Mersenne Primes in Certain Lucas Sequences

Ahmed H. Hadi[1], and *Hayder* R. Hashim [2*]

[1]Faculty of Computer Science and Mathematics, University of Kufa, Iraq
[2]Faculty of Computer Science and Mathematics, University of Kufa, Iraq

Abstract. Prime numbers are the most important numbers in number theory and cryptography. One of such special primes are given by the set of Mersenne primes, that are derived from the form $M_n = 2^n - 1$, where n is a prime number. In this paper, we examine the appearance of these primes in certain sequences of Lucas numbers of the first kind $\{U_n(P,Q)\}$ or the second kind $\{V_n(P,Q)\}$. Namely, we completely solve the Diophantine equation $M_n = U_n(P,Q)$ or $M_n = V_n(P,Q)$ for certain nonzero relatively prime parameters P and Q.

Keywords: Prime numbers, Mersenne prime number, Lucas sequences, Diophantine equation, Elliptic curve.

1 Introduction

The study of prime numbers represents one of the basic and most attractive branches of number theory. They are considered the basic building blocks of integers according to the basic theorem of arithmetic. Since prime numbers are infinite, special families emerge that are characterized by exceptional properties and beautiful mathematical formulas, the most prominent of which are Mersenne prime numbers [1]. These numbers have attracted the attention of mathematicians for centuries not only for their theoretical beauty but also for their profound practical applications in various fields such as cryptography and prime number testing. One of the well-known primes is called a Mersenne prime numbers, which are defined in the form

$$M_n = 2^n - 1, \qquad (1)$$

where n is a prime number. Mersenne numbers are named after the French monk Marin Mersenne [2], who studied them in the seventeenth century

although the study of these numbers' dates back to Greek mathematicians such as Euclid.
In 1749, Euler [3] stated Euclid– Euler's theorem fully links Mersenne prime numbers to even perfect numbers (numbers whose sum of positive divisors equals the number itself). This correlation states
that every prime Mersenne number $M_n = 2^n - 1$ generates an even perfect number with the formula

$$N = (2^n - 1).\, 2^{n-1}.$$

Also, these numbers are connected to primality tests such as the Lucas-Lehmer test, that is an effective and relatively quick method for determining the primality of Mersenne numbers [1]. It is still unknown whether the number of Mersenne prime numbers is finite or infinite. They are currently being searched collaboratively via the GIMPS (Great Internet Mersenne Prime Search) project. Other forms or primes introduced by Landau [4] in 1912, which he proved that for certain integers x, there are an infinite number of primes of the form

$$p = x^2 + 1. \qquad (2)$$

* Corresponding author: hayderr.almuswi@uokufa.edu.iq

In 1961, Shank [5] made a similar conjecture by stating that for certain integers x, there are an infinite number of primes of the form

$$p = x^4 + 1. \quad (3)$$

This conjecture has not yet been proven. Furthermore, he proved that for some integers x, there are an infinite number of primes of the form,

$$p = \frac{1}{2}(x^2 + 1), \quad (4)$$

which also has not yet been proven. The forms of these primes are closely related to Diophantine equations, which are algebraic equations requiring integer (or sometimes non-negative integer) solutions to variables in the

form

$$f(x_1, x_2, x_3, \dots, x_n) = 0$$

There are many well-known Diophantine equations, such as the linear equation

$$ax + by = c,$$

where $a, b, c \in Z$. This equation has either no solutions if $gcd(a, b) \nmid c$ or has infinitely many solutions if $gcd(a, b) \mid c$. One of the well studied Diophantine equations is the elliptic curve equation that has the form

$$y^2 = a_0 x^n + a_1 x^{n-1} + \cdots + a_n, \quad (5)$$

where $a_0 \neq 0, a_1, \dots, a_n$ are integers with $n \geq 3$. For more details on elliptic curves and their applications, see e.g. [6]. Baker [7] proved that the elliptic curve equation (5) has a finite number of solutions obtained by an explicit upper bound. A well-known example of elliptic curve is represented by

$$y^2 = ax^4 + bx^2 + c \quad (6)$$

whose discriminant is

$$\Delta = 16ac(b^2 - 4ac)^2.$$

Another example of Diophantine equations is given by Fermat's equation:

$$x^n + y^n = z^n,$$

where $n > 2$. It was formulated by Pierre de Fermat [8] in the margin of a book by Diophantus around 1637, and he claimed to have a "remarkable proof" for the insolvability of this equation but did not write it down. No general proof by Fermat was found, and thus the problem remained open for more than 350 years. In 1993, Wiles [8] proved Fermat conjecture by reducing it to an elliptic curve equation.

Another important aspect in number theory is presented by a linear recurrence sequence, where each of its terms is expressed in terms of a fixed number of preceding terms using a linear recurrence of order k with constant coefficients, is defined by

