Journal of Integer Sequences, Vol. 28 (2025),
Article 25.2.5

Some Remarks Concerning the Lucas-Lehmer Primality Test

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
hwilliam@ucalgary.ca

Abstract

In 1876 Lucas devised a test for the primality of Mersenne numbers M_n, where $n \equiv 3 \pmod 4$. He did so by calculating a recursive sequence (s_k) with $s_{k+1} = s_k^2 - 2$, using an initial value of $s_1 = 3$. Later, Lehmer refined Lucas' techniques and constructed a test for all Mersenne numbers with odd n $(n \geq 3)$; again he used the sequence (s_k), but with an initial value of 4. We investigate what initial values can be used in similar primality tests and for which values of n they can be used to test M_n. We also present some computational results.

1 Introduction

A perfect number P is defined to be an integer which is equal to the sum of its aliquot (proper) divisors, i.e., the divisors less than P. For example, $P = 6 = 1 + 2 + 3$. It is well known that if P is even, then it is both necessary and sufficient that $P = 2^{n-1}M_n$, where $M_n = 2^n - 1$ and M_n is a prime. Such primes are known today as Mersenne primes and integers of the form $2^n - 1$ are called Mersenne numbers. Clearly, in order for M_n to be a prime when $n > 2$, it is necessary that n be odd; indeed, n must be a prime.

In 1876 Lucas announced that he had proved that M_{127} is a prime. This was the first time that a number of this magnitude had been substantiated as a prime; furthermore, Lucas was able to achieve this without recourse to the tedious and time consuming process of trial division. A detailed discussion of Lucas' work, including references, can be found in Chapters 3 and 5 of [11] and Section 3.1 of [1].

Suppose for a given value of s_1 (the *seed*), we compute the sequence (s_n) recursively by

$$s_{i+1} = s_i^2 - 2 \quad (i \geq 1).$$

Indeed, sequences satisfying this recursion can be found in the *On-line Encyclopedia of Integer Sequences* (OEIS) [10]; in particular we mention that when $s_1 = 3$, as in the theorem below, we have A001566. Lucas proved the following result:

Theorem 1. *If $n \equiv 3 \pmod 4$, $n \geq 3$ and $s_1 = 3$, then M_n is a prime if and only if*

$$s_{n-1} \equiv 0 \pmod{M_n}.$$

For example, consider $M_7 = 127$. We have $s_1 = 3$, $s_2 = 7$, $s_3 = 47$, $s_4 = 2207 \equiv 48 \pmod{M_7}$, $s_5 \equiv 48^2 - 2 \equiv 16 \pmod{M_7}$, $s_6 \equiv 16^2 - 2 \equiv 0 \pmod{M_7}$. Thus, 127 is a prime by Theorem 1.

It was an early version of Theorem 1 that Lucas used to establish the primality of M_{127}. He proved this result by making use of the properties of the Fibonacci and Lucas numbers. However, there are values of $n \equiv 1 \pmod 4$, such as $n = 5$, for which M_n is a prime. Possibly, in order to deal with the case of $n \equiv 1 \pmod 4$, Lucas began his investigations into the features of (U_n), (V_n); these are respectively generalizations of the Fibonacci and Lucas numbers and are today referred to as the Lucas sequences.

If we select numbers P, Q such that $D = P^2 - 4Q \neq 0$, we define

$$U_n = U_n(P, Q) = \frac{\alpha^n - \beta^n}{\alpha - \beta} \quad \text{and} \quad V_n = V_n(P, Q) = \alpha^n + \beta^n, \tag{1}$$

where α, β are the zeros of $x^2 - Px + Q$. Note that $\alpha + \beta = P$ and $\alpha\beta = Q$. Also, $U_0 = 0$, $U_1 = 1$, $V_0 = 2$, $V_1 = P$. In addition both (U_n) and (V_n) satisfy the second order linear recurrence

$$X_{n+2} = PX_{n+1} - QX_n \quad (n \geq 0).$$

Thus, if P, Q are integers, then (U_n), (V_n) are both sequences of integers when $n \geq 0$.

By putting $P = 4$, $Q = 1$, Lucas was able to show that if $n > 1$, $n \equiv 1 \pmod 4$ and $s_1 = 4$, then M_n is a prime if $s_{n-1} \equiv 0 \pmod{M_n}$. Lucas' presentation of this result is somewhat confusing, but it seems that he was in possession of all the facts needed to prove it. Later, D. H. Lehmer [7] was able to prove the following result concerning A003010:

Theorem 2. *If $n \equiv 1 \pmod 2$, $n \geq 3$ and $s_1 = 4$, then M_n is a prime if and only if*

$$s_{n-1} \equiv 0 \pmod{M_n}.$$

This is the famous Lucas-Lehmer test for the primality of Mersenne numbers. It has been used to establish the primality of all known Mersenne numbers with $n > 127$. Lucas tried to prove this by putting $m = \frac{n-1}{2}$, $P = 2^{m+1}$, $Q = -1$, but while he got very close, he didn't quite complete the proof. Observe that $P^2 \equiv 2 \pmod{M_n}$. It is pointed out by Robinson in [9] that a similar test can be performed using the starting seed of $s_1 = 10$ (sequence A135927 in the OEIS); indeed, as discovered by Lehmer (see §5), any of the entries in A018844 is a valid starting value for a Lucas-Lehmer primality test like the one above.

Thus, we see by Theorem 1 that we can use $s_1 = 3$ to determine the primality of M_n whenever $n \equiv 3 \pmod 4$, but by Theorem 2, we can use $s_1 = 4$ to establish the primality of M_n when n is simply odd. The only real difference between the tests is the selection of the value of s_1. This suggests the following problem: Given some particular s_1, for what values of $n \geq 3$ does Assertion 3 hold?

Assertion 3. The Mersenne number M_n is a prime if and only if $s_{n-1} \equiv 0 \pmod{M_n}$.

We have seen that Assertion 3 holds for $n \equiv 3 \pmod 4$ whenever $s_1 = 3$ and that it holds for $n \equiv 1 \pmod 2$ whenever $s_1 = 4$. When Assertion 3 is true for a certain s_1, we say that s_1 is an *acceptable seed* for M_n. Since $n - 1 \geq 2$ and $s_2 = s_1^2 - 2$, we can always replace s_1 by $|s_1|$ with no loss of generality. Thus, we may assume that an acceptable seed is always nonnegative.

Because M_n can be a prime only when n is a prime, Jansen [6] calls a seed s_1 a *universal starting value* when it is acceptable for all (with a finite number of exceptions) M_n whenever n is a prime. Here we will be somewhat more general and define s_1 to be a *universal seed* if it is acceptable for all M_n with n odd and $n \geq 3$. Thus, 4 and 10 are universal seeds. In what follows we will find infinite families of universal seeds and we will also show how to determine those values of n for which a given integral value of s_1 is an acceptable seed for M_n.

2 The Lehmer sequences

In [7] Lehmer extended the Lucas sequences by permitting $P = \sqrt{R}$, where R and Q are coprime integers. By doing this he was able to have $D = R - 4Q \equiv 2$ or $3 \pmod 4$. We have

$$U_n = U_n(\sqrt{R}, Q), \quad V_n = V_n(\sqrt{R}, Q),$$

but if $\sqrt{R}$ is not an integer, (U_n) and (V_n) are no longer sequences of integers; however, when we set

$$\bar{U}_n = \bar{U}_n(\sqrt{R}, Q) = \begin{cases} U_n/\sqrt{R}, & \text{if } 2 \mid n; \\ U_n, & \text{if } 2 \nmid n, \end{cases}$$

$$\bar{V}_n = \bar{V}_n(\sqrt{R}, Q) = \begin{cases} V_n, & \text{if } 2 \mid n; \\ V_n/\sqrt{R}, & \text{if } 2 \nmid n, \end{cases}$$

then for $n \geq 0$ $(\bar{U}_n)$ and $(\bar{V}_n)$ are sequences of integers. We can deduce this by noting that

$$\bar{U}_0 = 0, \quad \bar{U}_1 = 1, \quad \bar{U}_2 = 1, \quad \bar{U}_3 = R - Q,$$
$$\bar{V}_0 = 2, \quad \bar{V}_1 = 1, \quad \bar{V}_2 = R - 2Q, \quad \bar{V}_3 = R - 3Q.$$

Also, it is easy to establish from (1) that both $(\bar{U}_n)$ and $(\bar{V}_n)$ satisfy the fourth order linear recurring sequence

$$X_{n+4} = (R - 2Q)X_{n+2} - Q^2 X_n \quad (n \geq 0). \tag{2}$$

Thus, we find by induction that $(\bar{U}_n)_{n\geq 0}$ and $(\bar{V}_n)_{n\geq 0}$ are sequences of integers. In what follows we will only consider $\bar{U}_n$ and $\bar{V}_n$ when $n \geq 0$.

