International Journal of Research in Engineering, Science and Management
Volume-2, Issue-9, September-2019
www.ijresm.com | ISSN (Online): 2581-5792

Theoretical Approaches in Number Theory and its Significance in Cryptography

K. Muthu[1], S. Revathi[2]
[1]*M.Phil. Scholar, Dept. of Mathematics, Ponnaiyah Ramajayam Inst. of Science and Tech., Thanjavur, India*
[2]*Assistant Professor, Dept. of Mathematics, Ponnaiyah Ramajayam Inst. of Science and Tech., Thanjavur, India*

***Abstract*: In this work, we have outlined some new definitions and created the transplantation of primitive Pythagoras tree and use this transplantation within the security of ATM pin for more secure authentication.**

***Keywords*: Number theory, cryptography, Pythagoras.**

1. Introduction

In the modern era of technology, it is necessary to create the more secure encryption methods for secure communication in the field of cryptography. In cryptography, number theory in provides security for transmitting messages and data. In particular, Pythagorean triples play a vital role in the field of cryptography for constructing strong secret key for secure communication [1].

2. Mathematic Formalism

A. Prime tree

If in a tree the number of edges (branches) incident at each node (vertex) are prime then it is called a prime tree. If the number of edges incident at any vertex are composite then the tree is called a composite tree and is the number of edges at each vertex are two then it is called a binary tree.

B. Multi-dimensional tree

A multidimensional tree with the root β is represented by,
$\beta\ i_1\ i_2\ i_3 \ldots\ldots\ i_n$,
which means the basis β has out degree i_1 with i_1^{th} branch has out degree i_2 with i_2^{th} branch has out degree i_3 and so on.

Theorem 1.1
The set of Pythagorean Triples is infinite.
Proof:
To prove this, consider a Pythagoras Triple (8,15,17).
Let n > 1 be any integer, then 8n, 15n, and 17n are also a set of Pythagorean Triples, which is true because:
$(8n)^2 + (15n)^2 = (17n)^2$

Examples:

n	(8n,15n,17n)
2	(16,30,34)
3	(24,45,51)

So we can make infinitely many triples just using the triple (8, 15, 17). Hence, the set of Pythagorean Triples is infinite.

C. Pythagoras triple and pythagoras primitive

A Pythagorean triple (a,b,c) is a set of integers that are the sides of a right triangle and thus $a^2+b^2 = c^2$.
Given a Pythagorean triple (a,b,c), (da,db,dc) is also a triple. A Pythagorean triple consists of numbers that are apparently prime.

D. Properties of pythagoras triple

A Pythagorean Triple always comprised of:

- All even numbers, or
- An even number and two odd numbers.
- A Pythagorean Triple can never be made-up of all odd numbers or one odd number and two even numbers. This is true as:
- The sum of an odd number and an even number is an odd number and the sum of two even numbers is an even number.

E. First few pythagorean primitives

Table 1. shows the Pythagoras Triples where a, b, and c are less than 1,000. But the table only has the first set (a,b,c) which is a Pythagorean Triple, called primitive Pythagorean Triple.

(3,4,5)	(5,12,13)	(7,24,25)	(8,15,17)	(9,40,41)
(11,60,61)	(12,35,37)	(13,84,85)	(15,112,113)	(16,63,65)
(17,144,145)	(19,180,181)	(20,21,29)	(20,99,101)	(21,220,221)
(23,264,265)	(24,143,145)	(25,312,313)	(27,364,365)	(28,45,53)
(28,195,197)	(29,420,421)	(31,480,481)	(32,255,257)	(33,56,65)
(33,544,545)	(35,612,613)	(36,77,85)	(36,323,325)	(37,684,685)
(39,80,89)	(39,760,761)	(40,399,401)	(41,840,841)	(43,924,925)
(44,117,125)	(44,483,485)	(48,55,73)	(48,575,577)	(51,140,149)
(52,165,173)	(52,675,677)	(56,783,785)	(57,176,185)	(60,91,109)

F. Tree of primitive Pythagoras triples

In mathematics, a tree of primitive Pythagorean triples is a data tree in which each node branches to more than one subsequent node with the infinite set of all nodes giving all (and only) Pythagorean triples without any duplication.
The set of all Pythagorean triples have the special structure of a rooted tree, specifically a ternary tree, in a natural way.

G. Span of Pythagoras tree

The distance of any node (a,b,c) of Pythagorean tree from the origin (0,0,0) is called the span of the Pythagorean tree with respect to that node and is defined as:

$$\text{Span} = \sqrt{[(a-0)^2 + (b-0)^2 + (c-0)^2]}$$

Example:

Let the node is (3,4,5) then the span of the tree with respect to this node is given by:

$$\text{Span} = \sqrt{[(3-0)^2 + (4-0)^2 + (5-0)^2]} = \sqrt{50} = 5\sqrt{2}.$$

H. Length of the branch of pythagorean tree

The length of any branch of Pythagorean tree is the distance between the two end nodes of that branch. If (a_1,b_1,c_1) and (a_2,b_2,c_2) be the two end nodes of a branch then the length of the branch is given by:

$$\text{Length of AB} = \sqrt{[(a_2-a_1)^2 + (b_2-b_1)^2 + (c_2-c_1)^2]}$$

Example:

let the two end nodes of a branch AB are A(5,12,13) and B(7,24,25), then the length of the branch AB is given by:

$$\text{Length of branch AB} = \sqrt{[(7-5)^2 + (24-12)^2 + (25-13)^2]}$$

$$= \sqrt{292} = 2\sqrt{73}.$$

I. Application of pythagorean primitives in cryptography

Application in the Security of ATM Password

Let the ATM password having all the different digits 2 7 3 5.

First find the sum of all the digits of the password as, 2 + 7 + 3 + 5 = 17

Add this sum to all the digits of the password to get the new digits as, 19 24 20 22

Each new digit can never be having more than two digits.

Find 19th, 24th, 20th and 22nd Pythagorean primitive (a,b,c) for transplantation (consider the sequence of Pythagoras primitive in increasing order of a).

19th Pythagoras primitive = (27, 364, 365)

24th Pythagoras primitive = (32, 255, 257)

20th Pythagoras primitive = (28, 45, 53) 22nd Pythagoras primitive = (29,420,421)

3. Conclusion

The transplantation of primitive Pythagoras tree is very useful in the cryptographic systems for making strong source for secure communication.

References

[1] D. M. Burton, Elementary Number Theory, Second Edition, Wm. C. Brown Company Publishers, 2006.