



---

## Some Formulae for Integer Sums of Two Squares

Lao Hussein Mude <sup>a\*</sup>

<sup>a</sup>Department of Pure and Applied Sciences, Kirinyaga University, P. O. Box 143-10300,  
Kerugoya, Kenya.

### Author's contribution

The sole author designed, analyzed, interpreted and prepared the manuscript.

### Article Information

DOI: 10.9734/JAMCS/2022/v37i430448

### Open Peer Review History:

This journal follows the Advanced Open Peer Review policy. Identity of the Reviewers, Editor(s) and additional Reviewers, peer review comments, different versions of the manuscript, comments of the editors, etc are available here: <https://www.sdiarticle5.com/review-history/87824>

Received: 01 April 2022

Accepted: 06 June 2022

Published: 25 June 2022

**Original Research Article**

---

## Abstract

The study of integer sums of two squares is still an open area of research. Much of the recent work done has put more attention on Fermat Sums of two square theorem with little attention given to new formulas of sums of two Squares. This work is set to partially overcome this knowledge gap by introducing new formulas for generating integer sums of two squares.

*Keywords:* Diophantine equation; sums of two squares.

**2010 Mathematics Subject Classification:** 53C25, 83C05, 57N16.

## 1 Introduction

Finding the relationship between integers and sums of two squares has become an interesting topic in the recent years. The Theory of sums of two squares was first pioneered by Fermat in 1640, where an odd prime  $p$  is expressible as a sum of two squares if and only if  $p \equiv 1 \pmod{4}$ . Euler succeeded in providing proof for Fermat's theorem on sums of two squares in 1749, The proof majorly relies on infinite descent, and was briefly sketched in a letter. The complete proof consists in five steps and was published in two papers. For reference see [1,2]. Since, Euler gave proof to this somewhat marvelous theorem, a number of researchers have provided alternative proof. For survey of this

---

\*Corresponding author: E-mail: hlao@kyu.ac.ke;

results reference can be made to [3,4,1,2]. Though a giant method the Fermat formula does not generate all integer sums of two squares since it is purely defined for an odd prime numbers which is congruent to 1 modulo  $p$ . Another limitation of Fermat Sums of two square theorem is that one has to determine  $p$  before splitting the number into a sum of two square number [5]. This study is set to overcome this challenges by introducing new formulas for integer sums of two squares which has the ability to generate a wide range of integer sums of two squares if not all.

## 2 Preliminary Results

In this section we present some interesting results related to integer sums of two squares

**Theorem 2.1** (Fermat). *An odd prime  $p$  is expressible as  $p = a^2 + b^2$  if and only if  $p \equiv 1 \pmod{4}$  with  $a$  and  $b$  as integers.*

The Brahmagupta Fibonacci identity known also as Diophantus identity expresses the product of two sums of two squares as a sum of two squares in two different ways. i.e

$$(u^2 + v^2)(w^2 + z^2) = (uw - vz)^2 + (uz + vw)^2 = (uw + vz)^2 + (uz - vw)^2$$

## 3 Some Identities of Sums of Two Squares

In the sequel some identities of sums of two squares are presented. In this study all the numbers are assumed to be integers with property that  $c > b > a$  and  $n$  is any non-negative exponent:

**Proposition 3.1.**  $b(a + c) + 2^{2n+1} = (a - 2^n + 2)^2 + (a + 2^n + 2)^2$  has solution in integers if  $a, b, c$  are consecutive integers of the same parity and  $n \geq 1$ .

*Proof.* Suppose  $a, b, c$  are consecutive integers of the same parity. Then,  $b = a + 2, c = a + 4$ . Thus,  $b(a + c) + 2^{2n+1} = (a + 2)(a + a + 4) + 2^{2n+1} = (a + 2)(2a + 4) + 2^{2n+1} = a(2a + 4) + 2(2a + 4) + 2^{2n+1} = 2a^2 + 4a + 4a + 8 + 2^{2n+1} \dots (*)$ .

On the other hand,  $(a - 2^n + 2)^2 + (a + 2^n + 2)^2 = a(a - 2^n + 2) - 2^n(a - 2^n + 2) + 2(a - 2^n + 2) + a(a + 2^n + 2) + 2^n(a + 2^n + 2) + a(a + 2^n + 2) = a^2 - a \cdot 2^n + 2a - a \cdot 2^n + 2^{2n} - 2^{n+1} + 2a - 2^{n+1} + 4 + a^2 + a \cdot 2^n + 2a + a \cdot 2^n + 2^{2n} + 2^{n+1} + 2a + 2^{n+1} + 4 = 2a^2 + 4a + 4a + 8 + 2^{2n+1} \dots (**)$ .