Lehmer deduced a number of properties of $(\bar{U}_n)$ and $(\bar{V}_n)$, but we will only mention those that will be useful in this investigation. We first note the simple identities:

$$\bar{U}_{2n} = \bar{V}_n \bar{U}_n, \tag{3}$$

$$\bar{V}_{2n} = \begin{cases} \bar{V}_n^2 - 2Q^n, & \text{if } 2 \mid n; \\ R\bar{V}_n^2 - 2Q^n, & \text{if } 2 \nmid n. \end{cases} \tag{4}$$

Also, when $n \geq 0$, we have $\gcd(\bar{U}_n, \bar{V}_n) \mid 2$. If we put $R' = R - 4Q = D$ and $Q' = -Q$, then $\bar{V}_0(R', Q') = 2 = \bar{V}_0(R, Q)$, $\bar{V}_2(R', Q') = R' - 2Q' = \bar{V}_2(R, Q)$ and $(\bar{V}_n(R', Q'))$ satisfies (2) when $2 \mid n$. Thus, whenever n is even we have $\bar{V}_n(R', Q') = \bar{V}_n(R, Q)$ or

$$\bar{V}_n(R, Q) = \bar{V}_n(D, -Q), \tag{5}$$

a result also noted by Lehmer.

For a given odd prime p, we define the *rank of appearance of p in $(\bar{U}_n)$* to be the least positive integer $r = r(p)$ such that $p \mid \bar{U}_r$. Lehmer showed (Theorem 1.8) that if $r = r(p)$, then $p \mid \bar{U}_n$ if and only if $r(p) \mid n$. Of course, it is possible that $r(p)$ might not exist. However, he also showed (Theorem 1.9) that if p is odd and $p \nmid RQ$, then $r(p)$ does exist and $r(p) \mid p - \epsilon\sigma$, where ϵ is the Legendre symbol $(D|p)$ and σ is the Legendre symbol $(R|p)$. In addition (Theorem 4.9), if p is an odd prime and $p \nmid RQ$, then $p \mid \bar{V}_{(p-\epsilon\sigma)/2}$ if and only if $\sigma = -\tau$, where τ is the Legendre symbol $(Q|p)$. Let p be any odd prime such that $p \nmid Q$ and $p \mid R$. In this case it can be shown by using the reasoning in Section 1.4 of [7] that $r(p)$

exists and $r(p) = 2p$. Furthermore if $p \nmid Q$ and $p \mid D$, then since $p \mid R - 4Q$, we cannot have $p \mid R$. Thus $r(p)$ exists and $r(p) \mid p - \epsilon\sigma$, where $\epsilon = (D|p) = 0$. Thus, in this case, $r(p) = p$.

From these results we can prove the following primality result concerning M_n.

Lemma 4. *Let n be odd and $n \geq 3$. If $\gcd(M_n, Q) = 1$ and $M_n \mid \bar{V}_{\frac{M_n+1}{2}}(R, Q)$, then M_n must be a prime.*

Proof. By (3) we must have $M_n \mid \bar{U}_{M_n+1}(R, Q)$. If p is any prime divisor of M_n, then $p \nmid Q$ and $r = r(p)$ must exist in $(\bar{U}_n(R, Q))$. If $p \mid R$, then $r = 2p$ and $2p \mid M_n + 1$, which means that $2p \mid 2^n$, an impossibility. Thus, $p \nmid QR$ and $r \mid p - \epsilon\sigma$. Since $r \mid M_n + 1$ and $p \mid \bar{V}_{\frac{M_n+1}{2}}(R, Q)$, we cannot have $r \mid \frac{M_n+1}{2}$ because in this case $p \mid \gcd(\bar{V}_{\frac{M_n+1}{2}}, \bar{U}_{\frac{M_n+1}{2}}) \mid 2$ and $p = 2$, which means that $r = 2^n$. Since $r \mid p - \epsilon\sigma$, we must have $p = k2^n \pm 1 \geq 2^n - 1$. But $2^n > 3$ means that $2^{2n} > 3 \cdot 2^n \to (2^n - 1)^2 > M_n$. Thus, $p > \sqrt{M_n}$ and therefore M_n must be a prime. □

We also have a simple condition which guarantees that $M_n \mid \bar{V}_{\frac{M_n+1}{2}}(R, Q)$ when M_n is a prime.

Lemma 5. *Let n be odd, $n \geq 3$ and M_n be a prime. If the Legendre symbols*

$$(DR|M_n) = (QR|M_n) = -1,$$

then $M_n \mid \bar{V}_{\frac{M_n+1}{2}}(R, Q)$.

Proof. If M_n is a prime, then $(DR|M_n) = -1$ implies that $\epsilon\sigma = -1$. Also, since $\tau = -\sigma$, we have $M_n \mid \bar{V}_{\frac{M_n+1}{2}}(R, Q)$. □

We next produce a criterion for M_n to be a divisor of $\bar{V}_{\frac{M_n+1}{2}}(R, Q)$ when $\gcd(Q, M_n) = 1$, by providing a reformulation of the sequence $\bar{V}_{2^i}(R, Q)$ in terms of the sequence s_i. We first observe that $\frac{M_n+1}{2} = 2^{n-1}$. Suppose we put

$$s_i \equiv \bar{V}_{2^i}(R, Q)Q^{-2^{i-1}} \pmod{M_n},$$

where $QQ^{-1} \equiv 1 \pmod{M_n}$ and $i \geq 1$. By (4) we have

$$\bar{V}_{2^{i+1}}(R, Q) \equiv \bar{V}_{2^i}^2(R, Q) - 2Q^{2^i} \pmod{M_n}.$$

Thus,

$$Q^{2^i} s_{i+1} \equiv (Q^{2^{i-1}} s_i)^2 - 2Q^{2^i} \pmod{M_n}$$

and

$$s_{i+1} \equiv s_i^2 - 2 \pmod{M_n}.$$

It follows that if $s_1 \equiv \bar{V}_2(R, Q)/Q \equiv RQ^{-1} - 2 \pmod{M_n}$, then

$$s_{n-1} \equiv Q^{-2^{n-2}} \bar{V}_{2^{n-1}}(R, Q) \pmod{M_n}.$$

If we combine this observation with Lemmas 4 and 5, we get the following generalization of Theorem 2.

Theorem 6. *Let n be odd and $n \geq 3$. If the Jacobi symbols $(RD|M_n) = (RQ|M_n) = -1$ and $s_1 \equiv RQ^{-1} - 2 \pmod{M_n}$, then M_n is a prime if and only if $s_{n-1} \equiv 0 \pmod{M_n}$, where*

$$s_{i+1} \equiv s_i^2 - 2 \pmod{M_n}.$$

If we consider the case of $R = 2$, $Q = -1$, we have $D = 6$. We observe that

$$M_n \equiv -1 \pmod{8}.$$

Hence $(R|M_n) = 1$, $(Q|M_n) = -1$, $(D|M_n) = -(M_n|3)$. We have $-(M_n|3) = -1$ since n is odd and $M_n \equiv 1 \pmod 3$. Thus, $(DR|M_n) = (QR|M_n) = -1$, $s_1 \equiv -4 \pmod{M_n}$, and we can put $s_1 = 4$ to get Theorem 2. Notice that because $P^2 \equiv 2 \pmod{M_n}$ in Lucas' attempted proof of Theorem 2, this result of Lehmer is essentially the same as that of Lucas, except that Lehmer completed the proof. While Lehmer did not mention Theorem 6 explicitly, he might have been aware of it. In the next three sections we will use Theorem 6 to produce other values of s_1 for which theorems like Theorem 2 also hold.

3 Rational seeds and permissible triplets

Suppose a, b are integers such that $\gcd(b, M_n) = 1$. If $s_1 \equiv ab^{-1} \pmod{M_n}$ and s_1 is an acceptable seed for M_n, we say that $s_1 = \frac{a}{b}$ is an acceptable *rational* seed for M_n. In this section we will show that there exists an infinitude of distinct universal rational seeds for any given M_n with n odd and $n \geq 3$. In [6] Jansen gave $s_1 = \frac{2}{3}$ and $s_1 = \frac{626}{363}$ as examples of rational universal seeds. Indeed, as shown later in Section 4, Jansen's seeds can be considered as $s_1 \equiv RQ^{-1} - 2 \pmod{M_n}$ for some R, Q. Although it was not part of the main goal of [6], he also provided a technique for finding an infinitude of rational and even irrational universal starting values. These latter seeds can be written as polynomials over the rationals $\mathbb{Q}$ in $\sqrt{2}$. To express $\sqrt{2}$ as an integer modulo M_n, he suggested using $2^{\frac{n+1}{2}}$ which satisfies $(2^{\frac{n+1}{2}})^2 \equiv 2 \pmod{M_n}$. In this paper we will focus our attention on rational seeds only. We will next show how to find an infinitude of rational universal seeds, but we will make use of more elementary methods than those employed in [6].

Lemma 7. *Let n be odd, $n \geq 3$ and M_n be a prime. If r, d, q, X, Y, Z are integers such that $\gcd(M_n, Y) = 1$,*

$$4qY^2 = rX^2 - dZ^2 \tag{6}$$

and the Legendre symbols $(rd|M_n) = (qr|M_n) = -1$, then

$$M_n \mid \bar{V}_{\frac{M_n+1}{2}}(R, Q)$$

where $R = rX^2$, $Q = qY^2$ $(D = dZ^2)$.

