Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 6, pp. 2261–2267
DOI : 10.47974/JDMSC-2564

Algebraic structure and a study of special Diophantine and Pythagorean equations

T. Srinivas
Department of Freshman Engineering
Audisankara (Deemed to be University)
Gudur
Nellore 524101
Andhra Pradesh
India

Abstract

This research paper explores advanced Diophantine equations with Pythagorean characteristics and their algebraic properties. The work extends classical number theory concepts into novel structural frameworks, particularly through its examination of solution spaces and binary operation. The core equation $kx^2 + y^2 = z^2$ transforms into normalized ellipse form of $k\left(\frac{x}{z}\right)^2 + \left(\frac{y}{z}\right)^2 = 1$. The reciprocal variant $\frac{k}{p^2} + \frac{1}{q^2} = \frac{1}{h^2}$ introduces new constraints of integer triples (p, q, h).

Also, the paper proposes a complex binary operation $P_1.P_2$ defined through component-wise combinations:

$$P_1.P_2 = \begin{Bmatrix} (kx_1x_2^2, y_1(y_2^2 + z_2^2) + 2y_2z_1z_2, z_1(y_2^2 + z_2^2) + 2y_1y_2z_2) \\ (kx_2x_1^2, y_2(y_1^2 + z_1^2) + 2y_1z_1z_2, z_2(y_1^2 + z_1^2) + 2y_1y_2z_1) \end{Bmatrix}.$$

Also focused Extension of Binomial Distribution for $kx^2 + y^2 = z^2$.

Subject Classification: *11D72, 11D61.*

Keywords: *Algebraic structure, Binary operation, Associative axiom.*

1. Introduction

The phrase "Algebraic Structure and A Study of Special Diophantine Pythagorean Equations" typically refers to a research-oriented theme that investigates integer solutions of Pythagorean-type Diophantine equations while endowing solution sets with algebraic structures like semigroups.

ORCID-ID: **0009-0001-6282-7762**

E-mail: **drtsrinivas80@gmail.com**

From the references [1] to [6], the binary operation of Algebraic structure and some inherent properties are extended in the present work.

The core equation $kx^2 + y^2 = z^2$, defines a **Pythagorean-type quadratic form** whose integer solutions can be used in embedded-system cryptography as sources of **structured randomness**, **key material**, or **lightweight trapdoor problems.**

Key features useful for cryptography:

- The solution set is infinite but sparse, so it is easy to generate many triples but hard to "guess" them at random.
- Solutions can be ordered by size of z, giving a natural sequence suitable for indexing keys or round constants.

In embedded settings this can be used for:

- Authentication tags,
- Lightweight signatures on constrained devices,
- Key-agreement hints that are combined with a stronger primitive in Elliptic curve cryptography(ECC) as follows:

Suppose, the Equation $2x^2 + y^2 = z^2$ is a homogeneous quadratic in three variables. So, it does not define elliptic curve. However, we can associate an elliptic curve to it by dehomogenizing and transforming to a cubic Weier strass model.

Step 1: De homogenize to a conic:

- Set X = $\frac{x}{z}$, Y= $\frac{y}{z}$ implies $2\left(\frac{x}{z}\right)^2 + \left(\frac{y}{z}\right)^2 = 1$ with $2X^2 + Y^2 = 1$. It is rational but not elliptic.

Step 2: Pass to cubic Model:

- According 2-descent type, from Jacobian suitable change of variable up to Isomorphism over Q, for equations of the form $Dx^2 + y^2 = z^2$ a common associated elliptic curve arises E: $y^2 = x^3 - D^2x$.
- Hence in this case D = 2, the Associated Elliptic curve E:

$y^2 = x^3 - 4x$, which is having infinitely many rational points, but only finitely many integer points,

- $y^2 = x(x-2)(x+2)$, with integer solutions are (x ,y) = $\{(0,0), (2,0), (-2,0)\}$

Also, its possible to express into **Quantum-resistance** in key generation as follows:

Primitive Diophantine triples enhance quantum-resistance in key generation by providing a sparse, high-entropy, and nonlinear source of deterministic randomness. The primitivity condition maximizes entropy per bit and avoids trivial reductions, while the absence of known efficient quantum

algorithms for inverting the triple-generation process makes the resulting key material heuristically resistant to quantum search and statistical attacks. When combined with nonlinear mixing and other post-quantum-safe components, primitive Diophantine triples can contribute to lightweight quantum-resistant symmetric-key schemes.

