INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

RESEARCH ARTICLE

Cryptographical Applications of Linear Transformations and Pell Equations: An R-Based Approach

K Kaleeswari[1], J Kannan[2]*, A Deepshika[1], M Mahalakshmi[1]

1 Ph.D. Research Scholar, Department of Mathematics, Ayya Nadar Janaki Ammal College (Autonomous, affiliated to Madurai Kamaraj University), Sivakasi, 626124, Tamil Nadu, India
2 Assistant Professor, Department of Mathematics, Ayya Nadar Janaki Ammal College (Autonomous, affiliated to Madurai Kamaraj University), Sivakasi, 626124, Tamil Nadu, India

OPEN ACCESS

Received: 15-11-2024
Accepted: 11-12-2024
Published: 27-12-2024

Citation: Kaleeswari K, Kannan J, Deepshika A, Mahalakshmi M (2024) Cryptographical Applications of Linear Transformations and Pell Equations: An R-Based Approach. Indian Journal of Science and Technology 17(47): 4959-4965. https://doi.org/10.17485/IJST/v17i47.3714

* **Corresponding author**.

jayram.kannan@gmail.com

Funding: None

Competing Interests: None

Published By Indian Society for Education and Environment (iSee)

ISSN
Print: 0974-6846
Electronic: 0974-5645

Abstract

Objective: This article's main aim is to encrypt and decrypt the message to be sent using matrices of the linear transformation and the fundamental solution of the Pell equation. R Programming is provided at the end of the article. **Methods:** The encryption and decryption algorithms were created using the fundamental solutions of the Pell equation $x^2 - py^2 = 1$, where p is a positive integer which is not a perfect square, and using the matrices of the linear transformations. The message to be sent is converted into block matrices of order 2. Based on the number of blocks, the prime p is determined. **Findings:** Here, we gave two examples: manually for the sentence "MATHS IS A UNIVERSAL SUBJECT" and using R programming for the word "PIE." **Novelty:** The concept of encrypting and decrypting a message or word already exists. Many algorithms have been created in different ways. But, in this article, we created the algorithms connecting the matrix of linear transformations and the fundamental solution of Pell equations.

2020 MSC Classification: 94A60, 15A04, 11C20.

Keywords: Cryptography; Linear transformation; Pell equation; Encryption; Decryption

1 Introduction

Cryptography is a secret method of sharing any message by employing encryption and decryption. Cryptography is crucial for our society[(1)]. Currently, numerous algorithms for encryption and decryption procedures have been developed. Today, we seek increased security when sharing messages. To encrypt and decrypt data, complex algorithms are required. Some known algorithms are DS, DES, AES, and RSA algorithms. Some have explored the encryption and decryption algorithms in number theory[(2–6)]. For instance, in[(7)] and[(8)], J. Kannan et.al created various algorithms using the Pell equation, which is a type of Diophantine equation. In[(9)], V. Pandichelvi encrypted and decrypted the message using a linear Diophantine equation with three variables $(x, y, and\ z)$ and the American Standard Code for Information Interchange (ASCII).

Inspired by the above, we constructed an algorithm employing the fundamental solutions of the Pell equation [10] $x^2 - py^2 = 1$, where p is a positive integer which is not a perfect square using the matrix of the linear transformation. The message to be sent is converted into block matrices of even order. Based on the number of blocks p can be determined. Following the introduction, the notations that are used in the article were displayed. After that, the positions of each alphabet were presented. The encryption and decryption algorithms will be shown in the next section. Two instances were explored utilizing the algorithms.

2 Methodology

2.1. Notations

- N1) $B \rightarrow$ an even-order square matrix formed by the given message.
- N2) $B_j \rightarrow j^{th}$ block of B whose size is 2.
- N3) $b \rightarrow$ number of blocks of B.
- N4) $\rho = \begin{cases} 2 & if\ b\ is\ 1\ or\ even \\ smallest\ prime\ which\ divides\ b, & if\ b\ is\ odd\ and\ greater\ than\ 1 \end{cases}$
- N5) The elements of B_j are given by $\begin{pmatrix} b_{j1} & b_{j2} \\ b_{j3} & b_{j4} \end{pmatrix}$
- N6) $Q_I = \begin{pmatrix} x_1 & 0 \\ 0 & y_1 \end{pmatrix}$
- N7) $Q_{II} = \begin{pmatrix} -x_1 & 0 \\ 0 & y_1 \end{pmatrix}$
- N8) $T_j : V_2(R) \rightarrow V_2(R)$ is the linear transformation where $V_2(R)$ defines R^2 is a vector space over R.
- N9) $\theta \rightarrow$ notation for space

2.2. Position of Characters

Table 1.

