World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:11, No:11, 2017

Pythagorean-Platonic Lattice Method for Finding all Co-Prime Right Angle Triangles

Anthony Overmars, Sitalakshmi Venkatraman

***Abstract*—**This paper presents a method for determining all of the co-prime right angle triangles in the Euclidean field by looking at the intersection of the Pythagorean and Platonic right angle triangles and the corresponding lattice that this produces. The co-prime properties of each lattice point representing a unique right angle triangle are then considered. This paper proposes a conjunction between these two ancient disparaging theorists. This work has wide applications in information security where cryptography involves improved ways of finding tuples of prime numbers for secure communication systems. In particular, this paper has direct impact in enhancing the encryption and decryption algorithms in cryptography.

***Keywords*—**Pythagorean triples, platonic triples, right angle triangles, co-prime numbers, cryptography.

I. Introduction

THE theory on Pythagorean triple has led to much research for several decades in the mathematical arena [1], and more recently in the computing field due to its increased application in information security where improved cryptosystems are warranted [2]. Generating Pythagorean triples is of interest, in particular, finding co-prime right angle triangles has utilisation in encryption, decryption, and public key cryptosystem for securing information [3], [4]. This paper proposes a new method of finding co-prime right angle triangles using the properties of Pythagorean triples.

A Pythagorean triple denoted by (a,b,c) is a solution of the equation $a^2 + b^2 = c^2$, where a,b,c are positive integers [5]. A Pythagorean triple (a,b,c) is considered to be primitive when a,b,c are co-prime to each other. In the other words, their greatest common divisor (gcd) is 1, i.e. $gcd(a,b,c) = 1$. The *Pythagorean family* of triples has a formula derived by Stark [6] as

$$P(a,b,c) = (2n+1, 2n^2+2n, 2n^2+2n+1),$$

where n is a positive integer. The triples can be enumerated as

$$P(a,b,c) = \{(3,4,5),(5,12,13),(7,24,25)...\}.$$

On the other hand, the *Platonic family* of triples is defined by $(4m^2 -1, 4m, 4m^2 +1)$, which can be enumerated as

$$P(a,b,c) = \{(3,4,5), (15,8,17), (35,12,37)...\}.$$

A. Overmars is with Melbourne Polytechnic, Preston, VIC 3181 Australia (e-mail: AnthonyOvermars@melbournepolytechnic.edu.au).

S. Venkatraman is with Melbourne Polytechnic, Preston, VIC 3181 Australia. (corresponding author, phone: 613-92691171; e-mail: SitaVenkat@melbournepolytechnic.edu.au).

The alert reader will immediately note that both the Pythagorean and Platonic families have a common triple such that: $P(a,b,c) = (3,4,5)$. It is also noted that this occurs when $m=1$ and $n=1$, such that $P(a,b,c) = (3,4,5) \Longrightarrow P(m,n) = (1,1)$. This describes the intersection between the Pythagorean and Platonian right angle triangles and the first point in the lattice. This triple has the much-desired property of being co-prime. The objective of this paper is to propose a method using this property to generate all the co-prime right angle triangles.

This paper is organized as follows. The next section (Section II) gives a literature review of other related work and how this topic has applications in cryptography. In Section III, our proposed method is described. The summary of findings is given in Section IV and finally our conclusions are provided in Section V.

II. Literature Review

There are several methods of generating Pythagorean triples reported in literature [7]-[9]. Some classical methods generate Pythagorean triples, mainly producing primitive triples, while some others generate all possible triples, including non-primitive triples. For example, the Euclid's classical formula states that for any two positive integers m and n with $m > n$, $a = m^2 - n^2$, $b = 2mn$, $c = m^2 + n^2$ form a Pythagorean triple and generates infinitely many primitive triples but not non-primitive ones [10]. In any primitive Pythagorean triple, either a or b is odd, and the other has to be even, and if a and b were both even then c would be even, violating primitivity. Previous work has shown that every primitive Pythagorean triple (a,b,c) with b even can be generated from the triple (3,4,5) as a starting triple [1], [11]. Another paper presents a direct method to generate all possible triples both primitive and non-primitive for any given number [12]. A recent previous work proposes a formula that parameterises the Pythagorean triples as elements of two series [13]. On the other hand, with the standard Euclidean formula, this parameterisation does not generate the Pythagorean triples where the elements of the triple are all divisible by 2. Since finding Pythagorean triples is equivalent to finding right triangles with integral sides, in this paper we propose a new method to find all the co-prime right triangles innovatively. We explore this idea by investigating the intersection of the Pythagorean and Platonic right angle triangles and the corresponding lattices produced. Our focus on finding co-prime right angle triangles is due to its application in cryptography and random number generation algorithms widely required in the computing field.