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k} + f(n),$$

where $c_1, c_2, \dots, c_k \in Z$, $a_{n-k} \neq 0$, k represents the order of the sequence and $f(n)$ is a function depending on n. If f (n) = 0, this kind of recurrence relation is known as homogeneous and nonhomogeneous if $f(n) \neq 0$. The definition of this sequence, together with the following related results, is retrieved from [9,10]. If k = 2, we call it a binary linear recurrence sequence. Among the most well-known binary linear recurrence sequences are the certain Lucas sequences of the first kind $\{U_n(P, Q)\}$ and the second kind $\{V_n(P, Q)\}$, which are defined by

$$\begin{array}{lll} U_0(P,Q) = 0, & U_1(P,Q) = 1, & U_n(P,Q) = PU_{n-1}(P,Q) - QU_{n-2}(P,Q), \\ V_0(P,Q) = 2, & V_1(P,Q) = P, & V_n(P,Q) = PV_{n-1}(P,Q) - QV_{n-2}(P,Q), \end{array}$$

where n ≥ 2 and P, Q are relatively prime integers and non-zero. Special cases of the Lucas sequences are given by

$$\begin{array}{ll} F_0 = 0, F_1 = 1, F_n = F_{n-1} + F_{n-2}, & for\ n \geq 2, \\ L_0 = 2, L_1 = 1, L_n = L_{n-1} + L_{n-2}, & for\ n \geq 2, \\ P_0 = 0, P_1 = 1, P_n = P_{n-1} + P_{n-2}, & for\ n \geq 2, \\ Q_0 = 2, Q_1 = 2, Q_n = Q_{n-1} + Q_{n-2}, & for\ n \geq 2, \end{array}$$

which are called Fibonacci, Lucas, Pell, and Pell-Lucas numbers, respectively. Their numbers refer to the generalized Lucas numbers, and it is also known that the first and second kind of Lucas sequences satisfied the identity

$$V_n^{\,2}(P,Q) = DU_n^{\,2}(P,Q) + 4Q^n \qquad (7)$$

where the discriminant of the sequences $D = P^2 - 4Q$. Also, the characteristic polynomial of these sequences is given by.

$$X^2 - PX + Q = 0,$$

where,

$$a = \frac{P+\sqrt{D}}{2}, \quad b = \frac{P-\sqrt{D}}{2}$$

represent its zeros. Consequently, these sequences are also described by

$$U_n(P,Q) = \frac{a^n - b^n}{a-b}, \qquad V_n(P,Q) = a^n + b^n \qquad for\ n \geq 0.$$

If (a/b) is not a root of unity, these sequences are considered nondegenerate, if not, they are considered degenerate. Consequently, it is proved that the only degenerate certain Lucas sequences are with $(P,Q) \in \{(\pm 1,1),(\pm 2,1)\}$. Note that we exclude the degenerate Lucas sequences for the following reasons. Let us consider the degenerate Lucas sequences of the second kind. As shown by Hashim [10], they have the following forms:

$$V_n(2,1) = 2,$$

$$V_n(-1,1) = \begin{cases} 2 & if\ 3 \mid n, \\ -1 & if\ 3 \nmid n, \end{cases}$$

$$V_n(-1,1) = \begin{cases} -1 & if\ n \equiv \{2,4\}\ (mod 6), \\ 1 & if\ n \equiv \{1,6\}\ (mod 6), \\ -2 & if\ n = 6t+3\ , t \geq 0, \\ 2 & if\ n = 6t\ \ , t \geq 0, \end{cases}$$

$$V_n(-2,1) = \begin{cases} 2 & if\ \ n = 2r\ , \quad r \geq 0, \\ -1 & if\ n = 2r+1\ , r \geq 0. \end{cases}$$

As shown above in the recurrence relations of these sequences, their terms can be easily identified as not prime numbers. But in our work, we are interested in the prime Lucas numbers that represent Mersenne numbers. Therefore, we exclude these sequences from our results. A similar idea applies to the Lucas sequences of the first kind.

In fact, the nondegenerate Lucas sequences have infinitely many prime numbers in their terms, as Lawrence and Michal [11] proved that there are infinitely many primes in certain Lucas sequences of the first and second kind. On the other hand, if k = 3, the linear recurrence sequence is called a ternary sequence. There are many well-known examples of such sequences. For instance, the Tribonacci sequence, that is defined by the relation

$$t_0 = t_1 = 0, t_2 = 1\ and\ t_n = t_{n-1} + t_{n-2} + t_{n-3} \quad if\ n \geq 3, \qquad (8)$$

and the Bertel's sequence, which is defined by the relation

$$b_0 = b_1 = 0, b_2 = 1\ and\ b_n = 2b_{n-1} - 4b_{n-2} + 4b_{n-3}\ if\ n \geq 3 \qquad (9)$$

Several authors have connected the study of Diophantine equations representing prime number forms with linear recurrence sequences. For example, Athab and Hashim [6] studied the solutions of Diophantine equations (2), (3) and (4), where $p = U_n(P,Q)$ and $x \in Z$ or $p = V_n(P,Q)$ and $x \in Z$ such that $1 \leq P \leq 15$ and $Q \in \{-1,1\}$.

In this paper, we extend the previous results by investigating whether or not there are still infinite numbers in the Mersenne primes belong to $\{U_n(P,Q)\}\ or\ \{V_n(P,Q)\}$. The research aims to study these numbers in depth, especially within certain Lucas sequences, to better understand their properties, relationships, and to prove hypotheses related to their limitations. In other words, we give an approach for solving equation (1) in the cases where $M_n = U_n(P,Q)$ or $M_n = V_n(P,Q)$ such that $P \geq 1\ and\ Q = \pm 1$. Furthermore, we investigate the values of the exponents n, that represent Lucas numbers of the first or second kind. In fact, we consider Q = ±1 because if we substitute other numbers, they yield an infinite number of elliptic curves, see the elliptic curve (11).

This study looks at the link between Mersenne prime numbers and linear recurrence sequences. While past research usually studied them separately, this work connects them in a more complete and organized way. The results give cryptologists an idea whether or not they can use these primes in designing public key cryptosystems.

