Optimality

www.opt.reapress.com

Opt. Vol. 2, No. 2 (2025) 93–99.

Paper Type: Original Article

Isosceles Trapezoid with Integer Area: Cryptographic Applications of Generalized Pell-Type Equations and Sphenic numbers

A. Deepshika[1,*], **J. Kannan**[1] **M. Mahalakshmi**[1]

[1]Department of Mathematics Ayya Nadar Janaki Ammal College, Sivakasi, Tamil Nadu, India; deepshi20mar@gmail.com; jayram.kannan@gmail.com; maha1607laksmi@gmail.com.

Citation:

Received: 03 October 2024 *Revised: 10 January 2025* *Accepted: 24 April 2025*	Deepshika, A., Kannan, J., & Mahalakshmi, M. (2025). Isosceles trapezoid with integer area: cryptographic applications of generalized pell-type equations and sphenic numbers. *Optimality, 2*(2), 93-99.

Abstract

The well-known generalized Pell equation, $x^2 - dy^2 = n$, was used to develop the algorithm in this study. d was fixed as a prime number, and n was the square of the sphenic number. In particular, we employ the assignments utilizing the area of the isosceles trapezoid with the non-parallel sides being $2n - 1$ and the parallel sides being n and $n + r$.

Keywords: Isosceles trapezoid, Generalized pell equation, Integer area, Sphenic numbers, Cryptography.

1|Introduction

One of the most popular and appealing theories in mathematics is number theory, which is a basket of characteristics of numbers, particularly integers. It is more advantageous subject to master because it encompasses a variety of elements. Diophantine equations are polynomial equations with integer coefficients and two or more unknowns such that the only solutions of interest are the integer ones. In number theory, geometric shapes were important, and most researchers used these Diophantine equations to develop new kinds of geometric shapes [5, 4, 6]. An isosceles trapezoid is a special type of trapezoid where the two non-parallel sides (legs) are equal in length, and the base angles are also equal. In other words, it's a trapezoid with a line of symmetry bisecting the two equal sides. Let the two non-parallel sides as c and two parallel sides as a, b for the isosceles trapezoid, then the area can be calculated by $A = \frac{a+b}{4}\sqrt{(a-b+2c)(b-a+2c)}$. Here we find the isosceles trapezoid with the parallel sides as $n, n+r$ and non parallel sides as $2n-1$ where $n, r \in \mathbb{N}$ having integer area.

Corresponding Author: deepshi20mar@gmail.com

https://doi.org/10.22105/opt.v2i2.79

Diophantine analysis, the mathematical study of Diophantine problems, comprises of a special type of equation, commonly known as Pell equation [1]. It is one among the various Diophantine equations and it takes the form

$$x^2 - dy^2 = 1 \tag{0.1}$$

where d is a fixed positive integer, not a perfect square. It also has been proved that equation (0.1) has infinitely many solutions in positive integers. This Pell equation is generalized as

$$x^2 - dy^2 = n \tag{0.2}$$

for some integer n.

Let p be a prime and (x_k, y_k) be positive integer solutions of the equation $x^2 - py^2 = 1$. Using these solutions we can define the matrix Q^{p*} as $Q^{p*} = \begin{pmatrix} x_1 & py_1 \\ y_1 & x_1 \end{pmatrix}$ [3]. The specialty of this matrix is its k^{th} power can be obtained directly from the k^{th} solution (x_k, y_k) of equation $x^2 - py^2 = 1$. That is, $(Q^{p*})^k = \begin{pmatrix} x_k & py_k \\ y_k & x_k \end{pmatrix}$.

In this paper, we construct a similar matrix $Q_a^{p*} = \begin{pmatrix} x_1 & py_1 \\ y_1 & x_1 \end{pmatrix}$ for the equation $x_1^2 - py_1^2 = a^2$, where $a \in \mathbb{Z}$. The r^{th} power of this matrix is $(Q_a^{p*})^r = a^{r-1} \begin{pmatrix} x_r & py_r \\ y_r & x_r \end{pmatrix}$ where (x_r, y_r) is a positive integer solution of $x^2 - py^2 = a^2$.

