Advances in Pure Mathematics, 2024, 14, 283-302
https://www.scirp.org/journal/apm
ISSN Online: 2160-0384
ISSN Print: 2160-0368

A New Proof for Congruent Number's Problem via Pythagorician Divisors

Léopold Dèkpassi Keuméan, François Emmanuel Tanoé

UFR Mathematics and Computer Science, Félix Houphouët Boigny University, Abidjan, Cote d'Ivoire
Email: dekpassileo@gmail.com; aziz_marie@yahoo.fr

How to cite this paper: Keuméan, L.D. and Tanoé, F.E. (2024) A New Proof for Congruent Number's Problem via Pythagorician Divisors. *Advances in Pure Mathematics*, **14**, 283-302.
https://doi.org/10.4236/apm.2024.144016

Received: February 7, 2024
Accepted: April 26, 2024
Published: April 29, 2024

Copyright © 2024 by author(s) and Scientific Research Publishing Inc.
This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).
http://creativecommons.org/licenses/by/4.0/
Open Access

Abstract

Considering Pythagorician divisors theory which leads to a new parameterization, for Pythagorician triplets $(a,b,c)\in\mathbb{N}^{3*}$, we give a new proof of the well-known problem of these particular squareless numbers $n\in\mathbb{N}^*$, called congruent numbers, characterized by the fact that there exists a right-angled triangle with rational sides: $\left(\frac{A}{\alpha}\right)^2+\left(\frac{B}{\beta}\right)^2=\left(\frac{C}{\gamma}\right)^2$, such that its area $\Delta=\frac{1}{2}\frac{A}{\alpha}\frac{B}{\beta}=n$; or in an equivalent way, to that of the existence of numbers $U^2,V^2,W^2\in\mathbb{Q}^{2*}$ that are in an arithmetic progression of reason *n*; Problem equivalent to the existence of: $(a,b,c)\in\mathbb{N}^{3*}$ prime in pairs, and $f\in\mathbb{N}^*$, such that: $\left(\frac{a-b}{2f}\right)^2$, $\left(\frac{c}{2f}\right)^2$, $\left(\frac{a+b}{2f}\right)^2$ are in an arithmetic progression of reason n; And this problem is also equivalent to that of the existence of a non-trivial primitive integer right-angled triangle: $a^2+b^2=c^2$, such that its area $\Delta=\frac{1}{2}ab=nf^2$, where $f\in\mathbb{N}^*$, and this last equation can be written as follows, when using Pythagorician divisors:

(1) $\Delta=\frac{1}{2}ab=2^{S-1}d\overline{e}\left(d+2^{S-1}\overline{e}\right)\left(d+2^S\overline{e}\right)=nf^2$;

Where $(d,\overline{e})\in(2\mathbb{N}+1)^2$ such that $gcd(d,\overline{e})=1$ and $S\in\mathbb{N}^*$, where 2^{S-1}, *d*, $\overline{e}$, $d+2^{S-1}\overline{e}$, $d+2^S\overline{e}$, are pairwise prime quantities (these parameters are coming from Pythagorician divisors). When $n=1$, it is the case of the famous impossible problem of the integer right-angled triangle area to be a square, solved by Fermat at his time, by his famous method of infinite descent. We propose in this article a new direct proof for the numbers $n=1$ (resp. $n=2$) to be non-congruent numbers, based on an particular induction method of resolution of Equation (1) (note that this method is efficient too for general

case of prime numbers $n = p \equiv a$ ($(\bmod 8)$, $gcd(a,8)=1$). To prove it, we use a classical proof by induction on k, that shows the non-solvability property of any of the following systems ($t=0$, corresponding to case $n=1$ (resp. $t=1$, corresponding to case $n=2$)): $(\Xi_{t,k})\begin{cases} X^2+2^t\left(2^kY\right)^2=Z^2 \\ X^2+2^{t+1}\left(2^kY\right)^2=T^2 \end{cases}$, where $k\in\mathbb{N}$; and solutions $(X,Y,Z,T)=(D_k,E_k,f_k,f'_k)\in(2\mathbb{N}+1)^4$, are given in pairwise prime numbers.

2020-Mathematics Subject Classification

11A05-11A07-11A41-11A51-11D09-11D25-11D41-11D72-11D79-11E25

Keywords

Prime Numbers-Diophantine Equations of Degree 2 & 4, Factorization, Greater Common Divisor, Pythagoras Equation, Pythagorician Triplets, Congruent Numbers, Inductive Demonstration Method, Infinite Descent, BSD Conjecture

1. Introduction

From a historical point of view, the search of square-free integers n called congruent numbers, whose problem statement is remarkably simple and dates from antiquity cf. [1] [2] [3] [4], see also: [5] [6] [7], remains to this day the last ancient mathematical problem bequeathed from antiquity and which is not entirely solved at this time day, despite the efforts and diligent work of mathematicians cf. [8] [9] [10] [11] p. 556, [12].

There is therefore a real global challenge to fully resolve this problem which is the subject of numerous contemporary publications.

In this article, to characterize the fact that an integer n is congruent, we will use a new method, using the notion of Pythagorician divisors (cf. § 2.6 & 2.7 and [13] [14]), and from there, deduce a new Diophantine proof of the problem of Diophantus's twentieth problem, also known as Fermat's right triangle theorem, which he himself had solved by his famous method of infinite descent.

Reminders and Notations

Let's remind and fix some notations cf. §2.6 & 2.7., especially in Definition 2.2. & 2.3., and Theorem 2.5, for the notion of Pythagorician divisors d and e.

Reminders 1.1 1) $\overline{T^+}$ *is the set of triplets* $(a,b,c)\in\left(\mathbb{N}^*\right)^3$, *solutions of Pythagoras equation:* $a^2+b^2=c^2$; *such that* a,b,c *are coprime in pairs, and* $(a,b=2^sb_1,c)\equiv(\pm1,0,1)(\bmod 4)$ *with* $b_1\equiv 1(\bmod 2)$.

2) Consider $(a,b=2^sb_1,c)\in\overline{T^+}$, we put $\lambda\in\{0,1\}$ such that:

$\frac{c-a}{2}\equiv\lambda(\bmod 2)$, and $S\in\mathbb{N}^*$, such that: $S=s-\lambda(s-1)$, from there we define:

- $\left(d, d''\right) = \left(gcd\left(a, c-b\right), \frac{a}{d}\right), and$

  $\left(e, e''\right) = \left(gcd\left(b, c-a\right), \frac{b}{e}\right) = \left(2^S \overline{e}, 2^{s-S} \frac{b_1}{\overline{e}}\right)$ where $\overline{e} \in 2\mathbb{N}+1$.

- $\begin{cases} a = d^2 + \left(2^S \overline{e}\right) d \\ b = \frac{\left(2^S \overline{e}\right)^2}{2} + \left(2^S \overline{e}\right) d \\ c = \frac{\left(2^S \overline{e}\right)^2}{2} + \left(2^S \overline{e}\right) d + d^2 \end{cases}$; and thus

  $\Delta = \frac{1}{2} ab = 2^{S-1} d\overline{e}\left(d + 2^{S-1}\overline{e}\right)\left(d + 2^S \overline{e}\right)$.

One remark that for such triplet $\left(a, b = 2^s b_1, c\right)$, there is a unique parametrization $\left(d, \overline{e}, S\right)$.

3) $\left(2\mathbb{N}+1\right) \underset{cop}{\times} \left(2\mathbb{N}+1\right) = \left\{\left(x, y\right) \in \left(2\mathbb{N}+1\right)^2 / gcd\left(x, y\right) = 1\right\}$.

Let's comme back to our problem, note that from Definition 2.1., a square-free natural number $n \neq 0$, is said to be congruent if and only if there exists a rational number V such that: $V^2 + n$ and $V^2 - n$ are simultaneously rational squares.

