $\psi_j \nmid \psi_{i+1}$ for all j such that $1 \leq j \leq i$. From results in [14, §9] we have the following theorems.

Theorem 8. *Suppose that r is a prime such that $r \nmid 6\Delta\Gamma R$ and let ϵ be the value of the Legendre symbol (Δ/r). If r has more than one rank of apparition in (U_n), then these ranks must all be divisors of $r - \epsilon$. Furthermore, if r has a single rank of apparition in (U_n), it must be a divisor of either $r - \epsilon$ or $r^2 + \epsilon r + 1$.*

Theorem 9. *Suppose that r is a prime such that $r \nmid 6\Delta\Gamma R$. If r is a divisor of some term U_n $(n \neq 0)$ of the sequence (U_n) then some rank of apparition of r in (U_n) must divide n.*

4 Some arithmetic properties of the $k = 3$ extended Lucas sequences

For $n \geq 1$, define $D_n = \gcd(W_n - 6R^n, U_n)$; by [13, Theorem 4] we know that (D_n) is a divisibility sequence. Let ω be the least positive value of n, if it exists, such that m divides the term D_n of the sequence (D_n) we call ω the rank of apparition of m in (D_n). We next present some additional arithmetic results concerning (D_n).

Theorem 10. *([13, Theorem 14]) If r is a prime such that $r \nmid 2R$, there exists a rank of apparition ω of r in (D_n); furthermore, if r divides any term D_m of (D_n), then ω must divide m.*

Theorem 11. *Suppose that r is a prime such that $r \nmid 2R$ and let ϵ be the value of the Legendre symbol $(\Delta|r)$. The rank of apparition of r in (D_n) is either a divisor of r, $r^2 - 1$ or of $r^2 + \epsilon r + 1$.*

Proof. Follows from the previous result and [13, Theorems 9 and 13]. □

We also have some results that can be applied to the problem of primality testing.

Lemma 12. *Let N be a positive integer such that $\gcd(N, 2R) = 1$ and n be a positive integer such that $\gcd(N, n) = 1$. If m is a positive integer such that $N \mid U_{mn}/U_m$, then $\gcd(N, D_m) = 1$.*

Proof. By [13, Theorem 8] we know that $\gcd(U_{mn}/U_m, D_m)$ must be a divisor of $2n^3$. The result now follows easily because
$\gcd(N, 2n) = 1$. □

We can now prove a theorem analogous to [15, Theorem 2.4].

Theorem 13. *Let N be a positive integer such that $\gcd(N, 2R) = 1$. Suppose that n is a positive integer such that $\gcd(N, n) = 1$ and that for some positive integer m we have $N \mid D_{mn}$ and $N \mid U_{mn}/U_m$. If r is a prime divisor of N and $\omega(r)$ is its rank of apparition in (D_n), then $\omega(r) \mid mn$ and $\omega(r) \nmid m$.*

Proof. Clearly, by Theorem 10 we must have $\omega(r) \mid mn$, because $r \mid D_{mn}$. Also, by Lemma 12, we see that r cannot divide D_m; hence, $\omega(r) \nmid m$. □

We next examine some values for N to which these results can be applied. Let p be an odd prime such that $p \equiv 1 \pmod 3$ and let $\lambda_n(p)$ be the least value of x such that

$$x^2 + x + 1 \equiv 0 \pmod{p^n} \text{ and } 1 < x < p^n.$$

If we let $Y_n(p)$ denote the set of all six distinct solutions of

$$x^6 - 1 = (x^2 - 1)(x^2 + x + 1)(x^2 - x + 1) \equiv 0 \pmod{p^n}, \tag{16}$$

it is easy to see that if $y = \lambda_n(p)$, then $Y_n(p) \equiv \{\pm 1, \pm y, \pm y^2\} \pmod{p^n}$; thus,

$$\Gamma_n(p) = \{1, p^n - 1, \lambda_n(p), p^n - 1 - \lambda_n(p), p^n - \lambda_n(p), 1 + \lambda_n(p)\}$$

is the set of all six solutions x of (16) such that $1 \le x < p^n$. Also, $Y_n(p)$ is a group under the operation of multiplication modulo p^n. Let $\gamma_n(p) \in \Gamma_n(p)$ and put

$$N_n = Ap^n + \gamma_n(p) \tag{17}$$

for some fixed positive integer A and $n > 1$. In what follows we will develop a technique that is sufficient for determining whether N_n is a prime.

We first observe that there are only two elements of $\Gamma_n(p)$ that are both bigger than 1 and odd; denote them by $\beta_n(p)$ and $\beta_n^*(p)$ and note that $\beta_n(p) + \beta_n^*(p) = p^n \pm 1$. If either $\beta_n(p)$ or $\beta_n^*(p)$ is a divisor of N_n, then since both exceed 1 and are less than p^n ($< N_n$), N_n cannot be a prime. We now establish the lemma below.

Lemma 14. *Let odd N_n be given by (17), where $n > 1$, $A < 2p^n$, and $\beta_n(p)$, $\beta_n^*(p)$ do not divide N_n, and N_n is not a perfect square. If N_n has at least one prime divisor $t \equiv \gamma \pmod{p^n}$, where $\gamma \in \Gamma_n(p)$, then N_n must be a prime.*

Proof. If N_n is composite, then $N_n = tT$, where $T > 1$. We have $\gamma T \equiv \gamma_n(p) \pmod{p^n}$; hence, $T \equiv \gamma^* \pmod{p^n}$, where $\gamma^* \in \Gamma_n(p)$. Thus, there exist integers m_1 and m_2 such that

$$Ap^n + \gamma_n(p) = N_n = (m_1 p^n + \gamma)(m_2 p^n + \gamma^*). \tag{18}$$

Since both t and T exceed 1 and neither γ nor γ^* divides N_n, we could only have m_1 or $m_2 = 0$ whenever the corresponding γ or γ^* is even, but this is impossible because both t and T are odd. It follows that $m_1 m_2 \ge 1$. If $m_1 m_2 \ge 2$, then by (18) we have $N_n \ge (p^n + 1)(2p^n + 1) > 2p^{2n} + \gamma_n(p)$, which means that $A > 2p^n$, a contradiction. Thus,

we can only have $m_1 = m_2 = 1$. In this event both γ and γ^* must be even. If $\gamma = \gamma^*$, we see that N_n a perfect integral square, which is not permitted. If γ and γ^* are distinct, then because $\gamma, \gamma^* \in \Gamma_n(p)$ and are both even, we have $\gamma + \gamma^* \geq p^n - 1$ and therefore one of γ or γ^* must exceed or equal $(p^n - 1)/2$. Also, since p^n cannot divide 2^6, we observe that $2 \notin \Gamma_n(p)$; thus, both γ and γ^* must be at least 4. We then have $\gamma\gamma^* \geq 2(p^n - 1) > \gamma_n(p)$. By (18) we get $Ap^n > p^{2n} + p^n(p^n - 1) = 2p^{2n} - p^n$, and consequently $A > 2p^n - 1$, which is also a contradiction. □