In [3], an encryption and decryption algorithms are developed using the Pell equation $x^2 - py^2 = 1$ and its corresponding matrix Q^{p*}. Likewise, in this work, we deal with the same algorithm with little modifications but we employ the generalized Pell equation $x^2 - py^2 = a^2$ and its corresponding matrix Q_a^{p*}. In particular, here we restrict a as a Sphenic number, a number which is a product of three distinct primes, but here a is chosen as product of three consecutive primes which has been chosen with the help of p in the equation $x^2 - py^2 = a^2$.

2|Isosceles Trapezoid with sides with integer area

Here we collect all isosceles Trapezoid with integer area. Let $ABCD$ be a isosceles Trapezoid with the sides $AB = n, BC = AD = 2n - 1, DC = n + r$, where $n, r \in \mathbb{N}$(as shown in figure 1). The area of Isosceles Trapezoid

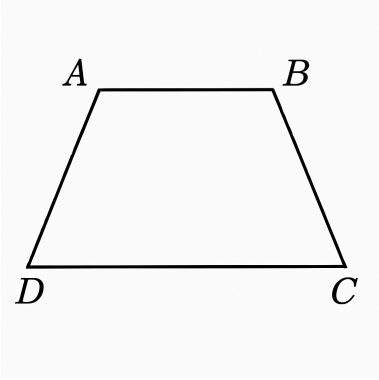

FIGURE 1. Isosceles Trapezoid

is calculated as

$$A = \frac{1}{4}\sqrt{(n+n+r)^2(n+r-n+2(2n-1))(n-n-r+2(2n-1))}$$

and after solving we get $A = \frac{(2n+r)}{4}\sqrt{(4n-2)^2 - r^2}$. For area $A \in \mathbb{Z}, (4n-2)^2 - r^2 = l^2$ for some integer l. This is of the form pythagorean equation [10] and it can be written as $(4n-2) = (u^2+v^2)k, r = 2uvk, l = (u^2-v^2)k$, for some integers u, v, k. From this n can be written as

$$n = \frac{(u^2+v^2)k}{4} + \frac{1}{2} \tag{0.3}$$

. We consider four cases for n.

Case 1

Suppose u and v are even $(ie., u = 2\alpha, v = 2\beta(\alpha, \beta \in \mathbb{Z}))$, then $n = \frac{1}{4} + (\alpha^2 k + \beta^2 k) \notin \mathbb{N}$. This case fails.

Case 2

Suppose u and v are odd $(ie., u = 2\alpha+1, v = 2\beta+1$ for some integers $\alpha, \beta)$,then $n = (\alpha^2+\beta^2+\alpha+\beta)k+\frac{k}{2}+\frac{1}{2}$.

Subcase 1

If $k = 2\gamma + 1, \gamma \in \mathbb{Z}$, then n becomes $(\alpha^2 + \beta^2 + \alpha + \beta)(2\gamma + 1) + \gamma + 1 \in \mathbb{N}$

Subcase 2

If $k = 2\gamma, \gamma \in \mathbb{Z}$, then $n = (\alpha^2 + \beta^2 + \alpha + \beta)2\gamma + \gamma + \frac{1}{2} \notin \mathbb{N}$.

Case 3

Suppose $u = 2\alpha + 1, v = 2\beta(\alpha, \beta \in \mathbb{Z}$. Then the value of $n = (\alpha^2 + \beta^2 + \beta)k + \frac{k}{4} + \frac{1}{2}$

Subcase 1

If $k = 2\gamma(\in \mathbb{Z})$,then $n = \frac{4\alpha+4\beta+4\beta^2+\gamma}{2} + \frac{1}{2} \in \mathbb{N}$ when γ is odd.

Subcase 2

If $k = 2\gamma + 1$,then $n = (\alpha^2 + \beta + \beta^2)(2\gamma + 1) + \frac{\gamma}{2} + \frac{3}{4} \notin \mathbb{N}$.