This Definition is equivalent (cf. Proposition 2.1.) to say that there is a right-angled triangle with rational sides, whose area is equal to *n*. This means (cf. Theorem 2.1.) that there exists a Pythagorician triplet of $\overline{T^+}$, whose area is equal to n times an integer squared, and in finality, taking account the Pythagorician parameterization (cf. Theorem 2.5.(iv)), we get:

n is congruent $\Leftrightarrow \exists\left(d, \overline{e}, S\right)$ where $\left(d, \overline{e}\right) \in \left(2\mathbb{N}+1\right) \underset{cop}{\times} \left(2\mathbb{N}+1\right)$, and

$S \in \mathbb{N}^*$ such that:

$$\Delta = 2^{S-1} d\overline{e}\left(d + 2^{S-1}\overline{e}\right)\left(d + 2^S \overline{e}\right) = nf^2. \tag{1.1}$$

Where the quantities: $2^{S-1}, d, \overline{e}, d + 2^{S-1}\overline{e}$ and $d + 2^S \overline{e}$ are pairwise prime.

It is therefore this Diophantine equation that we will use, to show that numbers 1 and 2 are not congruents.

We are now going to solve equation (1.1) for $n = 1$ and $n = 2$, provided that Lemmas 2.2 are true, with respect of definitions and theorems (including that of Pythagorician divisors and some other results), recalled in §2.6 & 2.7, and demonstrated in [14].

2. New Diophantine Proof of Fermat's Right-Angled Triangle Theorem

2.1. Some Definitions and Properties towards Congruent Numbers

Definition 2.1 *Let n be a positive integer, we say that n is a congruent number if there exists a rational number V such that* $V^2 - n$ *and* $V^2 + n$ *are simultaneously rational squares.*

See the examples below for concrete cases.

Proposition 2.1 *Let* $n \in \mathbb{N}^*$, *a square-free natural integer. There is equivalence between the following propositions:*

(i) n is congruent.

(ii) $\exists U, V, W \in \mathbb{Q}^*$ such that: $\begin{cases} U^2 + n = V^2; \\ V^2 + n = W^2. \end{cases}$

(iii) $\exists E, F, G \in \mathbb{Q}^*$ such that: $\begin{cases} E^2 + F^2 = G^2; \\ \frac{1}{2}EF = n. \end{cases}$

Proof 1 *From Definition* 2.1., *it is clear that* (i) $\Leftrightarrow$ (ii).

Let us show that (ii) $\Leftrightarrow$ (iii).

- If (ii) holds, then (iii) holds too with $\begin{cases} E = W - U; \\ F = W + U; \\ G = 2V. \end{cases}$
- Conversely if (iii) holds, then (ii) holds too, with $\begin{cases} U = \frac{F - E}{2}; \\ V = \frac{G}{2}; \\ W = \frac{F + E}{2}. \end{cases}$

Concerning equation (iii), we have the following additioning precisions:

Lemma 2.1 *Let* $n \in \mathbb{N}^*$, *a square-free natural integer, which is a congruent number, i.e. such that there exists* $\left(\frac{A}{\alpha}, \frac{B}{\beta}, \frac{C}{\gamma}\right)$ *a rational triplet, with* $\frac{A}{\alpha}, \frac{B}{\beta}, \frac{C}{\gamma}$ *irreducibles such that:* $\begin{cases} \left(\frac{A}{\alpha}\right)^2 + \left(\frac{B}{\beta}\right)^2 = \left(\frac{C}{\gamma}\right)^2; \\ \frac{1}{2}\frac{A}{\alpha}\frac{B}{\beta} = n. \end{cases}$

Then $D = gcd(A, B) = 1$ and $\delta = gcd(\alpha, \beta) = 1$.

Proof 2 *Note that we have:* $\frac{1}{2}\frac{A}{\alpha}\frac{B}{\beta} = n$, *from which we deduce that:* $(A\beta)(B\alpha) = 2n(\alpha\beta)^2$.

- Let us show first that $D = pgcd(A, B) \neq 2$:

Suppose that the converse holds: $D = gcd(A, B) = 2$:

Then α and β are odd because $\frac{A}{\alpha}$ and $\frac{B}{\beta}$ are irreducibles.

Moreover note that γ is odd too, because $C = 2C'$ is even (with C' odd), because otherwise we would have: $(A\beta\gamma)^2 + (B\alpha\gamma)^2 = (C\alpha\beta)^2$ odd, with $A\beta\gamma, B\alpha\gamma$ even, which is absurd. So as a consequence C is even and necessary γ is odd.

Consequently we have:

$$(A\beta\gamma)^2 + (B\alpha\gamma)^2 = 4(C'\alpha\beta)^2 \Leftrightarrow \left(\frac{A}{2}\beta\gamma\right)^2 + \left(\frac{B}{2}\alpha\gamma\right)^2 = (C'\alpha\beta)^2.$$

But then: $\gamma \mathbin{/} C'\alpha\beta \Rightarrow \left(\frac{A}{2}\beta\right)^2 + \left(\frac{B}{2}\alpha\right)^2 = \left(\frac{C'\alpha\beta}{\gamma}\right)^2$.

Note that $\frac{A}{2}$ and $\frac{B}{2}$ can't be both even, because $gcd(A,B)=2$, and that also $\frac{A}{2}$ and $\frac{B}{2}$ can't be both odd, because if it was the case, we would have $2 \equiv 0 \bmod 4$. Which is absurd.

So looking to the left side, as exactly one term between $\frac{A}{2}$ and $\frac{B}{2}$ is even, then in particular C' is odd.

But this would be contradictory since:
$\frac{1}{2}\frac{A}{\alpha}\frac{B}{\beta} = n \Rightarrow \frac{1}{2}AB = n\alpha\beta \Rightarrow 2\frac{A}{2}\frac{B}{2} = n\alpha\beta = 2n'\alpha\beta$, where $n = 2n'$, and n' odd without square factors.

But then $\frac{A}{2}\frac{B}{2} = n'\alpha\beta$ remains odd $\Rightarrow \frac{A}{2}$ and $\frac{B}{2}$ are both odd, which contradicts the previous fact that exactly one between $\frac{A}{2}$ and $\frac{B}{2}$ is necessarily even.

So necessarily $D = gcd(A,B) \neq 2$.

- So D is odd. Suppose that $D \neq 1$, then from $(A\beta)(B\alpha) = 2n(\alpha\beta)^2$ it comes $D^2 / 2n(\alpha\beta)^2$.

But as $gcd(D,\alpha\beta)=1 \Rightarrow D^2/2n \Rightarrow D^2/n$ which is absurd, because n is square free.

In conclusion: $D = gcd(A,B) = 1$.

Otherwise:

$$D^2\left(\frac{A}{d}\right)\left(\frac{B}{d}\right) = 2\delta^2\left(\frac{\alpha}{\delta}\right)\left(\frac{\beta}{\delta}\right)n \Rightarrow AB = 2\delta^2\left(\frac{\alpha}{\delta}\right)\left(\frac{\beta}{\delta}\right)n \Rightarrow \delta/AB \Rightarrow \delta = 1.$$

Because $pgcd(\delta, AB) = 1$.

We deduce the following theorem:

Theorem 2.1 *Let* $n \in \mathbb{N}^{\star}$ *a square-free natural integer, there is equivalence between the following propositions:*

(i) n is a congruent number.

(ii) There exists $f \in \mathbb{N}^*$ and $(a,b,c) \in \overline{T^+}$ (cf. Definition 2.2.), whose area $\Delta = \frac{1}{2}ab = nf^2$.

(iii) There exists $f \in \mathbb{N}^*$ and $(a,b,c) \in \mathbb{N}^*$ prime in pairs, such that:

$$\begin{cases} \left(\frac{a-b}{2f}\right)^2 + n = \left(\frac{c}{2f}\right)^2; \\ \left(\frac{c}{2f}\right)^2 + n = \left(\frac{a+b}{2f}\right)^2. \end{cases}$$

(i.e. $\left(\frac{a-b}{2f}\right)^2, \left(\frac{c}{2f}\right)^2, \left(\frac{a+b}{2f}\right)^2$ are in an arithmetic progression of reason n).

