The Solution of Fermat’s Two Squares Equation and Its Generalization In Lucas Sequences

Ali S. Athab, Hayder R. Hashim

Department of Mathematics, Faculty of Computer Science and Mathematics, University of Kufa, Al Najaf, Iraq.

Received 22/03/2023, Revised 18/06/2023, Accepted 20/06/2023, Published Online First 20/11/2023

Abstract

As it is well known, there are an infinite number of primes in special forms such as Fermat’s two squares form, \( p = x^2 + y^2 \) or its generalization, \( p = x^2 + y^4 \), where the unknowns \( x, y, \) and \( p \) represent integers. The main goal of this paper is to see if these forms still have an infinite number of solutions when the unknowns are derived from sequences with an infinite number of prime numbers in their terms. This paper focuses on the solutions to these forms where the unknowns represent terms in certain binary linear recurrence sequences known as the Lucas sequences of the first and second types.

Keywords: Diophantine equation, Elliptic curves, Fermat’s two squares Theorem, Lucas sequences, Prime numbers.

Introduction

Many scientists have been interested in the study of prime numbers because of their use and applications in many fields of science such as mathematics and computer science. Prime numbers are used to form private keys in many public key cryptosystems, including the RSA cryptosystem, the ElGamal cryptosystem, the Elliptic curve cryptosystem, and others. In fact, it is known that there are an infinite number of prime numbers with numerous well-known forms. For example, Edmund Landau conjectured that there are an infinite number of primes of the form \( p = x^2 + 1 \). Furthermore, Shanks conjectured that for some integer \( x \), there are infinite prime numbers of the form \( p = x^4 + 1 \) and \( p = \frac{1}{2} (x^2 + 1) \). Fermat also conjectured that any prime \( p = 4k + 1 \) can be written as \( p = x^2 + y^2 \), see e.g., Euler provided proof of this conjecture in 1749. Furthermore, Dirichlet proved that there are an infinite number of primes of the form \( p = ak + b \) if \( \gcd(a, b) = 1 \), where \( a \) and \( b \) are integers, see e.g., Indeed, this latter result demonstrates that there are an infinite number of primes of the form \( p = x^2 + y^2 \). Friedlander and Iwaniec proved that there are an infinite number of primes of the form \( p = x^2 + y^4 \) as a generalization of Fermat’s result.

On the other hand, it is known that certain types of linear recurrence sequences contain an infinite number of primes. For example, it is conjectured that the Fibonacci and Lucas number sequences have an infinite number of primes, where these sequences are defined by

\[
F_0 = 0, F_1 = 1, F_n = F_{n-1} + F_{n-2} \text{ for } n \geq 2
\]

and

\[
L_0 = 2, L_1 = 1, L_n = L_{n-1} + L_{n-2} \text{ for } n \geq 2.
\]

For more details, see for instance. Thereafter, Lawrence and Michal expanded this latter conjecture to more general sequences, referred to as the Lucas sequences of the first kind.
\{U_n(P,Q)\} (simply \{U_n\}) or the second kind \{V_n(P,Q)\} (simply \{V_n\}), which are defined by the relations:

\[
U_0(P,Q) = 0, U_1(P,Q) = 1, U_n(P,Q) = PU_{n-1}(P,Q) - QU_{n-2}(P,Q) \text{ for } n \geq 2.
\]

\[
V_0(P,Q) = 2, V_1(P,Q) = P, V_n(P,Q) = PV_{n-1}(P,Q) - QV_{n-2}(P,Q) \text{ for } n \geq 2,
\]

where P and Q are nonzero integers satisfying \(gcd(P,Q) = 1\). Furthermore, it is well known that the first and second kinds of Lucas sequences are connected in the identity

\[
V_n^2(P,Q) = DU_n^2(P,Q) + 4Q^n,
\]

where \(D = P^2 - 4Q\), as in [11]. The characteristic polynomial of these sequences is defined by

\[
X^2 - PX + Q = 0,
\]

where

\[
\alpha = \frac{P+\sqrt{D}}{2} \quad \text{and} \quad \beta = \frac{P-\sqrt{D}}{2}
\]

are the latter polynomial’s roots. Hence, these sequences can be respectively written by the following formulas which are known as Binet’s formulas:

\[
U_n(P,Q) = \frac{\alpha^n - \beta^n}{\alpha - \beta} \text{ for } n \geq 0.
\]

and

\[
V_n(P,Q) = \alpha^n + \beta^n \text{ for } n \geq 0,
\]

where \(\alpha\) is called the golden ratio and \(\beta = \frac{-1}{\alpha}\) .

Thus, if \(\alpha/\beta\) is not a root of unity then these sequences are said to be nondegenerate and degenerate otherwise. As a result, they are degenerate only with \((P,Q) \in \{(\pm 1, 1), (\pm 2, 1)\}\), for more details see e.g. [11]. Note that the terms of these sequences are called by the generalized Lucas numbers. Moreover, such results concerning primes in the Lucas sequences, see e.g. [12].

Regarding these sequences, when \((P,Q) = (1, -1)\), the Fibonacci and Lucas sequences are obtained. If \((P,Q) = (2, -1)\), the sequences known as Pell and Pell-Lucas are obtained, which are defined as follows:

\[
P_0 = 0, P_1 = 1, P_n = 2P_{n-1} + P_{n-2} \text{ for } n \geq 2.
\]

and

\[
Q_0 = 2, Q_1 = 2, Q_n = 2Q_{n-1} + Q_{n-2} \text{ for } n \geq 2.
\]

Note that Binet’s formulas for the sequences \{\(F_n\), \(L_n\), \(P_n\)\} and \{\(Q_n\)\} are defined as follows:

\[
F_n = \frac{\alpha^n - \beta^n}{\sqrt{5}}, L_n = \alpha^n + \beta^n, \quad \text{and} \quad P_n = \frac{\alpha^n - \beta^n}{\sqrt{5}}.
\]

where \((\alpha, \beta) = \left(\frac{1+\sqrt{5}}{2}, \frac{1-\sqrt{5}}{2}\right)\) and \((\alpha_2, \beta_2) = (1 + \sqrt{2}, 1 - \sqrt{2})\).

In general, the study of these sequences and other types of sequences connected to other areas of Mathematics has been recent of interest to many authors, see e.g. [13, 14].