2. Methods:

First, describing a computational-experimental study of a **special Diophantine equation of the form** $kx^2 + y^2 = z^2$ and its Reciprocal $\frac{k}{x^2} + \frac{1}{y^2} = \frac{1}{z^2}$ using of where k runs over integers from 2 to 21, and search for positive integer solutions (x, y, z) via a trial-and-error (brute-force) method.

Second, focused on reducing these Diophantine equations into the Ellipse form of $k\left(\frac{x}{z}\right)^2 + \left(\frac{y}{z}\right)^2 = 1$.

Third, Closure Axiom is defined as follows.

$$P_1.P_2 = \begin{Bmatrix}(kx_1{x_2}^2, y_1({y_2}^2 + {z_2}^2) + 2y_2z_1z_2, z_1({y_2}^2 + {z_2}^2) + 2y_1y_2z_2)\\(kx_2{x_1}^2, y_2({y_1}^2 + {z_1}^2) + 2y_1z_1z_2, z_2({y_1}^2 + {z_1}^2) + 2y_1y_2z_1)\end{Bmatrix}$$

Example design sketch for embedded system cryptography.

Suppose you want a **lightweight stream cipher** for an 8-bit microcontroller:

1. Fix a modulus m (e.g., 216).
2. Generate a sequence of primitive solutions (x_n, y_n, z_n) of
$$2x^2 + y^2 = z^2.$$
3. Define the key stream byte at step n by $k_n=(x_n+y_n+z_n) \bmod 256$.
4. Encrypt a plaintext byte p_n as $c_n= p_n \oplus k_n$.

This gives a **nonlinear, sparse keystream** with low computational overhead, suitable for low-power embedded platforms.

Main work:

Case 1: Consider the Diophantine equation $2x^2 + y^2 = z^2$ **that depends on a positive integer parameter n,** $x = 2^{n+1}$, $y = 2^n$ and $z = 3(2)^n$.

Design a integer solution, for some integer n, the different solution sets, since $2x^2 + y^2 = 2(2^{n+1})^2 + (2^n)^2 = (3(2)^n)^2 = z^2$.

Lemma 1: *Define two types of Binary Operations '*' on the Set of Stationary Points of the above quadratic Diophantine Equation,*

$$2x^2 + y^2 = z^2 \text{ with } P(x_1, y_1, z_1), Q(x_2, y_2, z_2)$$

$$\text{P*Q} = \begin{Bmatrix}(2x_1{x_2}^2, y_1({y_2}^2 + {z_2}^2) + 2y_2z_1z_2, z_1({y_2}^2 + {z_2}^2) + 2y_1y_2z_2)\\(2x_2{x_1}^2, y_2({y_1}^2 + {z_1}^2) + 2y_1z_1z_2, z_2({y_1}^2 + {z_1}^2) + 2y_1y_2z_1)\end{Bmatrix}$$

E.g. For n = 1, $P_1 = (4,2,6)$ and for n =2, $P_2 = (8,4,12)$ are satisfies $2x^2 + y^2 = z^2$. Also, above binary operation $P_1.P_2 = (512,896,1152)$ is satisfies $2x^2 + y^2 = z^2$.

Also, another binary operation $P_1.P_2 = (256,448,576)$ is satisfies $2x^2 + y^2 = z^2$. it follows that clearly (128,224,288), (64,112,144), (32,56,72), (16,28,36), (8,14,18), (4,7,9) are becomes to solutions of $2x^2 + y^2 = z^2$.

Case 2: Consider the Diophantine equation $3x^2 + y^2 = z^2$ having different sets of integer solutions $x = 3^n$, $y = 3^n$ and $z = 2(3)^n$. Here n is a positive integer.

With binary operation , for all $P_1, P_2 \in B$.

$$P_1.P_2 = \begin{Bmatrix}(3x_1{x_2}^2, y_1({y_2}^2 + {z_2}^2) + 2y_2z_1z_2, z_1({y_2}^2 + {z_2}^2) + 2y_1y_2z_2)\\(3x_2{x_1}^2, y_2({y_1}^2 + {z_1}^2) + 2y_1z_1z_2, z_2({y_1}^2 + {z_1}^2) + 2y_1y_2z_1)\end{Bmatrix}$$

Verification: We know that $x = 3^n$, $y = 3^n$ and $z = 2(3)^n$ are satisfied $3x^2 + y^2 = z^2$.