Proof. If $M_n \mid X$, then $4qY^2 \equiv -dZ^2 \pmod{M_n}$. Since $(-4dq|M_n) = (-4|M_n)(rd|M_n)(qr|M_n) = -1$, we must have $M_n \mid Y$, which is impossible. Similarly, $M_n \nmid Z$. Thus,

$$(DR|M_n) = (QR|M_n) = -1$$

and $M_n \mid \bar{V}_{\frac{M_n+1}{2}}(R, Q)$ by Lemma 5. □

We can now combine the results of Theorem 6 and Lemma 7 to obtain a universal rational seed s_1: we need first to find values of r, q, d such that $(rd|M_n) = (rq|M_n) = -1$ for all odd $n \geq 3$. Since $(-1|M_n) = -1$ when $n \geq 2$, this means that we must have

$$(r|M_n) = (-d|M_n) = (-q|M_n) \tag{7}$$

for all odd $n \geq 3$. Also, since (6) must have integer solutions X, Y, Z, there is no loss of generality in assuming $\gcd(r, q, d) = 1$.

We have already observed that if n is odd and $n \geq 3$, then

$$(3|M_n) = -1, \quad (-1|M_n) = -1, \quad (2|M_n) = 1, \quad \text{and} \quad (6|M_n) = -1.$$

We can therefore restrict the values of r, d, q to be in $\mathcal{S} = \{-6, -3, -2, -1, 1, 2, 3, 6\}$ because, in these cases the value of the Jacobi symbol does not depend on n. However, we could also use, if they exist, values of a not in $\mathcal{S}$ such that $(a|M_n)$ has a fixed value not depending on n (≥ 3). A computer search up to 10^8 for such a number eliminated all possible values of a except for $a = 76627 = 19 \cdot 37 \cdot 109 \equiv -1 \pmod 4$. Notice that for this remaining value of a we have $2^{36} \equiv 1 \pmod a$. We then determined that $(a|M_n) = -1$ for all odd $n \geq 3$ by verifying that

$$(M_n|19)(M_n|37)(M_n|109) = 1$$

for all odd n such that $3 \leq n \leq 35$. This same number had been found earlier, but in a somewhat different context, by Vardhana (see [6, p. 13]).

We define a *permissible* triplet to be a triplet (r, q, d) such that r, q, $d \in \mathcal{S}$, $\gcd(r, q, d) = 1$, (7) holds, and (6) has integer solutions. Notice that if (a, b, c) is a permissible triplet, then so is $(-a, -b, -c)$ and $(c, -b, a)$. We may therefore always assume that $r > 0$. Furthermore, if $q < 0$, then we must have $d > 0$ and if $d < 0$, then we must have $q > 0$. Since $\#\mathcal{S} = 8$, there $512 = 8^3$ possible permissible triplets, but many of these can be eliminated. For example, if $r = 3$, $q = d = 1$, then (7) holds and (6) becomes

$$Z^2 = 3X^2 - 4Y^2.$$

We may assume here that $\gcd(X, Y, Z) = 1$. Since $3 \mid Z^2 + Y^2$, we can only have $3 \mid Z$ and $3 \mid Y$, but this means that $3 \mid X$, which is not possible. Similarly, if $r = 1$, $q = 3$, $d = -1$, we get

$$-Z^2 = X^2 - 12Y^2,$$

which also has no integer solutions. Indeed if (6) reduces to a Diophantine equation of the form $az^2 = x^2 + y^2$, where a is a fixed integer such that $3 \mid a$, but $9 \nmid a$, then (6) cannot have integer solutions.

If we put $r = 2$, $q = 3$, $d = -1$, we have (7); we put

$$R = 2X^2, \quad Q = 3Y^2, \quad D = -Z^2,$$

and (6) becomes

$$12Y^2 = 2X^2 + Z^2.$$

Here we must have $2 \mid Z$ and $2 \mid X$ from which we deduce that

$$(Z/2)^2 = 3Y^2 - 2(X/2)^2.$$

We now consider the Diophantine equation

$$z^2 = 3y^2 - 2x^2. \tag{8}$$

We can find by using standard techniques (see, for example, Chapter 7, Theorem 4 of [8]) that all integral solutions of (8) with $\gcd(x, y, z) = 1$ are given by

$$\begin{aligned} x &= (3t^2 + 2u^2 - 6tu)/\delta = (3(t-u)^2 - u^2)/\delta \\ y &= (3t^2 + 2u^2 - 4tu)/\delta = (2(t-u)^2 + t^2)/\delta \\ z &= (3t^2 - 2u^2)/\delta. \end{aligned}$$

Here t, u are coprime integer parameters and

$$\delta = \gcd(3t^2 - 2u^2, 3t^2 + 2u^2 - 4tu, 3t^2 + 2u^2 - 6tu).$$

It is easy to show that δ must be a divisor of 6. We see, then, that for r, q, $d \in \mathcal{S}$, (6) will have integer solutions only if we can put it in the form (8).

By subjecting each of the 512 possible triplets (r, q, d) to the above checks, we found that only 24 permissible triplets remain. These are:

$$\begin{gathered}(1,-2,3),(1,-2,6),(1,3,-2),(1,3,6),(1,6,-2),(1,6,3),(2,1,3),(2,-1,6),\\ (2,3,6),(2,6,3),(3,1,-6),(3,2,-6),\end{gathered}$$

with the remaining 12 produced by using the transformations $(a, b, c) \to (c, -b, a)$ and $(a, b, c) \to (-a, -b, -c)$. For example, $(1, -2, 3) \to (3, 2, 1)$ and $(3, 2, -6) \to (-6, -2, 3) \to (6, 2, -3)$.

4 Universal rational seeds

Returning to the permissible triple $(2, 3, -1)$, let t, u be integer parameters such that $\gcd(t, u) = 1$ and

$$X = 2(3t^2 + 2u^2 - 6tu)/\delta,$$
$$Y = (3t^2 + 2u^2 - 4tu)/\delta,$$

we see by Theorem 6 that if $\gcd(M_n, 3t^2 + 2u^2 - 4tu) = 1$, then M_n is a prime if and only if

$$s_{n-1} \equiv 0 \pmod{M_n}$$

when

$$s_1 \equiv RQ^{-1} - 2 \equiv \frac{8(3t^2 + 2u^2 - 6tu)^2}{3(3t^2 + 2u^2 - 4tu)^2} - 2 \pmod{M_n}.$$

If we put $t = u = 1$, we get $Q = 3$,

$$s_1 \equiv \frac{8}{3} - 2 = \frac{2}{3} \pmod{M_n};$$

if we put $t = 3$, $u = 4$, we get $Q = 3 \cdot 11^2$. Since in this latter case we have $\gcd(M_n, Q) = 1$ for odd n, we can use

$$s_1 \equiv \frac{8(-13)^2}{3(11)^2} - 2 = \frac{626}{363} \pmod{M_n}.$$

Indeed, it is well known (see, for example, Chapter 1 of Cox [3]) that if p is any prime such that $p \equiv 3 \pmod 8$, then there must exist integers t, u such that $p = t^2 + 2(t-u)^2$. Since $p \equiv 3 \pmod 8$, we have $(2|p) = -1$ which means that $p \nmid 2^n - 1$ or $\gcd(p, M_n) = 1$ whenever n is odd. Since there are infinitely many primes p satisfying $p \equiv 3 \pmod 8$, it follows that there exists an infinitude of pairs (t, u), with $\gcd(t, u) = 1$ and $p = 3t^2 + 2u^2 - 4tu$ such that the values assumed by $3t^2 + 2u^2 - 4tu$ are all distinct and

$$\gcd(M_n, 3(3t^2 + 2u^2 - 4tu)) = 1.$$

For such pairs we have

$$\gcd(3t^2 + 2u^2 - 4tu, 3t^2 + 2u^2 - 6tu) = \gcd(3t^2 + 2u^2 - 4tu, 2tu) = \gcd(p, 2tu) = 1.$$

It follows that there must exist an infinitude of distinct universal rational seeds.

We now consider the permissible triple $(3, 1, 2)$. Note that $(3, 1, 2) = (c, -b, a)$ when $(a, b, c) = (2, -1, 3)$, so

$$2Z^2 = 3X^2 - 4Y^2 \tag{9}$$

has an infinitude of integer solutions. Indeed, all integer solutions of (9) with $\gcd(X, Y, Z) = 1$ can be written as

$$X = 2(3t^2 + 2u^2 - 4tu)/\delta,$$
$$Z = 2(3t^2 + 2u^2 - 6tu)/\delta,$$
$$Y = (3t^2 - 2u^2)/\delta,$$

where t, u are coprime integer parameters and

$$\delta = \gcd(3t^2 + 2u^2 - 4tu, 3t^2 + 2u^2 - 6tu, 3t^2 - 2u^2).$$

Suppose we put

$$s_1 = R/Q - 2 = 3X^2/Y^2 - 2 = \frac{12(3t^2 + 2u^2 - 4tu)^2}{(3t^2 - 2u^2)^2} - 2$$

for any integer parameters t and u. We see that s_1 is an acceptable rational seed for all M_n with n odd and $n \geq 3$.