As these sequences have infinitely many primes, the most interesting question one could ask is: are their infinity or finitely many primes of the abovementioned forms, namely \(p = x^2 + 1, x^2 + y^2, x^2 + y^4, \) and \(x^2 + y^4\), where \(p, x\) and \(y\) represent terms in \(\{U_n(P,Q)\}\) or \(\{V_n(P,Q)\}\) ?

In [15, 16] the above question is answered by studying such solutions to the equations: \(p = x^2 + 1, p = x^4 + 1\) and \(p = \frac{1}{2}(x^2 + 1)\). In fact, it turned out that the above equations have a finite number of solutions.

The aim of this paper is to finish answering the above question for the remaining forms, i.e.

\[
p = x^2 + y^2,
\]

and

\[
p = x^2 + y^4,
\]

where \((x, y, p) \in \{(U_i(P,Q), U_j(P,Q), U_k(P,Q), V_i(P,Q), V_j(P,Q), V_k(P,Q))\} \) with \(i, j, k \geq 1\) and P and Q are certain parameters. To be more precise, our argument is applied to study such
special solutions in the case of \(-2 \leq P \leq 3\) and \(Q = \pm 1\).

### Auxiliary Results
In this section, some results regarding the sequences of Fibonacci numbers, Lucas numbers, Pell numbers, and Pell-Lucas numbers are presented. These sequences satisfy the following inequalities that are utilized later in the proofs of the main results:

\[
\alpha_1^{n-2} \leq F_n \leq \alpha_1^{n-1} \quad \text{for} \quad n \geq 1, \tag{14}
\]

\[
\alpha_1^{n-1} \leq L_n \leq \alpha_1^{n+1} \quad \text{for} \quad n \geq 1, \tag{15}
\]

\[
\alpha_2^{n-2} \leq P_n \leq \alpha_2^{n-1} \quad \text{for} \quad n \geq 1, \tag{16}
\]

\[
\alpha_2^{n-1} \leq Q_n \leq \alpha_2^{n+1} \quad \text{for} \quad n \geq 1. \tag{17}
\]

Furthermore, Hashim, Szalay, and Tengely\(^{11}\) proved that if \(P \geq 2\) and \(-P - 1 \leq Q \leq P + 1\) then the Lucas sequences of the first and second kind satisfy the following inequalities:

\[
\alpha_1^{n-2} \leq U_n \leq \alpha_1^{2n} \quad \text{for} \quad n \geq 1, \tag{18}
\]

\[
2\alpha_1^{n-1} \leq V_n \leq \alpha_1^{2n} \quad \text{for} \quad n \geq 1. \tag{19}
\]

### Main Approach
This section presents a procedure for investigating the solutions \((x, y, p) = (R_i, R_j, R_k)\) with \(i, j, k \geq 1\) of Eqs. 12 and 13, where \(R_i\) denotes a generalized Lucas number of the first or second kind, namely \(R_i = U_i\) or \(V_i\). Indeed, the technique of this procedure is applied in case of \(-2 \leq P \leq 3\) and \(Q = \pm 1\), where \(\{U_n\}\) and \(\{V_n\}\) are nondegenerate sequences. For simplicity, the Lucas sequences with \((P, Q) \in \{(3, 1), (3, -1)\}\) are denoted by the following: \(U_n(3, 1) = M_n, V_n(3, 1) = N_n, U_n(3, -1) = D_n,\) and \(V_n(3, -1) = E_n\).

It is clear that Eqs. 12 and 13 have such special solutions only \(i < k\) and \(j < k\). Hence, in order to find all the solutions \((x, y, p) = (R_i, R_j, R_k)\) with \(i, j, k \geq 1\), the condition that \(i \leq j < k\) is fixed. The first two components of the obtained solutions are permuted. The following presents a summary of the general steps involved in finding the solutions \((x, y, p) = (R_i, R_j, R_k)\) of either Eq. 12 or 13, subject to the condition \(1 \leq i \leq j < k\). Let’s consider the procedure with the equation

\[
R_k = R_i^2 + R_j^2, \tag{20}
\]

with \(1 \leq i \leq j < k\) and \((R_i, R_j, R_k) = (U_i, U_j, U_k)\) or \((V_i, V_j, V_k)\). The idea goes similarly in the case of the other equation.

Step 1: To obtain an upper bound for \(i\), the process involves dividing Eq. 20 by \(R_j\), utilizing Binet’s formulas presented by 6 or 7 and incorporating with the inequalities presented by 14, 15, 16, 17, 18, and 19. After some simplifications, the resulting upper bound is denoted as \(i \leq L\).

Step 2: For \(i = 1, 2, \ldots, L\), a specific \(i\) is inserted into Eq. 20 to obtain

\[
R_k = R_j^2 + c \quad \text{for} \quad c = R_i^2. \tag{21}
\]

Step 3: Then substitute Eq. 21 in the identity relationship between Lucas numbers of the first and second kind presented by 5 gives the elliptic curves of the form

\[
y_1^2 = A_1x_1^4 + B_1x_1^2 + C_1, \tag{22}
\]

where \((x_1 = U_j\) or \(V_j\)). Note that Eq. 22 can be written in the form

\[
y^2 = X^3 + B_1X^2 + A_1C_1X, \tag{23}
\]

where \(Y = A_1x_1y_1\) and \(X = A_1x_1^2\).

Step 4: The values of \(X\) \((\text{with} \quad X = A_1x_1^2)\) in curve 23 can be found using the SageMath\(^{17}\) function integral_points().

Step 5: The values of \(j\) are calculated using the obtained value of \(x_i\).

Step 6: Plugging the obtained value of \(j\) in Eq. 21 to get the values of \(k\). Hence, all the values of \((i, j, k)\) in which Eq. 20 is satisfied are obtained.

Step 7: After obtaining all the possible solutions \((i, j, k)\) of Eq. 20 under the condition \(1 \leq i \leq j < k\), it remains to permute the components \(i\) and \(j\) in \((i, j, k)\) in order to have all the possible solutions of Eq. 20 \((\text{or Eq. 12})\) with \(i, j, k \geq 1\).
Results and Discussion

**Theorem 1**: If \((x, y, p) = (F_i, F_j, F_k)\) with \(i, j, k \geq 1\), then the solutions of Eq. 12 are given by
\[
(x, y, p) \in \{(1, 1, 2), (1, 2, 5), (2, 1, 5), (2, 3, 13), (3, 2, 13)\}.
\]

**Theorem 2**: Assume that \(x = L_i, y = L_j\) and \(p = L_k\) such that \(i, j, k \geq 1\), then Eq 12 has no solution in the integers \(x, y\) and \(p\).