Cryptography, derived from the Greek word "Kryptos",

means “hidden secret”, which is the practice and study of techniques for secure communication in the presence of third parties called adversaries [3]. Modern cryptography involves techniques to construct and analyse protocols that prevent third parties to read information. Its purpose is to hide information and to convert some secret information into non-readable formats and it covers various aspects in information security such as data integrity and confidentiality, authentication and non-repudiation that have real-life applications in electronic commerce, military message transmissions, computer passwords and ATM cards. One of the most difficult aspects of cryptography is in the generation of random numbers. In general, there are two kinds of random number generators: non-deterministic random number generators (true random number generators) and deterministic random number generators (pseudorandom number generators) [14]. The problem faced here is that a computer cannot produce true random data, and many cryptography algorithms uses both with a hardware random-number generator to periodically re-seed a deterministic random number generator. Hence, to achieve this, it is often necessary to find big prime numbers and the factors of large integers [15].

The well-known Rivest-Shamir-Aldeman (RSA) public key cryptographic system is based on the computational difficulty of factoring a big integer [16]. Here, two prime numbers p and q are chosen and a random number to be identified which has no common factor with (p − 1)(q − 1). In the Massy-Omura cryptosystem for message transmission, a random integer e is selected between 0 and q−1 such that gcd.(e,q −1) = 1 and, using the Euclidean algorithm, it computes its inverse d = e−1 mod q-1. In 1980, the first three-pass protocol was called the Shamir No-Key Protocol since the sender and the receiver do not exchange any public keys, and requires having only two private keys for encrypting and decrypting messages. This algorithm uses exponentiation modulo of a large prime for both the encryption (E) and decryption (D) functions [17]. This can be mathematically expressed as $E(e,m) = m^e \bmod p$ and $D(d,m) = m^d \bmod p$ where p is a large prime, e is the encryption exponent $1 \leq e \leq p\text{-}1$ with $\gcd(e,p\text{-}1) = 1$, d is the corresponding decryption exponent chosen such that $de \equiv 1 \pmod{p\text{-}1}$. The basis for this concept is derived from Fermat’s Little Theorem that $D(d,E(e,m)) = m^{de} \bmod p = m$.

Overall, it can be observed that the nice properties of co-prime right angle triangles help to build public key cryptosystems for satisfying the modern information security objectives in real-world applications. Hence, we propose a new method to achieve this as described in the next section.

III. Proposed Method

We propose a new method to determine all of the co-prime right angle triangles in the Euclidean field by considering the lattice points represented by the intersections of the Pythagorean and Platonic right angle triangles. This work advances previous research [13] and takes a step forward in proposing a conjunction between these two ancient disparaging theorists.

Let us consider the right angle triangle in Fig. 1, with sides a,b,c. We make use of Apollonius' theorem that states as the following:

> "the sum of the squares of any two sides of any triangle equals twice the square on half the third side, together with twice the square on the median bisecting the third side"

Using this theorem by Apollonius, we inscribe two circles (arcs) one from Point A with radius “a” and the other from Point B with radius “b” in Fig. 1. Next, we consider side “c” with segments d,e,f expressed as: $c = d + e + f$.

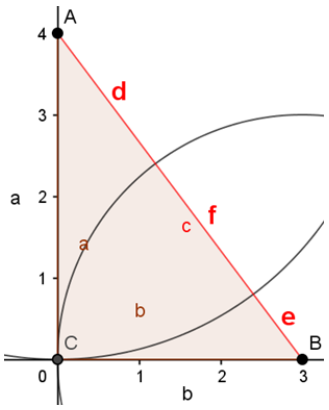

Fig. 1 Right angle triangle - Segmenting side “c”

Inscribe two circles (arcs) one from Point A with radius “d” and the other from Point B with radius “e” in Fig. 2.

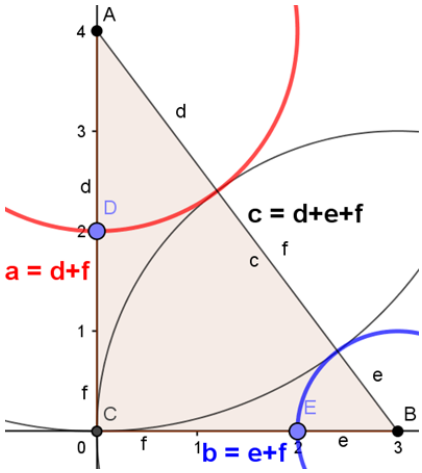

Fig. 2 Right angle triangle sides a,b,c as elements of d,e,f

From Fig. 2, $a = d + f, b = e + f, c = d + e + f$, as a matrix is given below:

$$\begin{bmatrix} a \\ b \\ c \end{bmatrix} = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} e \\ f \\ d \end{bmatrix}$$