2 Main Results

Theorem 1. Let M_n be a Mersenne number of the form (1) and $\{U_m(P,Q)\}$ be nondegenerate with $1 \leq P \leq 15 \; and \; Q \in \{-1,1\}$. If $M_n = U_n(P,Q)$ is a prime number, then the set of solutions to the equation (1) is given by $(P,Q,m,n) \in \{(7,\pm 1,2,3),(3,1,2,2),(1,-1,4,2),(3,-1,2,2)\}$.

Proof. We prove the theorem in two cases regarding whether n is odd or even.

Case 1: If n is odd. Let $n = 2k+1$ with $k \geq 1$, then equation (1) becomes

$$U_m(P,Q) = 2^{2k+1} - 1, \tag{10}$$

where $U_m(P,Q)$) is a prime number. Namely, we solve the Diophantine equation (10) by determining the values of m,k satisfying the equation with $1 \leq P \leq 15 \; and \; Q = \pm 1$. The approach follows directly by combining equation (10) with the identity relation between $\{U_m(P,Q)\}$ and $\{V_n(P,Q)\}$ given in (7) we get the equation

$$y^2 = D(2(2^k)^2 - 1)^2 + 4Q^m$$

which can be written in the form

$$y^2 = 4Dx^4 - 4Dx^2 + (D + 4Q^m), \tag{11}$$

where $y = V_m(P,Q), x = 2^k, D = P^2 - 4Q, 1 \leq P \leq 15$ and $Q = \pm 1$. Indeed, we suppose that equation (11) is an elliptic curve of the form (6). To show that, we must prove it has a non-zero discriminant. The discriminant of curve (6) is $\Delta = 16ac(b^2 - 4ac)^2$.
Hence, equation (11) has the discriminant

$$\Delta = -4096D^2 \, Q^m(D + 4Q^m).$$

• If $Q = 1$ such that the Lucas sequence is nondegenerate, i.e. $(P,Q) \notin \{(\pm 1,1),(\pm 2,1)\}$, then $D = P^2 - 4Q = P^2 - 4$ is greater than zero. Additionally, we have $D + 4 = (P^2 - 4 + 4) = P2 > 0 \; as \; P \geq 1$. Thus, $\Delta \neq 0$.

• If Q = −1, we obtain that $D = P^2 - 4Q = P^2 + 4 > 0$ if n is odd. Also, if n is even, we obtain that $D = P^2 - 4Q = P^2 - 4 > 0$ as the Lucas sequence is nondegenerate. Again, it is clear that $D + 4Q^2 > 0 \; as \; P \geq 1$. Hence, $\Delta \neq 0$.

From both cases, we have $\Delta \neq 0$. Therefore, equation (11) indeed represents an elliptic curve, whose integral solutions (x,y) are obtained by using the Magma software with the function [SIntegralLjunggrenPoints] [12]. Indeed, we are only interested in the values of $x = 2^k$ to get the values k. These values lead to the values of n. Let's explain some cases in detail, we substitute the values of (P, Q) = (3, 1) into equation (11) to obtain the elliptic equation

$$y^2 = 20x^4 - 20x^2 + 9$$

When using the Magma code [SIntegralLjunggrenPoints ([1,20, -20,9], [])], we get the positive x values of integer solutions as $x \in \{0,1\}$. Similarly, when substituting the values of $(P,Q) = (1,-1)$ into equation (11), we obtain the following two equations:

$$y^2 = 20x^4 - 20x^2 + 1$$

and

$$y^2 = 20x^4 - 20x^2 + 9,$$

which has the solution x ∈ {0, 1}. The other cases can be followed similarly, and Table 1 gives the results of computations for the coefficients and the nonnegative values of x coordinates of the solutions to the elliptic curve

$$y^2 = Ax^4 - Bx^2 + C,$$

which corresponds to the curve (11):

$$y^2 = 4Dx^4 - 4Dx^2 + (D + 4Q^m),$$

where $P^2 - 4Q = D, 1 \leq P \leq 15$ and Q in neither 1 nor −1 such that the Lucas sequences are nondegenerate

Table 1. Solutions of elliptic curve (11) with $1 \leq P \leq 15$ *and* $Q = \pm 1$.

$Q = 1$			$Q = -1$		
(P, Q)	$[A, B, C]$	$\{x\}$	(P, Q)	$[A, B, C]$	$\{x\}$
(3,1)	[20,-20,9]	0,1	(1,-1)	[20,-20,1]	0,1
				[20,-20,9]	0,1
(4,1)	[48,-48,16]	0,1	(2,-1)	[32,-32,4]	0,1
				[32,-32,12]	[ ]
(5,1)	[84,-84,25]	0,1	(3,-1)	[52,-52,9]	0,1
				[52,-52,17]	[ ]
(6,1)	[128,-128,36]	0,1	(4,-1)	[80,-80,16]	0,1
				[80,-80,24]	[ ]
(7,1)	[180,-180,49]	0,1,2	(5,-1)	[116,-116,25]	0,1
				[116,-116,33]	[ ]
(8,1)	[272,-272,64]	0,1	(6,-1)	[160,-160,36]	0,1
				[160,-160,44]	[ ]
(9,1)	[340,-340,81]	0,1	(7,-1)	[212,-212,49]	0,1
				[212,-212,57]	2
(10,1)	[384,-384,100]	0,1	(8,-1)	[272,-272,64]	0,1
				[272,-272,72]	[ ]
(11,1)	[468,-468,121]	0,1	(9,-1)	[340,-340,81]	0,1
				[340,-340,89]	[ ]
(12,1)	[560,-560,144]	0,1	(10,-1)	[416,-416,100]	0,1
				[416,-416,108]	[ ]
(13,1)	[660,-660,169]	0,1	(11,-1)	[500,-500,121]	0,1
				[500,-500,129]	[ ]
(14,1)	[768,-768,196]	0,1	(12,-1)	[592,-592,144]	0,1
				[592,-592,144]	[ ]
(15,1)	[884,-884,225]	0,1	(13,-1)	[692,-692,169]	0,1
				[692,-692,177]	[ ]
----------	----------	------	(14,-1)	[800,-800,196]	0,1
				[800,-800,204]	[ ]
----------	----------	-----	(15,-1)	[916,-916,225]	0,1
				[916,-916,233]	[ ]