Proof 3

- *Let's show that* (i) $\Rightarrow$ (ii). *i.e. Assume n is congruent number; then there exists* $\left(\frac{A}{\alpha},\frac{B}{\beta},\frac{C}{\gamma}\right)$ *a triple, as in Lemma 2.1., such that:*

$$\begin{cases}\left(\frac{A}{\alpha}\right)^2+\left(\frac{B}{\beta}\right)^2=\left(\frac{C}{\gamma}\right)^2;\\ \frac{1}{2}\frac{A}{\alpha}\frac{B}{\beta}=n.\end{cases}$$

Let $f'=\alpha\beta\gamma$, and multiply the two equations by f'^2, we obtain:

$$\begin{cases}(\beta\gamma A)^2+(\alpha\gamma B)^2=(\alpha\beta C)^2;\\ \frac{1}{2}\alpha\beta\gamma^2 AB=n(\alpha\beta\gamma)^2.\end{cases}\Rightarrow\begin{cases}(\beta\gamma A)^2+(\alpha\gamma B)^2=(\alpha\beta C)^2;\\ \frac{1}{2}(\beta\gamma A)(\alpha\gamma B)=nf'^2.\end{cases}$$

By setting $a'=\beta\gamma A; b'=\alpha\gamma B$ and $c'=\alpha\beta C$, we have:

$$\begin{cases}a'^2+b'^2=c'^2;\\ \frac{1}{2}a'b'=nf'^2.\end{cases}$$

Let $gcd(a',b',c')=D'$, and simply take $(a,b,c)=\left(\frac{a'}{D'},\frac{b'}{D'},\frac{c'}{D'}\right)\in\overline{T^+}$, and $f=\frac{f'}{D'}$, then the condition (ii) of the Theorem is demonstrated.

- Let's show that (ii) $\Rightarrow$ (iii). Assume (ii) realized, i.e. $a^2+b^2=c^2$, and $\frac{1}{2}ab=nf^2$, with a,b,c prime in pair, then:

$$\begin{cases}\left(\frac{a-b}{2f}\right)^2+n=\frac{a^2+b^2-2ab+4f^2n}{4f^2}=\left(\frac{c}{2f}\right)^2;\\ \left(\frac{c}{2f}\right)^2+n=\frac{a^2+b^2+4f^2n}{4f^2}=\frac{a^2+b^2+2ab}{4f^2}=\left(\frac{a+b}{2f}\right)^2.\end{cases}$$ i.e. (iii) is checked.

- Let's show that (iii) $\Rightarrow$ (i).

If (iii) holds, then Proposition 2.1., (ii) holds too:

With $U=\frac{a-b}{2f},V=\frac{c}{2f}$ and $W=\frac{a+b}{2f}$; so point (i) of Theorem is true because point (i) of the Proposition 2.1., is true.

In particular, as reminded in the introduction, we obtain formula (1.1), by applying Theorem 2.1., and taking into account the Pythagorician parameterization Theorem 2.5., and thus:

n is congruent $\Leftrightarrow\exists(d,\overline{e},S)$ where $(d,\overline{e})\in 2\mathbb{N}+1\underset{cop}{\times}2\mathbb{N}+1$, $S\in\mathbb{N}^*$ such that:

$$\Delta=2^{S-1}d\overline{e}\left(d+2^{S-1}\overline{e}\right)\left(d+2^S\overline{e}\right)=nf^2.$$

However, for a given *n*, we do not know (in general) if such a rational triplet exists, and if we do know it, we do not know from which primitive integer Pythagorician triplet it comes.

Exemples 2.1

- *Let us now consider these primitive integer Pythagorean triples as they vary and calculate the areas of the integer right-angled triangles* $a^2+b^2=c^2$ *such that* $\Delta=\frac{1}{2}ab=nf^2$ *where n is a squareless integer, which means that: n is a congruent number:*

We therefore see that the number 5 is congruent: Indeed very quickly, we obtain:

$9^2+40^2=41^2$ with: $\frac{1}{2}\times 9\times 40=180=5\times 6^2$.

In this example, the first right-angled integer triplet whose area is $5\times f^2$, is quite close in the list, and the corresponding rational right-angled triangle is:

$\left(\frac{3}{2}\right)^2+\left(\frac{20}{3}\right)^2=\left(\frac{41}{6}\right)^2$, with: $\frac{1}{2}\times\frac{3}{2}\times\frac{20}{3}=5$.

Compared to the Pythagoras equation with integer solutions: $9^2+40^2=41^2$, One find that

The squares $\left(\left(\frac{b-a}{2}\right)^2,\left(\frac{c}{2}\right)^2,\left(\frac{b+a}{2}\right)^2\right)=\left(\left(\frac{31}{2}\right)^2,\left(\frac{49}{2}\right)^2,\left(\frac{41}{2}\right)^2\right)$, are in arithmetic progression of reason 180, We deduce from that with respect to the following Pythagorician rational equation: $\left(\frac{3}{2}\right)^2+\left(\frac{20}{3}\right)^2=\left(\frac{41}{6}\right)^2$, that the squares $\left(\frac{31}{12}\right)^2;\left(\frac{49}{12}\right)^2$ and $\left(\frac{41}{12}\right)^2$, are in arithmetic progression with reason $5=\frac{180}{36}$.

- There are, however, complicated cases, because, although existing, the primitive right triangles we are looking for could be very far down the list: As a specific example, the number 23 turns out to be a congruent one:

And we find a primitive integer right-angled triangle (a,b,c) checking: $\frac{1}{2}ab=23f^2$ with $f\in\mathbb{N}^*$.

But this time, this one is far down the list. Indeed, we find:

$279340175^2+860959008^2=905141617^2$; with $\Delta_1=\frac{1}{2}ab=23\times 72306780^2$.

And the corresponding rational right-angled triangle is:

$\left(\frac{80155}{20748}\right)^2+\left(\frac{41496}{3485}\right)^2=\left(\frac{905141617}{72306780}\right)^2$, with: $\Delta_2=\frac{1}{2}\times\frac{80155}{20748}\times\frac{41496}{3485}=23$.

Which is also a caracterization cf. Proposition 2.1. (iii), so that 23 is congruent.

Thus (cf. Definition 2.1. & Theorem 2.1., (iii)) the squares in arithmetic progression of reason 23, are:

$$\left(\left(\frac{b-a}{2f}\right)^2,\left(\frac{c}{2f}\right)^2,\left(\frac{b+a}{2f}\right)^2\right)=\left(\left(\frac{581618833}{144613560}\right)^2,\left(\frac{905141617}{144613560}\right)^2,\left(\frac{1140299183}{144613560}\right)^2\right)$$

Thus, constructing with large calculators, tables of congruent integers *n* without squares and checking (with usual Pythagorician triplets parameterization):

$uv(u^2 - v^2) = nf^2$, where $u + v \equiv 1 (\bmod 2)$ and $gcd(u,v) = 1$,

is a priori feasible; but show that a given square-free integer n, is congruent or not, is a very difficult problem, and which remains open to this day, despite progress due to numerous works, based, among others, on elliptic curves, and the BSD conjecture cf. [8] [9] [15] [16] [17].

Remark 2.1 *The problem of determining congruent numbers, or properties concerning them, remains open. For example, let n and m be two congruent numbers, we can ask ourselves if nm can also be congruent ? In* [18]*, pp 44 and 65, this problem is stated, and certain families of congruent numbers n and m such that nm are congruents, are proposed.*

2.2. Use of Elliptic Curves for Solving the Problem of Congruent Numbers

Consider n, a congruent number, then cf. Proposition 2.1.: $\exists E, F, G \in \mathbb{Q}^*$, such that: $\begin{cases} E^2 + F^2 = G^2 \\ \frac{1}{2} EF = n \end{cases}$

But then by setting: $x = \left(\frac{G}{2}\right)^2$ et $y = (E^2 - F^2)\frac{G}{8}$, the following elliptic curve: $y^2 = x^3 - n^2 x$, admits rational points. We recall Tunnel's theorem (1983) cf. [8]:

Theorem 2.2 *Let* $n \in \mathbb{N}$, *and square free. Consider then the following cardinals:*

$$A_n = Card\left(\left\{x, y, z \in \mathbb{Z} \text{ such that} : n = 2x^2 + y^2 + 32z^2\right\}\right);$$

$$B_n = Card\left(\left\{x, y, z \in \mathbb{Z} \text{ such that} : n = 2x^2 + y^2 + 8z^2\right\}\right);$$

$$C_n = Card\left(\left\{x, y, z \in \mathbb{Z} \text{ such that} : n = 4x^2 + 2y^2 + 6z^2\right\}\right);$$

$$D_n = Card\left(\left\{x, y, z \in \mathbb{Z} \text{ such that} : n = 8x^2 + 2y^2 + 16z^2\right\}\right).$$

- If we assume that n is a congruent number then necessarily: $A_n = B_n$ if n is even and $2C_n = D_n$ if n is odd.
- Conversely if these equalities between cardinals hold, as well as the conjecture of Birch and Swinnerton-Dyer (cf. [9] and [10]), for the elliptic curve: $y^2 = x^3 - n^2 x$, then n is a congruent number. See also [17] for recent results using these methods.