In general, the determination of whether or not a given integer is a perfect square can be done quite easily, but in the above case it is even easier because if N_n is a perfect square, then $N_n = (p^n + \gamma)^2$, where $\gamma \in \Gamma_n(p)$ and $2 \mid \gamma$. As we must have $\gamma^2 \equiv \gamma_n(p) \pmod{p^n}$ and $2 \mid \gamma$, we can only have $\gamma = p^n - 1$ when $\gamma_n(p) = 1$. However, in this case we find that $N_n = (2p^n - 1)^2$, which since $A < 2p^n$, is impossible. Now it is easy to show that if $\gamma \in \Gamma_n(p)$ and $\gamma^2 \not\equiv 1 \pmod{p^n}$, then $\gamma^2 \equiv \lambda_n(p)$ or $\gamma^2 \equiv p^n - \lambda_n(p) - 1 \pmod{p^n}$. Thus, the only remaining possibilities for $\gamma_n(p)$ are either $\lambda_n(p)$ or $p^n - \lambda_n(p) - 1$ and in either case $\gamma_n(p)^2 + \gamma_n(p) + 1 \equiv 0 \pmod{p^n}$. Also, for each of these possibilities the corresponding γ is either $\gamma_n(p) + 1$ or $p^n - \gamma_n(p) - 1$. If we put $\kappa_n(p) = (\gamma_n(p)^2 + \gamma_n(p) + 1)/p^n$, we see that $N_n = (p^n + \gamma)^2$ only if $A = p^n + 2(\gamma_n(p) + 1) + \kappa_n(p)$ or $A = 4p^n - 4(\gamma_n(p) + 1) + \kappa_n(p)$. Thus, we can exclude the possibility that N_n is a perfect square in Lemma 14 if we assert that

$$\begin{aligned} &A \neq p^n + 2(\gamma_n(p) + 1) + \kappa_n(p) \text{ when } 2 \mid A \text{ or} \\ &A \neq 4p^n - 4(\gamma_n(p) + 1) + \kappa_n(p) \text{ when } 2 \mid A. \end{aligned} \tag{19}$$

Notice that if

$$\begin{aligned} &A = p^n + 2(\gamma_n(p) + 1) + \kappa_n(p) \text{ or} \\ &A = 4p^n - 4(\gamma_n(p) + 1) + \kappa_n(p), \end{aligned}$$

then N_n is a perfect square and therefore cannot be a prime.

With the above results we can now devise a sufficiency test for the primality of N_n.

Theorem 15. *Let odd N_n be given by (17), where $n > 1$, $A < 2p^n$, A satisfies (19), and $\beta_n(p)$, $\beta_n^*(p)$ do not divide N_n. Suppose* $\gcd(N_n, R) = 1$ *and m is some positive integer such that $p^{n-1} \mid m$. If $N_n \mid D_{mp}$ and $N_n \mid U_{mp}/U_m$, then N_n is a prime.*

Proof. Let r be a prime divisor of N_n, and let $\omega(r)$ denote its rank of apparition in (D_n). By Theorem 13, we must have $\omega(r) \mid mp$ and $\omega(r) \nmid m$; hence, $p^n \mid \omega(r)$. Since $\gcd(p, N_n) = 1$, we see that $p \neq r$. Thus, by Theorem 11, we must have $t \equiv \gamma \pmod{p^n}$, where $\gamma \in \Gamma_n(p)$; it follows by Lemma 14 that N_n is a prime. □

In order for Theorem 15 to be practical, we need to study how to compute W_{mn} and U_{mn}/U_m modulo N for a positive integer N such that $\gcd(N, R) = 1$. Let $e_i(x_1, x_2, \ldots, x_6)$ denote the i^{th} elementary symmetric polynomial of x_1, x_2,..., x_6 and put

$$A_i = e_i(\lambda_1^n, \lambda_2^n, \lambda_3^n, \ldots, \lambda_6^n)$$

for $i = 1, 2, \ldots, 6$. If $\mu_n = \lambda_1^n + \lambda_3^n + \lambda_5^n$, $\nu_n = \lambda_2^n + \lambda_4^n + \lambda_6^n$ and (13) and (14) hold, it is not difficult to show that

$$A_1 = \mu_n + \nu_n = W_n, A_2 = R^n(\mu_n + \nu_n) + \mu_n\nu_n,$$
$$A_3 = R^n(\mu_n + \nu_n)^2 - 2R^n\mu_n\nu_n + 2R^{3n}$$

and $A_4 = R^{2n}A_2$, $A_5 = R^{4n}A_1$, $A_6 = R^{6n}$. Also, since

$$\mu_n + \nu_n = W_n \text{ and } \mu_n - \nu_n = \delta U_n,$$

we find that $\mu_n\nu_n = (W_n^2 - \Delta U_n^2)/4$; hence,

$$A_2 = R^n W_n + (W_n^2 - \Delta U_n^2)/4.$$

In addition to this we note that since

$$\mu_{2n} + \nu_{2n} = (\mu_n + \nu_n)^2 - 2\mu_n\nu_n - 2R^n(\mu_n + \nu_n)$$

we get $W_{2n} = W_n^2 - 2\mu_n\nu_n - 2R^nW_n$ and $2\mu_n\nu_n = W_n^2 - W_{2n} - 2R^nW_n$. If we substitute this latter formula into the formulas for A_3 above, we get

$$A_3 = R^n(W_{2n} + 2R^nW_n + 2R^{2n}).$$

Since λ_i^n $(i = 1, 2, \ldots, 6)$ are the roots of $x^6 - A_1x^5 + A_2X^4 - A_3x^3 + A_4x^2 - A_5x + A_6$, we see that for a fixed n both (W_h) and (U_h) satisfy the linear recurrence

$$Z_{mn+6n} = A_1Z_{mn+5n} - A_2Z_{m+4n} + A_3Z_{mn+3n} - R^{2n}A_2Z_{mn+2n} + R^{4n}A_1Z_{mn+n} - R^{6n}Z_{nm}, \quad (20)$$

a generalization of (8).

Suppose that a given N is such that $\gcd(N, 2R) = 1$. For positive integers n and m define

$$X_n \equiv W_n/(2R^n), \tilde{D}_n \equiv \Delta U_n^2/(4R^{2n}),$$
$$Y_{n,m} \equiv U_{mn}/(U_mR^{mn-m}) \pmod{N}.$$

If we refer back to Theorem 15, we see that $N \mid D_{mp}$ and $N \mid U_{mp}/U_m$ if and only if $X_{mp} \equiv 3 \pmod{N}$ and $Y_{p,m} \equiv 0 \pmod{N}$.

In view of (20) we can use the arguments made by Roettger and Williams in [12, §3], to compute remote terms of both (U_n) and (W_n) modulo N. Indeed, 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 $\mathcal{S}_m$, we can compute $\mathcal{S}_{2m+1}$ or $\mathcal{S}_{2m}$ in 12 multiplications by using the formulas given in [12]. We remark here that there are some misprints in [12, formulas (14) and (15)]. 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 we put $x \equiv X_n$ 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 $k = \lceil \log N \rceil$.