For n = 1, $P_1 = (3,3,6)$ and for n =2, $P_2 = (9,9,18)$ are satisfies $3x^2 + y^2 = z^2$. Also, above binary operation $P_1.P_2 = (729,3159,3402)$ is satisfied $3x^2 + y^2 = z^2$.

Case 3: Consider the Diophantine equation $4x^2 + y^2 = z^2$ having different sets of integer solutions is (2x, y, z) is a Pythagorean triplet. It has different sets of Integer solutions for each odd integer x, then $y = x^2 - 1$ and $z = x^2 + 1$.

Similarly, we can verify the following results

C= $\{5x^2 + y^2 = z^2; with\ x = 4^{n+1},\ y = 4^n, z = 3(4)^n\}$

D= $\{6x^2 + y^2 = z^2; with\ x = 2^{n+1},\ y = 2^n, z = 5(2)^n\}$

E= $\{7x^2 + y^2 = z^2; with\ x = 3^n,\ y = 3^{n+1}, z = 4(3)^n\}$

F= $\{8x^2 + y^2 = z^2; with\ x = 2^n,\ y = 2^n, z = 3(2)^n\}$

G= $\{10x^2 + y^2 = z^2; with\ x = 6^{n+1},\ y = 6^n, z = 19(6)^n\}$

H= $\{11x^2 + y^2 = z^2; with\ x = 3^{n+1},\ y = 3^n, z = 10(3)^n\}$

I= $\{12x^2 + y^2 = z^2; with\ x = 2^{n+1},\ y = 2^n, z = 7(2)^n\}$

J= $\{13x^2 + y^2 = z^2; with\ x = 6^n,\ y = 6^{n+1}, z = 7(6)^n\}$

K= $\{14x^2 + y^2 = z^2; with\ x = 6^{n+1},\ y = 5(6)^n, z = 23(6)^n\}$

L= $\{15x^2 + y^2 = z^2; with\ x = 3^{n+1},\ y = 3^{n+1}, z = 12(3)^n\}$

M= $\{17x^2 + y^2 = z^2; with\ x = 3^{n+1},\ y = 4(3)^n, z = 13(3)^n\}$

N= $\{18x^2 + y^2 = z^2; with\ x = 2^{n+1},\ y = 3(2)^n, z = 9(2)^n\}$

O= $\{19x^2 + y^2 = z^2; with\ x = 3^{n+1},\ y = 5(3)^n, z = 14(3)^n\}$

Q= $\{20x^2 + y^2 = z^2; with\ x = 2^{n+1},\ y = 2^n, z = 9(2)^n\}$

R= $\{21x^2 + y^2 = z^2; with\ x = 2^n,\ y = 2^{n+1}, z = 5(3)^n\}$ AND

P= $\{(mx, y, z)\ is\ a\ Pythagorean\ triplet, m \in N: (mx)^2 + y^2 = z^2\}$.

Also, the binary operation on the above subsets of quadratic Diophantine Equation is defined as follows.

$$P_1.P_2 = \begin{Bmatrix} (kx_1{x_2}^2, y_1({y_2}^2 + {z_2}^2) + 2y_2z_1z_2, z_1({y_2}^2 + {z_2}^2) + 2y_1y_2z_2) \\ (kx_2{x_1}^2, y_2({y_1}^2 + {z_1}^2) + 2y_1z_1z_2, z_2({y_1}^2 + {z_1}^2) + 2y_1y_2z_1) \end{Bmatrix}$$

Extension of Binomial Distribution for $kx^2 + y^2 = z^2$

Consider $kx^2 + y^2 = z^2$ is having of $k\left(\frac{x}{z}\right)^2 + \left(\frac{y}{z}\right)^2 = 1$; Which is having simple form of ellipse $kp^2 + q^2 = 1$.

Hence $(kp^2 + q^2)^n = 1$, which implies $\sum_{x=0}^{n} n_{c_x} (kp^2)^x (q^2)^{n-x} = 1$.

