InPrime: Indonesian Journal of Pure and Applied Mathematics,
Vol. 3, No. 1 (2021), pp. 1 – 6, doi: 10.15408/inprime.v1i2.17922
p-ISSN 2686-5335, e-ISSN: 2716-2478

Some Results on a Generalized Version of Congruent Numbers

Leomarich F. Casinillo[1*] and Emily L. Casinillo[2]
[1,2]Department of Mathematics and Physics
Visayas State University, Visca, Baybay City, Leyte, Philippines
[*]Corresponding e-mail: leomarichcasinillo02011990@gmail.com

Abstract

This paper aims to construct a new formula that generates a generalized version of congruent numbers based on a generalized version of Pythagorean triples. Here, an elliptic curve equation is constructed from the derived generalized version of Pythagorean triples and congruent numbers and gives some new results.

Keywords: Pythagorean triple, congruent number, elliptic curve equation.

Abstrak

Artikel ini bertujuan untuk mengkonstruksi formula baru yang membangun versi yang lebih umum dari bilangan-bilangan kongruen berdasarkan versi triple Pythagoras yang diperumum. Di sini, akan dikonstruksi suatu persamaan kurva eliptik dari triple Pythagoras dan bilangan-bilangan kongruen dalam versi yang diperumum untuk menghasilkan hasil-hasil yang baru.

Kata kunci: *triple Phytagoras, bilangan kongruen, persamaan kurva eliptik.*
2010 Mathematics subject classification: 11A07, 11A41, 11D45, 11G07.

1. INTRODUCTION

A One of the interesting branches of discrete mathematics is number theory, which deals with integers' properties. Most of the number theory topics are easy to understand but hard to provide rigorous mathematical proof. Interesting topics in number theory can be found in [1][2][3][4][5]. One of the classical problems in number theory is found in the mathematical properties of *Pythagorean triples* and *congruent numbers*, which receives much attention to research [6][7][8][9][10]. A Pythagorean triple (X, Y, Z) is a triple of positive integers that satisfies the Diophantine equation $a^2 + b^2 = c^2$. A Pythagorean triple is said to be *primitive* if $\gcd(X, Y, Z) = 1$, and each pair of integers X, Y, and Z are relatively prime, otherwise known as *non-primitive*. For further concepts of a Pythagorean triple, readers may refer to [6][7][8][10]. A positive integer N is a *congruent number* if there exists a right triangle with rational sides so that the area of the triangle is the number N, that is, $N = \frac{1}{2}XY$, where X and Y are sides of the right triangle. The congruent numbers problem has been an interest of many number theorists and associated with the rational fields' elliptic curve concept. The rigorous concepts of congruent numbers and elliptic curves had been studied in [11][12][13][14][15]. This paper aims to construct new results on a generalized version of congruent numbers related to a generalized version of Pythagorean triples based on the paper of Casinillo and Casinillo [8]. A generalized version of Pythagorean triples is a formula that generates primitive and non-primitive Pythagorean triples that depends on two positive integers. However, the formula does not generate some triples that are scalar

Submitted October 27th, 2020, Revised February 28th, 2021, Accepted for publication February 28th, 2021.

multiple of the other triples. Elliptic curve equations are also developed based on a generalized version of congruent numbers and evaluated its solutions. Furthermore, a theorem that determines the congruent numbers with positive integer and rational sides was constructed. This paper will explain the new mathematical concepts of generalized congruent numbers and contribute to the body of literature, specifically in the field of elementary number theory.

2. RESULTS

First, we present the theorem of Casinillo and Casinillo [8] that deals with the new generalized formula that generates primitive and non-primitive Pythagorean triples. The formula is a function of all pairs of positive integers.