A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	2	3	4	5	6	7	8	9	10	11	12	13	14
O	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	θ	-
15	16	17	18	19	20	21	22	23	24	25	26	27	

2.3. Encryption Algorithm:

1. Construct the matrix B of even order for the given message.
2. Next divide the matrix B into blocks B_j of size 2 and find b.
3. Find p and the fundamental solution of $x^2 - py^2 = 1$.
4. Replace the alphabet in B_j by numerical values.
5. Find the matrix Q_I and Q_{II}.
6. Multiply the matrix B_j and the matrix Q_I and name it as B_{jI}.
7. Then again multiply the matrix B_{jI} with the matrix Q_{II} and name it as B_{jII}.
8. Let $T_j : V_2(R) \rightarrow V_2(R)$ be the linear transformation a linear transformation corresponding to the matrix B_{jII} with respect to the standard basis $\{e_1, e_2\}$ as a basis both for the domain and the range. Name it as $T_j(a_j, b_j) = (\alpha_j, \beta_j)$.
9. Finally, we construct the encrypted matrix as $E = \begin{pmatrix} \alpha_1 & \beta_1 \\ \alpha_2 & \beta_2 \\ \vdots & \vdots \\ \alpha_j & \beta_j \end{pmatrix}$

2.4. Decryption Algorithm

1. Find the number of rows from the encrypted matrix E. (Take it as ”b”)

2. Find p, where
3. $\rho = \begin{cases} 2 & if\ b\ is\ 1\ or\ even \\ smallest\ prime\ which\ divides\ b, & if\ b\ is\ odd\ and\ greater\ than\ 1 \end{cases}$
4. Find the fundamental solution of the equation $x^2 - py^2 = 1$. Let it be (x_1, y_1).
5. Using the matrix E, define a linear transformation $T_j : V_2(R) \to V_2(R)$ by $T_j(a_j, b_j) = (\alpha_j, \beta_j)$.
6. Find the matrix $C_j = \begin{pmatrix} c_1 & c_2 \\ c_3 & c_4 \end{pmatrix}$ corresponding to the linear transformation $T_j(a_j, b_j) = (\alpha_j, \beta_j)$ with respect to the standard basis $\{e_1, e_2\}$.
7. Find the matrix $D_j = \begin{pmatrix} d_1 & d_2 \\ d_3 & d_4 \end{pmatrix}$ where $d_1 = -\frac{c_1}{x_1}; d_2 = \frac{c_2}{y_1}; d_3 = -\frac{c_3}{x_1}; d_4 = \frac{c_4}{y_1}$.
8. Find the matrix $B_j = \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix}$ where $b_1 = \frac{d_1}{x_1}; b_2 = \frac{d_2}{y_1}; b_3 = \frac{d_3}{x_1}; b_4 = \frac{d_4}{y_1}$.
9. Finally, we get decrypted matrix B_j.
10. Then using the matrix B_j replace the number by alphabets and construct the matrix B.

3 Results and Discussion

Encrypt and decrypt the sentence "$MATHS\ IS\ A\ UNIVERSAL\ SUBJECT$".

Encryption

Consider the sentence "$MATHS\ IS\ A\ UNIVERSAL\ SUBJECT$" which is to be encrypted. Here,

$$B = \begin{pmatrix} M & A & T & H & S & \theta \\ I & S & \theta & A & \theta & U \\ N & I & V & E & R & S \\ A & L & \theta & S & U & B \\ J & E & C & T & \theta & \theta \\ \theta & \theta & \theta & \theta & \theta & \theta \end{pmatrix},$$