5 Some results concerning Gaussian and Jacobi sums

In this section we will review some of the properties of some special sums that will be of importance in the sequel. We first consider two distinct odd primes p, q, where $q \equiv 1 \pmod p$. Let χ denote a primitive Dirichlet character of order p. If t is a primitive root of q, we can define χ by $\chi(t^j) = \zeta_p^j$, where ζ_p is a fixed primitive p^{th} root of unity. It is well known, see, for example, Williams [20, Chapter 11] or Berndt et al. [2], that if $\tau(\chi)$ denotes the Gauss sum

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

where ζ_q is a primitive q^{th} root of unity, then

$$\tau(\chi)\tau(\chi^{-1}) = q. \tag{21}$$

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

$$(\tau(\chi^j))^p/q = \sum_{i=0}^{p-1} b_i\zeta_p^{ij}, \quad (j = 1, 2, \ldots, p-1). \tag{22}$$

This is a consequence of the fact that if $\chi_1\chi_2 \neq \chi_0$, the primitive Dirichlet character, then

$$\tau(\chi_1)\tau(\chi_2) = J(\chi_1, \chi_2)\tau(\chi_1\chi_2), \tag{23}$$

where $J(\chi_1, \chi_2)$ is the Jacobi sum. For much more information on Gaussian and Jacobi sums, see [2]. From (23) and (21), we easily deduce that

$$J(\chi^m, \chi^n)J(\chi^{-m}, \chi^{-n}) = q \tag{24}$$

and by [2, Theorem 2.1.5] we have

$$J(\chi^n, \chi^m) = J(\chi^m, \chi^n) = J(\chi^{-m-n}, \chi^m) = J(\chi^{-m-n}, \chi^n). \tag{25}$$

In [20, §11.1] one method of computing non-negative integers $B(i,j)$ $(0 \le i,j \le p-1)$ such that

$$J(\chi,\chi^j) = \sum_{i=0}^{p-1} B(i,j)\zeta_p^i \tag{26}$$

is discussed. There are other methods for computing the $B(j,1)$; for example, Whiteman [18, (5.8)] has given a general method that involves computing Jacobsthal sums.

In the case of $p = 7$, several properties of these Dickson-Hurwitz sums $B(i,j)$ are provided in Leonard and Williams [9, 10]. This will be discussed further in §7 below.

By using (24) and

$$(\tau(\chi))^p = q\prod_{i=1}^{p-2} J(\chi,\chi^i), \tag{27}$$

a consequence of (21) and (23), we see that all p values of the integers b_i in (22) can be computed in $O(p^3)$ arithmetic operations, once the p^2 values of $B(i,j)$ $(0 \le i,j \le p-1)$ have been calculated. Notice that the values of all of these integers depend only on the preselected values of p and q.

Let $\mathbb{K} = \mathbb{Q}(\zeta_p)$ be the cyclotomic field formed by adjoining ζ_p to the rationals. These fields have been the objects of much study (see, for example, Washington [17]), but we will only require a few simple results concerning them here. For j not divisible by p, we define the automorphism σ_j on $\mathbb{K}$ by $\sigma_j(\zeta_p) = \zeta_p^j$. Note that $\sigma_j(J(\chi^m,\chi^n)) = J(\chi^{jm},\chi^{jn})$. Let $\mathfrak{q}$ be a prime ideal lying over the principal ideal (q) in the ring $\mathcal{O}$ $(= \mathbb{Z}[\zeta_p])$ of algebraic integers in $\mathbb{K}$. Since $q \equiv 1 \pmod p$, we can write [2, p. 65]

$$q\mathcal{O} = \mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3\cdots\mathfrak{q}_{p-1},$$

where the $\mathfrak{q}_j$ $(j = 1,2,\ldots,p-1)$ are distinct prime ideals lying over q in $\mathcal{O}$ and $\mathfrak{q}_j = \sigma_j(\mathfrak{q})$. With this information, we can use [2, Theorem 2.1.14] to find the prime ideal decomposition of $J(\chi^n,\chi^m)$ in $\mathbb{K}$.

In the sequel we assume $p = 7$ and denote ζ_7 by ζ . For fixed j such that $7 \nmid j$ define

$$\xi(\chi^j) = \tau(\chi^j)^7\tau(\chi^{5j})^7. \tag{28}$$

By (27) and (25) we get

$$\begin{aligned}\tau(\chi^j)^7 &= qJ(\chi^j,\chi^j)^2J(\chi^j,\chi^{2j})^2J(\chi^j,\chi^{3j}) \text{ and}\\ \tau(\chi^{5j})^7 &= qJ(\chi^{5j},\chi^{5j})^2J(\chi^{5j},\chi^{3j})^2J(\chi^{5j},\chi^j).\end{aligned}$$

Also, by (25) we have

$$J(\chi^{-j},\chi^{-2j}) = J(\chi^{3j},\chi^{-2j}) = J(\chi^{3j},\chi^{5j});$$

hence, by (24) we get

$$\xi(\chi^j) = q^4J(\chi^j,\chi^j)^2J(\chi^{5j},\chi^{5j})^2J(\chi^j,\chi^{3j})J(\chi^{5j},\chi^j),$$

which since $J(\chi^{5j},\chi^j) = J(\chi^j,\chi^j)$, $J(\chi^j,\chi^{3j}) = J(\chi^{3j},\chi^{3j})$ (by (25)) means that we can write

$$\xi(\chi^j) = q^4 J(\chi^j,\chi^j)^3 J(\chi^{5j},\chi^{5j})^2 J(\chi^{3j},\chi^{3j}). \tag{29}$$

Thus, by (26) there must exist, independent of j, rational integers C_0, C_1, $C_2,\ldots,C_6$ such that if $h(x) = C_0 + C_1x + C_2x^2 + \cdots + C_6x^6$, then

$$\xi(\chi^j)/q^4 = J(\chi^j,\chi^j)^3(\sigma_5(J(\chi^j,\chi^j)))^2\sigma_3(J(\chi^j,\chi^j)) = h(\zeta^j) \tag{30}$$

for j such that $7 \nmid j$.