Clearly, (\*) and (\*\*) are equal. Hence  $b(a + c) + 2^{2n+1} = (a - 2^n + 2)^2 + (a + 2^n + 2)^2$ .  $\square$

**Proposition 3.2.**  $b(a + c) + 2^{2n+1} = (b - 2^n)^2 + (b + 2^n)^2$  has solution in integers if  $a, b, c$  are consecutive integers of the same parity.

*Proof.* See proposition 3.1.  $\square$

**Proposition 3.3.**  $b(a + c) + 2^{2n+1} = (c - 2^n - 2)^2 + (c + 2^n - 2)^2$  has solution in integers if  $a, b, c$  are consecutive integers of the same parity.

*Proof.* See proposition 3.1.  $\square$

**Proposition 3.4.**  $a(b + c) + 2^{2(n-1)} + 1 = (a + 1)^2 + (\frac{c+a}{2})^2$  has solution in integers if  $b = a + 2, c = a + 2^n$  and  $n \geq 1$ .

*Proof.* Suppose  $b = a + 2, c = a + 2^n$ . Then,  $a(b + c) + 2^{2(n-1)} + 1 = a(a + 2 + a + 2^n) + 2^{2(n-1)} + 1 = 2a^2 + 2a + a \cdot 2^n + 2^{2(n-1)} + 1 \dots (*)$ .

On the other hand,  $(a + 1)^2 + (\frac{c+a}{2})^2 = a^2 + 2a + 1 + \frac{1}{4}(2a + 2^n)^2 = a^2 + 2a + 1 + \frac{1}{4}(2a(2a + 2^n) + 2^n(2a + 2^n)) = a^2 + 2a + 1 + \frac{1}{4}(4a^2 + a \cdot 2^{n+1} + a \cdot 2^{n+1} + 2^{2n}) = a^2 + 2a + 1 + a^2 + a \cdot 2^{n-1} + a \cdot 2^{n-1} + 2^{2n-2} + 1 = 2a^2 + 2a + a \cdot 2^n + 2^{2n-2} + 1 \dots (**)$ . From (\*) and (\*\*) it is clear that  $a(b + c) + 2^{2(n-1)} + 1 = (a + 1)^2 + (\frac{c+a}{2})^2$ .  $\square$

**Proposition 3.5.**  $a(b+c) + 2^{2(n-1)} + 4 = (a+2)^2 + (\frac{a+c}{2})^2$  has solution in integers if  $b = a+4, c = a+2^n$  and  $n \geq 1$ .

*Proof.* Assume  $b = a+4, c = a+2^n$ . Then,  $a(b+c) + 2^{2(n-1)} + 4 = a(a+4+a+2^n) + 2^{2n-2} + 4$  since  $b = a+4, c = a+2^n$ . Thus,  $a(b+c) + 2^{2(n-1)} + 4 = a(2a+4+2^n) + 2^{2n-2} + 4 = 2a^2 + 4a + a \cdot 2^n + 2^{2n-2} + 4 \dots (*)$ .

On the other hand,  $(a+2)^2 + (\frac{a+c}{2})^2 = (a+2)^2 + (\frac{a+2^n+a}{2})^2 = a^2 + 4a + 4 + \frac{1}{4}(2a+2^n)^2 = a^2 + 4a + 4 + \frac{1}{4}(2a(2a+2^n) + 2^n(2a+2^n)) = a^2 + 4a + 4 + \frac{1}{4}(4a^2 + 2^{n+1} \cdot a + 2^{n+1} \cdot a + 2^{2n}) = a^2 + 4a + 4 + a^2 + 2^{n-1} \cdot a + 2^{n-1} \cdot a + 2^{2n-2} = 2a^2 + 4a + a \cdot 2^n + 2^{2n-2} + 4 \dots (**)$ . Clearly, from (\*) and (\*\*) the equality holds. Hence  $a(b+c) + 2^{2(n-1)} + 4 = (a+2)^2 + (\frac{a+c}{2})^2$ .  $\square$

**Proposition 3.6.**  $a(b+c) + 2^{2(n-1)} + 16 = (\frac{a+b}{2})^2 + (\frac{a+c}{2})^2$  has solution in integers if  $b = a+8, c = a+2^n$  and  $n \geq 1$ .