**Theorem 3**: Suppose that \((x, y, p) = (P_i, P_j, P_k)\) with \(i, j, k \geq 1\), then the complete set of solutions to Eq 12 is as follows:
\[
(x, y, p) \in \{(1, 1, 2), (1, 2, 5), (2, 1, 5), (2, 3, 5), (3, 2, 5)\}.
\]

**Theorem 4**: Eq 12 has no solution of the form \((x, y, p) = (Q_i, Q_j, Q_k)\) with \(i, j, k \geq 1\) such that \(x = Q_i, y = Q_j\) and \(p = Q_k\).

**Theorem 5**: Suppose that \(x = M_i, y = M_j\) and \(p = M_k\) with \(i, j, k \geq 1\), then Eq 12 has no solution of the form \((x, y, p) = (M_i, M_j, M_k)\).

**Theorem 6**: Eq 12 has no solution in \(x = N_i, y = N_j\) and \(p = N_k\), where \(i, j, k \geq 1\).

**Theorem 7**: The set of solutions to Eq 12 with \(i, j, k \geq 1\) and \((x, y, p) = (D_i, D_j, D_k)\) is as follows:
\[
(x, y, p) \in \{(3, 10, 109), (10, 3, 109), (10, 33, 1189), (33, 10, 1189)\}.
\]

**Theorem 8**: Assume that \(x = E_i, y = E_j\) and \(p = E_k\) with \(i, j, k \geq 1\), then Eq 12 has no solutions of the form \((x, y, p) = (E_i, E_j, E_k)\).

**Proposition 1**: If \((x, y, p) = (F_i, F_j, F_k)\) with \(i, j, k \geq 1\), then the solutions to Eq 13 are only given by \((x, y, p) = (1, 1, 2)\) and \((2, 1, 5)\).

**Proposition 2**: If \((x, y, p) = (L_i, L_j, L_k)\) with \(i, j, k \geq 1\) represents the solution to Eq 13, then it has no such solutions.

**Proposition 3**: If \((x, y, p) = (P_i, P_j, P_k)\) where \(i, j, k \geq 1\), then the solutions to Eq 13 are given by \((x, y, p) \in \{(1, 1, 2), (2, 1, 5)\}.

**Proposition 4**: Eq 13 has no solution in \(x = Q_i, y = Q_j\) and \(p = Q_k\), where \(i, j, k \geq 1\).

**Proposition 5**: Assume that \(x = M_i, y = M_j\) and \(p = M_k\) with \(i, j, k \geq 1\), then Eq 13 has no solution in \(x, y,\) and \(p\).

**Proposition 6**: If \(x = N_i, y = N_j\) and \(p = N_k\) with \(i, j, k \geq 1\) are the components of the solution \((x, y, p)\) to Eq 13, then it has no such solution.

**Proposition 7**: Eq 13 has no solution of the form \((x, y, p) = (D_i, D_j, D_k)\) with \(i, j, k \geq 1\).

**Proposition 8**: Eq 13 is not solvable in the integers \(x = E_i, y = E_j\) and \(p = E_k\) with \(i, j, k \geq 1\).

**Proofs**

**Proof of Theorem 1**: From the main approach section presented in Section 3, the first step is to obtain an upper bound for \(i\) in the equation
\[
F_k = F_i^2 + F_j^2,
\]
for \(i, j, k \geq 2\), since \(F_i = F_2 = 1\) so \(i \geq 2\) is assumed. The following summarizes the steps for obtaining this bound under the condition that \(i \leq j < k\):

- Dividing Eq 24 by \(F_j\) gives
\[
\frac{F_k}{F_j} = \frac{F_i^2}{F_j} + F_i.
\]

Since \(i \leq j\); that is, \(F_i \leq F_j\), so
\[
\frac{F_k}{F_j} \leq F_i + F_j.
\]

Substituting inequality 14 and (identity 6 or 10 with \((a_i, b_i) = ((1 + \sqrt{5})/2, (1 - \sqrt{5})/2))\) in inequality 25 gives that
\[
\alpha_i^k - \beta_i^k \leq (\alpha_i^j - \beta_i^j)(\alpha_i^{j-1} + \alpha_i^{j-1}) \leq \alpha_i^{j+i-1} + \alpha_i^{j+i-1} - \beta_i^{j+i-1} - \beta_i^{j+i-1}.
\]
From the fact that $\beta_1 = -\frac{1}{a_1}$ and the assumption of $i \leq j < k$, the latter inequality leads to

$$\alpha_1^k \leq 4 \alpha_1^{2j-1} \pm \frac{1}{\alpha_1^i}. \quad 26$$

Now, let’s take the absolute value of inequality 26 gives

$$|\alpha_1^k| \leq |4\alpha_1^{2j-1}| + \frac{1}{\alpha_1^i}.$$  

Hence,

$$\alpha_1^k \leq \frac{1}{\alpha_1^i}(5\alpha_1^{2j+i-1}) \quad 27$$
as $1 < \alpha_1^{2j+i-1}$.

Dividing inequality 27 by $\alpha_1^{2j+i-1}$ gives

$$\alpha_1^{k-2j-i+1} \leq \frac{5}{\alpha_1^i},$$
which can be written as

$$\frac{5}{|\alpha_1^{k-2j-i+1}|} \quad 28$$
where $l = k - 2j - i + 1$.

Suppose that

$$B = \min_{i \in \mathbb{Z}} |\alpha_1^i - 2.5|.$$  

If $i = 0$, then

$$B = 1.5.$$  

If $i \geq 1$, then $\alpha_1^i \geq \alpha_1^1 > 1.618$. This implies that

$$B > 0.882.$$  

Similarly, if $i \leq -1$ then

$$B > 1.882.$$  

This gives that $B \geq 0.882$. Therefore, inequality 28 gives that

$$\alpha_1^i < \frac{5}{B} < \frac{5}{0.882} < 5.669,$$
which implies that

$$i \leq \frac{\ln(5.669)}{\ln(\alpha_1)} < \frac{\ln(5.669)}{\ln(1.618)} < 3.606.$$  

Hence, $i \leq 3$.

According to the second step in our main approach, substituting each of the values of $i$ such that $2 \leq i \leq 3$ in Eq 24 is performed to change it with respect to $j$ and $k$. This can be summarized in the following steps:

- For $i = 2$, the following eq is obtained
  $$F_k = F_j^2 + 1. \quad 29$$

- For $i = 3$, then
  $$F_k = F_j^2 + 4. \quad 30$$

Finally, the values of $j$ and $k$ corresponding to each value of $i \in \{2, 3\}$ must be obtained.