2.3. New Diophantine Proof that 1 can't be a Congruent Number

Proposition 2.2 *There is equivalence between the following two propositions:*

(i) $\forall (a,b,c) \in \mathbb{N}^3$, $abc \neq 0$, $gcd(a,b) = 1$ and $a^2 + b^2 = c^2$ then $\frac{1}{2} ab \neq f^2$, $\forall f \in \mathbb{N}^*$.

(ii) $\forall (a,b,c) \in \overline{T^+}$ then $\frac{1}{2} ab \neq f^2$, $\forall f \in \mathbb{N}^*$.

Consequently, to solve the problem of Fermat's right-angled triangle theorem, it suffices to prove it only for right-angled triangles of $\overline{T^+}$.

Let us now show the following theorem, which is one of the aims of the article: To say that 1 is not a congruent number, amounts to solving equation (1.1) with $n=1$.

Theorem 2.3 *Let* $(a,b,c)\in\overline{T^+}$ *then* $\frac{1}{2}ab\neq f^2,\ \forall f\in\mathbb{N}^\star$.

Proof 4 *We have cf. Theorem 2.5.* $\exists!((d,\overline{e}),S)\in\left(2\mathbb{N}+1\underset{cop}{\times}2\mathbb{N}+1\right)\times\mathbb{N}^\star$ *such that:*

$$(a,b,c)=\left(d^2+\left(2^S\overline{e}\right)d,\frac{\left(2^S\overline{e}\right)^2}{2}+\left(2^S\overline{e}\right)d,\frac{\left(2^S\overline{e}\right)^2}{2}+\left(2^S\overline{e}\right)d+d^2\right).$$

We then show that equation (1.1) for $n=1$, is not solvable:

$$\Delta=2^{S-1}d\overline{e}\left(d+2^{S-1}\overline{e}\right)\left(d+2^S\overline{e}\right)=f^2.$$

<u>We distinguish 2 cases according to the parity of *S*:</u>

The 1st case: $S=2k$, $k\geq 1$ (which is trivial);

And the 2th case $S=2k+1$, $k\geq 0$.

In this latter case, we will distinguish $S=1$ odd, (which is also trivial); from case $S=2k+1\geq 3$ odd, which is more complex. Let's demonstrate.

- <u>1st case</u>: $S=2k$ is even, $k\geq 1$. Then:

$$(a,b,c)=\left(d^2+\left(2^{2k}\overline{e}\right)d,\frac{\left(2^{2k}\overline{e}\right)^2}{2}+\left(2^{2k}\overline{e}\right)d,\frac{\left(2^{2k}\overline{e}\right)^2}{2}+\left(2^{2k}\overline{e}\right)d+d^2\right).$$

Suppose there exists $f\in\mathbb{N}^\star\,/\,\frac{1}{2}ab=f^2$, then cf. (1.1) we get:

$$2^{2k-1}d\overline{e}\left(d+2^{2k-1}\overline{e}\right)\left(d+2^{2k}\overline{e}\right)=f^2\Rightarrow$$

$$2\left(\overline{e}d+2^{2k-1}\overline{e}^2\right)\left(d^2+\left(2^{2k}\overline{e}\right)d\right)=\left(\frac{f}{2^{k-1}}\right)^2\Rightarrow 2\equiv 0(\mathrm{mod}\,4),$$

which is absurd.

So $\frac{1}{2}ab\neq f^2,\forall f\in\mathbb{N}^\star$, in this first case .

- <u>2th case</u>

- <u>1er Subcase: *S* is odd, and $S=1$ (i.e. $k=0$).</u>

$$(a,b,c)=\left(d^2+(2\overline{e})d,\frac{(2\overline{e})^2}{2}+(2\overline{e})d,\frac{(2\overline{e})^2}{2}+(2\overline{e})d+d^2\right).$$

Suppose there exists $f\in\mathbb{N}^\star\,/\,\frac{1}{2}ab=f^2$, then cf. (1.1) we have:

$$d\overline{e}\left(d+\overline{e}\right)\left(d+2\overline{e}\right)=f^2.$$

Note that *f* is necessarily even, and that the four factors are pairwise prime.

Then $\exists D_1,E_1,f_1'\in 2\mathbb{N}+1$ and $f_1\in\mathbb{N}^\star$, Such that:

$$\begin{cases} d = D_1^2; \\ \overline{e} = E_1^2; \\ D_1^2 + E_1^2 = \left(2f_1\right)^2; \\ D_1^2 + 2E_1^2 = f_1'^2. \end{cases} \tag{2.1}$$

But the 3th equation $\Rightarrow 2 \equiv 0(\bmod 4)$, which is absurd.

Thus $\frac{1}{2}ab \neq f^2, \forall f \in \mathbb{N}^*$.

- 2th Subcase: S is odd, and $S = 2k+1 \geq 3$.

$$(a,b,c) = \left(d^2 + \left(2^{2k+1}\overline{e}\right)d, \frac{\left(2^{2k+1}\overline{e}\right)^2}{2} + \left(2^{2k+1}\overline{e}\right)d, \frac{\left(2^{2k+1}\overline{e}\right)^2}{2} + \left(2^{2k+1}\overline{e}\right)d + d^2 \right).$$

Suppose, for absurdity, that as above there exists: $f \in \mathbb{N}^* \diagup \frac{1}{2}ab = f^2$.

Then: $d\overline{e}\left(d + 2^{2k}\overline{e}\right)\left(d + 2^{2k+1}\overline{e}\right) = \left(\frac{f}{2^k}\right)^2 \equiv 1(\bmod 2)$.

$\Rightarrow \exists$ pairwise prime integers $D_k, E_k, f_k, f_k' \in 2\mathbb{N}+1$ such that:

$$\begin{cases} d = D_k^2; \\ \overline{e} = E_k^2; \\ D_k^2 + \left(2^k E_k\right)^2 = f_k^2; \\ D_k^2 + 2\left(2^k E_k\right)^2 = f_k'^2. \end{cases} \tag{2.2}$$

We then recognize the non-solvable system $\left(\Xi_{0,k}\right)$ of Lemma 2.2. (with here $k \geq 1$), which is found here, to be solvable, which is absurd.

Thus 1 is not congruent.

We now use similar approach to show that 2 is not congruent.

2.4. New Diophantine Proof That 2 Can't Be a Congruent Number

That is, to prove the following theorem:

Theorem 2.4 *Let* $(a,b,c) \in \overline{T^+}$ *Then* $\frac{1}{2}ab \neq 2f^2, \forall f \in \mathbb{N}^*$.

Proof 5 *Cf. Theorem 2.5.,* $\exists!$ $\left((d,\overline{e}),S\right) \in \left(2\mathbb{N}+1 \underset{cop}{\times} 2\mathbb{N}+1\right) \times \mathbb{N}^*$ *such that:*

$$(a,b,c) = \left(d^2 + \left(2^S\overline{e}\right)d, \frac{\left(2^S\overline{e}\right)^2}{2} + \left(2^S\overline{e}\right)d, \frac{\left(2^S\overline{e}\right)^2}{2} + \left(2^S\overline{e}\right)d + d^2 \right).$$

We then seek to solve (1.1) with $n = 2$; that is:

$$\Delta = 2^{S-1}d\overline{e}\left(d + 2^{S-1}\overline{e}\right)\left(d + 2^S\overline{e}\right) = 2f^2.$$

Let us show that this is impossible, by reasoning taking into account the parity of S: The 1st case, wich indeed trivial, corresponds to $S = 1$ and $S = 2k+1 \geq 3$, odd, and of is the same type as in the previous 1st case.