*Proof.* Suppose  $b = a+8, c = a+2^n$ . Then,  $a(b+c) + 2^{2(n-1)} + 16 = a(a+8+a+2^n) + 2^{2n-2} + 16 = 2a^2 + 8a + a \cdot 2^n + 2^{2n-2} + 16 \dots (*)$ .

On the other hand,  $(\frac{a+b}{2})^2 + (\frac{a+c}{2})^2 = \frac{1}{4}(a+c)^2 + \frac{1}{4}(a+b)^2 = \frac{1}{4}(a+a+2^n)^2 + \frac{1}{4}(a+a+8)^2 = \frac{1}{4}(2a+2^n)^2 + \frac{1}{4}(2a+8)^2 = \frac{1}{4}(2a(2a+2^n) + 2^n(2a+2^n)) + \frac{1}{4}(2a(2a+8) + 8(2a+8)) = \frac{1}{4}(4a^2 + a \cdot 2^{n+1} + a \cdot 2^{n+1} + 2^{2n}) + \frac{1}{4}(4a^2 + 16a + 16a + 64) = \frac{1}{4}(4a^2 + a \cdot 2^{n+2} + 2^{2n}) + \frac{1}{4}(4a^2 + 32a + 64) = a^2 + a \cdot 2^n + 2^{2n-2} + a^2 + 8a + 16 = 2a^2 + 8a + a \cdot 2^n + 2^{2n-2} + 16 \dots (**)$ . From (\*) and (\*\*) it is clear that  $a(b+c) + 2^{2(n-1)} + 16 = (\frac{a+b}{2})^2 + (\frac{a+c}{2})^2$ .  $\square$

**Proposition 3.7.**  $a(b+c) + 2^{2(n-1)} + 64 = (\frac{a+b}{2})^2 + (\frac{a+c}{2})^2$  has solution in integers if  $b = a+16, c = a+2^n$  and  $n \geq 1$ .

*Proof.* Suppose  $b = a+16, c = a+2^n$ . Then,  $a(b+c) + 2^{2(n-1)} + 64 = a(a+16+a+2^n) + 2^{2n-2} + 64 = a(2a+16+2^n) + 2^{2n-2} + 64 = 2a^2 + 16a + a \cdot 2^n + 2^{2n-2} + 64 \dots (*)$ .

On the other hand  $(\frac{a+b}{2})^2 + (\frac{a+c}{2})^2 = \frac{1}{4}(a+b)^2 + \frac{1}{4}(a+c)^2 = \frac{1}{4}(a+a+16)^2 + \frac{1}{4}(a+a+2^n)^2 = \frac{1}{4}(2a+16)^2 + \frac{1}{4}(2a+2^n)^2 = \frac{1}{4}(2a(2a+16) + 16(2a+16)) + \frac{1}{4}(2a(2a+2^n) + 2^n(2a+2^n)) = \frac{1}{4}(4a^2 + 32a + 32a + 256) + \frac{1}{4}(4a^2 + a \cdot 2^{n+1} + 2^{2n}) = a^2 + 8a + 8a + 64 + a^2 + a \cdot 2^n + 2^{2n-2} = 2a^2 + 16a + a \cdot 2^n + 2^{2n-2} + 64 \dots (**)$ . From (\*) and (\*\*) we have  $a(b+c) + 2^{2(n-1)} + 64 = (\frac{a+b}{2})^2 + (\frac{a+c}{2})^2$ .  $\square$

**Proposition 3.8.**  $a(b+c) + 2^{2(n-1)} + 256 = (\frac{a+b}{2})^2 + (\frac{a+c}{2})^2$  has solution in integers if  $b = a+32, c = a+2^n$  and  $n \geq 1$ .

*Proof.* Assume  $b = a+32, c = a+2^n$ . Then,  $a(b+c) + 2^{2(n-1)} + 256 = a(a+32+a+2^n) + 2^{2n-2} + 256 = a(2a+32+2^n) + 2^{2n-2} + 256 = 2a^2 + 32a + a \cdot 2^n + 2^{2n-2} + 256 \dots (*)$ .