6 Some special extended Lucas sequences

We now put $\lambda_1 = h(\zeta^j)$, $\lambda_3 = h(\zeta^{2j})$, $\lambda_5 = h(\zeta^{4j})$, $\lambda_2 = h(\zeta^{6j})$, $\lambda_4 = h(\zeta^{5j})$, $\lambda_6 = h(\zeta^{3j})$. We observe by (21) and (28) that if we put $R = q^3$, then

$$\lambda_1\lambda_2 = \lambda_3\lambda_4 = \lambda_5\lambda_6 = R^2.$$

Since $\lambda_1 = h(\zeta^j)$ and $\lambda_3 = h(\zeta^{2j})$, we see by (21) and (28) that

$$\begin{aligned} q^8\lambda_1\lambda_3 &= \xi(\chi^j)\xi(\chi^{2j}) = \tau(\chi^j)^7\tau(\chi^{5j})^7\tau(\chi^{2j})^7\tau(\chi^{3j})^7 \\ &= q^7\tau(\chi^j)^7\tau(\chi^{3j})^7 = q^7\xi(\chi^{3j}) = q^{11}h(\zeta^{3j}) = q^{11}\lambda_6, \end{aligned}$$

and therefore $\lambda_1\lambda_3 = R\lambda_6$. Similarly, we find that

$$\lambda_1\lambda_5 = R\lambda_4, \qquad \lambda_2\lambda_4 = R\lambda_5, \qquad \lambda_2\lambda_6 = R\lambda_3, \qquad \lambda_3\lambda_5 = R\lambda_2, \qquad \lambda_4\lambda_6 = R\lambda_1.$$

Thus, we see that λ_1, λ_2, λ_3, λ_4, λ_5, λ_6 satisfy (13) and (14). We also have

$$\begin{aligned} \mu &= \lambda_1 + \lambda_3 + \lambda_5 = 3C_0 + M_1\kappa + M_2\kappa^* \\ \nu &= \lambda_2 + \lambda_4 + \lambda_6 = 3C_0 + M_1\kappa^* + M_2\kappa, \end{aligned}$$

where

$$\begin{aligned} \kappa &= \zeta^j + \zeta^{2j} + \zeta^{4j}, \\ \kappa^* &= \zeta^{3j} + \zeta^{5j} + \zeta^{6j}, \\ M_1 &= C_1 + C_2 + C_4, \quad \text{and} \\ M_2 &= C_3 + C_5 + C_6. \end{aligned}$$

Since $\kappa+\kappa^* = -1$ and $\kappa\kappa^* = 2$, we deduce that $T_1 = \mu+\nu$ and $T_2 = \mu\nu$ are rational integers. Thus, by Proposition 7, we find that if we put, $S_1 = T_1$, $S_2 = RT_1 + T_2 - 3R^2$, and S_3 is given by (9), the corresponding sequences (U_n), (W_n) are particular instances of the $k = 3$ extended Lucas sequences. By [2, Theorem 2.1.4], we find that

$$J(\chi,\chi)\mathcal{O} = \mathfrak{q}_1\mathfrak{q}_4\mathfrak{q}_5, \qquad J(\chi^5,\chi^5)\mathcal{O} = \mathfrak{q}_4\mathfrak{q}_5\mathfrak{q}_6, \qquad J(\chi^3,\chi^3)\mathcal{O} = \mathfrak{q}_1\mathfrak{q}_3\mathfrak{q}_5; \tag{31}$$

however, in this case ($p = 7$) the cyclotomic field $\mathbb{K}$ has class number one and is therefore a unique factorization domain; it follows that we can put $\mathfrak{q}_j = \pi_j\mathcal{O}$ ($j = 1, 2, \ldots, p-1$), where π_j is some prime divisor of q in $\mathcal{O}$. Thus, we can write

$$J(\chi, \chi) = \pi_1\pi_4\pi_5, \qquad J(\chi^5, \chi^5) = \pi_4\pi_5\pi_6, \qquad J(\chi^3, \chi^3) = \pi_1\pi_3\pi_5,$$

where $\pi_j = \sigma_j(\pi_1)$.

It follows from (29) and (30) that $h(\zeta)$ is $\pi_1^4\pi_3\pi_4^5\pi_5^6\pi_6^2$. Suppose that $\gcd(S_1, S_2, R) > 1$; then $q \mid S_1$ and $q \mid S_2$. Now since $h(\zeta)$ must be one of the six roots of (15), we find that q must divide $h(\zeta)^6$, which means that π_2 must divide $h(\zeta)$, an impossibility. Thus, we must have $\gcd(S_1, S_2, R) = 1$ here. In what follows we will develop some properties of these special extended Lucas sequences that result for the values of S_1, S_2 and R given above.

We first observe that $\delta = \mu - \nu = (M_1 - M_2)(\kappa - \kappa^*)$; hence, since

$$(\kappa - \kappa^*)^2 = (\kappa + \kappa^*)^2 - 4\kappa\kappa^* = -7,$$

we get $\Delta = -7(M_1 - M_2)^2$. Thus, if r is a prime such that $r \nmid \Delta$, then $\epsilon = (\Delta/r) = (-7/r) = (r/7)$. Suppose $r \equiv \eta \pmod 7$, where $\eta = \pm 1$; in this case we have $\epsilon = \eta$ and we put $m(r) = (r - \epsilon)/7$. If $r \not\equiv \pm 1 \pmod 7$, then we have $7 \mid r^2 + \epsilon r + 1$, and in this case we put $m(r) = (r^2 + \epsilon r + 1)/7$.

Now let q be a fixed prime such $q \equiv 1 \pmod 7$ and r be an odd prime such that $r \neq 7, q$. Also, let $\mathbb{F}_t$ denote the finite field containing $t = r^n$ elements, where $n = 3(q-1)$. Since $\mathbb{F}_t^*$ is a cyclic group with generator γ, say, we can put $\zeta = \gamma^{(t-1)/7}$ and $\zeta_q = \gamma^{(t-1)/q}$ and repeat the arguments in the previous section concerning the Gauss and Jacobi sums in $\mathbb{F}_t$. We find that all the numbered results in that section hold in $\mathbb{F}_t$. Suppose we let g denote a fixed primitive root of q and put $\iota = \operatorname{ind}_g r$. Notice that $7 \nmid \iota$ if and only if $r^{(q-1)/7} \not\equiv 1 \pmod q$.

We will now conduct our calculations in $\mathbb{F}_t$. We observe that by (26) we have

$$J(\chi^j, \chi^{sj})^r = J(\chi^{rj}, \chi^{rsj}), \tag{32}$$

for s such that $7 \nmid s$. Also, from the definition of $\tau(\chi^j)$, we get

$$\tau(\chi^j)^r = \sum_{i=0}^{q-1} \chi^{rj}(i)\zeta_7^{ri} = \zeta^{\iota rj}\tau(\chi^{rj}). \tag{33}$$

If $m = (r - \epsilon)/7$, then by (33) and (21) we get

$$\tau(\chi^j)^{7m} = \zeta^{\iota rj}\tau(\chi^j)^{-\epsilon}\tau(\chi^{rj}) = \zeta^{\iota rj}\tau(\chi^j)^{-\epsilon}\tau(\chi^{\epsilon j}) = \zeta^{\iota rj}q^{(1-\epsilon)/2}. \tag{34}$$

It follows that since $q^{4m}\lambda_1^m = \tau(\chi^j)^{7m}\tau(\chi^{5j})^{7m}$, we can conclude from (34) that

$$\lambda_1^m = \zeta^{6\iota rj}q^{1-\epsilon-4m} = \zeta^{6\iota rj}q^{1-r+3m} = \zeta^{6\iota rj}R^m. \tag{35}$$