Case 4

If $u = 2\alpha, v = 2\beta + 1(\alpha, \beta \in \mathbb{Z}$. Proof is similar as above case. Hence, exccept the case 1, all others are possible ones.

Finding the integer area of isosceles trapezoid. The area of the given isosceles trapezoid is $A = \frac{((u^2+v^2)k+2+4uvk)(u^2k-v^2k)}{8}$. For area to be integer $8|((u^2 + v^2)k + 2 + 4uvk)(u^2k - v^2k)$. Then $((u^2 + v^2)k + 2 + 4uvk)(u^2k - v^2k) = 8z$ for some integer z.

For case 2

If $u, v, k \equiv 1 \pmod 2$ .That is $((u^2 + v^2)k + 2 + 4uvk)(u^2k - v^2k) \equiv 0 \pmod 2$.

For case 3

If $u \equiv 1 \pmod 2$ and $v, k \equiv 1 \pmod 2$ .Then is $((u^2 + v^2)k + 2 + 4uvk)(u^2k - v^2k) \equiv 0 \pmod 2$.

For case 4

Similar as above.

2.1|Python Programming for finding the integer area

```
#trapezium with the sides n,n+r,2n-1,2n-1
import math
from fractions import Fraction as frac
def trapezium():
 print('u\tv\tk\tl\tr\tn\tA1')
 for v in range(1,m+1):
    for u in range (v+1,m+1):
        for k in range (1,m+1):
          l=u**2*k-v**2*k
          r=2*u*v*k
          m1=u**2*k+v**2*k
          n1= u**2*k+v**2*k+2
          if n1 % (4) == 0:
            n=n1//4
            A1 = frac((r+2*n)* l,4)
            print(u,'\t',v,'\t',k,'\t',l,'\t',r,'\t',n,'\t',A1)
m =int(input("Enter the maximum range:"))
#m is the maximum range
trapezium()
```

Coding 1. Finding the integer area for thr isosceles trapezoid $ABCD$

```
Enter the maximum range:6
u       v       k       l       r       n       A1
2       1       2       6       8       3       21
2       1       6       18      24      8       180
3       1       1       8       6       3       24
3       1       3       24      18      8       204
3       1       5       40      30      13      560
4       1       2       30      16      9       255
4       1       6       90      48      26      2250
5       1       1       24      10      7       144
5       1       3       72      30      20      1260
5       1       5       120     50      33      3480
6       1       2       70      24      19      1085
6       1       6       210     72      56      9660
3       2       2       10      24      7       95
3       2       6       30      72      20      840
5       2       2       42      40      15      735
5       2       6       126     120     44      6552
4       3       2       14      48      13      259
4       3       6       42      144     38      2310
5       3       1       16      30      9       192
5       3       3       48      90      26      1704
5       3       5       80      150     43      4720
6       3       2       54      72      23      1593
6       3       6       162     216     68      14256
5       4       2       18      80      21      549
5       4       6       54      240     62      4914
6       5       2       22      120     31      1001
6       5       6       66      360     92      8976
>>>
```

Figure 2. Output: Coding 1

3|Notations

The notations used in this article are as follows.

(1) $\mathbb{P}$ - Set of all primes

(2) $\mathbb{B}$ - $2n \times 2n$ matrix which is constructed using the given message.

(3) $\mathbb{B}_k$ - k^{th} block of $\mathbb{B}$ with the size 2 (ie, 2×2 matrix).

(4) b - number of blocks of the matrix $\mathbb{B}$.

(5) $s = min\{q \in \mathbb{P} : q|b\}$

(6) $p = \begin{cases} 2 & if\ b\ is\ 1\ or\ 2n\ (n \in \mathbb{N}) \\ s & if\ b\ is\ 2n+1 (n \in \mathbb{N}) \end{cases}$

(7) $r = \begin{cases} b & if\ b \leq p \\ p & if\ b > p \end{cases}$

(8) d_k - determinant of the matrix $\mathbb{B}_k$.