The substitution of Eq 29 in identity 5 is applied to get the elliptic curves

$$Y^2 = X^3 + 10X^2 + 45X \text{ and } Y^2 = X^3 + 10X^2 + 5X,$$

where $X = 5x_1^2$ such that $x_1 = F_j$. By the SageMath function integral points (), the following points are obtained

$$(X, Y) \in \{(-9, 6), (-5, 10), (-1, 2), (0,0), (1, 4), (5, 20), (20, 110)\}.$$  

Since the positive values of $X$ are needed, then only the values of $X \in \{1, 5, 20\}$ are considered.

- For $1 = X = 5x_1^2 = 5F_j^2$; that is impossible.

- If $5 = 5F_j^2$, then $F_j^2 = 1$. Therefore, $j = 2$. By substituting $j = 2$ in Eq 29, then $F_k = F_2^2 + 1 = 2$ which gives $k = 3$. Hence, the corresponding solution of Eq 12 for $(i, j, k) = (2, 2, 3)$, with $i \leq j < k$ is $(x, y, p) = (F_2, F_2, F_3) = (1, 1, 2)$.
Finally, if \( X = 20 \), then \( F_j^2 = 4 \). This leads to \( j = 3 \). Similarly, the corresponding solution is \((x, y, p) = (1, 2, 5)\).

- Secondly, combining Eq 30 with identity 5 gives the elliptic curves

\[
Y^2 = X^3 + 20X^2 + 420X \quad \text{and} \quad Y^2 = X^3 + 20X^2 + 380X, 
\]

where \( X = 5x_1^2 \) such that \( x_1 = F_j \). Similarly, the following Sage Math function: integral points () gives that

\[
X \in \{5, 20, 21, 45, 76, 1520\}. 
\]

As done in the previous case, the solutions \( X \in \{5, 20, 45\} \) are gotten for \( X = 5F_j^2 \).

- For \( 5 = 5F_j^2 \), then \( F_j^2 = 1 \). Hence, \( j = 2 \), and this must be eliminated since gives \( i = 3 \) with the assumption that \( i \leq j < k \).

- For \( X = 20 \), then \( F_j = 2 \). Thus, \( j = 3 \). Again, substituting \( j = 3 \) in Eq 30 gives \( F_k = 8 \), which gives no solution.

- Finally, for \( X = 45 \) then \( j = 4 \) which implies that \( F_k = 13 \). Thus, \( k = 7 \). The corresponding solution to Eq 12 under the condition \( i \leq j < k \) is \((x, y, p) = (2, 3, 13)\).

According to the last step in the main approach, the permutation of the first two components in the following solutions is applied

\[
(x, y, p) \in \{(1, 1, 2), (1, 2, 5), (2, 3, 13)\}
\]

to obtain the complete set of solutions to Eq 12 with \( i, j, k \geq 2 \), which is given by

\[
(x, y, p) \in \{(1, 1, 2), (1, 2, 5), (2, 1, 5), (2, 3, 13), (3, 2, 13)\}.
\]

Hence, the proof of Theorem 1 is achieved.

**Proof of Theorem 2:** To begin the proof, it is necessary to find an upper bound for \( i \) in the equation

\[ L_k = L_j^2 + L_i^2, \]

where \( i, j, k \geq 1 \) under the the condition that \( i \leq j < k \). First, Eq. 31 is divided by \( L_j \) to obtain

\[ \frac{L_k}{L_j} = \frac{L_i^2}{L_j} + L_j. \]

Hence,

\[ \frac{L_k}{L_j} \leq L_i + L_j, \]

since \( i \leq j \). Subsequently, it can be determined that

\[
\alpha_i^k + \beta_i^k \leq (\alpha_i^j + \beta_i^j)(\alpha_i^{i+1} + \alpha_i^{j+1}) \leq \alpha_i^{i+j+1}
\]

\[
+\alpha_i^{2j+i+1} + \beta_i^{i+1} + \beta_i^{j+1}\alpha_i^{i+1},
\]

by substituting inequality 15 and (identity 7 or 10 in the case of Lucas sequence) in inequality 32. By using the condition that \( i \leq j < k \) with the fact \( \beta_1 = \frac{-1}{\alpha_i} \) in the latter inequality, it can be deduced that

\[
|\alpha_i^k| \leq |4\alpha_i^{2j+i+1}| + |\frac{1}{\alpha_i^i}|.
\]

It follows that

\[
\alpha_i^k \leq \frac{1}{\alpha_i^i}(5\alpha_i^{2j+i+1}).
\]

Dividing the last inequality by \( \alpha_i^{2j+i+1} \), the result shows that

\[
\alpha_i^i \leq \frac{5}{\alpha_i^i}
\]

where \( i = k - 2j - i - 1 \in Z \). By following the same approach in the proof of Theorem 1, it is indeed obtained that \( i \leq 3 \). The values of \( i \in \{1, 2, 3\} \) are substituted into Eq 31 in the following:

- If \( i = 1 \), then

\[ L_k = L_j^2 + 1. \]

- If \( i = 2 \), that gives

\[ L_k = L_j^2 + 9. \]

- Finally, if \( i = 3 \), then
\[ L_k = L_j^2 + 16. \]

The values of \( j \) and \( k \) that correspond to each value of \( i \) need to be determined.

\[ \Delta \]

The combination of Eq 33 with identity 5 yields the elliptic curves

\[ Y^2 = X^3 + 10X^2 + 125X \quad \text{and} \quad Y^2 = X^3 + 10X^2 - 75X, \]

where \( X = 5x_1^2 \) such that \( x_1 = L_j \). The points for \( (X,Y) \in \{(−15,0),(0,0),(5,0)\} \) are obtained using the SageMath function integral_points(). In the search for the positive of \( X \), the value of \( X = 5 \) is selected. Since \( 5 = X = 5x_1^2 = L_j^2 \), then \( L_j = 1 \).