We also find that

$$\lambda_2^m = \zeta^{\iota r j} R^m, \quad \lambda_3^m = \zeta^{5\iota r j} R^m, \quad \lambda_4^m = \zeta^{2\iota r j} R^m, \tag{36}$$
$$\lambda_5^m = \zeta^{3\iota r j} R^m, \quad \lambda_6^m = \zeta^{4\iota r j} R^m.$$

If $m = (r^2 + \epsilon r + 1)/7$, we find by repeated application of (33) that

$$\tau(\chi^j)^{7m} = \zeta^{\iota(1-r)j} \tau(\chi^j)\tau(\chi^{rj})^\epsilon \tau(\chi^{sj}),$$

where $s = r^2$. Since by (21) we have $\tau(\chi^{rj})^\epsilon = q^{(\epsilon-1)/2}\tau(\chi^{r\epsilon j})$, we get

$$\tau(\chi^j)^{7m} = \zeta^{\iota(1-r)j} q^{(\epsilon-1)/2} \tau(\chi^j)\tau(\chi^{r\epsilon j})\tau(\chi^{sj}).$$

Now by (23), we have

$$\tau(\chi^j)\tau(\chi^{sj}) = J(\chi^j, \chi^{sj})\tau(\chi^{sj+j}) = J(\chi^j, \chi^{sj})\tau(\chi^{-\epsilon r j});$$

hence, by (21) we find that

$$\tau(\chi^j)^{7m} = \zeta^{\iota(1-r)j} q^{(\epsilon+1)/2} J(\chi^j, \chi^{sj}).$$

By the reasoning used in the case where $m = (r - \epsilon)/7$, we discover that

$$\lambda_1^m = \zeta^{6\iota(1-r)j} q^{\epsilon+1-4m} J(\chi^j, \chi^{sj}) J(\chi^{5j}, \chi^{5sj}).$$

We observe that $s = r^2 \equiv 2$ or $4 \pmod 7$. By (25) and (24) we find that in either case, we get

$$J(\chi^j, \chi^{sj}) J(\chi^{5j}, \chi^{5sj}) = q.$$

Thus, since $\epsilon + 2 - 7m = (1 - r)(1 + r + \epsilon)$ we get

$$\lambda_1^m = \zeta^{6\iota(1-r)j} q^{\epsilon+2-4m} = \zeta^{6\iota(1-r)j} q^{\epsilon+2-7m} q^{3m} = \zeta^{6\iota(1-r)j} R^m, \tag{37}$$

and we also have

$$\lambda_2^m = \zeta^{\iota(1-r)j} R^m, \quad \lambda_3^m = \zeta^{5\iota(1-r)j} R^m, \quad \lambda_4^m = \zeta^{2\iota(1-r)j} R^m, \tag{38}$$
$$\lambda_5^m = \zeta^{3\iota(1-r)j} R^m, \quad \lambda_6^m = \zeta^{4\iota(1-r)j} R^m.$$

Thus, in either case when $m = m(r)$, we have $\mu_{7m} = \nu_{7m} = 3R^{7m}$. Also, if $r \equiv \pm 1 \pmod 7$ and $7 \nmid \iota$, then by (35) and (36) we have $\mu_m = KR^m$ and $\nu_m = K^*R^m$, where K, $K^* \in \mathbb{F}_t$, $K + K^* = -1$ and $KK^* = 2$. If $r \not\equiv \pm 1 \pmod 7$ and $7 \nmid \iota$, we also have $\mu_m = KR^m$ and $\nu_m = K^*R^m$, where K, $K^* \in \mathbb{F}_t$, $K + K^* = -1$ and $KK^* = 2$. Since $(K - K^*)^2 = -7$, we must have $\mu_m \neq \nu_m$ for $r \neq 7$, whenever $7 \nmid \iota$. Of course, if $7 \mid \iota$, then $\mu_m = \nu_m$.

We are now able to prove the following important result concerning these special extended Lucas sequences.

Theorem 16. *Let r be a prime such that $r \nmid q\Delta$ and let $m = m(r)$ be defined as above. If the sequences (U_n), (W_n) are the special extended Lucas sequences defined in this section, then $r \mid D_{7m}$ and $r \mid U_m$ if and only if $r^{(q-1)/7} \equiv 1 \pmod{q}$.*

Proof. This result follows easily from $\delta U_n = \mu_n - \nu_n$, $W_n = \mu_n + \nu_n$ and our above remarks. □

We are now able to present one of the main results of this paper. This result is the analogue of Theorems 1 and 5 above.

Theorem 17. *Let r be a prime such that $r \nmid 6q\Delta$. If $7 \nmid n$ and $r \mid U_n$, then $r^{(q-1)/7} \equiv 1 \pmod{q}$.*

Proof. If $r \mid \Gamma$ where Γ is given by equation (12), we know by results in [14, §9] that r has a single rank of apparition ψ in (U_n) and $\psi \mid r \pm 1$. Furthermore, it is easy to see from these results that if $r \mid U_n$, then $\psi \mid n$. If $r \nmid \Gamma$, by Theorem 9 we know that some rank of apparition ψ of r in (U_n) must divide n. Hence, in either case, we have $7 \nmid \psi$. Also, if $r^{(q-1)/7} \not\equiv 1 \pmod{q}$, then by Theorem 16 we have $r \nmid U_m$ and $r \mid U_{7m}$, where $m = m(r)$. If r has a single rank of apparition in (U_n), then it must be ψ and also a divisor of $7m$, but since $7 \nmid \psi$, we must have $\psi \mid m$, which is impossible because (U_n) is a divisibility sequence and $r \nmid U_m$. Thus, if r has more than one rank of apparition in (U_n), by Theorem 8 we can only have $\psi \mid r - \epsilon$, where $\epsilon = (r/7)$. If $r \equiv \pm 1 \pmod{7}$, then $m = (r - \epsilon)/7$ and since $7 \nmid \psi$ and $\psi \mid 7m$, we must have $\psi \mid m$, which we have already seen is a contradiction. If $r \not\equiv \pm 1 \pmod{7}$, then $m = (r^2 + \epsilon r + 1)/7$. By Theorems 9 and 8, this means that there must be some rank of apparition ϕ of r in (U_n) such that $\phi \mid 7m$ and $\phi \mid r - \epsilon$. Since $7m = (r - \epsilon)2 + 3\epsilon r$, this means that ϕ can only be 1 or 3. The former case is impossible because $U_1 = 1$. Thus, ϕ must be 3, but since $3 \mid m$, this is also impossible because $r \nmid U_m$. □

We next turn to the problem of finding an analogue to Theorems 3 and 4. This is provided by the next results; however, we must first impose some conditions on

$$N_n = A7^n + \gamma_n(7) \ (n > 1), \tag{39}$$

the number whose primality we wish to establish. By our results in §4, we may insist that

(i) $\beta_n(7) \nmid N_n$ and $\beta_n^*(7) \nmid N_n$;

(ii) $A \neq 7^n + 2(\gamma_n(7) + 1) + \kappa_n(7)$ when $2 \mid A$ or
$A \neq 4 \cdot 7^n - 4(\gamma_n(7) + 1) + \kappa_n(7)$ when $2 \nmid A$;

otherwise, N_n cannot be a prime.