Hence $B_1 = \begin{pmatrix} M & A \\ I & S \end{pmatrix}, B_2 = \begin{pmatrix} T & H \\ \theta & A \end{pmatrix}, B_3 = \begin{pmatrix} S & \theta \\ \theta & U \end{pmatrix}, B_4 = \begin{pmatrix} N & I \\ A & L \end{pmatrix}, B_5 = \begin{pmatrix} V & E \\ \theta & S \end{pmatrix},$
$B_6 = \begin{pmatrix} R & S \\ U & B \end{pmatrix}, B_7 = \begin{pmatrix} J & E \\ \theta & \theta \end{pmatrix}, B_8 = \begin{pmatrix} C & T \\ \theta & \theta \end{pmatrix}, B_9 = \begin{pmatrix} \theta & \theta \\ \theta & \theta \end{pmatrix}.$

Since there are 9 blocks, then $b = 9$. Therefore, $p = 3$ which divides b. Replace the entries of the matrix with numerals as in Position of Characters. Hence,

$B_1 = \begin{pmatrix} 13 & 1 \\ 9 & 19 \end{pmatrix}, B_2 = \begin{pmatrix} 20 & 8 \\ 27 & 1 \end{pmatrix}, B_3 = \begin{pmatrix} 19 & 27 \\ 27 & 21 \end{pmatrix}, B_4 = \begin{pmatrix} 14 & 9 \\ 1 & 12 \end{pmatrix}, B_5 = \begin{pmatrix} 22 & 5 \\ 27 & 19 \end{pmatrix},$
$B_6 = \begin{pmatrix} 18 & 19 \\ 21 & 2 \end{pmatrix}, B_7 = \begin{pmatrix} 10 & 5 \\ 27 & 27 \end{pmatrix}, B_8 = \begin{pmatrix} 3 & 20 \\ 27 & 27 \end{pmatrix}, B_9 = \begin{pmatrix} 27 & 27 \\ 27 & 27 \end{pmatrix}.$

And from the value of p we have to find the fundamental solution of $x^2 - 3y^2 = 1$.

Then $(x_1, y_1) = (2, 1)$. Hence, $Q_I = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$ and $Q_{II} = \begin{pmatrix} -2 & 0 \\ 0 & 1 \end{pmatrix}$

FOR BLOCK B_1:

Multiply the matrix B_1 and Q_I, we get $B_{1I} = \begin{pmatrix} 26 & 1 \\ 18 & 19 \end{pmatrix}$. Again, multiply the matrix B_{1I} and Q_{II} to get $B_{1II} = \begin{pmatrix} -52 & 1 \\ -36 & 19 \end{pmatrix}$. The linear transformation $T_1 : V_2(R) \to V_2(R)$ determined by the matrix $B_{1II} = \begin{pmatrix} -52 & 1 \\ -36 & 19 \end{pmatrix}$ with respect to the standard basis $\{e_1, e_2\}$ is $T_1(a_1, b_1) = (-52a_1 - 36b_1, 1a_1 + 19b_1)$. Similarly for the remaining blocks $(B_2, B_3, \cdots, B_9)$ corresponding linear transformations are,

$T_2(a_2, b_2) = (-80a_2 - 108b_2, 8a_2 + 1b_2), T_3(a_3, b_3) = (-76a_3 - 108b_3, 27a_3 + 21b_3),$
$T_4(a_4, b_4) = (-56a_4 - 4b_4, 9a_4 + 12b_4), T_5(a_5, b_5) = (-88a_5 - 108b_5, 5a_5 + 19b_5),$
$T_6(a_6, b_6) = (-72a_6 - 84b_6, 19a_6 + 2b_6), T_7(a_7, b_7) = (-40a_7 - 108b_7, 5a_7 + 27b_7),$
$T_8(a_8, b_8) = (-12a_8 - 108b_8, 20a_8 + 27b_8), T_9(a_9, b_9) = (-108a_9 - 108b_9, 27a_9 + 27b_9).$

From the linear transformations T_j, form (9×2) $matrix$.

