Journal of Algebraic Systems, Vol. 14(No. 2): (2026), pp 317-330.
https://doi.org/10.22044/JAS.2024.14045.1790

GENERALIZED LUCAS PRIMES IN THE FERMAT-EULER EQUATION

H. R. Hashim

Abstract. The property of having infinitely many prime numbers award these numbers to have many applications in various fields of sciences. One of the most important applications is their use in the creation of many public key cryptosystems' private keys. Therefore, the main aim of this paper is considering a well known form of primes generated by the Fermat-Euler equation $p = x^2 + dy^2$ and studying whether or not this form keeps the property of generating infinitely many primes if the unknowns x, y and p are terms in certain binary recurrence sequences called the Lucas sequences of the first kind $\{u_n(a,b)\}$ or the second kind $\{v_n(a,b)\}$. In other words, in this paper we present a technique for investigating the integer solutions (x,y,p) of the equation $p = x^2+dy^2$, where the unknowns are terms in $\{u_n(a,b)\}$ or $\{v_n(a,b)\}$. We also apply this technique for determining the solutions $(x,y,p) = (t_i(a,b), t_j(a,b), t_k(a,b))$ with $1 \leq i \leq j \leq k$, where $t_n(a,b)$ represents the general term $u_n(a,b)$ or $v_n(a,b)$ under certain conditions on the integers a and b.

1. Introduction

The problem of determining prime numbers in the form

$$p = x^2 + dy^2 \tag{1.1}$$

for a given positive integer d, where $x, y \in \mathbb{Z}$, has been in interest to many mathematicians. This problem dates back at least to Fermat (see e.g. [3]) who firstly conjectured the following problems concerning prime numbers of the form (1.1) in case of $d = 1, 2, 3$ and 4, respectively:

$$p = x^2 + y^2 \text{ if and only if } p \equiv 1 \pmod 4 \text{ or } p = 2, \tag{1.2}$$

$$p = x^2 + 2y^2 \text{ if and only if } p \equiv 1, 3 \pmod 8 \text{ or } p = 2, \tag{1.3}$$

$$p = x^2 + 3y^2 \text{ if and only if } p \equiv 1 \pmod 3 \text{ or } p = 3, \tag{1.4}$$

and

$$p = x^2 + 4y^2 \text{ if and only if } p \equiv 1 \pmod 4, \tag{1.5}$$

for some integers x and y. These above conjectures were studied deeply and proved by Euler who publish it in his Latin paper [4] (for more details, see

MSC(2020): Primary: 11D72; Secondary: 11B39, 11D45.
Keywords: Lucas sequences; Diophantine equation; Prime number; Fermat-Euler equation; Elliptic curve.
Received: 8 January 2024, Accepted: 24 September 2024.

e.g. [3]). However, for $d \geq 5$ Euler was unable to give a proof, but he could give conjectures for the cases of $d = 5, 6$; that are

$$p = x^2 + 5y^2 \text{ if and only if } p \equiv 1, 9 \pmod{20}, \tag{1.6}$$

$$p = x^2 + 6y^2 \text{ if and only if } p \equiv 1, 7 \pmod{24}, \tag{1.7}$$

for some integers x and y. These latter two conjectures were proved by Cox [3] who completely solved the general problem of determining the primes of the form (1.1) with $d > 4$ using some techniques from class field theory. More precisely, he proved the following result: if $\gcd(p, d) = 1$ and $\mathcal{O} = \mathbb{Z}[\sqrt{-n}]$ denotes the order in the field $K = \mathbb{Q}[\sqrt{-n}]$, then $x^2+dy^2 = p$ iff the Legendre symbol $\left(\frac{-n}{p}\right) = 1$ and $g_n(x) \equiv 0 \pmod{p}$ is solvable over integers, where $g_n(x) \in \mathbb{Z}[X]$ is the minimal polynomial of a real algebraic integer that generates $K_{\mathcal{O}}$ over K.

In fact, these above results (Euler's result and Cox's result) are very useful and important since they tell us that the number of the prime numbers of the form (1.1) is infinite for any given positive integer d, and the study of prime numbers has been in interest to many scientists for its use and applications in various areas of sciences. On of the most important applications of prime numbers is their use in forming public key cryptosystems' private keys such as RSA, ELGamal and Elliptic curve cryptosystems. Note that such equations of the form (1.1) are known as a type of Diophantine equations.