So, \( j = 1 \). By substituting \( j = 1 \) in Eq 33, then \( L_k = L_1^2 + 1 = 2 \) which gives \( k = 0 \). Since \( i < j \), this solution is excluded.

\[ \Delta \]

Next, substituting Eq 34 in identity 5 gives the elliptic curves

\[ Y^2 = X^3 + 90X^2 + 2125X \quad \text{and} \quad Y^2 = X^3 + 90X^2 + 1925X, \]

such that \( X = 5x_1^2 \) and \( x_1 = L_j \). Similarity, the SageMath function integral_points() leads to \( X \in \{45,27720,145968900\} \). As done in the previous case, \( 45 = X = L_j^2 \) since it implies a solution. Hence, \( L_j = 3 \). Thus, \( j = 2 \). Substituting \( j = 2 \) in Eq 34 implies that \( L_k = 18 \), which offers no solution.

\[ \Delta \]

Again, the combination of Eq 34 and identity 5 generates the elliptic curves

\[ Y^2 = X^3 + 160X^2 + 6500X \quad \text{and} \quad Y^2 = X^3 + 160X^2 + 6300X, \]

where \( X = 5x_1^2 \) such that \( x_1 = L_j \). Then \( X = 30 \) and 210, and these clearly give no solution.

As a result, Eq 12 with \( i,j,k \geq 1 \) has no solution, and the proof of Theorem 2 is completed.

**Proof of Theorem 3:** An upper bound for \( i \) in the equation

\[ P_k = P_j^2 + P_i^2 \]

with \( i,j,k \geq 1 \), is determined first. Using the same approach used in the proofs of Theorems 1 and 2 with the assumption of \( 1 \leq i \leq j < k \) gives that

\[ |a_j^2| \leq \left| \frac{5}{a_{j-2}^2+2.5} \right|. \]

Assume that

\[ B = \min_{i \in \mathbb{Z}} |a_j^2 - 2.5|. \]

If \( I = 0 \), that gives \( B = 1.5 \).

If \( I \geq 1 \), then \( a_j^2 \geq a_2^2 > 2.414 \). This means that \( B > 0.086 \).

Similarly, if \( I \leq -1 \) then \( B > 2.086 \).

As a result, \( B = 0.086 \) can be obtained. Thus, inequality 37 indicates that \( a_2^2 < 58.139 \), and it means that

\[ i \leq \frac{\ln(58.139)}{\ln(a_i^2)} < \frac{\ln(58.139)}{\ln(2.414)} < 4.61. \]

Therefore, \( i \leq 4 \). Next, the values of \( j \) and \( k \) corresponding to the values of \( 1 \leq i \leq 4 \) in Eq 36 with \( i,j,k \geq 1 \) are determined. The first step is determining the values of \( X \) derived from the integral points \((X,Y)\) of the curves presented by 23. Details of the calculations for the solutions \((x,y,p) = (P_i,P_j,P_k)\) of Eq 12 under the assumption that \( i \leq j < k \) are given in (Table 1), with an emphasis on the triples \([1,B_1,A_1C_1]\) representing the coefficients of elliptic curves of form 23 such that the values \( X = A_1x_1^2 \) with \( x_1 = P_j \) (Note that the third column contains only the positive values of \( X \) for which \( X = A_1x_1^2 = A_1P_j^2 \) provides an integer value for \( x_1 \) that represents a Pell-Lucas number).

**Table 1. Detail of computations of the solutions \((P_i,P_j,P_k)\) of Eq.12.**

<table>
<thead>
<tr>
<th>( i )</th>
<th>([1,B_1,A_1C_1])</th>
<th>( x )</th>
<th>((X_1,j))</th>
<th>( K )</th>
<th>((x,y,p))</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>[1, 16, 96]</td>
<td>8</td>
<td>(1, 1)</td>
<td>2</td>
<td>{(1, 1, 2)}</td>
</tr>
<tr>
<td></td>
<td>[1, 16, 32]</td>
<td>32</td>
<td>(2, 2)</td>
<td>3</td>
<td>{(1, 2, 5)}</td>
</tr>
<tr>
<td>2</td>
<td>[1, 64, 1056]</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>{}</td>
</tr>
</tbody>
</table>
Finally, the following set of solutions of Eq 12, with $i,j,k \geq 1$, are obtained by permuting the first two components in the solutions $(x,y,p) = (P_i,P_j,P_k)$:

$$\begin{align*}
& (x,y,p) = (P_i,P_j,P_k) \in \{(1,1,2), (1,2,5), (2,1,5), (2,2,5), (3,2,5)\}.
\end{align*}$$

So, the proof of Theorem 3 is totally completed.

**Proof of Theorem 4:** The proof begins by determining an upper bound for $i$ in the equation

$$Q_k = Q_j^2 + Q_i^2,$$

such that $i,j,k \geq 1$ and $i \leq j < k$. By following the argument applied in the proofs of the previous theorems, the solutions of Eq 38 are first found under the condition that $1 \leq i \leq j < k$. Dividing the latter equation by $Q_j$ with using the fact of inequality 17 and Binet’s formula of Pell-Lucas sequence presented in (7 or 11) imply that

$$a^k_2 + \rho^k_2 \leq (a^j_2 + \rho^j_2)(a^{j+1}_2 + a^{j+1}_2) \leq a^{j+1}_2 + \rho^j_2 a^{j+1}_2 + \rho^j_2 a^{j+1}_2.$$

It follows that

$$|a^k_2| \leq 4|a^{j+1}_2| + \frac{1}{a^2_2}.$$

Therefore,

$$a^{k-2j-l-1}_2 \leq \frac{5}{a^2_2}.$$

Thus, it can be concluded that

$$|a^k_2| \leq \frac{5}{a^2_2},$$

where $B = \min_{i \geq 2} \{a^j_2 - 2\}$ such that $l = k - 2j - i - 1$. In fact, $B \geq 0.414$ is obtained. So, the last inequality gives that

$$i \leq \frac{\ln(12.077)}{\ln(2414)} < 2.826.$$

This shows $i \leq 2$. The values of $j$ and $k$ corresponding to $i \in \{1,2\}$ can be found by plugging the values of $i$ in Eq 38.

If $i = 1$, that gives

$$Q_k = Q_j^2 + 4.$$

The substitution of the last equation in identity 5 is applied to get the elliptic curves

$$Y^2 = X^3 + 64X^2 + 800X \quad \text{and} \quad Y^2 = X^3 + 64X^2 + 480X,$$

with $X = 8x^2_1$ and $x_1 = Q_j$. Using the SageMath function `integral_points()` gives $X \in \{25, 32\}$. For $X = 8Q_j^2 = 25$ or 32, no solution exists.