Consequently, we can therefore solve the remaining case which corresponds to:

2^{th} case: $S = 2k$, even, with $k \geq 1$.

$\exists! \ \left((d,\overline{e}),S\right) \in \left(2\mathbb{N}+1 \underset{cop}{\times} 2\mathbb{N}+1\right) \times 2\mathbb{N}^*$ such that:

$$(a,b,c) = \left(d^2 + \left(2^{2k}\overline{e}\right)d, \frac{\left(2^{2k}\overline{e}\right)^2}{2} + \left(2^{2k}\overline{e}\right)d, \frac{\left(2^{2k}\overline{e}\right)^2}{2} + \left(2^{2k}\overline{e}\right)d + d^2\right).$$

Suppose by absurd that there exists $f \in \mathbb{N}^*$ such that $\frac{1}{2}ab = 2f^2$.

Then cf. (1.1): $2^{2k-1}d\overline{e}\left(d + 2^{2k-1}\overline{e}\right)\left(d + 2^{2k}\overline{e}\right) = 2f^2 \Rightarrow$

$$d\overline{e}\left(d + 2^{2k-1}\overline{e}\right)\left(d + 2^{2k}\overline{e}\right) = \left(\frac{f}{2^{k-1}}\right)^2 \equiv 1 \pmod 2.$$

From where:

$\exists D_{k-1}, E_{k-1}, f_{k-1}, f'_{k-1} \in 2\mathbb{N}+1$ such that:

$$\begin{cases} d = D_{k-1}^2; \\ \overline{e} = E_{k-1}^2; \\ D_{k-1}^2 + 2\left(2^{k-1}E_{k-1}\right)^2 = f_{k-1}^2; \\ D_{k-1}^2 + 4\left(2^{k-1}E_{k-1}\right)^2 = f_{k-1}'^2. \end{cases} \tag{2.3}$$

But here we recognize the non-solvable system $\left(\Xi_{1,k-1}\right)$ of Lemma 2.2., (with here $k \geq 1$), which is absurd. This shows that equation (1.1) is unsolvable in this case.

So as we had claimed: $\frac{1}{2}ab \neq 2f^2, \forall f \in \mathbb{N}^*$.

That is to say that the number 2 is not congruent.

2.5. Lemmas

Let us now state and establish the following Lemmas, which allowed our two previous proofs.

Lemma 2.2 *Let* $t \in \{0,1\}$, *and* $\forall k \in \mathbb{N}$, *then the system of equations* $\left(\Xi_{t,k}\right)\begin{cases} X^2 + 2^t\left(2^kY\right)^2 = Z^2, \\ X^2 + 2^{t+1}\left(2^kY\right)^2 = T^2; \end{cases}$ *does not admit any pairwise prime solution*

$$(X,Y,Z,T) = \left(D_k, E_k, f_k, f'_k\right) \in (2\mathbb{N}+1)^4.$$

Remark 2.2 a) *When* $t = 0$: *It is clear that* $\left(\Xi_{0,k}\right) \Leftrightarrow \begin{cases} T^2 + \left(2^kY\right)^2 = Z^2, \\ T^2 - \left(2^kY\right)^2 = X^2; \end{cases}$ *which is not solvable, because it is well known that the sum and the difference of two squares cannot both be squares.*

b) When $t = 1$: It is clear that $\left(\Xi_{1,k}\right) \Leftrightarrow \begin{cases} T^2 + X^2 = 2Z^2, \\ T^2 - X^2 = \left(2^{k+1}Y\right)^2; \end{cases}$ is not solvable, because we have:

$$T = u^2 + v^2 \quad , \quad X = u^2 - v^2 \quad , \quad 2^{k+1} Y = 2uv \quad \Rightarrow T^2 + X^2 = 2Z^2 \ \Rightarrow u^4 + v^4 = Z^2$$

which is not resolvable ([19]).

However, we are going to propose another proof of this lemma.

Proof 6 <u>*CASE 1*</u> *:* $t = 0$.

we will demonstrate by induction on *k*, the proposition :

$$\begin{cases} X^2 + \left(2^k Y\right)^2 = Z^2, \\ X^2 + 2\left(2^k Y\right)^2 = T^2; \end{cases} \quad \text{does not admit any pairwise prime solution}$$

$(X,Y,Z,T) = (D_k, E_k, f_k, f_k') \in (2\mathbb{N}+1)^4$.

- Note first that the proposition is true for $k = 0$ and $k = 1$.

Indeed, if $k = 0$ (resp. $k = 1$), then $(\Xi_{0,0}),(\Xi_{0,1})$ does not admit solutions in $(2\mathbb{N}+1)^4$, because otherwise we would have: $D_0^2 + E_0^2 = f_0^2$ (resp. $D_1^2 + (2E_1)^2 = f_1^2$) which in both cases is impossible.

- Assume now that $k \geq 2$, and let's suppose that this proposition is true until rank $k-1$, What forms our recurrence hypothesis:

$(\Xi_{0,\ell})$ does not admit, up to rank $k-1$, any pairwise prime solution in

$$(2\mathbb{N}+1)^4 \tag{2.4}$$

- Let's show that $(\Xi_{0,k})$ does not admit too, any pairwise prime solution in $(2\mathbb{N}+1)^4$.

Suppose the converse, that is: $\exists (D_k, E_k, f_k, f_k') \in (2\mathbb{N}+1)^4$, such that:

$$(\Xi_{0,k}) \begin{cases} X^2 + \left(2^k Y\right)^2 = Z^2, \\ X^2 + 2\left(2^k Y\right)^2 = T^2; \end{cases} \quad \text{is solvable in}$$

$(X,Y,Z,T) = (D_k, E_k, f_k, f_k') \in (2\mathbb{N}+1)^4$, and pairwise prime.

As a consequence: $(D_k, 2^k E_k, f_k')$ is a non-trivial and positive solution of $x^2 + 2y^2 = z^2$, then (*cf.* Proposition 2.5.):

$\exists!\ (\overline{e}_{k-1}, e''_{k-1}) \in (2\mathbb{N}+1) \underset{cop}{\times} (2\mathbb{N}+1)$; and $S_0 \in \mathbb{N}$, such that:

$$\begin{cases} D_k = (-1)^\beta \left(2\left(2^{S_0}\overline{e}_{k-1}\right)^2 - e''^2_{k-1}\right) = (-1)^\beta \left(2^{2k-1}\overline{e}^2_{k-1} - e''^2_{k-1}\right); \\ 2^k E_k = 2e''_{k-1}\left(2^{S_0}\overline{e}_{k-1}\right) = e''_{k-1}\left(2^k \overline{e}_{k-1}\right); \\ f_k' = e''^2_{k-1} + 2\left(2^{S_0}\overline{e}_{k-1}\right)^2 = e''^2_{k-1} + 2^{2k-1}\overline{e}^2_{k-1}. \end{cases}$$

Because $2^k E_k = 2e''_{k-1}\left(2^{S_0}\overline{e}_{k-1}\right) \Rightarrow S_0 = k-1$,
which implies:

$$\left(D_k, 2^k E_k, f_k'\right) = \left((-1)^\beta \times \left(2^{2k-1}\overline{e}^2_{k-1} - e''^2_{k-1}\right), 2^k e''_{k-1}\overline{e}_{k-1}, 2^{2k-1}\overline{e}^2_{k-1} + e''^2_{k-1}\right).$$

But then:

$$D_k^2 = \left(2^{2k-1}\overline{e}^2_{k-1} - e''^2_{k-1}\right)^2$$

$$= e''^4_{k-1} - 2^{2k}\overline{e}^2_{k-1}e''^2_{k-1} + \left(2^{2k-1}\overline{e}^2_{k-1}\right)^2; \text{ but as } \left(2^k E_k\right)^2 = 2^{2k}\overline{e}^2_{k-1}e''^2_{k-1}.$$

$$= e''^4_{k-1} - \left(2^k E_k\right)^2 + \left(2^{2k-1}\overline{e}^2_{k-1}\right)^2$$

$$\Rightarrow D_k^2 + \left(2^k E_k\right)^2 = e''^4_{k-1} + \left(2^{2k-1}\overline{e}^2_{k-1}\right)^2.$$

But $\left(\Xi_{0,k}\right)$ solvable $\Rightarrow D_k^2 + \left(2^k E_k\right)^2 = f_k^2 \Rightarrow e''^4_{k-1} + \left(2^{2k-1}\overline{e}^2_{k-1}\right)^2 = f_k^2$.