Let

$$\mathcal{C} = \{c : c = 3t^2 - 2u^2; t, u \in \mathbb{Z}; \gcd(t, u) = 1; \gcd(c, M_n) = 1 \text{ for all odd } n\}.$$

Note that 1 ($t = u = 1$), -2 ($t = 4$, $u = 5$), -5 ($t = 1$, $u = 2$), 19 ($t = 3$, $u = 2$) are in $\mathcal{C}$, so $\mathcal{C}$ is not empty. Indeed, we can assert that $\#\mathcal{C}$ is infinite. Let p be any prime such that $p \equiv 5$ or 19 (mod 24). We have $(6|p) = 1$, and consequently there exists some integer s such that $s^2 \equiv 6 \pmod{p}$. Let $\mathbb{K}$ denote the real quadratic field $\mathbb{Q}(\sqrt{6})$ with discriminant 24. The maximal order $\mathcal{O}$ of $\mathbb{K}$ is given by $\mathcal{O} = \mathbb{Z} + \sqrt{6}\mathbb{Z}$ and since $s^2 \equiv 6 \pmod{p}$, we see that the ideal $\mathfrak{p} = p\mathbb{Z} + (s + \sqrt{6})\mathbb{Z}$ is a prime ideal of $\mathcal{O}$ with norm $N(\mathfrak{p}) = p$. Also, $\mathfrak{t} = 2\mathbb{Z} + \sqrt{6}\mathbb{Z}$ is a prime ideal of $\mathcal{O}$ with $\mathfrak{t}^2 =$ the principal ideal (2) and $N(\mathfrak{t}) = 2$. Since the class number of $\mathbb{K}$ is 1, we know that the ideal $\mathfrak{m} = \mathfrak{t}\mathfrak{p}$ must be principal. Thus, there must exist some u', $t \in \mathbb{Z}$ and $\mu = u' + t\sqrt{6} \in \mathcal{O}$ such that $\mathfrak{m} = (\mu)$ and

$$2p = N(\mathfrak{m}) = |N(\mu)| = |u'^2 - 6t^2|.$$

Putting $u = u'/2$, we have

$$p = |2u^2 - 3t^2|$$

and $\gcd(t, u) = 1$. Since $(2|p) = -1$, we must, as noted earlier, have $\gcd(p, M_n) = 1$ for all odd n. Thus, either p or $-p$ must be in $\mathcal{C}$ and as there exists an infinitude of p, we see that $\#\mathcal{C}$ is infinite.

For each $c \in \mathcal{C}$, we have

$$s_1 = \frac{12(3t^2 + 2u^2 - 4tu)^2}{(3t^2 - 2u^2)^2} - 2 = \frac{12(c + 4u(u - t))^2}{c^2} - 2.$$

If we let s be any prime divisor of $\gcd(c, c + 4u(u - t))$, it is easy to show that $s \mid t$ and $s \mid u$, which is impossible by selection of c. Thus, we must have $\gcd(c, c + 4u(u - t)) = 1$, and therefore there must exist an infinitude of distinct rational values of s_1, each corresponding to some $c \in \mathcal{C}$.

We now make use of a result that goes back to Euler. Suppose that a, b, c are integers where $ab > 1$ and ab is not a perfect integral square. It is well known that the Pellian equation (see [5, Corollary 1.10] or [4, p. 377])

$$x^2 - aby^2 = 1 \tag{10}$$

has an infinitude of integer solutions (x_k, y_k) given by

$$x_k + \sqrt{ab}y_k = (x_1 + \sqrt{ab}y_1)^k,$$

where (x_1, y_1) is the *fundamental solution* (that solution (x, y) for which $x,\ y > 0$ and $x + y\sqrt{ab}$ is least) of (10). For example, if $ab = 6$, then it is easy to verify that $x_1 = 5$, $y_1 = 2$. The next result is an observation of Euler (see [4, p. 408]).

Theorem 8. *Let a, b be specified as above. If (T_1, U_1) is any given solution of the Diophantine equation*

$$aT^2 - bU^2 = c, \tag{11}$$

then there exists an infinitude of distinct solutions of (11) given by (T_k, U_k), where

$$\sqrt{a}T_k + \sqrt{b}U_k = (\sqrt{a}T_1 + \sqrt{b}U_1)(x_1 + \sqrt{ab}y_1)^{k-1}.$$

That is, $T_k = T_1x_{k-1} + bU_1y_{k-1}$, $U_k = aT_1y_{k-1} + U_1x_{k-1}$.

Notice that the sequences (T_k) and (U_k) both satisfy the linear recurrence

$$W_{k+2} = 2x_1W_{k+1} - W_k.$$

Suppose now that t_1, u_1 are some positive integers such that

$$3t_1^2 - 2u_1^2 = c$$

for some constant $c \in \mathcal{C}$. In this case we find that if we put

$$\sqrt{3}t_k + \sqrt{2}u_k = (\sqrt{3}t_1 + \sqrt{2}u_1)(5 + 2\sqrt{6})^{k-1} \quad (k \geq 1),$$

we get

$$t_2 = 5t_1 + 4u_1, \quad u_2 = 6t_1 + 5u_1$$

and

$$t_{j+2} = 10t_{j+1} - t_j, \quad u_{j+2} = 10u_{j+1} - u_j \quad (j \geq 1).$$

Also, for any $k \geq 1$

$$3t_k^2 - 2u_k^2 = c.$$

Furthermore, it is clear that the sequences (u_k) and $(u_k - t_k)$ are both strictly increasing with increasing k.

Putting

$$Y_k = (3t_k^2 - 2u_k^2)/\delta = c/\delta,$$

we get

$$\begin{aligned} X_k &= 2(3t_k^2 + 2u_k^2 - 4t_ku_k)/\delta \\ &= 2(c + 4u_k(u_k - t_k))/\delta. \end{aligned}$$

Thus, if for any fixed $k \geq 1$, we put

$$s_1 = RQ^{-1} - 2 = 3X_k^2 Y_k^{-2} - 2 = 12(c + 4u_k(u_k - t_k))^2/c^2 - 2, \tag{12}$$

then s_1 is a universal rational seed for M_n. Notice that $c+4u_k(u_k-t_k)$ is a strictly increasing function of k; thus, for each fixed $c \in \mathcal{C}$ there exists an infinitude of distinct universal rational seeds s_1 for M_n. Since there exists an infinitude of distinct $c \in \mathcal{C}$, we see that (12) is a doubly parametric set of distinct rational universal seeds s_1 for M_n for all odd $n \geq 3$.

Suppose we put

$$\begin{aligned}
\delta f_1(t,u) &= 3t^2 + 2u^2 - 6tu \\
\delta f_2(t,u) &= 3t^2 + 2u^2 - 4tu \\
\delta f_3(t,u) &= 3t^2 - 2u^2,
\end{aligned}$$

where, as earlier, $\delta = \gcd(3t^2 + 2u^2 - 6tu, 3t^2 + 2u^2 - 4tu, 3t^2 - 2u^2)$. We have

$$\gcd(f_1, f_2, f_3) = 1 \tag{13}$$

and

$$f_3^2 = 3f_2^2 - 2f_1^2, \tag{14}$$

where we write f_i for $f_i(t,u)$ $(i = 1,2,3)$. It turns out that we can find four families of universal rational seeds. These can be expressed as:

$$s_1 = 8f_1^2/3f_2^2 - 2$$

for each of the permissible triples $(2,3,-1)$, $(3,2,-6)$, $(6,1,-3)$, $(1,6,2)$;

$$s_1 = 12f_2^2/f_3^2 - 2$$

for $(1,3,6)$, $(1,-2,6)$, $(2,-1,3)$, $(2,6,3)$, $(3,-6,2)$, $(3,1,2)$, $(6,-3,1)$, $(6,2,1)$;

$$s_1 = 4f_3^2/3f_2^2 - 2$$

for $(1,3,2)$, $(2,6,-1)$, $(3,1,-6)$, $(6,2,-3)$;

$$s_1 = 6f_2^2/f_1^2 - 2$$

for $(1,-2,3)$, $(1,6,3)$, $(2,-1,6)$, $(2,3,6)$, $(3,-6,1)$, $(3,2,1)$, $(6,-3,2)$, $(6,1,2)$. Each of these families represents an infinitude of distinct universal rational seeds.

If $s_1 = 8f_1^2/3f_2^2 - 2$ or $s_1 = 4f_3^2/3f_2^2 - 2$ and s_1 is an integer, then $3 \mid f_1$ or $3 \mid f_3$. In either case, because of (14) we must have $3 \mid \gcd(f_1, f_2, f_3)$, which is impossible by (13). Thus, if $s_1 = 12f_2^2/f_3^2 - 2$ is an integer, then $f_3 \mid 2f_2$. If $2 \mid f_3$, then by (14) we get $2 \mid f_2$ and then $2 \mid f_1$, which is impossible. Hence $f_3 \mid f_2$ and by (14) $f_3 \mid f_1$, which means that $|f_3| = 1$ and we get

$$s_1 = 12f_2^2 - 2 = 8f_1^2 + 2.$$

Similarly, if $s_1 = 6f_2^2/f_1^2 - 2 \in \mathbb{Z}$, then

$$s_1 = 6f_2^2 - 2 = 2f_3^2 + 2.$$

In the next section we constrain the values of admissible seeds to be integral.