Theorem 1. [8] For any positive integers k and n, $(2n^2+2kn,\ 2kn+k^2,\ 2n^2+2kn+k^2)$ *is a* Pythagorean triple. Conversely, for any Pythagorean triple (X,Y,Z), there are positive integers k and n such that $X=2n^2+2kn,\ Y=2kn+k^2$ and $Z=2n^2+2kn+k^2$.

The next theorem is quick from Theorem 1. The theorem shows the formula of generating generalized congruent number N in regards to the generalized version of Pythagorean triples.

Theorem 2. Let $(X(k,n),Y(k,n),Z(k,n))$ be a generalized Pythagorean triple where k and n are positive integers. If N is a generalized congruent number, then $N=2kn^3+3k^2n^2+k^3n$.

Proof. Since $(X(k,n),Y(k,n),Z(k,n))$ is a generalized Pythagorean triple, then the area of a right triangle is $\frac{1}{2}X(k,n)Y(k,n)$. By Theorem 1, it follows that $N=\frac{1}{2}X(k,n)Y(k,n)=\frac{1}{2}(2n^2+2kn)(2kn+k^2)$. Simplifying the right-hand side of the equation, we end up with $N=2kn^3+3k^2n^2+k^3n$ where k and n are positive integers. And this completes the proof. □

The following result shows that the generalized congruent number N is always an even number for all pairs of positive integers k and n.

Corollary 3. If $N(k,n)$ is a generalized congruent number, then $N(k,n)\equiv 0(mod\ 2)$ for all positive integers k and n.

Proof. From Theorem 1, we obtain $N=\frac{1}{2}X(k,n)Y(k,n)$. Now, consider the factor $\frac{1}{2}X(k,n)$. This follows that $\frac{1}{2}X(k,n)=\frac{1}{2}(2n^2+2kn)=n^2+kn$. If n is an even number, then it is easy to check that $n^2+kn\equiv 0(mod\ 2)$ for all positive integer k. Clearly, $N(k,n)\equiv 0(mod\ 2)$. If n is odd and k is even, then $n^2+kn\equiv 1(mod\ 2)$. However, $Y(k,n)=2kn+k^2\equiv 0(mod\ 2)$. Hence, it implies that $N(k,n)\equiv 0(mod\ 2)$. This completes that proof. □

The next theorems shows that a right triangle with an area of congruent number N and sides of generalized Pythagorean triple gives rise to a rational point on an elliptic curve. An area N is related to the generalized Pythagorean triple (X,Y,Z).

Theorem 4. Let $(X(k,n),Y(k,n),Z(k,n))$ be a generalized Pythagorean triple where k and n are positive integers. If N is a generalized congruent number, then the following holds:

i. $y^2 = x^3 - N^2x$ produces a positive integer solution when $k \equiv 0 (mod\ 2)$; and
ii. $y^2 = x^3 - N^2x$ produces rational solutions when $k \equiv 1 (mod\ 2)$ with a denominator greater or equal to 2.

Proof. From the definition of Pythagorean triple and congruent number, we have

$$X^2 + Y^2 = Z^2, \tag{1}$$

and

$$N = \frac{1}{2}XY. \tag{2}$$

Multiplying both sides by 4 in equation (2), we obtain

$$4N = 2XY. \tag{3}$$

Adding equations (1) and (3), clearly follows that

$$X^2 + 2XY + Y^2 = Z^2 + 4N, \tag{4}$$

and

$$(X + Y)^2 = Z^2 + 4N. \tag{5}$$

On the other hand, subtracting equation (3) to equation (1), we have

$$X^2 - 2XY + Y^2 = Z^2 - 4N, \tag{6}$$

And

$$(X - Y)^2 = Z^2 - 4N. \tag{7}$$

Then, we multiply equations (5) and (7), so we obtain

$$(X + Y)^2\,(X - Y)^2 = (Z^2 + 4N)(Z^2 - 4N), \tag{8}$$

By simplifying equation (8), we get

$$(X^2 - Y^2)^2 = Z^4 - 16N^2. \tag{9}$$

Now, we divide equation (9) by 16, and it follows that

$$\left(\frac{X^2-Y^2}{4}\right)^2 = \left(\frac{Z}{2}\right)^4 - N^2. \tag{10}$$