Next, from the resulting values of x (where $x = 2k$) we obtain the corresponding values of $k \geq 1$ with which $M_n = U_m(P, Q) = 2x^2 - 1 = 2^{2k+1} - 1 = 2^n - 1$ is a prime number. It is clear to see that a prime number is obtained from the case where, $(P, Q) = (7, \pm 1)$ with $x = 2$. Namely, for $2 = x = 2^k$, we have $k = 1$. Hence,

$$U_m(7, \pm 1) = 2^{2(1)+1} - 1 = 7,$$

which implies that m = 2 and n = 3. Therefore, we get only two solutions, which are $(P, Q, m, n) = (7, \pm 1, 2, 3)$. Next, we consider the case where n is even.

Case 2: If n is even $(n = 2)$, then we have

$$U_m(P, Q) = 2^2 - 1 = 3,$$

which is a prime number. Next, we search for the values of P and Q such that $U_m(P, Q) = 3$, where $1 \leq P \leq 15$ *and* $Q = \pm 1$ such that the Lucas sequences are nondegenerate. By checking all the values of P and Q, we summarize the results in Table 2:

Table 2. Solutions of equation (10) with $n \geq 1$.

(P, Q)	m	n
(3,1)	2	2
(1,-1)	4	2
(3,-1)	2	2

which give the remaining solutions of equation (1). Hence, the theorem is completely proved.

Corollary 1. Suppose that $M_n = U_m(P_1, Q_1)$ and $n = U_r(P_2, Q_2)$are prime numbers such that $n, m, r \geq 2, 1 \leq P1, P2 \leq 15, Q_1, Q_2 \in \{\pm 1\}$ and the Lucas sequences are nondegenerate, then the solutions of equation (1) are given by

Table 3. Solutions of equation (1) with $M_n = U_m(P_1, Q_1)$ and $n = U_r(P_2, Q_2)$.

(P_1, Q_1)	m	(P_2, Q_2)	r
$(7, \pm 1)$	2	(3,1)	2
		(1,-1)	4
		(3,-1)	2
(3,1)	2	(1,-1)	3
		(2,-1)	2
(1,-1)	4	(1,-1)	3
		(2,-1)	2
(3,-1)	2	(1,-1)	3
		(2,-1)	2

Proof. From the results of Theorem 1, we obtained that $U_m(P_1, Q_1)$ is prime number only if

$$(P, Q, m, n) \in \{(7, \pm 1, 2, 3), (3, 1, 2, 2), (1, -1, 4, 2), (3, -1, 2, 2)\}.$$

• If n is odd, we got that

$$(P_1 Q_1, m, n) = (7, \pm 1, 2, 3),$$

which implies that

$$7 = U_m(P_1, Q_1) = U_m(7, \pm 1) = 2^n - 1 = 2^3 - 1 = 2^{U_r(P_2, Q_2)} - 1.$$

Hence, $U_r(P_2, Q_2) = 3$, where $r \geq 2, 1 \leq P2 \leq 15$ and $Q_2 = \pm 1$ so that the Lucas sequences are nondegenerate. It remains to find the values of r and (P_2, Q_2) such that $U_r(P_2, Q_2) = 3$. One can easily see these values are given by the set $(P_2, Q_2\ r) \in \{(3, 1, 2), (1, -1, 4), (3, -1, 2)\}$.

Therefore, the complete set of solutions in the case of n is odd is given by

$$(P_1, Q_1\ m, P_2, Q_2\ r) \in \{(7, \pm 1, 2, 3, 1, 2), (7, \pm 1, 2, 1, -1, 4), (7, \pm 1, 2, 3, -1, 2)\}.$$

• If n is even, (n = 2) we got from the results of Theorem 1 that

$$(P_1, Q_1\ m, n) \in \{(3, 1, 2, 2), (1, -1, 4, 2), (3, -1, 2, 2)\},$$

which implies that

$$3 = U_m(P_1, Q_1) = 2^n - 1 = 2^2 - 1 = 2^{U_r(P_2, Q_2)} - 1.$$

It remains to search for the values of r and (P_2, Q_2), such that $U_r(P_2, Q_2) = 2$, where $1 \leq P_2 \leq 15$ and $Q_2 = \pm 1$ such that the Lucas sequences are nondegenerate. The Table 4 below summarizes the calculations for the values of r and (P_2, Q_2) corresponding to each pair (P_1, Q_1):

Table 4: Values of (P_1, Q_1), m, (P_2, Q_2), and r.