On the other hand,  $(\frac{a+b}{2})^2 + (\frac{a+c}{2})^2 = \frac{1}{4}(a+b)^2 + \frac{1}{4}(a+c)^2 = \frac{1}{4}(a+a+32)^2 + \frac{1}{4}(a+a+2^n)^2 = \frac{1}{4}(2a+32)^2 + \frac{1}{4}(2a+2^n)^2 = \frac{1}{4}(2a(2a+32) + 32(2a+32)) + \frac{1}{4}(2a(2a+2^n) + 2^n(2a+2^n)) = \frac{1}{4}(4a^2 + 64a + 64a + 32^2) + \frac{1}{4}(4a^2 + a \cdot 2^{n+1} + a \cdot 2^{n+1} + 2^{2n}) = \frac{1}{4}(4a^2 + 128a + 32^2) + \frac{1}{4}(4a^2 + a \cdot 2^{n+2} + 2^{2n}) = a^2 + 32a + 256 + a^2 + a \cdot 2^n + 2^{2n-2} = 2a^2 + 32a + a \cdot 2^n + 2^{2n-2} \dots (**)$ . From (\*) and (\*\*) it follows that  $a(b+c) + 2^{2(n-1)} + 256 = (\frac{a+b}{2})^2 + (\frac{a+c}{2})^2$ .  $\square$

**Proposition 3.9.**  $a(b+c) + 2^{2n-1} = (\frac{a+b}{2})^2 + (\frac{a+c}{2})^2 = (\frac{a+b}{2})^2 + (\frac{a+b}{2})^2 = (\frac{a+c}{2})^2 + (\frac{a+c}{2})^2$  has solution in integers if  $b = a+2^n, c = a+2^n$  and  $n \geq 1$ .

*Proof.* Suppose  $b = a+2^n, c = a+2^n$ . Then,  $a(b+c) + 2^{2n-1} = a(a+2^n+a+2^n) + 2^{2n-1} = 2a^2 + a \cdot 2^{n+1} + a \cdot 2^{2n-1} \dots (*)$ .

On the other hand,  $(\frac{a+b}{2})^2 + (\frac{a+c}{2})^2 = \frac{1}{4}(a+b)^2 + \frac{1}{4}(a+c)^2 = \frac{1}{4}(a+a+2^n)^2 + \frac{1}{4}(a+a+2^n)^2 = \frac{1}{4}(2a+2^n)^2 + \frac{1}{4}(2a+2^n)^2 = \frac{1}{4}(2a(2a+2^n) + 2^n(2a+2^n)) + \frac{1}{4}(2a(2a+2^n) + 2^n(2a+2^n)) = \frac{1}{4}(4a^2 + a \cdot 2^{n+1} + a \cdot 2^{n+1} + 2^{2n}) + \frac{1}{4}(4a^2 + a \cdot 2^{n+1} + a \cdot 2^{n+1} + 2^{2n}) = \frac{1}{2}(4a^2 + a \cdot 2^{n+1} + a \cdot 2^{n+1} + 2^{2n}) = 2a^2 + a \cdot 2^{n+1} + 2^{2n-1} \dots (**)$ . From (\*) and (\*\*) it can be seen that  $a(b+c) + 2^{2n-1} = (\frac{a+b}{2})^2 + (\frac{a+c}{2})^2 = (\frac{a+b}{2})^2 + (\frac{a+b}{2})^2 = (\frac{a+c}{2})^2 + (\frac{a+c}{2})^2$ .  $\square$

**Proposition 3.10.** *Let  $a$  be any positive even integers and the exponent  $n$  be any non negative integer with zero included. Then  $2^n .a^a + 2^n = u^2 + v^2$ .*

*Proof. Case(i) when  $n = 0$ .  $2^0 .a^a + 2^0 = a^a + 1$ . Let  $a = 2m$ . Then  $a^a + 1 = 2m^{2m} + 1 = (4m^2)^m + 1$ . Let  $m^2 = k$  so that  $(4m^2)^m + 1 = (4k)^m + 1$ . Setting  $k = 1$  we have  $4^m + 1$ . Let  $R = \{4^m + 1 : k \in \mathbb{Z}^+\}$  and  $S = \{p \equiv 1 \pmod{4} \text{ where } p \text{ is an odd prime}\}$ . Clearly  $R \subseteq S$  and by fermat theorem of sums of two squares, the result easily follows.  $\square$*