Let $v = \frac{X^2-Y^2}{4}$ and $u = \frac{Z}{2}$. Then, we get

$$v^2 = u^4 - N^2, \tag{11}$$

and multiplying u^2 in equation (11), then we obtain

$$(uv)^2 = u^6 - N^2u^2. \tag{12}$$

Finally, if we let $x = u^2 = \left(\frac{Z}{2}\right)^2$ and $y = uv = \left(\frac{Z}{2}\right)\left(\frac{X^2-Y^2}{4}\right)$, then we end up with

$$y^2 = x^3 - N^2x. \tag{13}$$

By Theorem 1, if $k \equiv 0 (mod\ 2)$, then it follows that 4 divides $(X^2 - Y^2)$ and 2 divides Z, showing that v and u are positive integers. Then, equation (13) produces positive integer solutions. Hence, (i) holds. Again, by Theorem 1, if $k \equiv 1 (mod\ 2)$, then 4 does not divide $(X^2 - Y^2)$ and 2 does not divide Z. This implies that v and u are rational numbers with denominators greater than or equal to 2. Furthermore, equation (13) produces rational solutions with a denominator at least 2 as well. Thus, (ii) holds. And this completes the proof. □

Theorem 5. Let $N, x, y \in \mathbb{Z}^+$. Then, there exists a right triangle with positive integer sides and area N which corresponds to x such that $y^2 = x^3 - N^2x$.

Proof. Let $x = u^2$ with $u \in \mathbb{Z}^+$. We set $v = y/u$ so that $v^2 = \frac{(x^3-N^2x)}{x} = x^2 - N^2$. Hence, it follows that $x^2 = N^2 + v^2$. Then, it is easy to check that (t^2N, t^2v, t^2x) is a Pythagorean triple of integers. By Theorem 1, we get $t^2N = 2n^2 + 2kn,\ t^2v = 2kn + k^2$ and $t^2x = 2n^2 + 2kn + k^2$. Now, we consider the triple $X = \frac{2n}{t}$, $Y = \frac{2n+2k}{t}$ and $Z = 2u$. This follows that $X^2 + Y^2 = \frac{4n^2}{t^2} + \frac{4n^2+8nk+4k^2}{t^2} = \frac{4}{t^2}(2n^2 + 2nk + 4k^2) = \frac{4}{t^2}(t^2x) = 4x = 4u^2 = (2u)^2 = Z^2$. This implies that the right triangle has the sides X, Y and Z. And the area of this right triangle is given by $\frac{1}{2}XY = \frac{1}{2}\left(\frac{2n}{t}\right)\left(\frac{2n+2k}{t}\right) = \frac{1}{2}\left(\frac{4n^2+4kn}{t^2}\right) = \frac{2n^2+2kn}{t^2} = N$, and this completes the proof. □

Next, Theorem 6 below shows how to form a right triangle with rational sides regarding generalized congruent number N.

Theorem 6. Let N be a generalized congruent number. If $N = a^2A$ where a is a positive integer greater than or equal to 2, then A is a congruent number with rational sides, that is, $\left(\frac{X}{a}, \frac{Y}{a}, \frac{Z}{a}\right)$.

Proof. By Theorem 2, we have the congruent number as $N = 2kn^3 + 3k^2n^2 + k^3n$, where k and n are positive integers. Without loss of generality, we let $k = a^2$, where $a \in \mathbb{Z}^+\backslash\{1\}$. Then, it follows that $N = 2(a^2)n^3 + 3(a^2)^2n^2 + (a^2)^3n = a^2(2n^3 + 3a^2n^2 + a^4n) = a^2A$ where $A = 2n^3 + 3a^2n^2 + a^4n \in \mathbb{Z}^+$. By definition of the area of right triangle, we obtain $N = \frac{1}{2}XY = a^2A$. So, we have $A = \frac{1}{2}\left(\frac{XY}{a^2}\right) = \frac{1}{2}\left(\frac{X}{a}\right)\left(\frac{Y}{a}\right)$. Hence, A is a congruent number with rational sides. And this completes the proof. □

Corollary 7 is a quick consequence of Theorem 6 and Wilson's Theorem in [4][5], showing a prime congruent number.