(P_1, Q_1)	m	(P_2, Q_2)	r
(3,1)	2	(1,-1)	3
		(2,-1)	2
(1,-1)	4	(1,-1)	3
		(2,-1)	2
(3,-1)	2	(1,-1)	3
		(2,-1)	2

which gives the solutions in the case of n is even. Therefore, the corollary is proved.

Corollary 2 Suppose that $M_n = U_m(P_1, Q_1)$ and $n = V_r(P_2, Q_2)$are prime numbers such that $n, m, r \geq 2, 1 \leq P_1, P_2 \leq 15\ Q_1, Q_2 \in \{\pm 1\}$ and the Lucas sequences are nondegenerate, then the solutions of equation (1) are shown in Table 5:

Table 5. Solutions of equation (1) with $M_n = U_m(P_1, Q_1)$ and $n = V_r(P_2, Q_2)$.

(P_1, Q_1)	m	(P_2, Q_2)	r
(7,1)	2	(3,1)	1
(7,-1)		(1,-1)	2
		(3,-1)	1
(3,1)	2	All (P_2, Q_2) $where\ 1 \leq P_2 \leq 15\ and\ Q_2 = \pm 1$	0
(3,1)	2	(2,-1)	1
(1,-1)	4	All (P_2, Q_2) $where\ 1 \leq P_2 \leq 15\ and\ Q_2 = \pm 1$	0
(1,-1)	4	(2,-1)	1
(3,-1)	2	All (P_2, Q_2) $where\ 1 \leq P_2 \leq 15\ and\ Q_2 = \pm 1$	0
(3,-1)	2	(2,-1)	1

Proof. Following the same approach used in Corollary 1, depending on the obtained solutions in Theorem 1.
If n is even, we find that the values of r correspond to the power $n = 2$ with which $2 = n = V_r(P_2, Q_2)$.such that $r \geq 0, P_2 \in \{1, \ldots, 15\}, Q \in \{+1, -1\}$ and the sequences $\{U_m\}$ and $\{V_m\}$ are nondegenerate. The Table 6 summarizes the values in the case of$(P_1, Q_1) = (3,1)$:

Table 6. Values of $m, (P_2, Q_2)$. and $r = 0,1$ for $(3,1)$.

(P_1, Q_1)	m	(P_2, Q_2)	r
(3,1)	2	All (P_2, Q_2) $where\ 1 \leq P_2 \leq 15\ and\ Q_2 = \pm 1$	0
		(2,-1)	1

Similarly, we can find the values of r and (P_2, Q_2) for the remaining values of $(P_1, Q_1, m) \in \{(1, -1, 4), (3, -1, 2)\}$. In fact, we also get $r = 0$ for all $1 \leq P_2 \leq 15$ and $Q_1, Q_2 = \pm 1$.
For odd, n $(n = 3)$, we have that (P_1, Q_1, m, n)= (7, ±1, 2, 3). Thus,

$$7 = U_m(7, \pm 1) = 2^n - 1 = 2^3 - 1 = 2^{V_r(P_2, Q_2)} - 1.$$

Thus, we have the following values of r and (P_2, Q_2) such that $V_r(P_2, Q_2) = 3$
:

Table 7. Values of $m, (P_2, Q_2)$ and r for $(7, \pm 1)$.

(P_1, Q_1)	m	(P_2, Q_2)	r
(7,1)	2	(3,1)	1
(7,-1)		(1,-1)	2
		(3,-1)	1

The above tables establish the results of the corollary.

Theorem 2. Let the sequence $\{V_m(P, Q)\}$ denote the nondegenerate Lucas sequence of the second kind with $1 \leq P \leq 15$ and $Q \in \{-1, 1\}$. If $M_n = V_m(P, Q)$ is a prime number, then the set of solutions to the equation (1) is represented by

$$(P, Q, m, n) \in \{(3, 1, 2, 3), (7, 1, 1, 3), (1, -1, 4, 3)(7, -1, 1, 3), (3, 1, 1, 2), (1, -1, 2, 2), (3, -1, 1, 2)\}.$$

Proof. The proof of the theorem is divided into two cases, depending on whether the prime n is odd or even.

Case 1: If n odd. Let $n = 2k + 1$ with $k \geq 1$. We find the values of k satisfying

$$V_m(P, Q) = 2^{2k+1} - 1 \qquad (12)$$

where $V_m(P, Q)$ is a prime number that combines equation (12) with identity (7), leading to the equation

$$y^2 = 4Dx^4 - 4Dx^2 + D - 4DQ^m, \qquad (13)$$

with $y = DU_m, D = P^2 - 4Q$ (with $1 \leq P \leq 15, Q = \pm 1$) and $x = 2k$. Since the Lucas sequence of the second kind is assumed to be nondegenerate, the discriminants of equation (13) are actually defined by

$$\Delta v = 4096D^4(1 - 4Q^m).$$

The Lucas sequence of the second kind must be nondegenerate, resulting in $D \neq 0$. For all $1 \leq P \leq 15$ and Q_1, $Q_2 = \pm 1$. Therefore, $\Delta v \neq 0$ as $(1 - 4Q^m) \neq 0$ with $Q = \pm 1$ and $n \geq 0$. Thus, equation (13) displays an elliptic curve at every pair (P, Q) with $1 \leq P \leq 15$ and $Q = \pm 1$. In order to determine prime terms for $M_n = V_m(P, Q)$, the initial step is to compute the values of x to get the values of k based on the integral points (x, y) of equation (13).