*Proof. Case(ii) when  $n = 2k$ .  $2^{2k} .a^{2m} + 2^{2k} = (2^k .a^m)^2 + (2^k)^2$ . Let  $u = 2^k a^m$  and  $v = 2^m$ . So that  $2^n .a^a + 2^n = u^2 + v^2$ .  $\square$*

*Proof. Case(iii) when  $n = 2k+1$ .  $2^{2k+1} .a^{2m} + 2^{2k+1} = 2.(2^k .a^m)^2 + 2.(2^k)^2 = 2.((2^k .a^m)^2 + (2^k)^2)$ . Let  $u = 2^k a^m$  and  $v = 2^m$ . So that  $2^n .a^a + 2^n = 2.(u^2 + v^2) = (1^2 + 1^2).(u^2 + v^2)$  and by the identity  $(x^2 + y^2)(u^2 + v^2) = (xu + yv)^2 + (xv - yu)^2$  the proof follows.  $\square$*

**Proposition 3.11.** *Let  $p$  and  $x$  be any positive integers and  $n$  be any non negative exponent. Suppose that  $p \equiv 1 \pmod{b^2}$  where  $b$  is an non negative even integer. Then  $px^n - x^n = z^2$ . Moreover,  $z^2 = u^2 + v^2$  is a sum of two squares where  $u$  and  $v$  are integers.*

*Proof.* We want to show that  $px^n - x^n = z^2 = u^2 + v^2$ . If  $p \equiv 1 \pmod{b^2}$  then  $p = b^2 + 1$ . Put  $b = 2m$  so that  $p = 2m^{2m} + 1$ . Proving from L.H.S we have  $px^n - x^n = (2m^{2m} + 1).x^n - x^n = 2m^{2m}.x^n + x^n - x^n = 2m^{2m}.x^n$ . Set  $n = 2k$  to get  $px^n - x^n = 2m^{2m}.x^{2k} = (2^m .m^m)^2 (x^k)^2 = (2^m .m^m .x^k)^2$ . Set  $z = (2^m .m^m .x^k)$  proving the first part of the equation. To show that  $(2^m .m^m .x^k)^2$  is a sum of two squares, Let  $z = (2^m .m^m .x^k)$  and set  $m = 1$ . This means that  $z = (2.x^k) = (1+1).x^k = x^k + x^k$ . Assume  $k = 2t$ ,  $x^k + x^k = (x^t)^2 + (x^t)^2 = u^2 + v^2$  as desired. Thus  $px^n - x^n = z^2 = u^2 + v^2$ .  $\square$

**Conjecture 3.1.**  $a(b + c) + L = u^2 + v^2$  has no general solution in integers if  $a, b$  and  $c$  is not related.

## 4 Conclusion

This study has introduced some new formulas for integer sums of two squares. Up to now, much of the research done in this area is very scanty and we encourage other researchers to give more attention to this particular area of research. For instance there is very little information on the general formula for generating integer sums of two squares since not every multiple of sums of two squares with any number is a sum of two squares.

## Competing Interests

Author has declared no competing interest.

## References

- [1] Théry L. Numbers Equal to the Sum of Two Square Numbers. Formalizing 100 theorems in Coq; 2004.  
Available: <https://github.com/coq-contribs/sum-of-two-square>, accessed 22 August,2021.
- [2] Stillwell J. Mathematics and its history (2nd ed.), Springer, 2002;72–76.  
ISBN 978-0-387-95336-6

- [3] David A. A partition-theoretic proof of Fermat's Two Squares Theorem. Discrete Mathematics. 2016;339:4:1410–1411.  
DOI:10.1016/j.disc.2015.12.002
- [4] Heath-Brown D. A one-sentence proof that every prime  $p \equiv 1 \pmod{4}$  is a sum of two squares., Amer. Math. 1990;2:144.  
DOI:10.2307/2323918.
- [5] Zagier D. A one-sentence proof that every prime  $p \equiv 1 \pmod{4}$  is a sum of two squares, Amer. Math. Monthly. 1990;97:144. Mathematical Institute, 24–29, St. Giles', Oxford OX1 3LB UK  
rhb@.

---

© 2022 Mude; This is an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0>), which permits unrestricted use, distribution and reproduction in any medium, provided the original work is properly cited.

**Peer-review history:**

The peer review history for this paper can be accessed here (Please copy paste the total link in your browser address bar)

<https://www.sdiarticle5.com/review-history/87824>