If $i = 2$, then

$$Q_k = Q_j^2 + 36.$$

Now, the combination of the latter equation and identity 5 generates the elliptic curves

$$Y^2 = X^3 + 576X^2 + 83200X \quad \text{and} \quad Y^2 = X^3 + 576X^2 + 82688X,$$

where $X = 8x^2_1$ such that $x_1 = Q_j$. Thus, $X = 260$ and 320; this gives no solution.

Hence, Eq 12 with $i,j,k \geq 1$ has no solutions, and this proves Theorem 4.

**Proof of Theorem 5:** To start the proof, an upper bound for $i$ in the eq

$$M_k = M^2_j + M^2_i.$$
Must be obtained, where $i, j, k \geq 1$, and $i \leq j < k$. Using $i \leq j$ and dividing Eq 39 by $M_j$, it can be found that

$$\frac{M_k}{M_j} \leq M_i + M_j.$$  

Thus, it follows that

$$\alpha^k - \beta^k \leq (\alpha^i - \beta^i)(2\alpha^i + 2\alpha^j) \leq 2\alpha^{i+j} + 2\alpha^2 - 2\beta^i \alpha^i - 2\beta^j \alpha^j,$$

which can be obtained by combining inequality 18 with (identity 6 with $\alpha, \beta = ((3 + \sqrt{5})/2, (3 - \sqrt{5})/2)$) in inequality 40. Substituting the assumption $i \leq j < k$ with the fact $\beta = \frac{1}{\alpha}$ in the later inequality gives that

$$|\alpha^k| \leq 9|\alpha^{2j}| + \left|\frac{1}{\alpha^i}\right|.$$  

Hence,

$$\alpha^k \leq \frac{1}{\alpha^i}(9\alpha^{2j+i}).$$

So, dividing the last inequality by $\alpha^{2j+i}$ gives

$$\alpha^{k-2j-i} \leq \frac{9}{\alpha^i}.$$  

This can be written as

$$|\alpha^i| \leq \left|\frac{9}{\alpha^i-2}\right|$$  

such that $I = k - 2j - i$.  

Now, let

$$B = \min_{i \in \mathbb{Z}} |\alpha^i - 2|.$$  

- If $I = 0$, then $B = 1$.
- If $I \geq 1$, then $\alpha^i \geq \alpha^1 > 2.618$. Thus, $B > 0.618$.
- Similarly, if $I \leq -1$ then $B > 2.118$. This gives that $B \geq 0.618$. Thus, inequality 41 gives that

$$i < \frac{\ln(14.563)}{\ln(2.618)} < 2.783.$$  

Therefore, $i \leq 2$. The next step is substituting the values of $i$ in Eq 39 to determine the values of $j$ and $k$ corresponding to $i = 1$ and 2.

If $i = 1$, the following eq is obtained

$$M_k = M_j^2 + 1.$$  

The latter equation is then substituted in identity 5, resulting in the elliptic curve

$$Y^2 = X^3 + 10X^2 + 45X$$

with $X = 5x_1^2$ and $x_1 = M_j$. By using the Sage Math function integral points (), it leads to $(X, Y) = (0, 0)$. Therefore, no has solution.

If $i = 2$, then

$$M_k = M_j^2 + 9.$$  

Finally, the last equation is combined with identity 5 to obtain the equation

$$Y^2 = X^3 + 90X^2 + 2045X,$$

where $X = 5x_1^2$ such that $x_1 = M_j$. The result is $X = 0$, but once again there is no solution.

As a consequence, Eq 12 with $i, j, k \geq 1$ has no solution, and the proof of Theorem 5 is accomplished.

**Proof of Theorem 6**: Once more, the proof begins with determining the upper bound of $i$ in the equation

$$N_k = N_j^2 + N_i^2,$$  

for $i, j, k \geq 1$. Following the same strategy used in the proofs of the previous theorems with the assumption of $1 \leq i \leq j < k$ gives that

$$\alpha^i \leq \frac{9}{\beta^i}$$  

where $B = \min_{i \in \mathbb{Z}} |\alpha^i - 2.5|$ such that $\alpha = (3 + \sqrt{5})/2$.

- If $I = 0$, this means that $B = 1.5$.
- If $I \geq 1$ then $\alpha^i \geq \alpha^1 > 2.618$. It follows that $B > 0.118$.  

$$i < \frac{\ln(14.563)}{\ln(2.618)} < 2.783.$$  

-
Similarly, if $I \leq -1$ then $B > 2.118$.

Therefore, $B > 0.118$. As a result, inequality 43 shows that $\alpha^I < 76.271$, which implies that

$$i \leq \frac{\ln(76.271)}{\ln(\alpha)} < \frac{\ln(76.271)}{\ln(2.618)} < 4.503.$$ 

Hence, $i \leq 4$. The next step is finding the values of $j$ and $k$ that correspond to the values of $i \in \{1, 2, 3, 4\}$ with $i, j, k \geq 1$. Now, the values of $X$ are determined from the integral points $(X,Y)$ of the curves shown in 23. The specifics of calculations for the solutions $(x,y,p) = (N_l, N_j, N_k)$ of Eq 12 under the assumption of $1 \leq i \leq j < k$ are given in (Table 2), emphasizing that the triples $[1, B_1, A_1 C_1]$ representing the coefficients of elliptic curves of form 23 such that the values of $X = A_1 x_1^2$ with $x_1 = N_j$.

**Table 2. Detail of computations of the solutions $(N_l, N_j, N_k)$ of Eq.12.**

<table>
<thead>
<tr>
<th>i</th>
<th>$[1, B_1, A_1 C_1]$</th>
<th>X</th>
<th>$(x_1, j)$</th>
<th>k</th>
<th>$(x,y,p)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$[1, 90, 2125]$</td>
<td>0</td>
<td>-</td>
<td>-</td>
<td>{}</td>
</tr>
<tr>
<td>2</td>
<td>$[1, 490, 6025] $</td>
<td>0</td>
<td>-</td>
<td>-</td>
<td>{}</td>
</tr>
<tr>
<td>3</td>
<td>$[1, 3240, 2624500]$</td>
<td>0</td>
<td>-</td>
<td>-</td>
<td>{}</td>
</tr>
<tr>
<td>4</td>
<td>$[1, 22090, 121992125]$</td>
<td>0</td>
<td>-</td>
<td>-</td>
<td>{}</td>
</tr>
</tbody>
</table>

So, Eq 12 with $i,j,k \geq 1$ has no solution, and Theorem 6 has been proved.