Thereby:

$$e''^4_{k-1} = f_k^2 - \left(2^{2k-1}\overline{e}^2_{k-1}\right)^2 \Rightarrow e''^4_{k-1} = \left(f_k - 2^{2k-1}\overline{e}^2_{k-1}\right)\left(f_k + 2^{2k-1}\overline{e}^2_{k-1}\right).$$

These two factors being coprimes, there exists odd coprimes numbers f'_{k-1}, D_{k-1}, such that: $\begin{cases} D^4_{k-1} = f_k - 2^{2k-1}\overline{e}^2_{k-1}; \\ f'^4_{k-1} = f_k + 2^{2k-1}\overline{e}^2_{k-1}. \end{cases}$

As a result:

$f_k = \dfrac{f'^4_{k-1} + D^4_{k-1}}{2}$ and $2^{2k-1}\overline{e}^2_{k-1} = \dfrac{f'^4_{k-1} - D^4_{k-1}}{2}$, from where : $2^{2k}\overline{e}^2_{k-1} = f'^4_{k-1} - D^4_{k-1}$

Thus: $D^4_{k-1} + 2^{2k}\overline{e}^2_{k-1} = f'^4_{k-1}$;

Let's rewrite that like this: $\left(D^2_{k-1}\right)^2 + \left(2^k\overline{e}_{k-1}\right)^2 = \left(f'^2_{k-1}\right)^2$, that is a Pythagoras equation:

Thus $\left(D^2_{k-1}, 2^k\overline{e}_{k-1}, f'^2_{k-1}\right)$ is a Pythagorician triplet of $\overline{T^+}$. (Note that then necessarily $k \ge 2$).

If we denote $\left(2^k E_{k-1}, f_{k-1}\right)$ as the Pythagorician divisors coming from $2^k\overline{e}_{k-1}$ (cf. Definition 2.3.), with respect that here $\lambda = 0$, then:

$$2^k E_{k-1} = gcd\left(2^k\overline{e}_{k-1}, f^2_{k-1} - D^2_{k-1}\right), \text{ and } 2^k E_{k-1} f_{k-1} = 2^k\overline{e}_{k-1}.$$

And the Pythagorician divisors theorem (cf. Theorem 2.5.) implies that:

$$\begin{cases} f'^2_{k-1} - D^2_{k-1} = \dfrac{\left(2^k E_{k-1}\right)^2}{2} = 2\left(2^{k-1}E_{k-1}\right)^2; \\ f'^2_{k-1} + D^2_{k-1} = 2f^2_{k-1}. \end{cases}$$

We therefore obtain on the one hand:

$$D^2_{k-1} + 2\left(2^{k-1}E_{k-1}\right)^2 = f'^2_{k-1}.$$

And on the other hand:

$$\left(D^2_{k-1} + 2\left(2^{k-1}E_{k-1}\right)^2\right) + D^2_{k-1} = 2f^2_{k-1} \Rightarrow D^2_{k-1} + \left(2^{k-1}E_{k-1}\right)^2 = f^2_{k-1}.$$

And as a result we have:

$\begin{cases} D^2_{k-1} + \left(2^{k-1}E_{k-1}\right)^2 = f^2_{k-1}; \\ D^2_{k-1} + 2\left(2^{k-1}E_{k-1}\right)^2 = f'^2_{k-1}. \end{cases} \Rightarrow \left(\Xi_{0,k-1}\right)$ is solvable, which contradicts the assumption of recurrence assumed to be true up to rank $k-1$.

So the Lemma when $t = 0$, is proved. ■

CASE 2 : $t = 1$.

In this case too, we will demonstrate by induction on *k*, the proposition:

$$\begin{cases} X^2 + 2\left(2^k Y\right)^2 = Z^2, \\ X^2 + 4\left(2^k Y\right)^2 = T^2; \end{cases}$$ does not admit any pairwise prime solution

$(X,Y,Z,T) = (D_k, E_k, f_k, f'_k) \in (2\mathbb{N}+1)^4$.

- This proposition is true for $k=0$. Because if not, then $(\Xi_{1,0})$ should admit solutions in $(2\mathbb{N}+1)^4$, consequently we would have: $D_0^2 + 2E_0^2 = f_0^2 \Rightarrow 3 \equiv 1 (\bmod 4)$, which is absurd.
- Assume now that $k \geq 1$, and let's suppose that this proposition is true until rank $k-1$, What forms our recurrence hypothesis:

$(\Xi_{1,\ell})$ does not admit, up to rank $k-1$, any pairwise prime solution in

$$(2\mathbb{N}+1)^4 \tag{2.5}$$

- Let's show that $(\Xi_{1,k})$ does not admit too, any pairwise prime solution in $(2\mathbb{N}+1)^4$.

Suppose the converse, that is: $\exists (D_k, E_k, f_k, f'_k) \in (2\mathbb{N}+1)^4$, such that:

$$\begin{cases} D_k^2 + 2\left(2^k E_k\right)^2 = f_k^2; \\ D_k^2 + 4\left(2^k E_k\right)^2 = f_k'^2. \end{cases} \tag{2.6}$$

Let's solve by factorization the equation $D_k^2 + 4\left(2^k E_k\right)^2 = f_k'^2$.

Define $\beta \in \{0,1\}$ such that $\dfrac{f'_k + (-1)^\beta D_k}{2} \equiv 0 (\bmod 2)$.

Then: $\exists (\overline{e}_{k-1}, e''_{k-1}) \in (2\mathbb{N}+1) \underset{cop}{\times} (2\mathbb{N}+1)$ such that:

$$\frac{f'_k + (-1)^\beta D_k}{2} \times \frac{f'_k - (-1)^\beta D_k}{2} = \left(2^k E_k\right)^2 \Rightarrow \begin{cases} \dfrac{f'_k + (-1)^\beta D_k}{2} = 2^{2k} \overline{e}_{k-1}^2; \\ 2^k E_k = 2^k \overline{e}_{k-1} e''_{k-1}; \\ \dfrac{f'_k - (-1)^\beta D_k}{2} = e''^2_{k-1}. \end{cases}$$

Then:

$$\begin{cases} D_k = (-1)^\beta \left(2^{2k} \overline{e}_{k-1}^2 - e''^2_{k-1}\right); \\ 2^k E_k = 2^k \overline{e}_{k-1} e''_{k-1}; \\ f'_k = 2^{2k} \overline{e}_{k-1}^2 + e''^2_{k-1}. \end{cases}$$

$$\begin{aligned} \Rightarrow (D_k)^2 &= \left(2^{2k} \overline{e}_{k-1}^2\right)^2 + \left(e''^2_{k-1}\right)^2 - 2\left(2^k \overline{e}_{k-1} e''_{k-1}\right)^2 \\ &= \left(2^{2k} \overline{e}_{k-1}^2\right)^2 + \left(e''^2_{k-1}\right)^2 - 2\left(2^k E_k\right)^2; \end{aligned}$$

$$\Rightarrow (D_k)^2 + 2\left(2^k E_k\right)^2 \underset{\text{recurrence hypothesis}}{=} f_k^2 = \left(2^{2k} \overline{e}_{k-1}^2\right)^2 + \left(e''^2_{k-1}\right)^2;$$

$$\Rightarrow f_k^2 - \left(2^{2k} \overline{e}_{k-1}^2\right)^2 = \left(e''^2_{k-1}\right)^2;$$

$$\Rightarrow \left(f_k - 2^{2k} \overline{e}_{k-1}^2\right)\left(f_k + 2^{2k} \overline{e}_{k-1}^2\right) = e'^4_{k-1};$$