Now introduce to define special PMF of Binomial Distribution is $P(X = x) = n_{c_x}(kp^2)^x(q^2)^{n-x}$.

Property 1: Expectation of above probability mass function

$P(X = x) = n_{c_x}(kp^2)^x(q^2)^{n-x}$ is nkp^2.

Proof: Expectation of x is a first moment about the origin, which is denoted by

E(X) = $\sum_{x=0}^{n} x\, P(X = x) = \sum_{x=0}^{n} x\, n_{c_x}(kp^2)^x(q^2)^{n-x}$

$= \sum_{x=0}^{n} x \frac{n!}{x!(n-x)!}(kp^2)^x(q^2)^{n-x} = \sum_{x=0}^{n} \frac{n(n-1)!}{(x-1)!(n-x)!} kp^2(kp^2)^{x-1}(q^2)^{n-x}$

$= \text{n k } p^2(kp^2 + q^2)^{n-1} = nkp^2.$

Property 2: Variance of above probability mass function

$P(X = x) = n_{c_x}(kp^2)^x(q^2)^{n-x}$ is nkp^2q^2.

Proof: Variance of x is a Second moment about the mean, which is denoted by V(x) = E(X^2)−(E(X))^2

Consider E(X^2) $= \sum_{x=0}^{n} x(x-1)\frac{n!}{x!(n-x)!}(kp^2)^x(q^2)^{n-x} + nkp^2 =$

$\sum_{x=0}^{n} \frac{n(n-1)(n-2)!}{(x-2)!(n-x)!}(kp^2)^2(kp^2)^{x-2}(q^2)^{n-x} + nkp^2$

$= n(n-1)(kp^2)^2(kp^2 + q^2)^{n-2} + nkp^2 = n(n-1)(kp^2)^2 + nkp^2.$

Hence V(x) = E(X^2)−$\left(\text{E(X)}\right)^2 = n(n-1)(kp^2)^2 + nkp^2 - (nkp^2)^2$

$= nkp^2(1 - kp^2) = nkp^2q^2.$

Some special Diophantine Pythagorean Equations

From the References [3], [4], [5], [6] to study following case:

Case 4: Diophantine equations of higher degrees, like the quartic form

$\alpha(X^4 + Y^4)((2P_nP_{n+1})^2 + (P_{n+1}^2 - \text{P}_\text{n}^2)^2) = (\text{P}_{\text{n+1}}^2 + \text{P}_\text{n}^2)^2(C^2 - D^2)(Z^2 + W^2)P^\beta$, play a meaningful role in generating special elliptic curves that are crucial for cryptography and secure communications. With the sequence of Pell numbers is $(\{0, 1, 2, 5, 12, 29, 70, 169 \ldots\ldots\})$ satisfies Recurrence Relation $\text{P}_\text{n} = 2\text{P}_{\text{n}-1} + \text{P}_{\text{n}-2}$ for $n \geq 2$, with $\text{P}_0 = 0$, $\text{P}_1 = 1$, with $(2P_nP_{n+1})^2 + (P_{n+1}^2 - \text{P}_\text{n}^2)^2 = (\text{P}_{\text{n+1}}^2 + \text{P}_\text{n}^2)^2$

Having integer design of solutions for $\beta > 2$ is parameterized by integers k and n, with variables defined as: x = $k^n, y = k^{n+1}, z = k^{n+3}, w = k^{n+2}, p = k^n$,

$$\alpha = (1 + k^4)(k^6 + k^4)k^{(\beta-2)n}n^2,$$

$$\left\{\begin{matrix} C = \left(\left(\frac{1+k^4}{2}\right)^2 + 1\right)n, D = \left(\left(\frac{1+k^4}{2}\right)^2 - 1\right)n, & if\ 1 + k^4\ is\ even \\ C = \left(\frac{\left(1+k^4\right)^2+1}{2}\right)n, D = \left(\frac{\left(1+k^4\right)^2-1}{2}\right)n, & if\ 1 + k^4\ is\ odd \end{matrix}\right\}.$$