5 Integral seeds

We have already seen that we can assume an acceptable seed for M_n when $n \geq 3$ is nonnegative. For integral values of s_1, we have $|s_i| \leq 2$ for all $i \geq 1$ whenever $s_1 = 0, 1, 2$. Thus we may assume further that a universal integral seed s_1 for M_n ($n \geq 3$) must be such that $s_1 \geq 3$

In section 5 of [7] Lehmer considered the case of n odd, $n \geq 3$ and $Q = 1$, $R = -X^2$, $-2X^2$, $3X^2$, $6X^2$ and $D = Z^2$, $2Z^2$, $-3Z^2$, $-6Z^2$. On referring to (5) (by interchanging the values of R and D we can get $Q = -1$) he found that the only Diophantine equations (6) that had solutions which could be produced from these values of R and D, subject to the constraint that $D - R = -4$, are

$$2Z^2 - 3X^2 = -4 \quad (R = 3X^2,\ D = 2Z^2),$$

and

$$2Z^2 - 6X^2 = -4 \quad (R = 6X^2,\ D = 2Z^2).$$

These correspond to the permissible triples $(3, 1, 2)$ and $(6, 1, 2)$. There can be no solution of (6) for $(6, 1, -3)$ or $(3, 1, -6)$ because 3 must be a divisor of Q in these cases and this is not possible because $Q = 1$. Each of these Diophantine equations has an infinitude of integer solutions. In the case of the first equation, we get

$$X = 2w_k, \quad Z = z_k \quad (k \geq 1),$$

where

$$3w_k^2 - 2z_k^2 = 1.$$

Here we can put $w_1 = 1$, $w_2 = 9$ and $w_{j+2} = 10w_{j+1} - w_j$ ($j \geq 1$) and

$$s_1 = 12w_k^2 - 2.$$

In the case of the second equation, we get

$$X = w_k \quad (k \geq 1),$$

where $w_1 = 1$, $w_2 = 3$, $w_{j+2} = 4w_{j+1} - w_j$ ($j \geq 1$) and

$$s_1 = 6w_k^2 - 2.$$

Thus, there exists an infinitude of universal integral seeds for all M_n with n odd and $n \geq 3$. For such s_1, we have

$$s_1 \in \{4, 10, 52, 724, 970, 10084, 95050, \ldots\}.$$

If we consider $s_1 = 3$, we know that s_1 is acceptable for all M_n with $n \equiv 3 \pmod 4$. We now consider the problem of finding other values of s_1 which are acceptable for such M_n. We first observe that

$$M_n = 2^{4m+3} - 1 \equiv 2 \pmod 5.$$

Thus, $(M_n|5) = (2|5) = -1$. We can then put $R = 5X^2$, $Q = 1$ and $D = Z^2$ and derive the Diophantine equation

$$Z^2 - 5X^2 = -4.$$

The well-known Fibonacci numbers $(F_k)_{k\geq 0}$ and the Lucas numbers $(L_k)_{k\geq 0}$ each satisfy the linear recurrence

$$X_{k+2} = X_{k+1} + X_k,$$

with $F_0 = 0$, $F_1 = 1$, $L_0 = 2$, $L_1 = 1$. Furthermore, we also know that

$$L_k^2 - 5F_k^2 = 4(-1)^k.$$

It follows that if we put $s_1 = 5F_k^2 - 2 = L_k^2 + 2$ for odd k, then

$$s_1 \in \{3, 18, 123, 843, \ldots\}$$

is acceptable for all M_n with $n \equiv 3 \pmod 4$. However, these are not the only such seeds. If we put $R = 10X^2$, $Q = 1$, $D = Z^2$, then we can show that if $w_0 = 0$, $w_1 = 6$ and

$$w_{k+2} = 38w_{k+1} - w_k,$$

then $s_1 = 40w_j^2 - 2$ $(j \geq 1)$ is also such a seed. Furthermore, such a value for s_1 can never be of the form $5F_k^2 - 2$ for any $k \geq 1$.

In the next section we will turn our attention to the problem of finding those values of n for which a given integral s_1 is an acceptable seed for M_n.

6 Acceptable integral seeds

We begin by stating a simple criterion for a given s_1 to be an acceptable integral seed for M_n. This criterion is given in a more general setting as Theorem 2.1 of [6].

Theorem 9. *Let s_1 be a given integer, then s_1 is an acceptable seed for M_n if and only if*

$$(s_1 + 2|M_n) = -1 \quad \textit{and} \quad (s_1 - 2|M_n) = 1.$$

Proof. Let R, Q be integers such that $\gcd(Q, M_n) = 1$ and $s_1 + 2 \equiv RQ^{-1} \pmod{M_n}$. We have

$$\begin{aligned} Q(s_1 + 2) &\equiv R \pmod{M_n}, \\ Q(s_1 - 2) &\equiv R - 4Q = D \pmod{M_n}. \end{aligned}$$

Thus,

$$(RQ|M_n) = (Q^2(s_1 + 2)|M_n) = (s_1 + 2|M_n)$$

and

$$(RD|M_n) = (Q^2(s_1 + 2)(s_1 - 2)|M_n) = (s_1 + 2|M_n)(s_1 - 2|M_n).$$

We have $(RQ|M_n) = -1$ and $(RD|M_n) = -1$ if and only if

$$(s_1 + 2|M_n) = -1 \quad \text{and} \quad (s_1 - 2|M_n) = 1,$$

and therefore by Theorem 6, Assertion 3 holds for M_n. □

If N is any positive integer, we can write $N = m^2k$, where m^2 is the largest possible square divisor of N. We call the positive squarefree integer k here the *squarefree part* of N and denote this by

$$k = \text{sfp}(N).$$

For example, $1 = \text{sfp}(9)$, $5 = \text{sfp}(20)$, $3 = \text{sfp}(27)$, $10 = \text{sfp}(360)$. We now define for a given positive integer N

$$N^* = \begin{cases} \text{sfp}(N), & \text{when } 2 \nmid \text{sfp}(N); \\ \text{sfp}(N)/2, & \text{when } 2 \mid \text{sfp}(N). \end{cases}$$

Note that N^* is positive, odd and if $\gcd(N, M_n) = 1$, then

$$(N|M_n) = (N^*|M_n).$$

We next put $s_1^+ = (s_1 + 2)^*$ and $s_1^- = (s_1 - 2)^*$ and observe that $\gcd(s_1^-, s_1^+) = 1$. We can write

$$2^\alpha m_1^2 s_1^- = s_1 - 2, \quad 2^\beta m_2^2 s_1^+ = s_1 + 2, \tag{15}$$

where m_1, m_2 are odd integers and α, $\beta \geq 0$. Also, if s_1 is an acceptable seed for M_n, then by Theorem 9

$$-1 = (s_1 + 2|M_n) = (2^\beta m_2^2 s_1^+|M_n) = (s_1^+ m_2^2|M_n).$$

Thus, if $s_1^+ = 1$, we cannot have s_1 as an acceptable seed for M_n. For example, $s_1 = 7$, 14, 16, 23, ... cannot be acceptable seeds for M_n with odd $n \geq 3$.

We next prove a theorem which is suggested by the results in Section 5.

Theorem 10. *Let s_1 be any acceptable seed for M_n and define s_1^-, s_1^+ as above. There exists an infinitude of distinct acceptable seeds S_1 for M_n such that $S_1^- = s_1^-$, $S_1^+ = s_1^+$.*

Proof. We let α, β, s_1^-, s_1^+ be defined as in (15). If we put $a = 2^\alpha s_1^-$ and $b = 2^\beta s_1^+$, then (m_1, m_2) is a solution of

$$ax^2 - by^2 = c, \tag{16}$$

where $c = -4$. Since we must have $s_1^+ > 1$, we must have $ab > 1$ and ab cannot be a perfect integral square. By Theorem 8, we know there must exist an infinitude of distinct solutions to (16). If we let (X, Y) be one of these, we can put

$$S_1 = 2^\alpha s_1^- X^2 + 2 = 2^\beta s_1^+ Y^2 - 2.$$

Hence,

$$S_1^- = (S_1 - 2)^* = s_1^- \quad \text{and} \quad S_1^+ = (S_1 + 2)^* = s_1^+.$$

□

Let

$$s_1^+ = (s_1+2)^* = \prod_{i=1}^{j} q_i \quad \text{and} \quad s_1^- = (s_1-2)^* = \prod_{i=1}^{k} r_i,$$

where r_i $(i = 1, 2, \ldots, k)$, q_i $(i = 1, 2, \ldots, j)$ are distinct odd primes. For any odd prime p we define $\eta_n(p)$ to be the value of the Legendre symbol $(2^n - 1|p) = (M_n|p)$. By quadratic reciprocity we have

$$\begin{aligned}(s_1^+|M_n) &= (-1)^{\frac{s_1^+-1}{2}}(M_n|s_1^+) \\ &= (-1)^{\frac{s_1^+-1}{2}} \prod_{i=1}^{j} \eta_n(q_i)\end{aligned}$$

and

$$(s_1^-|M_n) = (-1)^{\frac{s_1^--1}{2}} \prod_{i=1}^{k} \eta_n(r_i).$$

It follows from Theorem 9 that s_1 is an acceptable seed for M_n if and only if

$$s_1^- = 1 \quad \text{or} \quad \prod_{i=1}^{k} \eta_n(r_i) = (-1)^{\frac{s_1^--1}{2}} \quad \text{when } s_1^- > 1 \quad \text{and} \quad \prod_{i=1}^{j} \eta_n(q_i) = (-1)^{\frac{s_1^++1}{2}}. \tag{17}$$

For any odd integer m, we define $\omega(m)$ to be the order of 2 modulo m; that is, $\omega(m)$ is the least positive integer k such that $2^k \equiv 1 \pmod{m}$. Such a value of k always exists and $k \mid \phi(m)$, where ϕ is the the Euler totient function. It is easy to establish the following proposition.