Hence the encrypted matrix E is $\begin{pmatrix} (-52a_1-36b_1) & (1a_1+19b_1) \\ (-80a_2-108b_2) & (8a_2+1b_2) \\ (-76a_3-108b_3) & (27a_3+21b_3) \\ (-56a_4-4b_4) & (9a_4+12b_4) \\ (-88a_5-108b_5) & (5a_5+19b_5) \\ (-72a_6-84b_6) & (19a_6+2b_6) \\ (-40a_7-108b_7) & (5a_7+27b_7) \\ (-12a_8-108b_8) & (20a_8+27b_8) \\ (-108a_9-108b_9) & (27a_9+27b_9) \end{pmatrix}$

Decryption

Given that the encrypted matrix is $E = \begin{pmatrix} (-52a_1-36b_1) & (1a_1+19b_1) \\ (-80a_2-108b_2) & (8a_2+1b_2) \\ (-76a_3-108b_3) & (27a_3+21b_3) \\ (-56a_4-4b_4) & (9a_4+12b_4) \\ (-88a_5-108b_5) & (5a_5+19b_5) \\ (-72a_6-84b_6) & (19a_6+2b_6) \\ (-40a_7-108b_7) & (5a_7+27b_7) \\ (-12a_8-108b_8) & (20a_8+27b_8) \\ (-108a_9-108b_9) & (27a_9+27b_9) \end{pmatrix}$

Since the number of rows = 9, then $b = 9$ and $p = 3$. Let the fundamental solution of the equation $x^2 - 3y^2 = 1$. Then $(x_1, y_1) = (2, 1)$. Take each row of the encrypted matrix as the linear transformation.

Now, $T_1(a_1, b_1) = (-52a_1 - 36b_1, 1a_1 + 19b_1)$, $T_2(a_2, b_2) = (-80a_2 - 108b_2, 8a_2 + 1b_2)$,
$T_3(a_3, b_3) = (-76a_3 - 108b_3, 27a_3 + 21b_3)$, $T_4(a_4, b_4) = (-56a_4 - 4b_4, 9a_4 + 12b_4)$,
$T_5(a_5, b_5) = (-88a_5 - 108b_5, 5a_5 + 19b_5)$, $T_6(a_6, b_6) = (-72a_6 - 84b_6, 19a_6 + 2b_6)$,
$T_7(a_7, b_7) = (-40a_7 - 108b_7, 5a_7 + 27b_7)$, $T_8(a_8, b_8) = (-12a_8 - 108b_8, 20a_8 + 27b_8)$,
$T_9(a_9, b_9) = (-108a_9 - 108b_9, 27a_9 + 27b_9)$.

For obtaining the matrix representing the linear transformation $T_1 : V_2(R) \to V_2(R)$ given by $T_1(a_1, b_1) = (-52a_1 - 36b_1, 1a_1 + 19b_1)$ with respect to the standard basis $\{e_1, e_2\}$. Thus the matrix representing T_1 is $\begin{pmatrix} -52 & 1 \\ -36 & 19 \end{pmatrix}$.

To find the matrix $D_1 = \begin{pmatrix} d_1 & d_2 \\ d_3 & d_4 \end{pmatrix}$. Since $c_1 = -52; c_2 = 1; c_3 = -36; c_4 = 19$. Therefore $D_1 = \begin{pmatrix} 26 & 1 \\ 18 & 19 \end{pmatrix}$.

Then $B_1 = \begin{pmatrix} 13 & 1 \\ 9 & 19 \end{pmatrix}$. Similarly for remaining linear transformations $(T_2, T_3, \cdots T_9)$ corresponding matrices are $B_2 = \begin{pmatrix} 20 & 8 \\ 27 & 1 \end{pmatrix}$, $B_3 = \begin{pmatrix} 19 & 27 \\ 27 & 21 \end{pmatrix}$, $B_4 = \begin{pmatrix} 14 & 9 \\ 1 & 12 \end{pmatrix}$, $B_5 = \begin{pmatrix} 22 & 5 \\ 27 & 19 \end{pmatrix}$, $B_6 = \begin{pmatrix} 18 & 19 \\ 21 & 2 \end{pmatrix}$,
$B_7 = \begin{pmatrix} 10 & 5 \\ 27 & 27 \end{pmatrix}$, $B_8 = \begin{pmatrix} 3 & 20 \\ 27 & 27 \end{pmatrix}$, $B_9 = \begin{pmatrix} 27 & 27 \\ 27 & 27 \end{pmatrix}$.

Replace the entries of the each matrices into the characters according to its positions.