However, it is well known that the number of primes in integers is infinite, it is also proved that there are infinitely many primes in certain types of binary linear recurrence sequences such as the Lucas sequences of the first kind or the second kind whose general terms are respectively denoted by $u_n(a, b)$ or $v_n(a, b)$, which are defined by the relations (see e.g. [9]):

$$u_0(a, b) = 0, u_1(a, b) = 1, \quad u_n(a, b) = au_{n-1}(a, b) - bu_{n-2}(a, b), \tag{1.8}$$

$$v_0(a, b) = 2, v_1(a, b) = a, \quad v_n(a, b) = av_{n-1}(a, b) - bv_{n-2}(a, b), \tag{1.9}$$

where $n \geq 2$ and the integers a and b are nonzero with $\gcd(a, b) = 1$. In fact, both of these sequences are called by the Lucas sequences and their terms (called generalized Lucas numbers) can be also obtained by what are so called Binet's formulas:

$$u_n(a, b) = \frac{\delta^n - \gamma^n}{\delta - \gamma} \text{ and } v_n(a, b) = \delta^n + \gamma^n, \tag{1.10}$$

with $n \geq 0$ and

$$\delta = \frac{a + \sqrt{a^2 - 4b}}{2} \text{ and } \gamma = \frac{a - \sqrt{a^2 - 4b}}{2} \tag{1.11}$$

represent the zeros of the following characteristic polynomial of these sequences:

$$X^2 - aX + b = 0.$$

Note that δ is known as the golden ratio and $\gamma = \frac{b}{\delta}$. For certain values of a and b, we get some well known sequences that have been investigated by a various number of mathematicians. If $(a, b) = (1, -1)$ then the Lucas sequences respectively give the sequences of Fibonacci numbers $\{u_n(1, -1)\} = \{F_n\}$ and Lucas numbers $\{v_n(1, -1)\} = \{L_n\}$. Also, if $(a, b) = (1, -2)$, that leads to the Jacobsthal sequence $\{u_n(1, -2)\} = \{J_n\}$ and Jacobsthal-Lucas sequence $\{v_n(1, -2)\} = \{j_n\}$. On the other hand, in case of $(a, b) = (2, -1)$ we get the Pell seqence $\{P_n\} = \{u_n(2, -1)\}$ and Pell-Lucas sequence $\{Q_n\} = \{v_n(2, -1)\}$.

Since the infiniteness property of the prime numbers is what makes them very useful to be used in cryptography, one may ask whether or not this property stays true if these primes (particularly, of the form (1.1)) are derived from certain linear recurrence sequences, e.g. the Lucas sequences defined by the relations (1.8) or (1.9). Such a problem was studied partially by Athab and Hashim [1] in which they determined the primes of the form (1.1) in case of the unknowns are terms in Lucas sequences and $d = 1$ (namely, the equation of the form (1.2)) with $(a, b) \in \{(1, -1), (2, -1), (3, -1), (3, 1)\}$. In this paper, we extend this result by presenting a technique for studying the integer solutions

$$(x, y, p) \in \{(u_i(a, b), u_j(a, b), u_k(a, b)), (v_i(a, b), v_j(a, b), v_k(a, b))\}$$

with $i, j, k \geq 1$ of equation (1.1) for any given integer $d \geq 2$ and any pair of nonzero integers (a, b) such that $a \geq 2$, $-a - 1 \leq b \leq a - 1$ and $a^2 - 4b > 0$. Note that we here exclude the case with $a = 1$ and $d = 1$ as it was partially studied in [1] and in order of having a simpler presentation. It is important to remark that in our study, we only focus on the nondegenerate Lucas sequences that is defined as follows: the Lucas sequence at the nonzero parameters a and b is called nondegenerate iff if δ/γ is not a root of unity, and otherwise it is called degenerate. Thus, it is nondegenerate only if $(a, b) \notin \{(\pm 1, 1), (\pm 2, 1)\}$, see e.g. [8]. In fact, investigating the solutions of certain types of Diophantine equations in some Lucas sequences has been in interest to many authors, see e.g. [5], [6] and [7].

2. Auxiliary results

Here, we introduce some previous results which are used latter in the proof of our main results. Firstly, we present the following two lemmas due to the result of Tengely, Szalay and Hashim in [5]:

Lemma 2.1. *If a and b are nonzero integers with $a \geq 2$,*

$$\gcd(a,b) = 1, -a-1 \leq b \leq a-1$$

and $a^2 - 4b > 0$, then the Lucas sequences satisfy the following:

$$\delta^{n-2} \leq u_n(a,b) \leq 2\delta^n, \tag{2.1}$$

$$2\delta^{n-1} \leq v_n(a,b) \leq 2\delta^n \tag{2.2}$$

for $n \geq 1$.