Proposition 11. *If m_1 and m_2 are odd integers such that $\gcd(m_1, m_2) = 1$, then*

$$\omega(m_1 m_2) = \operatorname{lcm}(\omega(m_1)\omega(m_2)).$$

We next observe that

$$\eta_n(p) = \eta_m(p)$$

if $n \equiv m \pmod{\omega(p)}$. For any positive integer m, we define

$$\Omega(m) = \begin{cases} 2\omega(m), & \text{when } 2 \nmid \omega(m); \\ \omega(m), & \text{otherwise.} \end{cases}$$

Put $\Omega = \Omega(s_1^- s_1^+)$ and

$$\mathcal{A}(s_1) = \{n \pmod{\Omega} : n \text{ odd}, 1 \le n < \Omega, (17) \text{ holds}\}.$$

It is not difficult to see that s_1 is an acceptable seed for M_n if and only if $n \equiv m \pmod{\Omega}$ for some $m \in \mathcal{A}(s_1)$. For example, consider $s_1 = 37$; we have $s_1^- = 35$ and $s_1^+ = 39$. Also,

$\omega(5) = 4$, $\omega(7) = 3$, $\omega(3) = 2$ and $\omega(13) = 12$. Hence, $\omega(s_1^-) = \omega(s_2^+) = 12$ and $\Omega = 12$. We consider the odd values of n (mod 12) and find that (17) holds only for $n \equiv 7 \pmod{12}$. Thus, $\mathcal{A}(37) = \{7\}$. It follows that 37 is an acceptable seed for M_n if and only if $n \equiv 7 \pmod{12}$. During the process of testing whether (17) holds, we found that $\eta_3(7) = (2^3 - 1|7) = 0$ and $\eta_9(7) = (2^9 - 1|7) = 0$. Indeed, we have the following proposition.

Proposition 12. *Let p be either r_i $(i = 1, 2, \ldots, k)$ or q_i $(i = 1, 2, \ldots, j)$. If $\eta_n(p) = 0$, then* $\gcd(n, \Omega) > 1$.

Proof. We have $\omega(p) \mid \Omega$ and $p \mid 2^n - 1$. Since $\omega(p) > 1$ and $\omega(p) \mid n$, we have $\gcd(n, \Omega) > 1$. □

As we shall see below, the converse of this result is not true.

We also observe that if $d = \gcd(n, \Omega)$, then $2^d - 1 \mid 2^n - 1$ and M_n cannot be a prime. Thus, before testing (17), we could eliminate all values of n from $\mathcal{A}(s_1)$ when $\gcd(n, \Omega) \neq 1$. We can now define

$$\mathcal{A}'(s_1) = \{n \pmod{\Omega} : \gcd(n, \Omega) = 1,\ 1 \leq n < \Omega,\ (17) \text{ holds}\}.$$

We see that $\mathcal{A}'(s_1) \subseteq \mathcal{A}(s_1)$, but $\mathcal{A}'(s_1) \neq \mathcal{A}(s_1)$ for infinitely many values of s_1. For example, if $s_1 = 9$, then $s_1^- = 7$, $s_1^+ = 11$ and $\Omega = 30$. Thus,

$$\mathcal{A}(s_1) = \{5, 11, 29\}, \quad \text{but} \quad \mathcal{A}'(s_1) = \{11, 29\}.$$

Suppose $2 \mid m$. In what follows we will denote by $\mathcal{T}(m)$, resp. $\mathcal{R}(m)$, the set of all odd residues modulo m, resp. the set of reduced residues modulo m. That is,

$$\mathcal{T}(m) = \{n \pmod{m} : n \text{ odd},\ 1 \leq n < m\},$$
$$\mathcal{R}(m) = \{n \pmod{m} : \gcd(n, m) = 1,\ 1 \leq n < m\}.$$

Since m is even, we have $\#\mathcal{T}(m) = m/2$ and $\#\mathcal{R}(m) = \phi(m)$. Hence

$$\#A(s_1) \leq \#\mathcal{T}(\Omega) = \Omega/2 \tag{18}$$

and

$$\#A'(s_1) \leq \#\mathcal{R}(\Omega) = \phi(\Omega). \tag{19}$$

If we define $l(s_1) = \#A(s_1)$, resp. $l' = \#A'(s_1)$ and put

$$q = q(s_1) = \frac{2l(s_1)}{\Omega}, \quad q' = q'(s_1) = \frac{l'(s_1)}{\phi(\Omega)}$$

we see by (18) and (19) that $q,\ q' \leq 1$. Furthermore, q represents the proportion of all possible values of n ($n \geq 3$, n odd) which can be acceptable seeds for M_n. Thus, if $q(s_1) = 1$, then s_1 is a universal seed for M_n. Since $\mathcal{R}(\Omega) \subseteq \mathcal{T}(\Omega)$, we see that if $q(s_1) = 1$, then $q'(s_1) = 1$. It follows that if $q'(s_1) \neq 1$, then $q(s_1) \neq 1$, an observation we will make use of in Section 8.

7 Some computational results

We begin with some examples. If $s_1 = 4$, then $s_1^- = 1$ and $s_1^+ = 3$. We get $\Omega = 2$, $\mathcal{A}(4) = \{1\}$, $l = 1$ and $q = q(4) = 1$. If $s_1 = 3$, then $s_1^- = 1$ and $s_1^+ = 5$. We get $\Omega = 4$, $\mathcal{A}(3) = \{3\}$, $l = 1$ and $q = q(3) = 1/2$. That is, 3 is an acceptable seed for M_n for 1/2 of all the possible values of n ($n \equiv 3 \pmod 4$). If $s_1 = 22$, then $s_1^- = 5$, $s_1^+ = 3$, $\Omega = 4$, $\mathcal{A}(22) = \{1\}$; that is, 22 is an acceptable seed for 1/2 of all the possible M_n (in this case those for which $n \equiv 1 \pmod 4$). If $s_1 = 20$, then $s_1^- = 1$ and $s_1^+ = 11$. We get $\Omega = 10$, $\mathcal{A}(20) = \{1, 5, 9\}$, $l = 3$ and $q = q(20) = 3/5$. Thus, $s_1 = 20$ is an acceptable seed for M_n for 3/5 of all the possible values of n. This is not as good as the case of $s_1 = 4$, but is better than $s_1 = 3$.

The above process was programmed on a computer, and the following tables were produced.

s_1	s_1^-	s_1^+	Ω	$\mathcal{A}(s_1)$	l	q
3	1	5	4	$\{3\}$	1	1/2
4	1	3	2	$\{1\}$	1	1
9	7	11	30	$\{5, 11, 29\}$	3	1/5
10	1	3	2	$\{1\}$	1	1
11	1	13	12	$\{3, 5, 11\}$	3	1/2
12	5	7	12	$\{1\}$	1	1/6
13	11	15	20	$\{13, 17\}$	2	1/5
15	13	17	24	$\{13, 19, 21\}$	3	1/4
17	15	19	36	$\{3, 15, 19, 27, 35\}$	5	5/18
18	1	5	4	$\{3\}$	1	1/2
19	17	21	24	$\{17, 23\}$	2	1/6
20	1	11	10	$\{1, 5, 9\}$	3	3/5
21	19	23	198	$\{5, 7, 13, 23, 29, 41, 49, 67, 79, 85, 95,$	20	20/99
				$101, 115, 133, 137, 139, 151, 155, 167, 173\}$		
22	5	3	4	$\{1\}$	1	1/2
24	11	13	60	$\{3, 17, 23, 27, 47, 53\}$	6	1/5
25	23	3	22	$\{3, 9, 15, 17, 21\}$	5	5/11
27	1	29	28	$\{5, 7, 9, 11, 15, 25, 27\}$	7	1/2
28	13	15	12	$\{1, 9\}$	2	1/3
31	29	33	140	$\{3, 13, 17, 23, 47, 57, 73, 77, 87, 97, 103, 107, 113, 133\}$	14	1/5
32	15	17	8	$\{3\}$	1	1/4
33	31	35	60	$\{37, 47, 49, 59\}$	4	2/15
35	33	37	180	$\{5, 15, 25, 29, 35, 41, 49, 51, 61, 65, 69, 71, 85, 89, 99,$	27	3/10
				$101, 105, 121, 125, 135, 141, 149, 159, 161, 169, 171, 179\}$		
36	17	19	72	$\{1, 9, 15, 17, 33, 39, 55, 57, 63, 71\}$	10	5/18
37	35	39	12	$\{7\}$	1	1/6