The matrix $B = \begin{pmatrix} M & A & T & H & S & \theta \\ I & S & \theta & A & \theta & U \\ N & I & V & E & R & S \\ A & L & \theta & S & U & B \\ J & E & C & T & \theta & \theta \\ \theta & \theta & \theta & \theta & \theta & \theta \end{pmatrix}$

Hence, the decrypted sentence is "$MATHS\ IS\ A\ UNIVERSAL\ SUBJECT$"

4 R Coding for the three-letter word ”PIE”

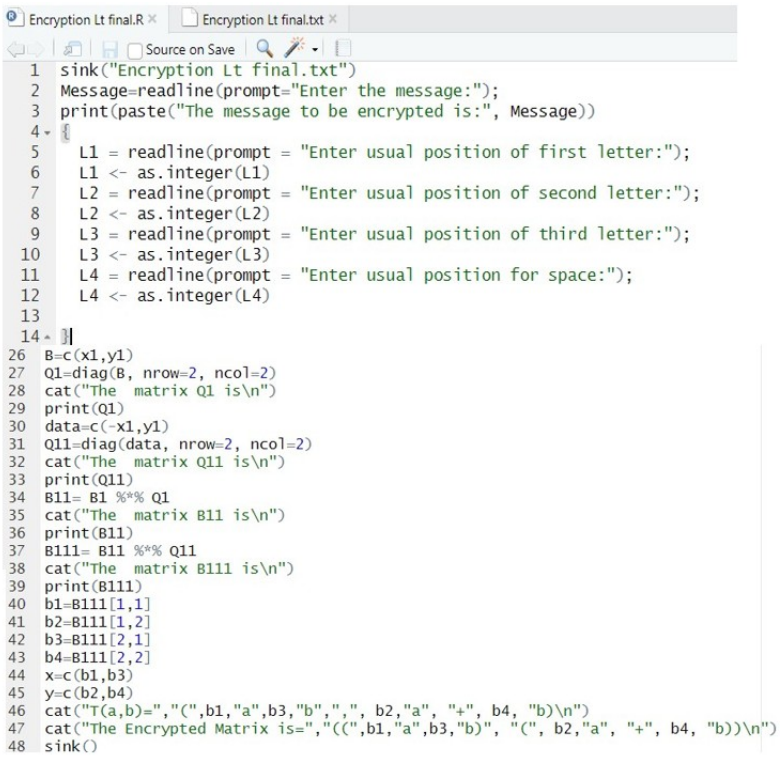

Fig 1. Encryption Code

```
[1] "The message to be encrypted is: PIE"
The  matrix B1 is
     [,1] [,2]
[1,]   16    9
[2,]    5   27
The  matrix Q1 is
     [,1] [,2]
[1,]    3    0
[2,]    0    2
The  matrix Q11 is
     [,1] [,2]
[1,]   -3    0
[2,]    0    2
The  matrix B11 is
     [,1] [,2]
[1,]   48   18
[2,]   15   54
The  matrix B111 is
     [,1] [,2]
[1,] -144   36
[2,]  -45  108
T(a,b)= ( -144 a -45 b , 36 a + 108 b)
The Encrypted Matrix is= (( -144 a -45 b) ( 36 a + 108 b))
```

Fig 2. Output for Encryption Code

Decryption Lt final.R | Decryption Lt final.txt*

Source on Save

```
sink("Decryption Lt final.txt")
cat("T(a,b)="," ( ",-144,"a",-45,"b"," , ", 36,"a", "+", 108, "b)")
{
  t1 = readline(prompt = "Enter first position of the matrix:");
  t1 <- as.integer(t1)
  t2 = readline(prompt = "Enter second position of the matrix:");
  t2 <- as.integer(t2)
  t3 = readline(prompt = "Enter third position ofthe matrix:");
  t3 <- as.integer(t3)
  t4 = readline(prompt = "Enter fourth position of the matrix:");
  t4 <- as.integer(t4)
}
m=c(t1,t2,t3,t4)
m=as.integer(m)
T=matrix(m, nrow = 2, ncol =2, byrow = TRUE)
cat("The  matrix T is\n")
print(T)
{
  x1= readline(prompt = "The fundamental solution of x^2-2y^2=1, x1:")
  x1 <- as.integer(x1)
  y1= readline(prompt = "The fundamental solution of x^2-2y^2=1, y1:")
  y1 <- as.integer(y1)
}
d1= -t1/ x1
d2= t2/ y1
d3= -t3/ x1
d4= t4/ y1
d=c(d1,d2,d3,d4)
d=as.integer(d)
D=matrix(d, nrow=2, ncol=2, byrow = TRUE)
cat("The  matrix D is\n")
print(D)
b1= d1/ x1
b2= d2/ y1
b3= d3/ x1
b4= d4/ y1
e=c(b1,b2,b3,b4)
e=as.integer(e)
B1=matrix(e, nrow=2, ncol=2, byrow = TRUE)
cat("The  matrix B1 is\n")
print(B1)
cat("The usual positions of alphabets are\n")
print(c(b1,b2,b3,b4))
sink()
```