Lemma 2.2. *Let a and b be nonzero integers such that $\gcd(a,b) = 1$ with $a \geq 2$, $-a-1 \leq b \leq a-1$ and $a^2-4b > 0$, then the roots of the characteristic polynomial of Lucas sequences (i.e. δ and γ that are defined in (1.11)) satisfy the following inequalities:*

$$\delta \geq 2 \quad \textit{and} \quad |\gamma| \leq 1.$$

Furthermore, the general terms of Lucas sequences are connected in an identity given in the following lemma (see e.g. [8]):

Lemma 2.3. *Suppose that $c = a^2 - 4b$ such that the integers a and b are nonzero with $\gcd(a,b) = 1$, then the following identity holds for all $n \geq 0$:*

$$v_n^2(a,b) = cu_n^2(a,b) + 4b^n. \tag{2.3}$$

3. Main approach

Here, we present a technique for determining the solutions

$$(x,y,p) = (t_i(a,b), t_j(a,b), t_k(a,b))$$

with $i,j,k \geq 1$ of equation (1.1), where $t_n(a,b)$ represents the general term of either the nondegenerate Lucas sequence of the first kind or the second kind at the nonzero relatively prime parameters a and b with which $a \geq 2$, $-a-1 \leq b \leq a-1$ and $a^2-4b > 0$. For simplicity, we denote the term $t_n(a,b)$ by t_n, and similar idea goes to the general terms of Lucas sequences, i.e. we denote $u_n(a,b)$ by u_n and $v_n(a,b)$ by v_n. So, our technique can be used to obtain complete set of the solution (i,j,k) with $i,j,k \geq 1$ in any equation of the form

$$t_k = t_i^2 + dt_j^2 \tag{3.1}$$

for any given positive integer d, where $t_n = u_n$ or v_n.

Remark 3.1. Note that it is easy to see that the latter equation is satisfied only with $i < k$ and $j < k$. So in order to obtain all the values of i, j and k (with $i, j, k \geq 1$) with which equation (3.1) holds, we only need to obtain such values with $i \leq j$ and $j \leq i$. Indeed, to make the presentation simpler we only solve the equation with $1 \leq i \leq j < k$, and the other (i.e. $1 \leq j \leq i < k$) will be achieved similarly. Then, merging the solutions for both cases will give the complete set of solutions. In other words, without loss of generality and in order to have a simpler presentation, in this paper we only consider the former case.

Indeed, our technique mainly depends on the following arguments:

`(I)` Obtaining an upper bound for i in equation (3.1). That would be by substituting the Binet's formulas of Lucas sequences given in (1.10) and their related inequalities given in (2.1) or (2.2) with the help of (2.2). Indeed, we get after some simplifications an upper bound for i, we may call it by L, i.e $i \leq L$.

`(II)` For each i, we obtain the values of j and k as follows:

- Substituting each i in equation (3.1) to get the equation

$$t_k = dt_j^2 + g, \tag{3.2}$$

  where $g = t_i^2$.
- Next, by substituting the latter equation in the identity (2.3) (where $t_k = u_k$ or v_k) we get the elliptic curve equation

$$Y_1^2 = A_1 X_1^4 + B_1 X_1^2 + C_1, \tag{3.3}$$

  where $X_1 = u_j$ or v_j and the coefficients depend on the values of d, g, c and b^n. Note that we ignore the corresponding values of Y_1 since we are mainly interested in determining the j values which correspond to the values of $X_1 = u_j$ or v_j. In fact, the values of X_1 can be determined by the algorithm `SIntegralLjunggrenPoints()` that's implemented in Magma software [2]. Thus, for each value of X_1, the corresponding value of j is obtained.
- By substituting each value of j in (3.2), we obtain the corresponding value of k. Hence, with this step we obtain the values of i, j and k with $i \leq j < k$ with which equation (3.1) holds. Namely, we obtain all the solutions (i, j, k) of equation (3.1) with $i \leq j < k$.

4. Main results and applications

Here, we first give a result related to the upper bound of i in equation (3.1) as mentioned in argument (I) of the main approach Section. Then, we apply the second argument (i.e. (II)) in solving (3.1) with certain pair of parameters a and b and some positive integer d. Without loss of generality and in order to make the presentation of our result simpler, here we first assume that $b = \pm 1$. Moreover, in order to get a clear and an uncomplicated formula for the upper bounds of i we also assume that $k > 2j + i - 5$. Summing everything up, our main results and their applications are obtained in case of $a \geq 2$, $b = \pm 1$, $2 \leq d \leq 10$ and $k > 2j + i - 5$ with $1 \leq i \leq j < k$.