38	1	5	4	$\{3\}$	1	1/2
39	37	41	180	$\{3, 9, 11, 23, 31, 37, 43, 57, 83, 91, 103, 109, 111,$	18	1/5
				$117, 129, 131, 151, 163\}$		
40	19	21	18	$\{5, 11\}$	2	2/9
41	39	43	84	$\{5, 15, 23, 27, 29, 35, 41, 47, 51, 63, 65, 71, 75, 77, 83\}$	15	5/14
42	5	11	20	$\{1, 5, 9\}$	3	3/10
43	41	5	20	$\{7, 15, 19\}$	3	3/10
44	21	23	66	$\{1, 7, 13, 19, 49\}$	5	5/33
45	43	47	322	$\{3, 25, 39, 81, 87, 95, 129, 157, 171, 179, 185, 199,$	22	22/161
				$213, 221, 249, 255, 263, 269, 277, 291, 305, 311\}$		
46	11	3	10	$\{3, 7\}$	2	2/5
49	47	51	184	$\{7, 9, 17, 31, 55, 57, 63, 73, 89, 97, 103, 105,$	22	11/46
				$113, 119, 135, 137, 143, 145, 151, 159, 169, 183\}$		
51	1	53	52	$\{5, 7, 9, 11, 17, 23, 27, 31, 33, 37, 39, 49, 51\}$	13	1/2
52	1	3	2	$\{1\}$	1	1
53	51	55	40	$\{3, 5, 21, 27, 29\}$	5	1/4
54	13	7	12	$\{1, 7\}$	2	1/3
55	53	57	468	$\{13, 25, 29, 41, 43, 47, 65, 67, 77, 95, 97, 119, 133, 139,$	52	2/9
				$149, 151, 157, 169, 175, 185, 191, 203, 209, 211, 221,$		
				$223, 227, 229, 263, 275, 281, 295, 301, 313, 331, 337,$		
				$347, 353, 355, 365, 367, 383, 385, 389, 407, 409, 419,$		
				$437, 445, 457, 461, 463\}$		

Table 1: Values for s_1 up to 55.

s_1	s_1^-	s_1^+	Ω	l	q	s_1	s_1^-	s_1^+	Ω	l	q
3	1	5	4	1	1/2	598	149	3	148	37	1/2
4	1	3	2	1	1	650	1	163	162	41	41/81
10	1	3	2	1	1	673	671	3	60	15	1/2
11	1	13	12	3	1/2	678	1	85	8	2	1/2
18	1	5	4	1	1/2	724	1	3	2	1	1
20	1	11	10	3	3/5	731	1	733	244	61	1/2
22	5	3	4	1	1/2	786	1	197	196	49	1/2
27	1	29	28	7	1/2	843	1	5	4	1	1/2
38	1	5	4	1	1/2	862	215	3	28	7	1/2
51	1	53	52	13	1/2	884	1	443	442	111	111/221
52	1	3	2	1	1	963	1	965	96	24	1/2
66	1	17	8	2	1/2	970	1	3	2	1	1
74	1	19	18	5	5/9	1012	505	3	100	30	3/5

83	1	85	8	2	1/2	1026	1	257	16	4	1/2
100	1	51	8	2	1/2	1060	1	59	58	15	15/29
102	1	13	12	3	1/2	1081	1079	3	492	123	1/2
106	13	3	12	3	1/2	1091	1	1093	364	91	1/2
123	1	5	4	1	1/2	1174	293	3	292	73	1/2
145	143	3	60	15	1/2	1227	1	1229	1228	307	1/2
146	1	37	36	9	1/2	1252	1	627	90	23	23/45
164	1	83	82	21	21/41	1298	1	13	12	3	1/2
171	1	173	172	43	1/2	1348	673	3	48	14	7/12
202	1	51	8	2	1/2	1354	1	339	28	10	5/7
214	53	3	52	13	1/2	1371	1	1373	1372	343	1/2
227	1	229	76	19	1/2	1446	1	181	180	45	1/2
244	1	123	20	6	3/5	1450	181	3	180	45	1/2
291	1	293	292	73	1/2	1460	1	731	56	14	1/2
292	145	3	28	8	4/7	1523	1	61	60	15	1/2
298	37	3	36	9	1/2	1602	1	401	200	50	1/2
340	1	19	18	5	5/9	1684	1	843	70	19	19/35
382	95	3	36	9	1/2	1732	865	3	172	44	22/43
394	1	11	10	3	3/5	1766	1	221	24	6	1/2
402	1	101	100	25	1/2	1802	1	451	20	6	3/5
452	1	227	226	57	57/113	1851	1	1853	72	18	1/2
484	241	3	24	6	1/2	1924	1	107	106	27	27/53
486	1	61	60	15	1/2	1938	1	485	48	12	1/2
531	1	533	60	15	1/2	1942	485	3	48	12	1/2
580	1	291	48	14	7/12						

Table 2: Values for s_1 up to 2000, where $q \geq 1/2$.

s_1	s_1^-	s_1^+	Ω	l	q	s_1	s_1^-	s_1^+	Ω	l	q
4	1	3	2	1	1	1252	1	627	90	23	23/45
10	1	3	2	1	1	1348	673	3	48	14	7/12
20	1	11	10	3	3/5	1354	1	339	28	10	5/7
52	1	3	2	1	1	1684	1	843	70	19	19/35
74	1	19	18	5	5/9	1732	865	3	172	44	22/43
164	1	83	82	21	21/41	1802	1	451	20	6	3/5
244	1	123	20	6	3/5	1924	1	107	106	27	27/53
292	145	3	28	8	4/7	2180	1	1091	1090	273	273/545
340	1	19	18	5	5/9	2644	1321	3	60	22	11/15
394	1	11	10	3	3/5	2698	336	3	42	12	4/7

452	1	227	226	57	57/113	3044	1	1523	1522	381	381/761
580	1	291	48	14	7/12	3202	1	89	22	8	8/11
650	1	163	162	41	41/81	3466	433	3	72	22	11/18
724	1	3	2	1	1	3530	1	883	882	221	221/441
884	1	443	442	111	111/221	3748	1873	3	936	242	121/234
970	1	3	2	1	1	4052	1	2027	2026	507	507/1013
1012	505	3	100	30	3/5	4420	1	2211	330	83	83/165
1060	1	59	58	15	15/29	4610	1	1153	288	76	19/36

Table 3: Values for s_1 up to 5000, where $q > 1/2$.

On examining Table 3, we see that seeds s_1 producing values of q such that $1 > q > 1/2$ do occur, but are not frequent. It is of some interest to consider the case of $s_1 = 3202$ where $\Omega = 22$ and $q = 8/11$. Here we have

$$\mathcal{A}(s_1) = \{3, 5, 7, 9, 13, 15, 17, 19\},$$

which is the set of all possible integers k in $\mathcal{T}(\Omega)$, except for $k = 1$, 11 and $k = 21$ $(= 22-1)$. Note that for any odd prime p such that $\omega(p) \mid \Omega$

$$(2^{\Omega-n} - 1|p) = (-2^n|p)(2^n - 1|p) = (-2|p)(2^n - 1|p). \tag{20}$$

Since for $p \equiv 1 \pmod 8$, we have $(-2|p) = 1$, we see that

$$(2^{\Omega-n} - 1|p) = (2^n - 1|p)$$

in this case. Thus, putting $n = 1$, we find that

$$(2^{21} - 1|89) = (2^1 - 1|89) = 1 \neq (-1)^{\frac{89+1}{2}}.$$

Also, $89 \mid 2^{11} - 1$. Hence, *a priori* we could not have 1, 11, $21 \in \mathcal{A}(s_1)$ when $s_1 = 3202$, but all other possibilities are in $\mathcal{A}(s_1)$, a most remarkable situation. It would be of some interest to find some s_1 for which $q \neq 1$ and $q > 8/11$.

8 The case of $q = 1$

A short inspection of Table 2 reveals that the only values of s_1 with $s_1 \leq 2000$ for which $q = 1$ are those found by Lehmer. It is an interesting problem to determine whether there can exist values of s_1 not predicted by Lehmer for which $q = q(s_1) = 1$. That is, do there exist values for s_1 such that $s_1^- \neq 1$ or $s_1^+ \neq 3$ for which $q(s_1) = 1$?

To proceed any further, we need two simple lemmas.

Lemma 13. *If $s_1^- \equiv -1 \pmod 4$, then (17) cannot hold for all $n \in \mathcal{R}(\Omega)$.*

Proof. We note that $1 \in \mathcal{R}(\Omega)$ and

$$\eta_1(r_i) = (2^1 - 1|r_i) = (1|r_i) = 1.$$

Thus,

$$\prod_{i=1}^{k} \eta_1(r_i) = 1 \neq (-1)^{\frac{s_1^- - 1}{2}},$$

and therefore (17) cannot hold for $n = 1$. □

Lemma 14. *If $s_1^+ \equiv 1 \pmod 4$, then (17) cannot hold for all $n \in \mathcal{R}(\Omega)$.*

Proof. Similar to that of the previous result. □

It is now a simple matter to prove the following theorem.