Let $\epsilon(N_n)$ be the value of the Legendre symbol $(N_n/7) = (\gamma_n(7)/7)$. If $\gamma_n(7) \equiv \pm 1 \pmod{7}$, then $\gamma_n(7) \equiv \epsilon(N_n) \pmod{7}$ and we put $m(N_n) = (N_n - \gamma_n(7))/7$. Since $N_n^3 \equiv \epsilon(N_n) \pmod{7}$, we see that $7 \mid (N_n^2 + \epsilon(N_n)N_n + 1)$ when $\gamma_n(7) \not\equiv \pm 1 \pmod{7}$, and we put $m(N_n) = (N_n^2 + \epsilon(N_n)N_n + 1)/7$. In either case $m(N_n)$ is an integer. Furthermore, when

$\gamma_n(7) \not\equiv \pm 1 \pmod 7$, we must by definition of $\gamma_n(7)$ have $N_n^2 + sN_n + 1 \equiv \gamma_n(7)^2 + s\gamma_n(7) + 1 \equiv 0 \pmod{7^n}$ for some $s \in \{1, -1\}$; it follows that s can only be $\epsilon(N_n)$, and therefore $7^n \mid 7m(N_n)$.

Theorem 18. *Let N_n be given by (39) such that $\gcd(N_n, 2q\Delta) = 1$. Suppose further that N_n satisfies the conditions (i) and (ii). If $A < 2 \cdot 7^n$, $m = m(N_n)$, and $N_n^{(q-1)/7} \not\equiv 1 \pmod q$, then N_n is a prime if and only if $N_n \mid D_{7m}$ and $N_n \mid U_{7m}/U_m$.*

Proof. We have seen by Theorem 15 that if $N_n \mid D_{7m}$ and $N_n \mid U_{7m}/U_m$, then N_n is a prime. Also, by Theorem 16, we see that if N_n is a prime, then $N_n \nmid U_m$, $N_n \mid U_{7m}$ and $N_n \mid W_{7n} - 6R^{7n}$. It follows that $N_n \mid D_{7m}$ and $N_n \mid U_{7m}/U_m$. □

Theorem 19. *Let N_n be given by (39) such that $\gcd(N_n, 2q\Delta) = 1$. Suppose further that N_n satisfies the conditions (i) and (ii). If $A < 2 \cdot 7^n$, $m = m(N_n)$, and $N_n^{(q-1)/7} \not\equiv 1 \pmod q$, then N_n is a prime if and only if*

$$W_m \equiv -R^m \qquad \textit{and} \qquad \Delta U_m^2 \equiv -7R^{2m} \pmod{N_n}.$$

Proof. Since $W_m = \mu_m + \nu_m$ and $\delta U_m = \mu_m - \nu_m$, we see by our remarks following (38) that if N_n is a prime, then $W_m \equiv -R^m \pmod{N_n}$ and $\Delta U_m^2 \equiv -7R^{2m} \pmod{N_n}$. If $W_m \equiv -R^m \pmod{N_n}$ and $\Delta U_m^2 \equiv -7R^{2m} \pmod{N_n}$, then because

$$F_7(-1/2, -7/4) = 3 \qquad \text{and} \qquad G_7(-1/2, -7/4) = 0,$$

we must have $W_{7m} \equiv 6R^{7m} \pmod{N_n}$ and $N_n \mid U_{7m}/U_m$ by our results at the conclusion of §4 above. It follows from Theorem 18 that N_n must be a prime. □

7 Computation and an example

We will now discuss how to compute, given q, values for S_1 and S_2 for the special extended Lucas sequences introduced in the previous section. Since $\mu = \lambda_1 + \lambda_3 + \lambda_5 = 3C_0 + M_1\kappa + M_2\kappa^*$ and $\nu = \lambda_2 + \lambda_4 + \lambda_6 = 3C_0 + M_1\kappa^* + M_2\kappa$, where $\kappa + \kappa^* = -1$ and $\kappa\kappa^* = 2$, we see that $\mu + \nu = 6C_0 - M_1 - M_2$ and $\mu\nu = 9C_0^2 - 3C_0(M_1 + M_2) + 2(M_1 + M_2)^2 - 7M_1M_2$. It follows that

$$\begin{aligned} S_1 &= 6C_0 - M_1 - M_2, \\ S_2 &= (3C_0 + R)^2 - (3C_0 + R)(M_1 + M_2) + 2(M_1 + M_2)^2 - 7M_1M_2 - 4R^2. \end{aligned} \tag{40}$$

Since $M_1 = C_1 + C_2 + C_4$ and $M_2 = C_3 + C_5 + C_6$, where

$$h(\zeta^j) = C_0 + C_1\zeta^j + C_2\zeta^{2j} + \cdots + C_6\zeta^{6j}$$

and by (30)

$$h(\zeta^j) = J(\chi^j, \chi^j)^3(\sigma_5(J(\chi^j, \chi^j)))^2\sigma_3(J(\chi^j, \chi^j)), \tag{41}$$

we see that we need to determine $B(i,1)$ $(0 \le i \le 6)$, where

$$J(\chi^j, \chi^j) = \sum_{i=0}^{6} B(i,1)\zeta^{ij},$$

and then use (41) to compute the coefficients C_i $(i = 0, 1, 2, \ldots, 6)$.

We have already mentioned one method for computing $B(i,1)$ $(0 \le i \le 6)$, but in the case of $p = 7$ we know by results of Leonard and Williams [9, 10] that there exist integers $x_1, x_2, \ldots, x_6$, such that

$$x_1 \equiv 1 \pmod 7, \tag{42}$$

$$72q = 2x_1^2 + 42(x_2^2 + x_3^2 + x_4^2) + 343(x_5^2 + 3x_6^2), \tag{43}$$

$$12x_2^2 - 12x_4^2 + 147x_5^2 - 441x_6^2 + 56x_1x_6 + 24x_2x_3 - 24x_2x_4 + 48x_3x_4 + 98x_5x_6 = 0, \tag{44}$$

$$12x_3^2 - 12x_4^2 + 49x_5^2 - 147x_6^2 + 28x_1x_5 + 28x_1x_6 + 48x_2x_3 + 24x_2x_4 + 24x_3x_4 + 490x_5x_6 = 0. \tag{45}$$

Also, if there is a nontrivial (x_5 and x_6 not both zero) solution to (42)-(45), we can put $B(0,1) = (q - 2 + x_1)/7$ and $B(i,1) = a_i + B(0,1)$, where

$$12a_1 = -2x_1 + 6x_2 + 7x_5 + 21x_6, \qquad 12a_2 = -2x_1 + 6x_3 + 7x_5 - 21x_6,$$
$$12a_3 = -2x_1 + 6x_4 - 14x_5, \qquad 12a_4 = -2x_1 - 6x_4 - 14x_5,$$
$$12a_5 = -2x_1 - 6x_3 + 7x_5 - 21x_6, \qquad 12a_6 = -2x_1 - 6x_2 + 7x_5 + 21x_6.$$