Theorem 4.1. *Let a and b be nonzero integers with $a \geq 2$, $b = \pm 1$ and $a^2 - 4b > 0$. If $(x, y, p) = (u_i, u_j, u_k)$ or (v_i, v_j, v_k) with $1 \leq i \leq j < k$ and $k > 2j + i - 5$ is a solution of equation (1.1) in case of $d \leq 10$, then*

$$i \leq \left\lfloor \frac{\ln(45\delta^5)}{\ln(\delta)} \right\rfloor, \tag{4.1}$$

where $\delta = \frac{a+\sqrt{a^2-4b}}{2}$.

Proof. In order to prove this theorem, we firstly consider in detail the case of the triples $(x, y, p) = (u_i, u_j, u_k)$ and the other (i.e. $(x, y, p) = (v_i, v_j, v_k)$) can be achieved similarly.

More precisely, if we substitute the triple $(x, y, p) = (u_i, u_j, u_k)$ in equation (1.1), we obtain the equation

$$u_k = u_i^2 + du_j^2, \tag{4.2}$$

where $1 \leq i \leq j < k$. Since $d \leq 10$, we get that

$$u_k = u_i^2 + du_j^2 \leq u_i^2 + 10u_j^2.$$

Next, we divide the latter inequality by u_j as it is greater than zero we obtain that

$$\frac{u_k}{u_j} \leq \frac{u_i^2}{u_j} + 10u_j. \tag{4.3}$$

As $j \geq i$, inequality (4.3) becomes $\frac{u_k}{u_j} \leq u_i + 10u_j$, that can be rewritten as

$$u_k \leq u_j(u_i + 10u_j). \tag{4.4}$$

By substituting the Binet's formula of the Lucas sequence $\{u_n\}$ given in (1.10) in some of the terms of inequality (4.4), we get that

$$\delta^k - \gamma^k \leq (\delta^j - \gamma^j)(u_i + 10u_j),$$

or

$$\delta^k \leq (\delta^j - \gamma^j)(u_i + 10u_j) + \gamma^k. \tag{4.5}$$

Taking the absolute value to inequality (4.5) with the use of inequality (2.1) implies that $|\delta^k| \leq |(\delta^j - \gamma^j)(2\delta^i + 20\delta^j) + \gamma^k|$, which can be simplified as follows:

$$|\delta^k| \leq |2\delta^{i+j} + 20\delta^{2j} - 2\gamma^j\delta^i - 20\delta^j\gamma^j + \gamma^k|.$$

Since $|\gamma| = |\frac{b}{\delta}| = |\frac{1}{\delta}|$ with using the assumptions that $i \leq j$ and $-k < -i$, we obtain that $|\delta^k| < |44\delta^{2j}| + |\delta^{-i}|$. After some simplifications, the latter inequality can be written as $|\delta^i| < \frac{45}{|\delta^{k-2j-i}|}$. Since we have assumed that $k > 2j + i - 5$, then $|\delta^i| < \frac{45}{|\delta^{-5}|} < 45\delta^5$ as $\delta \geq 2$ by Lemma 2.2. Therefore,

$$i \leq \left\lfloor \frac{\ln(45\delta^5)}{\ln(\delta)} \right\rfloor. \tag{4.6}$$

Similarly, as done in the previous case we plug the triple $(x, y, p) = (v_i, v_j, v_k)$ in equation (1.1) to get the equation

$$v_k = v_i^2 + dv_j^2, \tag{4.7}$$

where $1 \leq i \leq j < k$ and $d \leq 10$. Similarly, by dividing the latter inequality by v_j with substituting the Binet's formula of $\{v_n\}$ in v_k/v_j, we again get that $\delta^k \leq (\delta^j - \gamma^j)(v_i + 10v_j) + \gamma^k$. Without repeating the detail of computations that are done on inequality (4.5) we get, by taking the absolute value to the above inequality with the use of inequality (2.2) and the assumptions of $i \leq j$, $-k < -i$ and $k > 2j + i - 5$, that

$$i \leq \left\lfloor \frac{\ln(45\delta^5)}{\ln(\delta)} \right\rfloor. \tag{4.8}$$

Hence, the upper bound of i obtained in (4.6) or (4.8) proves the result of Theorem 4.1. □

The following corollary is an application of Theorem 4.1 for showing the upper bounds of i in equations (4.2) and (4.7) with any positive integer d in case of the Lucas sequences are nondegenerate with $2 \leq a \leq 10$ and $b = \pm 1$. Suppose that the upper of i that is given in (4.6) or (4.8) is denoted by L.