for $\beta = 1$ is x = $k^n, y = k^{n+1}, z = k^{n+3}, w = k^{n+2}, p = k^{2n}$,

$$\alpha = (1 + k^4)(k^6 - k^4)n^2,$$

$$\left\{\begin{matrix} C = \left(\left(\frac{1+k^4}{2}\right)^2 + 1\right)n, D = \left(\left(\frac{1+k^4}{2}\right)^2 - 1\right)n, & if\ 1 + k^4\ is\ even \\ C = \left(\frac{\left(1+k^4\right)^2+1}{2}\right)n, D = \left(\frac{\left(1+k^4\right)^2-1}{2}\right)n, & if\ 1 + k^4\ is\ odd \end{matrix}\right\}.$$

for $\beta = 2\ is$ x = $k^n, y = k^{n+1}, z = k^{n+3}, w = k^{n+2}, p = k^n$,

$$\alpha = (1 + k^4)(k^6 + k^4)n^2.$$

$$\left\{\begin{matrix} C = \left(\left(\frac{1+k^4}{2}\right)^2 + 1\right)n, D = \left(\left(\frac{1+k^4}{2}\right)^2 - 1\right)n, & if\ 1 + k^4\ is\ even \\ C = \left(\frac{\left(1+k^4\right)^2+1}{2}\right)n, D = \left(\frac{\left(1+k^4\right)^2-1}{2}\right)n, & if\ 1 + k^4\ is\ odd \end{matrix}\right\}$$

3. Conclusion

This paper first focused on studying infinitely many integer solutions of the different special Diophantine Equations.

The core equation $kx^2 + y^2 = z^2$ paper proposes a complex binary operation $P_1.P_2$ defined through component-wise combinations:

$$P_1.P_2 = \left\{\begin{matrix} (kx_1{x_2}^2, y_1({y_2}^2 + {z_2}^2) + 2y_2z_1z_2, z_1({y_2}^2 + {z_2}^2) + 2y_1y_2z_2) \\ (kx_2{x_1}^2, y_2({y_1}^2 + {z_1}^2) + 2y_1z_1z_2, z_2({y_1}^2 + {z_1}^2) + 2y_1y_2z_1) \end{matrix}\right\}.$$

The core equation $kx^2 + y^2 = z^2$, defines a Pythagorean-type quadratic form whose integer solutions can be used in embedded-system cryptography as sources of structured randomness, key material, or lightweight trapdoor problems. It also, very useful for quantum cryptography, since Primitive Diophantine triples enhance quantum-resistance in key generation by providing a sparse, high-entropy, and nonlinear source of deterministic randomness. The primitivity condition maximizes entropy per bit and avoids trivial reductions, while the absence of known efficient quantum algorithms for inverting the triple-generation process makes the resulting key material heuristically resistant to quantum search and statistical attacks. When combined with nonlinear mixing and other post-quantum-safe components, primitive Diophantine triples can contribute to lightweight quantum-resistant symmetric-key schemes.

References

[1] K. Sridevi and T. Srinivas, "Transcendental representation of the Diophantine equation and some of its inherent properties," *Mater.* Today: Proc., vol. 80, pp. 1822–1825 (2023).

[2] T. Srinivas and K. Dhanumjaya, "Integer solutions parameterized by k, m, n yielding unified crypto-control pipelines," *Int. J. Adv. Sci. Tech. Res.* (IJASTR), vol. 16, no. 1, pp. 208–220 (2026), doi: 10.5281/zenodo.18368265.

[3] K. Sridevi and T. Srinivas, "Cryptographic coding to define binary operation on a set of Pythagorean triplets," *Mater. Today: Proc.*, vol. 80, pp. 1822–1825 (2023).

[4] T. Srinivas, "A study on quadratic and quintic Diophantine equation in embedded cryptographic coprocessors," *Int. J. Comput. Appl.* (IJCA), vol. 16, no. 1, pp. 22/1–22/12 (2026). doi: 10.26808/RS.2026.c1fb5f

[5] Siswanto and Sahmura Maula Al-Maghribi, "Solving the eigenproblems of triangular and diagonal strictly double R-astic matrices over min-plus algebra," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 28, no. 6, pp. 2237–2245 (2025), doi: 10.47974/JDMSC-2188.

[6] S. Muthuvel and R. Venkatraman "An exponential Diophantine equation x^2 + 3^a*73^b = y^n," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 28, no. 6, pp. 2289–2296 (2025), doi: 10.47974/JDMSC-2225.

Received May, 2025