Corollary 7. Let $N = a^2A$ and $\rho(A) = cos^2\left[\pi\frac{(A-1)!+1}{A}\right]$. If $\rho(A) = 1$, then A is a prime congruent number.

It is worth noting that in elementary number theory, a positive integer n is a *square-free* if $\forall$ prime p, p^2 does not divide n [5]. In other words, no prime factor divides it more than once, i.e., the largest power of a prime factor that divides positive integer n is 1. Hence, the following result is immediate from classifying congruent numbers that are square-free and in view of Theorem 6.

Corollary 8. If N is a square-free positive integer, then there is a one-to-one correspondence between generalized Pythagorean triple (X, Y, Z) and generalized congruent number N.

The following results below gives another form of a Pythagorean triple (X, Y, Z) and congruent number *N* that is immediate from Theorem 1 and Theorem 2 above.

Theorem 9. Let (X, Y, Z) be a generalized Pythagorean triple. Then, there exists $x, y \in \mathbb{Z}^+$ such that $X = 2xy$, $Y = x^2 - y^2$ and $Z = x^2 + y^2$ where $x > y$.

Proof. Since (X, Y, Z) is a generalized Pythagorean triple, then by Theorem 1, we have $X = 2n^2 + 2kn$. By factoring the expression, we get $X = 2n(n + k)$. Now, we let $x = n + k$ and $y = n$. This immediately follows that $x > y$ for all pairs of positive integer k and n. This implies that $x + y = 2n + k$ and $x - y = k$. Clearly, by Theorem 1, we have $Y = (x + y)(x - y) = x^2 - y^2 = 2kn + k^2$ and $Z = x^2 + y^2 = (n + k)^2 + n^2 = 2n^2 + 2nk + k^2$, and this completes the proof. □

Corollary 10. For any $x, y \in \mathbb{Z}^+$, $N = x^3y - xy^3$ is a congruent number $\forall\ x > y$.

Proof. Immediate from Theorem 9. □

The next remark is a direct consequence of Theorem 9 and Corollary 10.

Remark 11. For any $x \in \mathbb{Z}^+$, $N = x^3 - x$ is a congruent number that corresponds to the Pythagorean triple $(2x, x^2 - 1, x^2 + 1)$.
In view of Theorem 9, the following result generates a primitive Pythagorean triple and a right triangle that has a pair-wise relatively prime side.

Theorem 12. Let $P = (2xy,\ x^2 - y^2,\ x^2 + y^2)$ be a Pythagorean triple. *If* $x = y + 1$, then P is a primitive Pythagorean triple.

Proof. Note that in Theorem 1, we have $X = 2n^2 + 2kn = 2n(n + k)$. Let $x = n + k$ and $y = n$. Obviously, if $x = y + 1$, then it follows that $k = 1$. By substituting $k = 1$ to generalized Pythagorean triple in Theorem 1, we obtain $X = 2n^2 + 2n$, $Y = 2n + 1$ and $Z = 2n^2 + 2n + 1$. This immediately follows that $\gcd(X, Y, Z) = 1$ and the hypothesis holds. This completes the proof. □

Corollary 13. Let $x, y \in \mathbb{Z}^+$. If $x = y + 1$, then a congruent number $N = x^3y - xy^3$ produces a right triangle with a pair-wise relatively prime side.