Corollary 4.2. *If the sequences $\{u_n\}$ and $\{v_n\}$ are nondegenerate with $2 \leq a \leq 10$ and $b = \pm 1$, then the upper bounds of i (call it by L), in which the equations (4.2) and (4.7) (with any integer $2 \leq d \leq 10$) are satisfied, are given as follows:*

Table 1: Upper bounds for i

(a,b)	L	(a,b)	L
$(2,-1)$	10	$(3,1)$	8
$(3,-1)$	8	$(4,1)$	7
$(4,-1)$	7	$(5,1)$	7
$(5,-1)$	7	$(6,1)$	7
$(6,-1)$	7	$(7,1)$	6
$(7,-1)$	6	$(8,1)$	6
$(8,-1)$	6	$(9,1)$	6
$(9,-1)$	6	$(10,1)$	6
$(10,-1)$	6	–	–

Without loss of generality and by following the results of Theorem 4.1 and Corollary 4.2, we determine the set of the triples $(x,y,p)=(u_i,u_j,u_k)$ or (v_i,v_j,v_k) satisfying equation (1.1) under some conditions on the indices with certain values of a and b given in Table 1 and all the values of d such that $2\leq d\leq 10$. More precisely, in the following we give results for the solutions of equation (1.1) for some cases e.g. $(a,b)=(2,-1)$ and $(3,-1)$, and the idea can be applied similarly for any values of a and b with $a\geq 2$, $-a-1\leq b\leq a-1$ and $a^2-4b>0$.

Theorem 4.3. *If $x=P_i, y=P_j, p=P_k$ with $1\leq i\leq j<k$ and $2\leq d\leq 10$, then the complete set of solutions (x,y,p,d) to equation (1.1) is given by*

$$(x,y,p,d)\in\{(1,1,5,4),(1,2,29,7)\}.$$

Proof. Since $\{P_n\}=\{u_n(2,-1)\}$, then from Table 1 we see the upper bound of i is 10. Let's first consider $d=2$ and then search for the solutions of equation (1.1) with $x=P_i, y=P_j, p=P_k$ such that $1\leq i\leq j<k$ (since the upper bounds in Table 1 are computed under the condition that $k>2j+i-5$, so this condition is fixed while determining the solutions); namely we investigate the values of i,j and k satisfying the following equation:

$$P_k=P_i^2+2P_j^2. \tag{4.9}$$

Now, by applying Argument (I) of the main approach Section in which we substitute each of $i\in\{1,2,\ldots,10\}$ in equation (4.9) in order to obtain elliptic

curves of the form (3.3), particularly curves of the form

$$Y_1 = 8(dX_1^2 + P_i^2)^2 \pm 4,$$

where $X_1 = P_j$. Indeed, Table 2 gives a summary to the computations of obtaining these curves (i.e. curves of the form $Y_1^2 = A_1X_1^4 + B_1X_1^2 + C_1$) and their solutions (particularly, the positive x coordinate as $X_1 = P_j$, and note that the empty set $\{\}$ means the corresponding elliptic curve has no positive x coordinate in its solutions) for each of the value of $i \in \{1, 2, \ldots, 10\}$.

Table 2: Elliptic curves and their solutions in $\{P_n\}$ with $d = 2$

i	$[A_1, B_1, C_1]$	$\{(X_1, j)\}$
1	$[32, 32, 4]$	$\{\}$
	$[32, 32, 12]$	$\{\}$
2	$[32, 128, 124]$	$\{\}$
	$[32, 128, 132]$	$\{(2, 2)\}$
3	$[32, 800, 4996]$	$\{\}$
	$[32, 800, 5004]$	$\{\}$
4	$[32, 4608, 165884]$	$\{\}$
	$[32, 4608, 165892]$	$\{\}$
5	$[32, 26912, 5658244]$	$\{\}$
	$[32, 26912, 5658252]$	$\{\}$
6	$[32, 156800, 192079996]$	$\{\}$
	$[32, 156800, 192080004]$	$\{\}$
7	$[32, 913952, 6525845764]$	$\{\}$
	$[32, 913952, 6525845772]$	$\{\}$
8	$[32, 5326848, 221682106364]$	$\{\}$
	$[32, 5326848, 221682106372]$	$\{\}$
9	$[32, 31047200, 7530692404996]$	$\{\}$
	$[32, 31047200, 7530692405004]$	$\{\}$
10	$[32, 180956288, 255821704427644]$	$\{\}$
	$[32, 180956288, 255821704427652]$	$\{\}$