Pythagorean triples (a,b,c) = $(2n+1, 2n^2+2n, 2n^2+2n+1)$ as a matrix is represented below:

$$\begin{bmatrix} a \\ b \\ c \end{bmatrix} = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} 2n^2 \\ 2n \\ 1 \end{bmatrix}$$

Platonic triples (a,b,c) = ($4m^2-1$, $4m$, $4m^2+1$) as a matrix is:

$$\begin{bmatrix} a \\ b \\ c \end{bmatrix} = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} 2 \\ 2(2m-1) \\ (2m-1)^2 \end{bmatrix}$$

Combining Pythagorean and Platonic triples [13], we get:

$$\begin{bmatrix} a \\ b \\ c \end{bmatrix} = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} 2n^2 \\ 2n(2m-1) \\ (2m-1)^2 \end{bmatrix}$$

From this matrix, we arrive at the following:

$$e = 2n^2, d = (2m-1)^2, f = 2n(2m-1).$$

Redefining P(a,b,c) in terms of P(m,n), we get:

$$a = d + f = 4mn - 2n + 4m^2 - 4m + 1 \quad (1)$$

$$b = e + f = 2n^2 + 4mn - 2n \quad (2)$$

$$c = d + e + f = 2n^2 + 4mn - 2n + 4m^2 - 4m + 1 \quad (3)$$

This produces the lattice of triples as shown in Fig. 3.

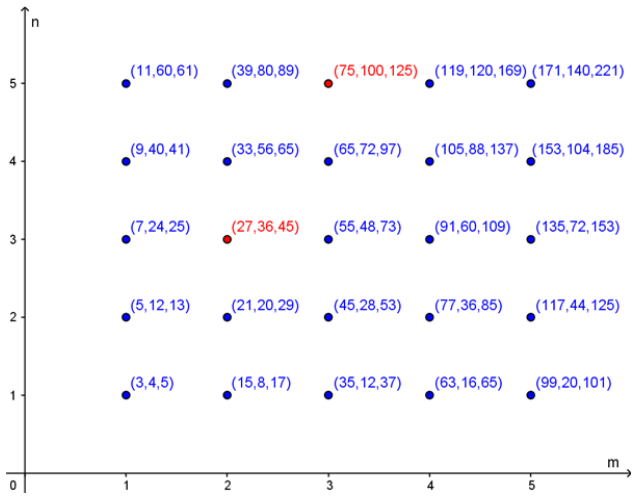

Fig. 3 Lattice of triples P(a,b,c) for P(m,n)

It can be seen from Fig. 3, that some of the lattice triples, $P(2,3) = (27,36,45)$ *and* $P(3,5) = (75,100,125)$, are not co-prime when n=$2m-1$. The next non-co-prime is $P(4,7) = (147,196,245)$.

The greatest common divisor (gcd) for these triples is given as:

$$\gcd[P(2,3)] = 9,\ \gcd[P(3,5)] = 25,\ \gcd[P(4,7)] = 49$$
$$\Rightarrow \gcd[P(m, 2m-1)] = (2m-1)^2$$

The general expression for non-co-prime triples as follows:

$$n = m^y(2m-1)^z, m > 1, y \geq 0, z > 0$$

The general expression for the gcd factor when $n = m^y(2m-1)^z$ is given below:

$$\gcd\{P[m, m^y(2m-1)^z]\} = [m^y(2m-1)^z]^2, \quad m > 1, y \geq 0, z > 0 \quad (4)$$

IV. Summary of Findings

The co-prime triples, $P(a,b,c)$ can be expressed in terms of m,n such that $P(m,n)$ represents the lattice of the Platonic triples, $P(m)$ and the Pythagorean triples, $P(n)$:

$$P(m,n) = P(a,b,c)$$

$P(a,b,c)$ can now be expressed in terms of m,n:

$$a = 4mn - 2n + 4m^2 - 4m + 1$$
$$b = 2n^2 + 4mn - 2n$$
$$c = 2n^2 + 4mn - 2n + 4m^2 - 4m + 1$$

The general expression for the gcd factor for non-co-prime triples is given below:

$$\gcd\{P[m, m^y(2m-1)^z]\} = [m^y(2m-1)^z]^2, \quad m > 1, y \geq 0, z > 0$$

V. Conclusion

This paper combines two methods of generating right angle triangles, Pythagoras and Plato, for finding all co-prime right angle triangles. We made use of the property that a Pythagorean triple $P_n(a,b,c)$ and a Platonic triple $P_m(a,b,c)$ when expressed in terms (m,n) can be combined such that $P(a,b,c) = P(m,n)$. A lattice for $P(m,n)$ was given and the condition describing non-co-prime triples, within this lattice, was considered. This work was motivated by its application in cryptography and random number generation algorithms where improved ways of generating prime numbers forms a challenge.