Theorem 15. *If $q'(s_1) = 1$, then $s_1^- \equiv 1 \pmod 4$ and $s_1^+ \equiv -1 \pmod 4$.*

Corollary 16. *If s_1 is odd, then $q'(s_1) \neq 1$.*

Proof. From (15), we have

$$2^\alpha m_1^2 s_1^- = s_1 - 2, \quad 2^\beta m_2^2 s_1^+ = s_1 + 2,$$

where m_1 and m_2 are odd integers and integers α, $\beta \geq 0$. Since s_1 here is odd, we have $\alpha = \beta = 0$, both m_1 and m_2 are odd and $(m_1 m_2)^2 \equiv 1 \pmod 4$. Also,

$$m_1^2 m_2^2 s_1^- s_2^+ = s_1^2 - 4$$

means that

$$s_1^- s_2^+ \equiv 1 \pmod 4 \quad \text{or} \quad s_1^- \equiv s_1^+ \pmod 4.$$

□

In order for $q'(s_1) = 1$, we need

$$s_1^- \equiv 1 \pmod 4 \quad \text{and} \quad s_1^+ \equiv -1 \pmod 4 \tag{21}$$

If (21) holds, then (17), becomes

$$\prod_{i=1}^{k} \eta_n(r_i) = 1 \quad \text{and} \quad \prod_{i=1}^{j} \eta_n(q_i) = 1, \tag{22}$$

respectively. Since $\Omega - 1 \in \mathcal{R}(\Omega)$ and by (20)

$$\eta_{\Omega - n}(p) = (-2|p)\eta_n(p),$$

we see that if $k = 1$, then $s_1^- = r_1 \equiv 1 \pmod 4$ and if $r_1 \equiv 5 \pmod 8$, then

$$\eta_{\Omega-1}(r_1) = -1.$$

Thus, (22) cannot hold for $n = \Omega - 1$ when s_1^- is a prime and $s_1^- \equiv 5 \pmod 8$. Similarly (22) cannot hold for $n = \Omega - 1$ when s_1^+ is a prime and $s_1^+ \equiv 7 \pmod 8$. In either case $q_1(s_1) \neq 1$.

More generally, suppose that p is any odd prime and observe that $2^n - 1$ is never a perfect integral square when $n > 1$. Since for any given a not a perfect square, the probability that $(a|p) = 1$ is about $1/2$, we expect that for any $n \geq 3$ the likelihood that $\eta_n(p) = \epsilon$, where $\epsilon \in \{1, -1\}$ to be about $1/2$. Suppose that p_1, $p_2, \ldots, p_m$ are m distinct odd primes. Put $\omega = \omega(p_1 p_2 \cdots p_m)$ and let each of ϵ_1, $\epsilon_2, \ldots, \epsilon_m$ have fixed values selected from $\{1, -1\}$. For a particular $n \in \mathcal{R}(\omega)$, the probability that

$$\eta_n(p_i) = \epsilon_i \quad (i = 1, 2, \ldots, m)$$

is about $1/2^m$. Also, since there are 2 possible values for $\eta_n(p_i)$ $(\neq 0)$ for $i = 1, 2, \ldots, m-1$ and only one possible value for $\eta_n(p_m)$ such that

$$\prod_{i=1}^{m} \eta_{p_i}(n) = 1, \tag{23}$$

there can be only 2^{m-1} possible sets of values of $(\epsilon_1, \epsilon_2, \ldots, \epsilon_m)$ such that (23) holds. Thus, we anticipate that the probability that (23) is true for any fixed $n \in \mathcal{R}(\omega)$ should be about

$$2^{m-1} \times \frac{1}{2^m} = \frac{1}{2}.$$

Under the not unreasonable assumption that for distinct n_1, $n_2 \in \mathcal{R}(\omega)$, the events

$$\prod_{i=1}^{m} \eta_{n_1}(p_i) = 1 \quad \text{and} \quad \prod_{i=1}^{m} \eta_{n_2}(p_i) = 1$$

are independent, we would predict the probability that

$$\prod_{i=1}^{k} \eta_n(r_i) = 1 \quad \text{for all} \quad n \in \mathcal{R}(s_1^-)$$

is $\approx (1/2)^{\phi(\Omega_1)}$ and the probability that

$$\prod_{i=1}^{j} \eta_n(q_i) = 1 \quad \text{for all} \quad n \in \mathcal{R}(s_1^+)$$

is $\approx (1/2)^{\phi(\Omega_2)}$, where $\Omega_1 = \Omega(s_1^-)$, $\Omega_2 = \Omega(s_1^+)$. These probabilities will generally tend to be rather small.

The above reasoning suggests that for most values of s_1 there should be values of $n \in \mathcal{R}(\Omega)$ such that either statement in (22) is false. We programmed a computer to search for all even s_1 up to some bound $\mathcal{B}$ for which $q'(s_1) \neq 1$. The computer examined each value of s_1 satisfying (21) and eliminated this candidate as soon as it found some value of $n \in \mathcal{R}(\Omega_1)$ such that (22) is false or some value of $n \in \mathcal{R}(\Omega_2)$ such that (22) is false. We ran the program up to $\mathcal{B} = 10^8$ and found only the following where the second statement in values of s_1 for which $q'(s_1)$ (or $q(s_1)$) could be 1:

$$s_1 = 4, 10, 52, 724, 970, 10084, 95050, 140452, 1956244, 9313930, 27246964.$$

Indeed, as we have seen in Section 5, Lehmer had shown $q(s_1) = 1$ for all of these values of s_1. Thus, it might appear that if $q(s_1) = 1$, then $s_1^- = 1$ and $s_1^+ = 3$. By the results at the end of Section 4, this would certainly be the case if the only integers a such that the Jacobi symbol $(a|M_n)$ has a fixed value for all odd $n \geq 3$ must be in $\mathcal{S}$, but we have seen in Section 3 that this is not true; thus, it might well be that Lehmer did not find all the values for s_1 for which $q(s_1) = 1$. Of course, if we allow s_1 to be rational, then as shown in Section 4, there are vastly more possibilities.

9 Conclusion

We have seen that there exists an infinitude of rational universal seeds s_1; in fact, we can produce simple parametric formulas for such seeds. We have also produced a simple process which will tabulate those values of n for which a given integral s_1 is acceptable for M_n. Furthermore, we found those integers s_1 ($s_1 \leq 5000$) such that $q(s_1)$ satisfies $1/2 < q(s_1) < 1$.

Lehmer found an infinite set of integral s_1 for which $q(s_1) = 1$. These all have the same property that $s_1^- = 1$ and $s_1^+ = 3$. A computer search for all integral s_1 up to to 10^8 for which $q(s_1) = 1$ did not produce any other s_1; however, it is possible that there might exist some s_1 which Lehmer did not find such that $q(s_1) = 1$. This needs further investigation.

We close by mentioning the following interesting result, which can be easily deduced from Theorem 3 of Berrizbeitia and Berry [2].

Theorem 17. *If n is odd, $n \geq 3$ and s_1 is the rational seed $6/5$, then M_n is prime if and only if*

$$\begin{aligned} s_{n-1} &\equiv 0 \pmod{M_n} \quad \textit{when} \quad n \equiv 3 \pmod 4 \\ s_{n-2} &\equiv 0 \pmod{M_n} \quad \textit{when} \quad n \equiv 1 \pmod 4. \end{aligned}$$

The proof of the first part of this result can be easily deduced by putting $R = 4$ and $Q = 5$ above, but the second part requires the properties of the biquadratic residue symbol. It would be of some interest to investigate the existence of similar theorems with different s_1 (and n).

10 Acknowledgments

We are very grateful to an anonymous referee, whose careful reading and several suggestions have resulted in a much more presentable version of this paper from that originally submitted. We also wish to thank Jeffrey Shallit for bringing Jansen's interesting thesis [6] to our attention.

References

[1] Christian J.-C. Ballot and Hugh C. Williams, *The Lucas Sequences: Theory and Applications*, CMS/CAIMS Books in Mathematics, Volume **8**, Springer Nature, 2023.

[2] Pedro Berrizbeitia and T. G. Berry, Biquadratic reciprocity and a Lucasian primality test, *Math. Comput.* **73** (2003), 1559–1564.

[3] David A. Cox, *Primes of the Form* $x^2 + ny^2$, Wiley-Interscience, 1989.

[4] Leonard Eugene Dickson, *History of the Theory of Numbers*, Carnegie Institute of Washington, Volume **II**, G. E. Stechert & Co., 1934.

[5] Michael J. Jacobson, Jr. and Hugh C. Williams, *Solving the Pell Equation*, CMS Books in Mathematics, Springer, New York, NY, 2009.

[6] B. J. H. Jansen, *Mersenne primes and class field theory*, PhD thesis, Mathematical Institute, Faculty of Science, Leiden University, 2012. Available at https://hdl.handle.net/1887/20310.

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

[8] L. J. Mordell, *Diophantine Equations*, Academic Press, 1969.

[9] R. M. Robinson, Mersenne and Fermat numbers, *Proc. Amer. Math. Soc.* **5** (1954), 842–846.

[10] N. J. A. Sloane et al., The On-Line Encyclopedia of Integer Sequences, 2024. Available at https://oeis.org.

[11] H. C. Williams, *Édouard Lucas and Primality Testing*, CMS series of Monographs and Advanced Texts, Volume **22**, John Wiley & Sons, 1998.

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

(Concerned with sequences A001566, A003010, A018844, and A135927.)

Received July 25 2024; revised version received September 27 2024; March 22 2025. Published in *Journal of Integer Sequences*, March 23 2025.

Return to Journal of Integer Sequences home page.