From Table 2, we see that the right hand side of equation (4.9) is satisfied only in case of $i = 2$ and $j = 2$. Hence, these imply that $P_k = P_2^2 + 2P_2^2 = 12 = P_3$, but this is not a prime number. So, we exclude this solution. Therefore, we conclude that equation (1.1) has no solution in the integers $x = P_i$, $y = P_j, p = P_k$ such that $1 \leq i \leq j < k$ in case of $d = 2$. In fact, by following the same approach, same conclusion can be gotten with $d = 3, 5, 6, 8$ and 10. Hence, we omit the details of computations for determining the corresponding elliptic curves and their solutions.

Next, we determine the solutions of equation (1.1) where $d = 4$, namely we determine the triples (i, j, k) with $1 \leq i \leq j < k$ and $k > 2j + i - 5$ of the equation

$$P_k = P_i^2 + 4P_j^2. \tag{4.10}$$

The latter equation can be indeed rewritten as follows:

$$p = X^2 + Y^2, \tag{4.11}$$

where $(X, Y, p) = (P_i, 2P_j, P_k)$ In fact, this equation was studied in [1], and its set of solutions in the sequence of Pell numbers is given by

$$(X, Y, p) = (P_i, P_j, P_k) \in \{(1, 1, 2), (1, 2, 5), (2, 5, 29)\},$$

where $1 \leq i \leq j < k$. Now, we examine which of these solutions of equation (4.11) also satisfies equation (4.10). The first solution $(X, Y, p) = (1, 1, 2)$ is ignored since here we have that $Y = 1$, and there is no Pell number satisfies $2P_j = Y = 1$. From the solution $(1, 2, 5)$, we have that $2P_j = Y = 2$ which gives $j = 1$. Hence, we obtain that $(i, j, k) = (1, 1, 3)$ in which equation (4.10) is satisfied with the conditions of $1 \leq i \leq j < k$ and $k > 2j + i - 5$. That means we get that $(x, y, p, d) = (1, 1, 5, 4)$ as a solution to equation (1.1). Finally, we consider the solution $(X, Y, p) = (p_2, p_3, p_5) = (2, 5, 29)$ of equation (4.11). On the other hand, the solution of equation (4.10) are obtained only with having $2P_j = Y = p_3 = 5$ which is impossible. Thus, this solution is also excluded. Note that by following the same approach with having $d = 9$, we obtain no solution to equation (1.1). So, we again omit the details of computations.

Finally, it remains to investigate the solutions of equation (1.1) with $d = 7$, and that can be achieved by determining the values of i, j, k, with $1 \leq i \leq j < k$ and $k > 2j + i - 5$, in which the following equation holds:

$$P_k = P_i^2 + 7P_j^2. \tag{4.12}$$

By following the exact approach applied earlier with $d = 2$, we firstly form elliptic curves of the form $Y_1^2 = A_1X_1^4 + B_1X_1^2 + C_1$ for each value of i with $1 \leq i \leq 10$. In fact, only in case of $i = 1$ we get an elliptic curve that have a positive x-coordinate in its solutions. In other words, with $i = 1$ we have the elliptic curves

$$Y_1^2 = 392X_1^4 + 112X_1^2 + 4,$$
$$Y_1^2 = 392X_1^4 + 112X_1^2 + 12,$$

where $X_1 = P_j$. We solve the above curves by the Magma algorithm `SIntegralLjunggrenPoints()`, and then we only get $X_1 = 2$ as a positive x-coordinate of the solutions of the former equation. But, the latter equation has no integer solutions. Therefore, $2 = X_1 = P_j$ implies that $j = 2$. Finally, substituting $i = 1$ and $j = 2$ in equation (4.12) gives that $P_k = P_1^2 + 7P_2^2 = 1^2 + 7(2^2) = 29$ which gives $k = 5$. Thus, we have the triples $(i, j, k) = (1, 2, 5)$ with which equation (4.12) is held. Indeed, this triple with $d = 7$ leads to $(x, y, p, d) = (1, 2, 29, 7)$ which is the final claimed solution of equation (1.1). Hence, Theorem 4.3 is completely proved. □

Theorem 4.4. *The Diophantine equation* (1.1) *with* $2 \leq d \leq 10$ *has no solution in the integers* x, y *and* p *if* $(x, y, p) = (v_i(3, -1), v_j(3, -1), v_k(3, -1))$ *with* $1 \leq i \leq j < k$.