**Proof of Theorem 7:** Similarly, an upper bound is obtained for $I$ (with $1 \leq i \leq j < k$) in the eq

$$D_k = D_j^2 + D_i^2.$$  

$$\frac{D_k}{D_j} = \frac{D_j^2}{D_j} + D_j.$$  

As $i \leq j$, it can be concluded that

$$\frac{D_k}{D_j} \leq D_i + D_j.$$  

By substituting inequality 18 and identity 6 into inequality 45 (with $(\alpha, \beta) = ((3 + \sqrt{13})/2, (3 - \sqrt{13})/2)$) gives that

$$\alpha^k - \beta^k \leq (\alpha^i - \beta^i)(2\alpha^i + 2\beta^i) - 2\alpha^{i+j} + 2\beta^j - 2\beta^i \alpha^i - 2\beta^i \alpha^j.$$  

From the assumption of $i \leq j < k$ with $\beta_1 = \frac{1}{\alpha_1}$, the latter inequality leads to

$$\alpha^k \leq 8\alpha^{2j} \pm \frac{1}{\alpha_1}.$$  

Now, let’s apply the absolute value to the latter inequality to get

$$|\alpha^k| \leq |8\alpha^{2j}| + \frac{1}{|\alpha|^1}.$$  

Therefore,

$$\alpha^k \leq \frac{1}{\alpha^i} (9\alpha^{2j+i})$$  

as $1 < \alpha^{2j+i}$.

Dividing inequality 46 by $\alpha^{2j+i}$ gives

$$\alpha^{k-2j-i} \leq \frac{9}{\alpha^i}.$$  

After simplifying, it can be deduced that $\alpha^i < 45.455$, resulting in $i < 3.195$.

Thus, $i \leq 3$. According to the second step of the main approach, each value of $i$ such that $i \in \{1, 2, 3\}$ in Eq.44 must be replaced; namely,

- For $i = 1$, the following eq is obtained
  $$D_k = D_j^2 + 1.$$  

- For $i = 2$, then
  $$D_k = D_j^2 + 9.$$  

- For $i = 3$, then
  $$D_k = D_j^2 + 9.$$
Finally, if \( i = 3 \) then
\[
D_k = D_j^2 + 100. \tag{49}
\]

The values of \( j \) and \( k \) that correspond \( i = 1, 2, \) and 3 are then determined.

Firstly, Eq 47 is combined with identity 5 to obtain the elliptic curves
\[
Y^2 = X^3 + 26X^2 + 221X \quad \text{and} \quad Y^2 = X^3 + 26X^2 + 117X,
\]
where \( X = 13x_1^2 \) such that \( x_1 = D_j \). Using the Sage – Math function integral points () gives that
\[
(X, Y)\in\{(-13, 26), (-9, 18), (0, 0), (1, 12), (117, 1704)\}.
\]

\( X = 1 \) and 117 are chosen since only positive values of \( X \) are being searched for.

- For \( X = 1 \) and \( = 13x_1^2 = 13D_j^2 \) : that is impossible.

- If \( 117 = 13D_j^2 \), then \( D_j^2 = 9 \). Hence, \( j = 2 \). Substituting \( j = 2 \) in Eq.47 results in
\[
D_k = D_j^2 + 101 = 10, \quad \text{which yields no solution.}
\]

Next, substituting Eq 48 in identity 5 gives the elliptic curves
\[
Y^2 = X^3 + 234X^2 + 13741X \quad \text{and} \quad Y^2 = X^3 + 234X^2 + 13637X,
\]
such that \( X = 13x_1^2 \) and \( x_1 = D_j \). Similarly, using Sage Math software gives that
\[
X \in \{13, 1049, 1300, 122733\}.
\]

Solutions for \( X = 13D_j^2 \) are obtained only when \( X = 13 \) and 1300. Thus,

- If \( X = 13 \), then \( D_j = 1 \). Thus, \( j = 1 \). Substituting \( j = 1 \) in Eq 48 results in
\[
D_k = 10, \quad \text{and this has no solution.}
\]

Similarly, for \( X = 1300, j = 3 \) is obtained, implying that \( D_k = 109 \). Hence, \( k = 5 \). The corresponding solution to Eq 12 with \( i \leq j < k \) is \((x, y, p) = (3, 10, 109)\).

Finally, combining Eq 49 with identity 5 generates the elliptic curves
\[
Y^2 = X^3 + 2600X^2 + 1690052X \quad \text{and} \quad Y^2 = X^3 + 2600X^2 + 1689948X,
\]
where \( X = 13D_j^2 \). Here, it is obtained that
\[
X\in\{117, 1472, 3925, 14157, 14444, 23552, 168994800\}.
\]

Similarly, \( X = 117 \) and 1472 are the only choices.

If \( 117 = 13D_j^2 \), then \( D_j = 3 \) and \( j = 2 \). In this case, \( i = 3 \), and it was assumed that \( i \leq j < k \), hence this solution is excluded.

For \( X = 14157 \), then \( D_j = 33 \). This leads to \( j = 4 \) and \( k = 7 \). So, the corresponding solution is \((x, y, p) = (10, 33, 1189)\).

The complete set of solutions to Eq 12 with \( i, j, k \geq 1 \) is obtained by permuting the first two components in the obtained solutions \((x, y, p) = (D_i, D_j, D_k)\) with \( i \leq j < k \), and it indeed is as follows:
\[
(x, y, p) = (D_i, D_j, D_k) \in \{(3, 10, 109), (10, 3, 109), (10, 33, 1189), (33, 10, 1189)\}.
\]

Thus, the proof of Theorem 7 is completed.

**Proof of Theorem 8:** To start, an upper bound for \( i \) is determined in the equation
\[
E_k = E_j^2 + E_i^2,
\]
where \( i, j, k \geq 1 \) and \( i \leq j < k \). Again, dividing the latter equation by \( E_j \), using the fact of inequality 19
and Binet's formula stated in 7 (with \((\alpha, \beta) = ((3 + \sqrt{13})/2, (3 - \sqrt{13})/2))\), leads to the conclusion that
\[
\alpha^k + \beta^k \leq (\alpha^i + \beta^i)(2\alpha^i + 2\alpha^j) \leq 2\alpha^{i+j} + 2\alpha^2j + 2\beta^ia^i + 2\beta^j \alpha^j.
\]

Consequently, after some simplification, it is determined that \( i \leq 2 \).
In order to determine the values of \( j \) and \( k \) corresponding to the values of \( i \in \{1, 2\} \), the values of \( i \) are substituted into Eq 50 as follows:

- If \( i = 1 \), the following equation is obtained:
  \[
  E_k = E_f^2 + 9.
  \]
  Combining the above equation with identity 5 yields the elliptic curves
  \[
  Y^2 = X^3 + 234X^2 + 14365X \quad \text{and} \quad Y^2 = X^3 + 234X^2 + 13013X,
  \]
  where \( X = 13x^2 \) such that \( x_1 = E_f \). Using the SageMath function integral points() gives \( X \in \{-143, -91, 0\} \). Since only positive solutions are being sought, it is concluded that this equation is unsolvable.