References

[1] B. Berggren. Pytagoreiska trianglar (in Swedish). Tidskrift fo¨r elementa¨r mamematik, fysik och kemi 17: 129–139, 1934.
[2] S. Kak, and M. Prabhu, Cryptographic applications of primitive Pythagorean triples. Cryptologia, 38:215–222, 2014.
[3] R. L. Rivest, Cryptography. In J. Van Leeuwen. Handbook of Theoretical Computer Science. 1. Elsevier, 1990.
[4] Frank R. Bernhart, and H. Lee Price, Pythagoras' garden, revisited, Australian Senior Mathematics, 26(1):29-40, 2012.
[5] E. Maor. The Pythagorean theorem, a 4,000-year history. Princeton University Press. Princeton, New Jersey, 2007.
[6] H. M. Stark, An Introduction to Number Theory. Cambridge, MA: MIT Press, 1994.
[7] W. Sierpinski. Pythagorean triangles, Scripta Mathematica Studies, No. 9, Yeshiva University, New York, 1962.
[8] R. A. Saunders, and T. Randall, The family tree of the Pythagorean triplets revisited, Mathematical Gazette, JSTOR, 78: 190–193, 1994.
[9] J. Rukavicka, Dickson's Method for Generating Pythagorean Triples Revisited, European Journal of Pure and Applied Mathematics ISSN

1307-5543, 6(3): 363-364, 2013.
[10] Euclid. (1908) 1956. The thirteen books of Euclid's Elements. Translated from the text of Heiberg, with introduction and commentary by Sir Thomas L. Heath. Second edition. Three volumes. New York: Dover Publications.
[11] A. Hall. Genealogy of Pythagorean Triads, The Mathematical Gasette, 54(390):377–379, 1970.
[12] T. Roy, and F. J. Soni, A Direct Method To Generate Pythagorean Triples And Its Generalization To Pythagorean Quadruples And n-tuples, arXiv:1201.2145 (math.NT), 1-11, 2012
[13] A. Overmars, and L. Ntogramatzidis, A new parameterisation of Pythagorean triples in terms of odd and even series, Cornell University, arXiv:1504.03163 (math.HO), 1-9, 2015
[14] A. J. Menezes, P. C. van Oorschot, and S. Vanstone, A. Handbook of Applied Cryptography. CRC Press, USA, 1996.
[15] N. Biggs, Codes: An introduction to Information Communication and Cryptography. Springer. p. 171, 2008.
[16] R. L. Rivest, A. Shamir, and L. Adleman, A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM. Association for Computing Machinery. 21 (2): 120–126, 1978.
[17] A. Menezes, P. Van Oorschot, S. Vanstone, Handbook of Applied Cryptography, Boca Raton, FL, CRC Press, Taylor & Franscis Group, 1997.

Anthony Overmars has a background in electrical engineering, robotics, control systems. He has Masters in Engineering and a PhD from Swinburne University of Technology, a Bachelor of Commerce from the University of Melbourne and a Grad Dip Ed from Australian Catholic University.

Anthony founded Softronics which initially developed and manufactured emulators allowing users to develop and debug processing systems, on chip, at the micro code level.

Anthony is a Fellow of the Australian Computer Society (2007). He has been the beneficiary of a number of scholarships (B.Eng and PhD), two ARC grants and various awards including the Pearcey (2006). He has played an active role in research and post-graduate programs at Swinburne University, The University of Melbourne and Latrobe University.

Anthony was previously a Senior Researcher at UoM (NICTA) and is now a lecturer at Melbourne Polytechnic. His areas of interest are Boolean algebra, Number theory and Cryptography.

Sitalakshmi Venkatraman obtained doctoral degree in Computer Science, from National Institute of Industrial Engineering, India in 1993 and MEd from University of Sheffield, UK in 2001. Prior to this, she had completed MSc in Mathematics in 1985 and MTech in Computer Science in 1987, both from Indian Institute of Technology, Madras, India. This author is Member (M) of IAENG, Senior Member (SM) of IASCIT, and on Editorial Board of WASET since 2011.

In the past 30 years, Sita's work experience involves both industry and academics - developing turnkey projects for IT industry and teaching a variety of IT courses for tertiary institutions, in India, Singapore, New Zealand, and more recently in Australia since 2007. She currently works as Lecturer (Information Technology) at Melbourne Polytechnic, Australia. She also serves as Member of Register of Experts at Australia's *Tertiary Education Quality and Standards Agency* (TEQSA).

Sita has published seven book chapters and more than 90 research papers in internationally well-known refereed journals and conferences that include *Information Sciences*, *Journal of Artificial Intelligence in Engineering*, *International Journal of Business Information Systems*, and *Information Management & Computer Security*. She serves as Program Committee Member of several international conferences and Senior Member of professional societies and editorial board of selected international journals.