A table of nontrivial solutions of (42)-(45) for all $q \equiv 1 \pmod 7$ and $q < 1000$ appears in Williams [22]. For example, if $q = 29$ this table lists $x_1 = 1$, $x_2 = -2$, $x_3 = -3$, $x_4 = -2$, $x_5 = -1$, $x_6 = 1$ and we find that $a_1 = 0$, $a_2 = -4$, $a_3 = 0$, $a_4 = 2$, $a_5 = -1$, $a_6 = 2$. Thus, in this case, we get

$$B(0,1) = 4, B(1,1) = 4, B(2,1) = 0, B(3,1) = 4,$$
$$B(4,1) = 6, B(5,1) = 3, B(6,1) = 6.$$

Williams's technique for tabulating solutions of (42)-(45) requires that we first have some prime factor λ of q in $\mathcal{O}$. From this is easy to find some associate π_1 of λ such that $J(\chi, \chi) = \pi_1\pi_4\pi_5$, and we can then compute the values of $B(i,1)$ $(0 \le i \le 6)$. The main problem here is that of finding some λ (Williams used an old table of Kummer), but since $\mathcal{O}$ here is norm-Euclidean, we have an efficient algorithm for computing λ as the greatest common divisor of q and $\zeta - g^h$, where $h = (q-1)/7$. This is all explained in great detail in the Master's thesis of Caranay [4].

As mentioned earlier [22, Table 2] provides solutions to the quadratic partition described by equations (42)-(45) for all primes $q < 1000$ such that $q \equiv 1 \pmod 7$. By use of this table and methods mentioned above we used a computer to calculate the values of S_1 and S_2 for each value of $q < 1000$. The values for S_1 and S_2 for each q are given in the table below.

q	S_1	S_2
29	14965	−1017406826
43	272957	21858615700
71	−1040033	326748793138
113	2975587	731201875780
127	3699863	−97933301720
197	−4964135	−144000965801744
211	−26590621	179982347982148
239	−40502099	526271548075978
281	29450665	−606639016188536
337	−80516773	−201075257844008
379	−107119195	−5558958106936166
421	206278211	10161855131659180
449	213162529	6646761776500900
463	111923783	−13852858246492778
491	95772025	−25034062770947666
547	918783725	281059458133383676
617	−548612555	40672461475028416
631	485050586	4945779937081660
659	−498921389	−313908392056365122
673	89928278	−145075204278786308
701	−386848421	−422179587542810582
743	918668743	100597296170580172
757	−848906535	−647877968552066604
827	−762742499	−1133671841709810608
883	−1331064561	−1555728581709172068
911	1688430505	401503472607970444
953	95807830	−2154081956136898244
967	−2183072893	−504443123489474738

Table 2: Values of S_1 and S_2 for each value of $q < 1000$

We next tabulate $S_3 = RS_1^2 - RS_2 - 4R^3$, where $R = q^3$ and the factorization of the corresponding Δ, as this is useful in applying the theorems in the previous section.

q	S_3	Δ
29	−2939567318323	$-7^7 \cdot 41^2$
43	437514319995271	-7^{11}
71	−30146872474620481	$-7^7 \cdot 1987^2$
113	−1350685445842116019	$-7^7 \cdot 1511^2$
127	−5937522515922653501	$-7^7 \cdot 2689^2$

197	602743276360621183481	$-7^7 \cdot 83^2 \cdot 211^2$
211	−55305165497468656769	$-7^7 \cdot 50147^2$
239	−2151851544923374759681	$-7^7 \cdot 77237^2$
281	2471371627931491315493	-7^{11}
337	39263510618353883256277	$-7^7 \cdot 165719^2$
379	584554850719077350566147	$-7^7 \cdot 174859^2$
421	−3333118453246404690503	$-7^7 \cdot 13^6 \cdot 29^2$
449	−57018536315736139357387	$-7^7 \cdot 71^2 \cdot 743^2$
463	82195167713946458240623	$-7^7 \cdot 84211^2$
491	378058321944546499176803	$-7^7 \cdot 84211^2$
547	28624865948434380013954111	$-7^3 \cdot 233617^2$
617	−247393375351235843201779	$-7^7 \cdot 113^2 \cdot 9941^2$
631	−68093007179758866284193 68	$-2^6 \cdot 7^7 \cdot 32159^2$
659	157152662797406306447103779	$-7^7 \cdot 41^2 \cdot 43^2 \cdot 139^2$
673	−22381922654581541570716952	$-2^6 \cdot 7^7 \cdot 29^2 \cdot 3067^2$
701	17890735984947848149782 9701	$-7^7 \cdot 13^2 \cdot 29191^2$
743	−12390466262878082841792637	$-7^7 \cdot 127^2 \cdot 2297^2$
757	54817984868523438515755 9841	$-3^6 \cdot 7^7 \cdot 29^2 \cdot 911^2$
827	88770361086569701684337 9663	$-7^7 \cdot 251^2 \cdot 2939^2$
883	20566193788293438077943 16247	$-3^6 \cdot 7^7 \cdot 113^2 \cdot 421^2$
911	−18047434838230174811999 0917	$-7^7 \cdot 785779^2$
953	11432016839974739731485 92744	$-2^6 \cdot 7^7 \cdot 71^2 \cdot 349^2$
967	22643376690421853340719 59087	$-7^7 \cdot 41^2 \cdot 211^2 \cdot 421^2$

Table 3: Values of S_3 and Δ

The following two tables provide the values of the first 26 terms of (U_n) when $q = 29$ and display how (U_n) is analogous to the (G_n) given in Table 1. Notice for (U_n) the terms with subscripts divisible by 7 tend to have many small factors belonging to no particular residue class, while the other terms satisfy Theorem 17.

n	U_n
0	0
1	1
2	63743
3	−178130527
4	−7682842247401
5	866655108578870099
6	−7573915228698089372963
7	−68399003482887202746501 5352
8	−23976393924147777046275 33089857

9	−22408683611098412939809100875710563
10	998749219544949068374614639693399640597
11	86083430660651144394984616218844903262150707
12	−744603639251416281181958726630900817210441654623
13	791504002265519992711978661880777629855646968535130 43
14	296539832439228684555683867184027511323226853256183 0767808
15	−566763266702553885028876637943038377385405707725711 78015273923
16	−136101552561095318102200483955964758336846652893173 8949569426882481
17	900974591404181669530727185663463044965078113607329 6448298340027827709
18	−440810292281876727626223093083385382065568423941096 7968458790962530526427797
19	−883415092917308410341478004881335927504876075643566 6192525146740054105545398437
20	366474365369871419422551402809377272895434714580280 0845069295056319861525848019 4601
21	138353761716273184823923842079896157272158666142471 0168014981086555139364346950488151000
22	396555374482458085998549585110564489118464444214556 5571250102789585852886477181934157303758 99
23	521844552443392142081249812412252143396303148636315 2233362945200754150357516907879932060934212437
24	−176249448788214627969811858494667349579382590158574 9842201032900330349269812604886510037926577766168223
25	675739548674286160310534875288000108035240684343625 188770153722669664064432521414254825560912252408993951