The Table 8 provides the computations for obtaining the coefficients and the non-negative x values for the elliptic curve

$$y^2 = Ax^4 + Bx^2 + C,$$

which corresponds to equation (13) for every pair (P, Q) such that $(P, Q) \notin \{(\pm 1, 1), (\pm 2, 1)\}$:
Let's explain one case in details we substituted the values $(P, Q) = (3, 1)$ into equation (13) to obtain the elliptic equation

$$y^2 = 20x^4 - 20x^2 - 15,$$

when using the Magma code [SIntegralLjunggrenPoints ([1,20, -20, -15], [])], we found the solution to the final equation $x = 2$. And also, when substituting the values $(P, Q) = (1, -1)$ into equation (13), we obtain two equations. $y^2 = 20x^4 - 20x^2 - 15$, which has the solution $x = 2$ and $y^2 = 20x^4 - 20x^2 + 15$, has the solutions $x \in \{0, 1, 10\}$.
The other cases can be followed similarly, as show in Table 8

Table 8. Solutions of the elliptic curve (13) with $1 \leq P \leq 15$ and $Q = \pm 1$.

$Q = 1$			$Q = -1$		
(P, Q)	$[A, B, C]$	$\{x\}$	(P, Q)	$[A, B, C]$	$\{x\}$
(3,1)	[20,-20,-15]	[2]	(1,-1)	[20,-20,25]	[0,1,10]
				[20,-20,-15]	[2]
(4,1)	[48,-48,-36]	[ ]	(2,-1)	[32,-32,40]	[ ]
				[32,-32,-24]	[ ]
(5,1)	[84,-84,-63]	[ ]	(3,-1)	[52,-52,65]	[ ]
				[52,-52,-39]	[ ]
(6,1)	[128,-128,-96]	[ ]	(4,-1)	[80,-80,100]	[0,1,10]
				[80,-80,-60]	[2]
(7,1)	[180,-180,-135]	[2]	(5,-1)	[116,-116,145]	[ ]
				[116,-116,-87]	[ ]
(8,1)	[240,-240,-180]	[ ]	(6,-1)	[160,-160,200]	[ ]
				[160,-160,-120]	[ ]
(9,1)	[308,,-308,-231]	[ ]	(7,-1)	[212,-212,265]	[2]
				[212,-212,-159]	[ ]
(10,1)	[384,-384,-288]	[ ]	(8,-1)	[272,-272,340]	[ ]
				[272,-272,-204]	[ ]
(11,1)	[468,-468,-35]	[ ]	(9,-1)	[340,-340,425]	[ ]
				[340,-340,-225]	[ ]
(12,1)	[560,-560,-420]	[ ]	(10,-1)	[416,-416,520]	[ ]
				[416,-416,-312]	[ ]
(13,1)	[660,-660,-495]	[ ]	(11,-1)	[500,-500,625]	[0,1,10]
				[500,-500,-375]	[2]
(14,1)	[768,-768,-576]	[ ]	(12,-1)	[592,-592,740]	[ ]
				[592,-592,-444]	[ ]
(15,1)	[884,-884,-663]	[ ]	(13,-1)	[692,-692,865]	[ ]
				[692,-692,-519]	[ ]
----------	----------	-------	(14,-1)	[800,-800,1000]	[ ]
				[800,-800,-600]	[ ]
----------	----------	-------	(15,-1)	[916,-916,1145]	[ ]
				[916,-916,-687]	[ ]

From the resulting values of x (where $x = 2k$), we search for $k \geq 1$ such that

$$M_n = V_m(P,Q) = 2x^2 - 1 = 2^{2k+1} - 1 = 2^n - 1$$

Is prime. It is clear that a prime number can only be obtained from the pairs $(P,Q)\ \{(3,1),(7,\pm1),(1,-1)\}$. If $(P,Q) = (3,1)$ with $x = 2$, we have $2 = x = 2^k$. Hence, $k = 1$.

Therefore,

$$V_m(3,1) = 2^{2(1)+1} - 1 = 7,$$

which implies $m = 2$ and $n = 3$.

Similarly, for $(P,Q) = (7,1)$ with $x = 2$, we get $k = 1$ and $V_m(7,1) = 7$. This implies $m = 1$ and $n = 3$. In the same way, we can get the values m,n for the pairs $(1,-1),(7,-1)$. Therefore, the set of solutions is as follows.

$$(P,Q,m,n) \in \{(3,1,2,3),(7,1,1,3),(1,-1,4,3),(7,-1,1,3)\}.$$

Case 2: If n even ($n = 2$), then

$$M_n = V_m(P,Q) = 2^n - 1 = 2^2 - 1 = 3$$

Next, we search for values of P and Q such that $V_m(P,Q) = 3$ where $1 \le P \le 15$ and $Q = \pm1$. By checking all values of P and Q, we summarize the results in the Table 9

Table 9. Solutions of equation (12) with $n \ge 2$.

(P,Q)	m	n
(3,1)	1	2
(1,-1)	2	2
(3, -1)	1	2

Hence, the theorem is proved whether n is even and odd. Thus, Theorem 2 is completely proved.

Corollary 3. Suppose that $M_n = V_m(P_1,Q_1)$ and $n = U_r(P_2,Q_2)$ are prime numbers such that $r \ge 2, m \ge 0, 1 \le P_1,P_2 \le 15, Q_1,Q_2 = \pm1$ and the Lucas sequences are nondegenerate. Then the complete form of solutions to equation (1) are shown in the table 10:

Table 10. Solutions of equation (1) with $M_n = V_m(P_1,Q_1)$ and $n = U_r(P_2,Q_2)$.