Then $\exists$ $(D_{k-1}, f'_{k-1}) \in (2\mathbb{N}+1) \underset{cop}{\times} (2\mathbb{N}+1)$ such that:

$$\begin{cases} D_{k-1}^4 = f_k - 2^{2k}\overline{e}_{k-1}^2, \\ f_{k-1}'^4 = f_k + 2^{2k}\overline{e}_{k-1}^2; \end{cases} \Rightarrow \left(f_{k-1}'^2\right)^2 - \left(D_{k-1}^2\right)^2 = 2\left(2^{2k}\overline{e}_{k-1}^2\right);$$

And $\exists\left(E_{k-1}, f_{k-1}\right) \in (2\mathbb{N}+1) \underset{cop}{\times} (2\mathbb{N}+1)$ such that:

$$\Rightarrow \left(f_{k-1}'^2 - D_{k-1}^2\right)\frac{f_{k-1}'^2 + D_{k-1}^2}{2} = 2^{2k}\overline{e}_{k-1}^2 \Rightarrow \begin{cases} f_{k-1}'^2 - D_{k-1}^2 = 2^{2k}E_{k-1}^2; \\ f_{k-1}'^2 + D_{k-1}^2 = 2f_{k-1}^2. \end{cases} \Rightarrow$$

$D_{k-1}^2 + \left(2^k E_{k-1}\right)^2 = f_{k-1}'^2$ which can be rewritten in one hand:

$D_{k-1}^2 + 4\left(2^{k-1}E_{k-1}\right)^2 = f_{k-1}'^2$;

and, on the other hand:

$$f_{k-1}'^2 + D_{k-1}^2 = 2f_{k-1}^2 \Rightarrow \left(D_{k-1}^2 + 4\left(2^{k-1}E_{k-1}\right)^2\right) + D_{k-1}^2 = 2f_{k-1}^2 \Rightarrow$$

$$D_{k-1}^2 + 2\left(2^{k-1}E_{k-1}\right)^2 = f_{k-1}^2.$$

So as a result:

$$\Rightarrow \begin{cases} D_{k-1}^2 + 2\left(2^{k-1}E_{k-1}\right)^2 = f_{k-1}^2; \\ D_{k-1}^2 + 4\left(2^{k-1}E_{k-1}\right)^2 = f_{k-1}'^2. \end{cases} \Rightarrow \left(\Xi_{1,k-1}\right)$$ is solvable, which contradicts the assumption of recurrence assumed to be true up to rank $k-1$.

So the Lemma is proved. ■

Note that these two Lemmas induce the following Corollary:

Corollary 2.1 $\forall k,t \in \mathbb{N}$, *the systems of equations*

$$\left(\Xi_{t,0}\right)\begin{cases} X^2 + 2^t\left(2^k Y\right)^2 = Z^2, \\ X^2 + 2^{t+1}\left(2^k Y\right)^2 = T^2; \end{cases}$$ *don't admit any solutions in*

$(X,Y,Z,T) = \left(D_k, E_k, f_k, f_k'\right) \in (2\mathbb{N}+1)^4$, *and pairwise prime.*

Proof 7 *It suffices to consider the cases t even (resp. t odd), which lead in one, or the other of the cases, of the previous lemmas.*

Let us recall here some results and definitions used in various proofs above.

2.6. Pythagoras Equation: Notations-Reminders-Pythagorician Divisors

All these concepts, definitions and proofs are found in [13] or [14].

Convention 2.1 *Let* $(a,b,c) \neq (0,0,0)$ *be a solution of the Pythagoras equation:* $a^2 + b^2 = c^2$. *We agree for the following, unless otherwise stated, that* $(a,b,c) \equiv (\pm 1, 0, 1) \pmod 4$.

This in no way restricts the expression of the generality of the solutions of said equation, because (b,a,c) is also a solution called "associated with (a,b,c)", such that $(b,a,c) \equiv (0,\pm 1,1) \pmod 4$.

Definition 2.2 $\overline{T^+}$ *: is the set of non-trivial, primitive and positive Pythagoras solutions of the type* $\left(a, b = 2^s b_1, c\right) \equiv (\pm 1, 0, 1) \pmod 4$.

It is well known that:

Proposition 2.3

$$\overline{T^+} = \left\{\left(u^2 - v^2, 2uv, u^2 + v^2\right); u, v \in \mathbb{N}, u > v > 0, u + v \equiv 1(\bmod 2) \text{ and } gcd(u, v) = 1\right\}.$$

2.7. Pythagorician Divisors

Definition 2.3 *Let* $(a, b = 2^s b_1, c) \in \overline{T^+}$, $s \geq 2$, b_1 *odd.*

-Denote by $(d, d'') = \left(gcd(a, c-b), \frac{a}{d}\right)$ and $(e, e'') = \left(gcd(b, c-a), \frac{b}{e}\right) = \left(2^S \overline{e}, 2^{s-S}\frac{b_1}{\overline{e}}\right)$, this quantities are the Pythagorician divisors of (a, b, c). The first ones are said coming from *a*, and the second coming from *b*.

-The number $S \in \mathbb{N}^*$, is defined by: $S = s - \lambda(s-1)$, where $\lambda \in \{0,1\}$ is such that: $\frac{c-a}{2} \equiv \lambda(\bmod 2)$, and $\overline{e}$ is the suitable odd integer.

Let's recall cf. [13] [14].

Theorem 2.5 ***(Of Pythagorician divisors).*** *Let* $(a, b = 2^s b_1, c) \in \overline{T^+}$, $s \geq 2$, b_1 *odd.*

There is equivalences between the following propositions:

(i) $a^2 + b^2 = c^2$.

(ii) $\begin{cases} c - b = d^2; \\ c + b = d''^2. \end{cases}$

(iii) $\begin{cases} c - a = \dfrac{e^2}{2} = \dfrac{\left(2^S \overline{e}\right)^2}{2}; \\ c + a = 2e''^2 = 2\left(2^{s-S}\dfrac{b_1}{\overline{e}}\right)^2. \end{cases}$

(iv) $\begin{cases} a = d^2 + \left(2^S \overline{e}\right)d; \\ b = \dfrac{\left(2^S \overline{e}\right)^2}{2} + \left(2^S \overline{e}\right)d; \\ c = \dfrac{\left(2^S \overline{e}\right)^2}{2} + \left(2^S \overline{e}\right)d + d^2. \end{cases}$

Remark 2.3 *About the Pythagirican divisors's Theorem one can says that* $(a, b = 2^s b_1 \neq 0, c) \in \overline{T^+}$*, is a Pythagorician triplet if and only if* $\exists$ *d odd divisor of a,* $\exists$ *e even divisor of b such that:* $\begin{cases} \dfrac{a}{d} = d + e; \\ \dfrac{b}{e} = d + \dfrac{e}{2}; \\ c = a + \dfrac{e^2}{2} = b + d^2. \end{cases}$

Let's put:

Definition 2.4 $2\mathbb{N}+1 \underset{cop}{\times} 2\mathbb{N}+1 = \left\{(x, y) \in (2\mathbb{N}+1)^2 \,/\, gcd(x, y) = 1\right\}$.