Proof. In order to achieve the proof, we follow the same strategies applied in the proof of Theorem 4.3 with less details. So, we now need to solve equation (1.1) in case of $(x, y, p) = (v_i(3, -1), v_j(3, -1), v_k(3, -1))$ with $2 \leq d \leq 10$ and $1 \leq i \leq j < k$ under the condition of $k > 2j + i - 5$. Namely, we solve the following equation completely:

$$v_k(3, -1) = v_i(3, -1)^2 + dv_j(3, -1)^2. \tag{4.13}$$

From Table 1, we have $i \leq 8$. As done in the proof of the previous theorem, we apply Argument (I) of the main approach Section in which we substitute each of $i \in \{1, 2, \ldots, 8\}$ in equation (4.13). Then we substitute the obtained equation in identity (3.1) to get elliptic curves of the form

$$Y_1{}^2 = 13[(dX_1{}^2 + v_i(3, -1)^2)^2 \pm 4], \tag{4.14}$$

where $X_1 = v_j(3, -1)$ and $2 \leq d \leq 10$. After some simplifications, let's assume that the latter curve is written in the form $Y_1^2 = A_1X_1^4 + B_1X_1^2 + C_1$. The next step is for each $d \in \{2, 3, \ldots, 10\}$, we determine the corresponding elliptic curves for every $i \in \{1, 2, \ldots, 8\}$. In fact, the integral points on these curves are obtained using the Magma algorithm

`SIntegralLjunggrenPoints()`. In fact, without loss of generality and repeating the strategy (as done in the proof of the previous theorem) of obtaining the elliptic curves and their solutions, in the following we only deal in details with the case of $d = 3$. The other cases are handled similarly. The following table summarizes the computations of calculating the elliptic curves' coefficients (i.e. curves of the form (4.14) with $d = 3$) and the $x-$ coordinates of their solutions in which $X_1 = v_j(3, -1)$:

Table 3: Elliptic curves and their solutions in $\{v_n(3, -1)\}$ with $d = 3$

i	$[A_1, B_1, C_1]$	$\{(X_1, j)\}$
1	$[117, 702, 1105]$	$\{(3, 1)\}$
	$[117, 702, 1001]$	$\{\}$
2	$[117, 9438, 190385]$	$\{\}$
	$[117, 9438, 190281]$	$\{\}$
3	$[117, 101088, 21835060]$	$\{\}$
	$[117, 101088, 21834956]$	$\{\}$
4	$[117, 1104558, 2606940921]$	$\{\}$
	$[117, 1104558, 2606941025]$	$\{\}$
5	$[117, 12047022, 310108416865]$	$\{\}$
	$[117, 12047022, 310108416761]$	$\{\}$
6	$[117, 131414712, 36901338739460]$	$\{\}$
	$[117, 131414712, 36901338739356]$	$\{\}$
7	$[117, 1433512782, 4390937812302041]$	$\{\}$
	$[117, 1433512782, 4390937812302145]$	$\{\}$
8	$[117, 15637227918, 522484822562988545]$	$\{\}$
	$[117, 15637227918, 522484822562988441]$	$\{\}$

From the above table, we only get a positive solution to the elliptic curve

$$Y_1 = 117{X_1}^4 + 702{X_1}^2 + 1105,$$

that is given by $(X_1, Y_1) = (3, 130)$ in the case of $i = 1$. We only consider the value of $X_1 = 3$ since $3 = X_1 = v_j(3, -1)$, and this gives $j = 1$. By substituting $i = j = 1$ with $d = 3$ in equation (4.13), we obtain that

$v_k(3,-1) = 9 + 3(9) = 36$ or $k = 3$. But 36 is not a prime number, so we ignore this solution. Similarly, one can easily show that the equation (4.13) is again not solvable in case of the other values of d, so we omit the detail of computations. Thus, Theorem 4.4 is proved. □

Remark 4.5. By following the same approach used in the proof of Theorems 4.3 and 4.4, one can completely solve equation (1.1) with any positive value of d and $(x, y, p) = (v_i(a,b), v_j(a,b), v_k(a,b))$ such that $1 \le i \le j \le k$, $a \ge 2$, $-a-1 \le b \le a-1$ and $a^2-4b > 0$. However, from the results of Theorem 4.1 and Corollary 4.2 and by following the result of Theorem 4.4 we conjecture the following result:

`Conjecture 1.` The Diophantine equation (1.1) with $2 \le d \le 10$ has no solution in the integers x, y and p if $x = v_i(a,b), z = v_j(a,b)$ and $p = v_k(a,b)$ with $1 \le i \le j \le k$ and all pairs of (a,b) given in Table 1 (including $(a,b) = (3,-1)$, that is already considered in Theorem 4.4).