(P_1,Q_1)	m	(P_2,Q_2)	r
(3,1)	2	(3,1)	2
		(1,-1)	4
		(3,-1)	2
$(7,\pm1)$	2	(3,1)	2
		(1,-1)	4
		(3,-1)	2
(1,-1)	4	(3,1)	2
		(1,-1)	4
		(3,-1)	2
(3,1)	1	(3,1)	2
		(1,-1)	4
		(3,-1)	2
(1,-1)	2	(3,1)	2
		(1,-1)	4
		(3,-1)	2
(3,-1)	1	(3,1)	2
		(1,-1)	4
		(3,-1)	2

Proof. From the results of Theorem 2, we have that

$$(P_1,Q_1,m,n) \in \{(3,1,2,3),(7,1,1,3),(1,-1,4,3),(7,-1,1,3),(3,1,1,2),(1,-1,2,2),(3,-1,1,2)\}.$$

If(P_1, Q_1, m, n) $\in \{(3,1,2,3),(7,1,1,3),(1,-1,4,3),(7,-1,1,3)\}$, we have that

$$7 = V_m(P_1, Q_1) = 2^3 - 1 = 2^{U_r(P_2,Q_2)} - 1.$$

Hence, it remains to find the values of $r \geq 2$ and (P_2, Q_2) with $1 \leq P2 \leq 15$ and $Q_2 = \pm 1$ such that $U_r(P_2, Q_2) = 3$. The Table 11 provides a summary of the computation details:

Table 11. Values of (P_1, Q_1), (P_2, Q_2) and r.

(P_1, Q_1)	m	(P_2, Q_2)	r
(3,1)	2	(3,1)	2
		(1,-1)	4
		(3,-1)	2
$(7, \pm 1)$	2	(3,1)	2
		(1,-1)	4
		(3,-1)	2
(1,-1)	4	(3,1)	2
		(1,-1)	4
		(3,-1)	2

Next, we consider the values of $(P_1, Q_1, m, n) \in \{(3,1,1,2),(1,-1,,2,2),(3,-1,1,2)\}$. If $(P_1, Q_1) = (3,1)$, we solve the following equation for r and (P_2, Q_2):

$$V_m(3,1) = 2^{U_r(P_2,Q_2)} - 1 = 2^2 - 1 = 3,$$

with $r \geq 2, 1 \leq P_2 \leq 15$ and $Q_2 = \pm 1$. Here, we get the solutions

$$(P_1, Q_1, P_2, Q_2, m, r) \in \{(3,1,1,-1,1,3),(3,1,2,-1,1,2)\}.$$

Similarly, if $(P_1, Q_1) = (1,-1)$ we search for (P_2, Q_2) and r satisfying

$$V_m(1,-1) = 2^{U_r(P_2,Q_2)} - 1 = 3 = 2^2 - 1.$$

Thus, we obtain that

$$(P_1, Q_1, P_2, Q_2, m, r) \in \{(1,-1,1,-1,2,3),(1,-1,2,-1,2,2)\}.$$

Finally, by following the same approach for (P1, Q1) = (3, −1), we get that

$$(P_1, Q_1, P_2, Q_2, m, r) \in \{(3,-1,1,-1,1,3),(3,-1,2,-1,1,2)\}.$$

The results of the above cases prove Corollary 3.

Corollary 4. Suppose that $M_n = V_m(P_1, Q_1)$ and $n = V_r(P_2, Q_2)$ are prime numbers with $m, r \geq 0, n \geq 2, 1 \leq P_1, P_2 \leq 15$ and $Q_1, Q_2 = \pm 1$ such that the Lucas sequences are nondegenerate. Then the solutions of the equation (1) are completely given by

Table 12. Solutions of equation (1) with $M_n = V_m(P_1, Q_1)$ and $n = V_r(P_2, Q_2)$.

(P_1, Q_1)	m	(P_2, Q_2)	r
(3,1)	2	(3,1)	1
		(1,-1)	2
		(3,-1)	1
(7,1)	1	(3,1)	1
(7,-1)		(1,-1)	2
		(3,-1)	1
(1,-1)	4	(3,1)	1
		(1,-1)	2
		(3,-1)	1
(3,1)	1	All $(P_2, Q_2) where\ 1 \leq P_2 \leq 15\ and\ Q_2 = \pm 1$	0
(3,1)	1	(2,-1)	1
(1,-1)	2	All $(P_2, Q_2)\ where\ 1 \leq P_2 \leq 15\ and\ Q_2 = \pm 1$	0
(1,-1)	2	(2,-1)	1
(3,-1)	1	All $(P_2, Q_2)\ where\ 1 \leq P_2 \leq 15\ and\ Q_2 = \pm 1$	0
(3,-1)	1	(2,-1)	1

Proof. The proof of this corollary is derived from the results of Theorem 2, with the same methodology used in the proof of Corollary 2. We determine the values of r and (P_2, Q_2) corresponding to the values of $n = 3$ or 2.