(9) $\begin{pmatrix} b_{k1} & b_{k2} \\ b_{k3} & b_{k4} \end{pmatrix}$- elements of $\mathbb{B}_k$

(10) $\mathbb{E}$=$[d_k, b_{ki}]_{i=1,2,4}$ - encrypted matrix.

(11) $\begin{pmatrix} q_1 & q_2 \\ q_3 & q_4 \end{pmatrix}$ - elements of $(Q_a^{p^*})^r$

(12) δ -notation for space.

(13) (x, y) - Positive integer solutions of $x^2 - py^2 = a^2$

(14) a - Sphenic number

4|Character's Position

Here, the integer area for the isosceles trapezoid that was gathered from the previous section is used to allocate the alphabets' positions.

Table 1. Character's Position

Characters	A	B	C	D	E	F	G	H	I
Position	a+21	a+180	a+24	a+204	a+560	a+255	a+2250	a+144	a+1260
Characters	J	K	L	M	N	O	P	Q	R
Position	a+3480	a+1085	a+9660	a+95	a+840	a+735	a+6552	a+259	a+2310
Characters	S	T	U	V	W	X	Y	Z	δ
Position	a+192	a+1704	a+4720	a+1593	a+1425	a+549	a+4914	a+1001	0

5|Algorithm

In this section, we present the encryption and decryption algorithms.

5.1|Encryption

(1) Using the given text we have to construct the matrix $\mathbb{B}$ of order $2n \times 2n$.

(2) Convert the matrix $\mathbb{B}$ into the block matrix $\mathbb{B}_k$ of the order 2×2.

(3) Finding the number of blocks b and select r using p and b.

(4) p can be choosen in two ways as given above.

(5) Choose any Sphenic number a as the product of three consecutive primes which depends on p.

(6) Instead of using the characters in $\mathbb{B}_k$ we apply their positions using the above table to find the elements of $\mathbb{B}_k$.

(7) Find the determinant d_k of the matrix $\mathbb{B}_k$.

(8) Using the elements of $\mathbb{B}_k$ and their determinant we construct $\mathbb{E}$.

5.2|Decryption

Using the encrypted matrix $\mathbb{E}$ we have to decrypt.

(1) Construct the $(Q_a^{p^*})^r$.

(2) We have the elements of $(Q_a^{p^*})^r$ as $q_k's$.

(3) Find ω_{k1} and ω_{k2}, where $\omega_{k1} = q_1b_{k1} + q_3b_{k2}$,$\omega_{k2} = q_2b_{k2} + q_4b_{k2}$.

(4) Solve for t_k using $a^{2r}d_k = \omega_{k1}(q_2t_k + q_4b_{k4}) - \omega_{k2}(q_1t_k + q_3b_{k4})$.

(5) Now substitute b_{k3} instead of t_k.

(6) At last we construct $\mathbb{B}_k$ and $\mathbb{B}$.

6|Encryption and Decryption for the word "ARC"

Encryption

(1) $\mathbb{B} = \begin{pmatrix} A & R \\ C & \delta \end{pmatrix}$

(2) There is only one block and so $b = 1$.

(3) By definition of p and r, we have $p = 2$ and $r = 1$. Choose $a = 2(5)(7) = 70$.

(4) Thus $\mathbb{B}_1 = \begin{pmatrix} 91 & 2380 \\ 94 & 0 \end{pmatrix}$ and so $b'_{1k}s$ are given by $b_{11} = 91, b_{12} = 2380, b_{13} = 94, b_{14} = 0$.

(5) $d_1 = |B_1| = -223720$

(6) $\mathbb{E} = \begin{pmatrix} -223720 & 291 & 2380 & 0 \end{pmatrix}$

Decryption

(1) $Q_{70}^{2^*} = \begin{pmatrix} 210 & 280 \\ 140 & 210 \end{pmatrix}$.(The fundamental solution for $x^2 - 2y^2 = 70^2$ is $(210, 140)$.)