Acknowledgments

The author wishes to thank the editor for handling the paper and the referees for the careful reading of the manuscript and many useful comments and remarks.

References

1. A. S. Athab and H. R. Hashim, The solution of Fermat's two squares equation and its generalization in Lucas sequences, *Baghdad Sci. J.*, **21** (2024), 2079–2092.
2. W. Bosma, J. Cannon and C. Playoust, The Magma algebra system I: The user language, *J. Symbolic Comput.*, **24** (1997), 235–265.
3. D. Cox, *Primes of the form x^2+ny^2: Fermat, class field theory, and complex multiplication with solutions*, AMS Chelsea Publ., **387**, 2022.
4. L. Euler, Demonstratio theorematis Fermatiani omnem numerum primum formae $4n+1$ esse summam duorum quadratorum, *Novi commentarii academiae scientiarum Petropolitanae*, (1760), 3–13.
5. H. R. Hashim, L. Szalay and Sz.Tengely, Markoff-Rosenberger triples and generalized Lucas sequences, *Period. Math. Hungar.*, **85** (2022), 188–202.
6. H. R. Hashim and Sz.Tengely, Solutions of a generalized Markoff equation in Fibonacci numbers, *Math. Slovaca*, **70** (2020), 1069–1078.
7. F. Luca and A. Srinivasan, Markov equation with Fibonacci components, *Fibonacci Quart.*, **56** (2018), 126–129.
8. P. Ribenboim, *My numbers, my friends: Popular lectures on number theory*, New York, NY: Springer, 2000.
9. L. Somer and M. Kříž, On primes in Lucas sequences, *Fibonacci Quart.*, **53** (2015), 2–23.

Hayder Raheem Hashim
Faculty of Computer Science and Mathematics, University of Kufa, P.O. Box 21, 54001, Al Najaf, Iraq.
Email: hayderr.almuswi@uokufa.edu.iq

Journal of Algebraic Systems

GENERALIZED LUCAS PRIMES IN THE FERMAT–EULER EQUATION

H. R. HASHIM

اعداد اول لوکاس تعمیم‌یافته در معادله فرما–اویلر

حیدر رحیم هاشم

دانشکده علوم کامپیوتر و ریاضی، دانشگاه کوفه، نجف، عراق

خاصیت داشتن بی‌نهایت عدد اول، این اعداد را برای کاربردهای فراوان در شاخه‌های گوناگون علوم سودمند می‌سازد. یکی از مهم‌ترین کاربردها، استفاده از آن‌ها در تولید کلیدهای خصوصی بسیاری از رمزنگاری‌های کلید عمومی است. از این‌رو، هدف اصلی این مقاله بررسی یک فرم شناخته‌شده از اعداد اول حاصل از معادله فرما–اویلر $p = x^2 + dy^2$ و مطالعه این موضوع است که آیا این فرم همچنان ویژگی تولید بی‌نهایت عدد نخست را حفظ می‌کند یا نه، هنگامی که مجهول‌های x و y و p جمله‌هایی از برخی دنباله‌های بازگشتی دوتایی خاص، موسوم به دنباله‌های لوکاس از نوع اول $\{u_n(a,b)\}$ یا نوع دوم $\{v_n(a,b)\}$ باشند. به عبارت دیگر، در این مقاله روشی برای بررسی حل‌های صحیح (x,y,p) از معادله $p = x^2 + dy^2$ ارائه می‌کنیم، جایی که مجهول‌ها جمله‌هایی از $\{u_n(a,b)\}$ یا $\{v_n(a,b)\}$ هستند. همچنین، این روش را برای تعیین حل‌های $(x,y,p) = (t_i(a,b), t_j(a,b), t_k(a,b))$ با شرط $1 \le i \le j \le k$ به‌کار می‌بریم، جایی که $t_n(a,b)$ جمله عمومی $u_n(a,b)$ یا $v_n(a,b)$ را تحت شرایطی بر اعداد صحیح a و b نشان می‌دهد.

کلمات کلیدی: دنباله‌های لوکاس، معادله دیوفانتین، عدد اول، معادله فرما–اویلر، خم بیضوی.