Table 4: U_n values for $q = 29$

n	U_n
0	0
1	1
2	63743
3	$41^2 \cdot 105967$
4	$-63743 \cdot 120528407$
5	$18080861 \cdot 47932181359$
6	$-41^2 \cdot 1217 \cdot 63743 \cdot 105967 \cdot 548099$

7	$-2^3 \cdot 3^3 \cdot 7^3 \cdot 13 \cdot 83 \cdot 113 \cdot 127 \cdot 181 \cdot 4327 \cdot 22637 \cdot 33629$
8	$-63743 \cdot 2023951 \cdot 120528407 \cdot 154192040407$
9	$-41^2 \cdot 105967 \cdot 352043 \cdot 8608823 \cdot 41508639603521$
10	$63743 \cdot 199289 \cdot 18080861 \cdot 47932181359 \cdot 90718179089$
11	$307 \cdot 190553764987279 \cdot 14715114880461221343631791 19$
12	$-41^2 \cdot 1217 \cdot 1931 \cdot 63743 \cdot 105967 \cdot 528611 \cdot 548099 \cdot 120528407$ $\cdot 799092083$
13	$911 \cdot 868829859786520299354532010846078627729933792 9213$
14	$2^6 \cdot 3^3 \cdot 7^3 \cdot 13^3 \cdot 43 \cdot 83 \cdot 113 \cdot 127 \cdot 181 \cdot 461 \cdot 827 \cdot 1093 \cdot 4327$ $\cdot 7043 \cdot 8807 \cdot 22637 \cdot 33629 \cdot 45263 \cdot 63743$
15	$-41^2 \cdot 1259 \cdot 4409 \cdot 10499 \cdot 33391 \cdot 105967 \cdot 18080861$ $\cdot 47932181359 \cdot 188657402425248539369$
16	$-63743 \cdot 2023951 \cdot 3655681 \cdot 120528407 \cdot 154192040407$ $\cdot 270791233327 \cdot 573424602581099359$
17	$131243294444234697389707283 21$ $\cdot 6864919043822128050927809378510681236184 29$
18	$-41^2 \cdot 1217 \cdot 63743 \cdot 105967 \cdot 352043 \cdot 548099 \cdot 8608823$ $\cdot 41508639603521 \cdot 462650775088987947659434651$
19	$-3191 \cdot 290737 \cdot 19018201 \cdot 5006892565699708008126210 56$ $0049425129045409521906956962476568 11$
20	$63743 \cdot 199289 \cdot 18080861 \cdot 120528407 \cdot 47932181359$ $\cdot 90718179089 \cdot 3044372090579643555605227086611260 19$
21	$2^3 \cdot 3^6 \cdot 5^3 \cdot 7^3 \cdot 13 \cdot 41^2 \cdot 43 \cdot 83 \cdot 113 \cdot 127 \cdot 181 \cdot 379 \cdot 4409$ $\cdot 4327 \cdot 11801 \cdot 12263 \cdot 22637 \cdot 33629 \cdot 46831 \cdot 85639 \cdot 105967$ $\cdot 116423 \cdot 887492677 \cdot 780831241$
22	$307^3 \cdot 190553764987279 \cdot 14715114880461221343631791 19$ $\cdot 63743 \cdot 97789 \cdot 7841244907646133326488341710420059$
23	$2517907877440181139467776912362257470 3 \cdot 207253234766$ $4454194975192853095647170999315682812432728003 79$
24	$-41^2 \cdot 1217 \cdot 1931 \cdot 3191 \cdot 63743 \cdot 105967 \cdot 528611 \cdot 548099$ $\cdot 2023951 \cdot 2425751 \cdot 120528407 \cdot 799092083 \cdot 154192040407$ $\cdot 979868147236664181519036 73$
25	$349^3 \cdot 2801 \cdot 18080861 \cdot 47932181359 \cdot 617499370923509368494901$ $\cdot 106049134110713626118959617341790809755579125138099 01$

Table 5: U_n values factored for $q = 29$

Note that in this example each prime divisor r of U_n when $7 \nmid n$ is such that $r \equiv \pm 1$, $\pm 17 \pmod{58}$. This is because ± 1 and ± 17 are the only values of $x \pmod{29}$ such that $x^4 = x^{(29-1)/7} \equiv 1 \pmod{29}$.

References

[1] M. Abrate, S. Barbero, U. Cerutti, and N. Murru, Linear divisibility sequences and Salem numbers, *Pub. Math. Debrecen* **91** (2017), 247–259.

[2] Bruce C. Berndt, Ronald J. Evans, and Kenneth S. Williams, *Gauss and Jacobi Sums*, John Wiley and Sons, 1998.

[3] David Bressoud and Stan Wagon, *A Course in Computational Number Theory*, Key College Publishing, 2000.

[4] Perlas Caranay, On Residue Symbols and Kummer's Reciprocity Law of Degree Seven, Master's thesis, University of Calgary, 2009.

[5] David A. Cox, *Primes of the Form* $x^2 + ny^2$, John Wiley and Sons, 1989.

[6] R. Crandal and C. Pomerance, *Prime Numbers: A Computational Perspective, second edition*, Springer-Verlag, 2005.

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

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

[9] P. A. Leonard and K. S. Williams, A Diophantine system of Dickson, *Rend. Accad.Naz. Lincei.* **56** (1974), 145–150.

[10] P. A. Leonard and K. S. Williams, The cyclotomic numbers of order seven, *Proc. Amer. Math. Soc.* **51** (1975), 295–300.

[11] P. Ribenboim, *The Book of Prime Number Records*, Springer-Verlag, 2 edition, 1989.

[12] E. L. Roettger and H. C. Williams, Public-key cryptography based on a cubic extension of the Lucas functions, *Fund. Inform.* **114** (2012), 325–344.

[13] E. L. Roettger and H. C. Williams, Some arithmetic properties of certain sequences, *J. Integer Sequences* **18** (2015), Article 15.6.2.

[14] E. L. Roettger, H. C. Williams, and R. K. Guy, Some extensions of the Lucas functions, in *Number Theory and Related Fields: In Memory of Alf van der Poorten*, Vol. 43, pp. 271–311, Springer, 2013.

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

[16] N. J. A. Sloane et al., The On-Line Encyclopedia of Integer Sequences, 2020. Available at https://oeis.org.

[17] Lawrence C. Washington, *Introduction to Cyclotomic Fields*, Springer-Verlag, 1982.

[18] A. L. Whiteman, Cyclotomy of Jacobsthal sums, *Amer. J. Math* **74** (1952), 89–99.

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

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

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

[22] K. S. Williams, A quadratic partition of primes $\equiv 1 \pmod 7$, *Math. Comp* **28** (1974), 1133–1136.

2010 *Mathematics Subject Classification*: Primary 11B37; Secondary 11Y11, 11B50.
Keywords: linear recurrence, Lucas function, primality testing.

(Concerned with sequences A001351, A001945, A006235 and A180510.)

Return to Journal of Integer Sequences home page.