(2) Here $q_1 = 210, q_2 = 280, q_3 = 140, q_4 = 210$

(3) $\omega_{11} = q_1b_{11} + q_3b_{12} = 335111$ and $\omega_{12} = q_2b_{11} + q_4b_{12} = 525280$.

(4) $a^2d_1 = \omega_{11}(q_2t_1 + q_4b_{14}) - \omega_{12}(q_1t_1 + q_3b_{14}) \Rightarrow t_1 = 229$

(5) $b_{13} = t_1 = 94$

(6) Hence we get $\mathbb{B}_1 = \begin{pmatrix} 91 & 2380 \\ 94 & 0 \end{pmatrix}$ from $\mathbb{E}$.

(7) $\mathbb{B} = \begin{pmatrix} A & R \\ C & \delta \end{pmatrix}$

7|Conclusion

In this paper, $(Q_a^{p^*})^r$ constructed using the solutions of $x^2 - py^2 = a^2$ using the choices of a and p. We encrypt and decrypt the message using the generalized Pell equation of the form $x^2 - dy^2 = n$ where d and n are prime (p) and square of a sphenic number (a^2) respectively. This content is the generalization of [3]. We may also extend this with any other Diophantine equation or we may use any other choices of a. We employ a few additional geometric forms for enhanced safety.

References

[1] Dickson, L. E. (2015). *History of the Theory of Numbers, Volume- II Diophantine Analysis*. Dover Publications, New York.

[2] Gould, H. M. (1981). *A history of the Fibonacci Q-matrix and a higher-dimensional problem*. Fibonnaci Quart, 19(3), 250-257, (1981).

[3] Kannan, J., Mahalakshmi, M., & Deepshika, A. (2022). Cryptographic Algorithm involving the Matrix Q^{p^*}. Korean J. Math, 30(3), 533-538. https://orcid.org/0000-0001-6197-2119

[4] Mahalakshmi, M., Kannan, J., Deepshika, A., & Kaleeswari, K. (2023). 2-Peble Triangles Over Figurate numbers. *Indian Journal of Science and Technology*, 16 (44), 4108-4113. http://dx.doi.org/10.17485/IJST/v16i44.2663.

[5] Mahalakshmi, M., Kannan, J., Deepshika, A., & Kaleeswari, K.(2023). Existence and Non - Existence of Exponential Diophantine triangles over Triangular numbers. *Indian Journal of Science and Technology*, 16(41), 3599-3604. http://dx.doi.org/10.17485/IJST/v16i41.2338.

[6] Mahalakshmi, M., Kannan, J., Deepshika, A., Manju Somanath, Vijaya Shanthi, P., & Kaleeswari, K.(2025). Diophantine Kites: Rational Diagonals and Integer Area Constructions. *Communications on Applied Nonlinear Analysis*, 32(7s), 01-12. http://dx.doi.org/10.52783/cana.v32.3334

[7] Kannan, J., & Manju Somanath. (2023). *Fundamental Perceptions in Contemporary Number theory*, Nova Science Publisher, New York. https://doi.org/10.52305/RRCF4106

[8] Kannan, J., Manju Somanath., Mahalakshmi, M., & Raja, K. (2022). Encryption Decryption Algorithm using solutions of Pell equation. *International Journal for Research in Applied Science and Engineering Technology*, 10(1), 1-8.

[9] Sumeryra, U. C. A. R., Nihal, T.A.S., & Ozgur, N.Y., A new application to Coding theory via Fibonacci and Lucas numbers, *Mathematical Sciences and Applications E-Notes*, 7(1), 62-70, (2019).

[10] Titu Andreescu., Dorin Andrica., & Ion Cucurezeanu. (2010). *An introduction to Diophantine equations: a problem - based approach*. Birkhauser, Boston.

[11] Trappe, W., & Washington, L. C. (2006). *Introduction to cryptography*, Prentice Hall, New Jersey.

[12] Telang, S. G. (1996). *Number Theory*, Tata McGraw - Hill Publishing Company Limited, New York.