• Case 1: If $n = 3$. We solve $V_r(P_2, Q_2) = 3$ such that $r \geq 1, 1 \leq P_2 \leq 15$ and $Q_2 = \pm 1$, following the sequence $\{V_r(P_2, Q_2)\}$ nondegenerate. In fact, the results are given by the set $(P_1, Q_1, P_2, Q_2, m, r) \in$
$\{(3,1,3,1,2,1), (3,1,1,-1,2,2), (3,1,3,-1,2,1), (7,\pm 1,3,1,1,1), (7,\pm 1,1,-1,1,2),$
$(7,\pm 1,3,-1,1,1), (1,-1,3,1,4,2), (1,-1,1,-1,4,4), (1,-1,3,-1,4,2)\}$.
• Case 2: If $n = 2$. We solve $\{V_r(P_2, Q_2)\} = 2$ so that $r \geq 0, 1 \leq P_2 \leq 15$ and $Q_2 = \pm 1$, under the condition that the sequence $\{V_r(P_2, Q_2)\}$ is nondegenerate. The results are given by the Table 13:

Table 13. Values of (P_1, Q_1), m, and the corresponding pairs (P_2, Q_2) with r.

(P_1, Q_1)	m	(P_2, Q_2)	r
(3,1)	1	All (P_2, Q_2) $where$ $1 \leq P_2 \leq 15$ and $Q_2 = \pm 1$	0
(3,1)	1	(2, -1)	1
(1, -1)	2	All (P_2, Q_2) $where$ $1 \leq P_2 \leq 15$ and $Q_2 = \pm 1$	0
(1, -1)	2	(2, -1)	1
(3, -1)	1	All (P_2, Q_2) $where$ $1 \leq P_2 \leq 15$ and $Q_2 = \pm 1$	0
(3, -1)	1	(2, -1)	1

Therefore, Cases 1 and 2 prove the results of the corollary.

3 Conclusions

The study proved that the intersection of Mersenne numbers with non-degenerate Lucas sequences produces a finite and limited set of solutions. And despite the infinite properties of each separately, their joint appearance is considered a unique mathematical event. The research succeeded in employing elliptic curves as an effective analytical tool to accurately identify the rational points of repetitive sequences. This connection provided a strong mathematical proof supporting the theoretical results derived thru advanced algebraic computation software. The results confirm that using these numbers in public key encryption systems poses a security risk due to their ease of enumeration and prediction. The limited nature of this set makes the algorithms built on it at risk of breaches, leading to the search for more random alternatives. This study opens the door to investigating higher-order or greater-coefficient recurrence sequences outside of the current scope of research. It also opens the way for studying other families of prime numbers, such as Fermat numbers, and their relationship with various linear sequences.

Author contribution: Ahmed Hamza Hadi (Master's researcher): Derivation and proof, field research on extracting new mathematical relationships linking the general formula for Mersenne numbers
$M_n = 2^n - 1$ and Lucas sequence terms $\{U_n\}$. Numerical calculations verify the hypotheses using symbolic computation programs (such as Sage math and Magma) to find common identities. Studying the properties of the numbers resulting from the combination of the two sequences.
Asst. Prof. Dr. Haider Rahim Hashim (Academic Supervisor) is, establishing the general framework for the research and selecting open problems that need to be solved in the context of linear recurrence sequences. Reviewing complex proofs and ensuring they are free of logical errors, especially when dealing with exponential equations. Connecting the results achieved by the student to larger theories in number theory.

Acknowledgments

The authors express their gratitude to the editor for landing the article and to the referees for their thorough review and helpful comments that improved the paper's quality.

References

1. D. H. Lehmer, Note on Mersenne numbers, *Amer. Math. Mon.*, **38**, 383-384, (1932), 10.1090/S0002-9904-1932-05396-4.
2. R. L. Graham, D. E. Knuth and O. Patashnik, Concrete Mathematics: A Foundation for Computer Science, (Addison-Wesley, Reading MA), 131-135, (1994).
3. P. Yiu, The Elementary Mathematical Works of Leonhard Euler, *Univ. Central Florida*, 798, (1999).
4. E. Landau, Collected works, *Thales Verlag*, 1-9, (1987).
5. D. Shanks, On numbers of the form $x^4 + 1$, *Math. Comput.*, **15**, 186-189, (1961), 10.2307/2004227.

6. A. Sahan and H. R. Hashim, On certain prime numbers in Lucas sequences, *J. Interdiscip. Math.*, **26**, 2-10, (2023), 10.47974/JIM-1616.
7. A. Baker, Contributions to the theory of diophantine equations. I: On the representation of integers by binary forms, *Proc. Royal Soc. London*, 173-191, (1968), 10.1016/j.jnt.2024.11.008.
8. J. Park, B. Poonen and M. Stoll, Explicit methods for modularity of elliptic curves over totally real fields, *J. Inst. Math. Jussieu*, **22**, 1-51, (2023), 10.1017/S1474748022000115.
9. H. R. Hashim, Solutions of the Markoff equation in Tribonacci numbers, *Rad Hrvat. Akad. Znan. Umjet. Mat. Znan.*, **555**, 71-79, (2023), 10.21857/yq32ohx069.
10. H. R. Hashim, Curious properties of generalized Lucas numbers, *Bol. Soc. Mat. Mex.*, **27**, 10, (2021), 10.1007/s40590-021-00391-7.
11. L. Somer and M. Kříž, On primes in Lucas sequences, *Fibonacci Q.*, **53**, 2-23, (2015).
12. W. Bosma, J. Cannon, C. Fieker and A. Steel, Magma Computational Algebra System, *Version 2.26-15, Univ. Sydney*, (2024), https://magma.maths.usyd.edu.au.