Proof. Immediate from Theorem 12. □

3. CONCLUSIONS

In this paper, a new formula for generating congruent numbers was developed in view of the generalized version of Pythagorean triples. It is proven that it is always an even number. The paper had developed new theorems that had shown that there exists a right triangle with positive integer sides and area N given an elliptic curve equation $y^2 = x^3 - N^2x$. A theorem also had been developed, which shows that x and y are positive integers in the elliptic curve $y^2 = x^3 - N^2x$ in view of a generalized version of Pythagorean triples given some conditions. This paper also presented some results that generate a right triangle with rational sides and congruent prime numbers. Finally, some new forms of Pythagorean triples and congruent numbers were constructed regarding the generalized version of Pythagorean triples.

Acknowledgment
The authors would like to thank the referees for the rigorous review and for providing significant comments for the improvement of this paper.

REFERENCES

[1] L. F. Casinillo, "Some New Notes on Mersenne Primes and Perfect Numbers," *Indonesian J. Mathematics Education*, vol. 3, no. 1, pp. 15–22, 2020, doi: 10.31002/ijome.v3i1.2282.

[2] E. L. Casinillo, L. F. Casinillo, J. S. Valenzona, and D. L. Valenzona, "On Triangular Secure Domination Number," *Inprime: Indonesian Journal of Pure Applied Mathematics*, vol. 2, no. 2, pp. 105–110, 2020, doi: 10.15408/inprime.v2i2.15996.

[3] L. F. Casinillo and L. A. Mamolo, "Alternative Formula for the Series of Consecutive m-

Squares under Alternating Signs," *Inprime: Indonesian Journal of Pure Applied Mathematics*, vol. 2, no. 2, pp. 91–96, 2020, doi: 10.15408/inprime.v2i2.15845.

[4] I. Niven, H. S. Zuckerman, and H. L. Montgomery, *An Introduction to the Theory of Numbers*. John Wiley and Sons, Inc. Canada, 1991.

[5] K. H. Rosen, *Elementary Number Theory & Its Applications (3th Edition)*. Addison-Wesley Publishing Company, USA, 1993.

[6] L. E. Dickson, *History of the theory of numbers.* Chelsea Pub. Co., New York, 1971.

[7] D. Vazzana, A., Erickson, M., & Garth, *Introduction to Number Theory (1st ed.)*. Chapman and Hall/CRC, 2007.

[8] L. Casinillo and E. L. Casinillo, "Some Notes on a Generalized Version of Pythagorean Triples," *Jurnal Riset dan Aplikasi Matematika (JRAM)*, vol. 4, no. 2, pp. 103–107, 2020.

[9] J. S. Chahal, "Congruent numbers and elliptic curves," *The American Mathemathical Monthly*, vol. 113, no. 4, pp. 308–317, 2006, doi: 10.2307/27641916.

[10] J. V Leyendekkers and A. Shannon, "The number of primitive Pythagorean triples in a given interval," *Notes Number Theory Discrete Mathematics*, vol. 18, no. 1, pp. 49–57, 2012.

[11] L. Djerassem and D. Tieudjo, "On Congruent Numbers Elliptic Curves," *IOSR Journal of Mathemathics*, vol. 16, no. 3, pp. 1–5, 2020, doi: 10.9790/5728-1603030105.

[12] J. Brown, "Congruent numbers and elliptic curves," 2007, [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.538.9723&rep=rep1&type=pdf.

[13] P. Monsky, "Mock heegner points and congruent numbers," *Mathematische Zeitschrift*, vol. 204, no. 1, pp. 45–67, 1990, doi: 10.1007/BF02570859.

[14] R. Alter, "The Congruent Number Problem," *The American Mathematical Monthly*, vol. 87, no. 1, pp. 43–45, 1980, doi: 10.2307/2320381.

[15] M. Kan, "θ-congruent numbers and elliptic curves," *Acta Arithmetica*, vol. 94, pp. 153–160, 2000.