Fig 3. Decryption Code

```
T(a,b)= ( -144 a -45 b , 36 a + 108 b)
The  matrix T is
     [,1] [,2]
[1,] -144   36
[2,]  -45  108
The  matrix D is
     [,1] [,2]
[1,]   48   18
[2,]   15   54
The  matrix B1 is
     [,1] [,2]
[1,]   16    9
[2,]    5   27
The usual positions of alphabets are
[1] 16  9  5 27
```

Fig 4. Output for Decryption Code

5 Conclusion

In this article, the encryption and decryption algorithms were developed using some linear transformations and the fundamental solutions of the Pell equation $x^2 - py^2 = 1$, where p is a positive integer which is not a perfect square that can be determined by the number of blocks in the matrices. To increase security, one can use the negative Pell equation or any other Diophantine equation.

References

1) Douglas R, Maura BS. Cryptography theory and Practice-4th edition. CRC Press. Taylor and Francis Group. 2019. Available from: https://www.ic. unicamp.br/~rdahab/cursos/mo421-mc889/Welcome_files/Stinson-Paterson_CryptographyTheoryAndPractice-CRC%20Press%20%282019%29.pdf.
2) Veena T. Encryption and decryption of messages by using matrices. *International Journal of Scientific Research in Modern Science and Technology*. 2023;2(9):1–7. Available from: http://dx.doi.org/10.59828/ijsrmst.v2i9.140.
3) Mandle AK, Namdeo V. Encryption and Decryption of a Message Involving Byte Rotation Technique and Invertible Matrix. *International Journal of Engineering and Advanced Technology*. 2019;9(2):1160–1162. Available from: http://dx.doi.org/ijeat.B3393.129219.
4) Fenolahy F, Ramanantsoa H, Totohasina A. Note on encryption decryption algorithm using solutions of Pell's equation. *International Journal of Multidisciplinary Research and Growth Evaluation*. 2022;3(5):357–363. Available from: https://www.allmultidisciplinaryjournal.com/uploads/archives/ 20220927202513_E-22-46.1.pdf.
5) Nguyen-Thi TG. An improvement of newton - krylov method for solution of nonlinear equations. *HPU2 Journal of Science: Natural Sciences and Technology*. 2023;2(1):46–52. Available from: https://doi.org/10.56764/hpu2.jos.2023.1.2.46-52.
6) Deepshika A, Kannan J, Mahalakshmi M, Kaleeswari K. Cryptographic algorithm based on permutation ciphers. *International Journal of Mathematics and its Applications*. 2023;11(4):1–7. Available from: https://ijmaa.in/index.php/ijmaa/article/view/1379/1374.
7) Kannan J, Mahalakshmi M, Deepshika A. Cryptographic algorithm involving the matrix Qp*. *Korean Journal of Mathematics*. 2022;30(3):533–538. Available from: https://doi.org/10.11568/kjm.2022.30.3.533.
8) Kannan J, Somanath M, Mahalakshmi M, Raja K. Encryption decryption algorithm using solutions of pell equation. *International Journal for Research in Applied Science and Engineering Technology*. 2022;10(1):1–8. Available from: https://ijmaa.in/index.php/ijmaa/article/view/7/7.
9) Pandichelvi V, Umamaheswari B. Leverage of linear diophantine equation in encryption and decryption. *International Research Journal of Modernization in Engineering Technology and Science*. 2024;6(6):2102–2105. Available from: https://www.doi.org/10.56726/IRJMETS59088.
10) Taher B, Lassri R, Zioua M, D. Solutions of Pell equation x^2-dy^2=±1 via linearly recurring sequences and continued fractions. *Palestine Journal of Mathematics*. 2024;13(3):673–689. Available from: https://pjm.ppu.edu/sites/default/files/papers/PJM_13%283%29_2024_673_to_689.pd.