- If \( i = 2 \), then
  \[
  E_k = E_f^2 + 121.
  \]
  Now, substituting this equation in identity 5 gives the equations
  \[
  Y^2 = X^3 + 33696X^2 + 283855780X \quad \text{and} \quad Y^2 = X^3 + 33696X^2 + 283854428X,
  \]
  with \( 13E_f^2 \cdot X \in \{-1599, -1547, 0\} \) is obtained, and once again, no solution is found.

Thus, Eq 12 has no solutions of the form \( (x, y, p) = (E_i, E_j, E_k) \) with \( i, j, k \geq 1 \). Hence, Theorem 8 is proved.

**Proof of Proposition 1:** According to the result of Theorem 1, the set of solutions to Eq 12 is given by (assuming that \( i, j, k \geq 2 \)).

\[
(x, y, p) = (F_i, F_j, F_k) \in \{(1,1,2), \quad (1,2,5), (2,1,5), (2,3,13), (3,2,13)\}
\]

To consider the set of solutions of Eq.13 where \( i, j, k \geq 2 \), Eq 13 can be rewritten as equation Eq 12, namely \( p = x^2 + Y^2 \) with \( Y = y^2 \). Therefore, the solutions of Eq 13 can be obtained from the above set of solutions to Eq 12 with which the component \( y \) can be square rooted. Hence, the solution to Eq 13 gives by

\[
(x, y, p) \in \{(1,1,2), (2,1,5)\}.
\]

As a result, Proposition 1 is completely proven.

**Proof of Proposition 3:** The proof of this proposition can be followed from the result of Theorem 3, which presents the set of solutions to Eq.12 as

\[
(x, y, p) = (P_i, P_j, P_k) \in \{(1,1,2), 
(1,2,5), (2,1,5), (2,3,5), (3,2,5)\},
\]

where \( i, j, k \geq 1 \). To find the set of solutions to Eq 13 where \( (x, y, p) = (P_i, P_j, P_k) \) and \( i, j, k \geq 1 \), this eq is rewritten as \( p = x^2 + Y^2 \) where \( Y = y^2 \). Consequently, the solutions of Eq 13 may be found from the above set of solutions \( (x, y, p) \) of Eq 12 such that \( y \) can be square rooted. Thus, the solutions to Eq 13 are \( (x, y, p) = (1,1,2) \) and \( (2,1,5) \). So, the proof of Proposition 3 is achieved.

**Proof of Proposition 7:** Similarly, Eq 13 can be rewritten as \( p = x^2 + Y^2 \) with \( Y = y^2 \). According to the result of Theorem 7, the solutions \( (x, y, p) = (D_i, D_j, D_k) \) with \( i, j, k \geq 1 \) of the equation \( p = x^2 + y^2 \) are given by the set

\[
\{(3,10,109), (10,3,109), 
(10,33,1189), (33,10,1189)\}.
\]

Therefore, the triple \( (D_i, D_j, D_k) \) (with \( i, j, k \geq 1 \)) that satisfies Eq.13 can be obtained from the above set of solutions where the component \( y \) can be square rooted. It is clear that there are no such solutions. So, Proposition 7 is completely proven.

**Proof of Propositions 2,4,5,6 and 8:** The proofs of these propositions can be obtained from the results of Theorems 2, 4, 5, 6, and 8, respectively. As there are no solutions for Eq 12 where

\[
(x, y, p) \in \{(L_i, L_j, L_k), (Q_i, Q_j, Q_k), (M_i, M_j, M_k), 
(N_i, N_j, N_k), (E_i, E_j, E_k)\},
\]

it can be easily concluded that Eq 13 does not have such solutions. Hence, the proofs for these propositions are obtained.
Conclusion

The equations $p = x^2 + y^2$ and $p = x^2 + y^4$, which have an infinite number of solutions over rational integers, have only a finite number of solutions $(x, y, p)$, where $x, y,$ and $p$ are Lucas numbers of the first or second kind.

Acknowledgment

The authors would like to thank the referee for their careful reading and comments that improved the articles quality.

Authors’ Declaration

- Conflicts of Interest: None.
- Ethical Clearance: The project was approved by the local ethical committee in University of Baghdad.

Authors’ Contribution Statement

A. S. A. and H. R. H. investigated the equations presented, then developed the theory and performed the computations. The authors both discussed the findings and contributed to the final manuscript.

References

2. Shanks D. An analytic criterion for the existence of infinitely many primes of the form $\frac{1}{2}(n^2 + 1)$. Ill. J. Math. 1964; 8: 377–379. [https://projecteuclid.org/10.1215/1256059560].
 حلول معادلة مربعٍ فيرما وتعميمها في متواليات لوكاس
علي صحن عذاب ، حيدر رحيم هاشم
قسم الرياضيات، كلية علوم الحاسوب والرياضيات، جامعة الكوفة، النجف، العراق.

الخلاصة
من المعروف أن هناك عدد غير منتهي من الأعداد الأولية في أشكال خاصة مثل شكل مربع فيرما
\[ \ p = x^2 + y^2, \] أو تعميمها الذي يحتوي على الشكل \[ \ p = x^2 + y^4. \]
الهدف الرئيسي من هذه الورقة هو التحقق مما إذا كانت الأشكال أعلاه لا تزال تحتوي على العديد من الحلول
أي أنه إذا كانت الأشكال أولية، تعتبر أدق في حلول هذه الأشكال عبارة عن تحليل قياسي تكرار خطئي
ثاني معينة متبقي متواليات لوكاس من النوع الأول والنوع الثاني.

الكلمات المفتاحية: معادلة ديوفانتاين، المنحنات الأهلية، نظرية مربع فيرما، متواليات لوكاس، الأعداد الأولية.