We have the following corollary:

Corollary 2.2 $\overline{T^+}$ *is in bijection with:* $\left(2\mathbb{N}+1 \underset{cop}{\times} 2\mathbb{N}+1\right)\times\mathbb{N}^*$, *as follows:*

$$\pi:\overline{T^+}\to\left(2\mathbb{N}+1 \underset{cop}{\times} 2\mathbb{N}+1\right)\times\mathbb{N}^*$$

$$\begin{pmatrix}a\\b\\c\end{pmatrix}\mapsto(d,\overline{e},S)_{(a,b,c)}=\begin{pmatrix}d=gcd(a,c-b)\\ \overline{e}=\dfrac{gcd(b,c-a)}{2^S}\\ S\end{pmatrix}$$

Where $S=s-\lambda(s-1)$ with $s=v_2(b)$ and λ defined in Definition 2.3.;

Whose reciprocal bijection is:

$$\pi^{-1}:\left(2\mathbb{N}+1 \underset{cop}{\times} 2\mathbb{N}+1\right)\times\mathbb{N}^*\to\overline{T^+}$$

$$\begin{pmatrix}d\\ \overline{e}\\ S\end{pmatrix}\mapsto(a,b,c)_{(d,\overline{e},S)}=\begin{pmatrix}a=d^2+\left(2^S\overline{e}\right)d\\ b=\dfrac{\left(2^S\overline{e}\right)^2}{2}+\left(2^S\overline{e}\right)d\\ c=\dfrac{\left(2^S\overline{e}\right)^2}{2}+\left(2^S\overline{e}\right)d+d^2\end{pmatrix}$$

In particular we get the proposition:

Proposition 2.4

$$\overline{T^+}=\left\{\left(d^2+\left(2^S\overline{e}\right)d,\frac{\left(2^S\overline{e}\right)^2}{2}+\left(2^S\overline{e}\right)d,\frac{\left(2^S\overline{e}\right)^2}{2}+\left(2^S\overline{e}\right)d+d^2\right)/(d,\overline{e})\in 2\mathbb{N}+1 \underset{cop}{\times} 2\mathbb{N}+1 \text{ and } S\in\mathbb{N}^*\right\}.$$

From all the above, we have:

Theorem 2.6 *Let* $(a,b,c)\in\overline{T^+}$ *, whose area is* $\Delta=\frac{1}{2}ab$. *Then* $\exists!$ $(d,\overline{e},S)\in\left(2\mathbb{N}+1 \underset{cop}{\times} 2\mathbb{N}+1\right)\times\mathbb{N}^*$, *such that:*

1) $$\begin{cases}a=d^2+\left(2^S\overline{e}\right)d;\\ b=\dfrac{\left(2^S\overline{e}\right)^2}{2}+\left(2^S\overline{e}\right)d;\\ c=\dfrac{\left(2^S\overline{e}\right)^2}{2}+\left(2^S\overline{e}\right)d+d^2.\end{cases}$$

2) $\Delta=\frac{1}{2}ab=2^{S-1}d\overline{e}\left(d+2^S\overline{e}\right)\left(2^{S-1}\overline{e}+d\right)$.

With: $2^{S-1},d,\overline{e},\left(d+2^S\overline{e}\right),\left(2^{S-1}\overline{e}+d\right)$, pairwise prime.

Remark 2.4 *Other interesting parametrizations of Pythagorician triplets can be found in* [20], [21] *or* [22].

We now giving the positive, non-null and non-trivial primitive solutions (i.e. $\neq(1,0,1)$), of the equation $x^2+2y^2=z^2$, cf. [14]. These solutions are necessary to solve the Fermat's Theorem of the right-angled triangle, and that of the non-congruence of 2.

Solution of the Diophantine Equation $x^2+2y^2=z^2$

We get the following theorem cf. [13] [14]:

Proposition 2.5 *There is an equivalence between the following propositions (the solutions are supposed to be non-null, non-trivial, primitive and positive).*

(i) $x^2+2y^2=z^2$ is solvable;

(ii) $\exists$ $e'', \overline{e}$ coprimes, such that:

$$\begin{cases} x=(-1)^{\beta}\left(2\left(\dfrac{e}{2}\right)^2-e''^2\right), \text{ where } \beta\in\{0,1\} \text{ and } (-1)^{\beta}=sign\left(2\left(2^{S''}\overline{e}\right)^2-e''^2\right); \\ y=2e''\left(\dfrac{e}{2}\right); \\ z=e''^2+2\left(\dfrac{e}{2}\right)^2. \end{cases}$$

Remark 2.5 1) *$\beta\in\{0,1\}$ is defined by:* $\dfrac{z+(-1)^{\beta}x}{2}\equiv 0(\bmod 2)$.

2) e'' is an odd integer, as well as $\overline{e}$, and are such that: $e=2^s\overline{e}$, and so $y=2^s\overline{e}e''$.

$$\begin{cases} e''=\dfrac{y}{gcd\left(y,\dfrac{z+(-1)^{\beta}x}{2}\right)}; \\ \overline{e}=\dfrac{gcd\left(y,\dfrac{z+(-1)^{\beta}x}{2}\right)}{2\times 2^{S''}}; \\ S''=s-1\in\mathbb{N}. \end{cases}$$

2.8. Conclusions and Perspectives

The Pythagorician divisors theorem, gives a new, simple original proof of Fermat's right-angled triangle theorem, and that number 2 is not a congruent number. We do believe, that such a method seems to be usable for the general problem of congruent numbers, namely for other values of square-free integers *n*, and in particular for those where: $n=p$ prime. With this method, we have been able to show that any prime number $p\equiv 3(\bmod 8)$, is not congruent; and that any prime number $p\equiv 5,7(\bmod 8)$ are congruents. We seek to show, with our method, the resolution of the problem of congruent numbers for the prime numbers $p\equiv 1(\bmod 8)$. Note that for this last case, using the theory of elliptic curves, Evink, Top and Top, J., D. cf. [17], showed on the one hand, that there exists an infinity of prime numbers $p\equiv 1(\bmod 8)$, which are not congruent (these being of density $>\frac{1}{8}$), and on the other hand, that the infinity of the prime numbers of $f(\mathbb{Z})$ are congruents, where $f(x)=8x^4+16x^3+12x^2+4x+1$, is a polynomial verifying the conjecture of Bouniakowsky, see also [23] [24], for related results.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Diophanti, A. (1670) Arithmeticorum libri sex et de numeris multangulis liber vnus: Cum commentariis C. G. Bacheti. & observationibus de Fermat; accessit doctrinae analyticae inventum novum collectum ex varijs eiusdem de Fermat epistolis; Publisher excudebat Bernardus Bosc, è regione Collegij Societatis Iesu; National Library of Naples. http://books.google.com/books?id=TbE_3aglZl4C&hl=&source=gbs_api

[2] Genocchi, A. (1855) Sopra tre scritti inediti di Leonardo Pisano, pubblicati da B. Boncompagni Annali di Scienze Matematiche e Fisiche, t. 5 e 6, 161-185.

[3] Dickson, L. E. (1952) History of Number Theory, Vol. 2. Chealsea Publishing Company (Reprinted), New York.

[4] Cuculière, R. (1988) Mille ans de chasse aux nombres congruent. *Séminaire de Philosophie et Mathématiques*, **2**, 1-17. http://www.numdam.org/item?id=SPHM_1988___2_A1_0

[5] Ramacciotti, F. R. (2003) Angelo Genocchi e il suo contributo alla Teoria dei numeri, Sintesi della tesi di Laurea in Matematica, Relatore Prof. Universit a degli studi di Roma Tre, Roma.

[6] Fresnel, J. (2006) Géométrie et arithmétique. *APMEP*, No. 466, pp. 699-713. https://www.apmep.fr/IMG/pdf/AAA06073.pdf

[7] Coates J., (2005) The Congruent Number Problem. Enrichment Programme for Young Mathematics Talents, Dept of Math & IMS CUHK Guest Lecture Series Autumn Class 2002/03, Chinese University of Hong Kong, Shatin.

[8] Tunnel, J.B. (1983) A Classical Diophantine Problem and Modular form of Weight 3/2. *Inventiones Mathematicae*, **72**, 323-334. https://doi.org/10.1007/BF01389327

[9] Birch, B.J. and Swinnerton-Dyer, H.P.F. (1963) Notes on Elliptic Curves. I. *Journal für die reine und angewandte Mathematik*, **1963**, 7-25. https://doi.org/10.1515/crll.1963.212.7

[10] Birch, B.J. and Swinnerton-Dyer, H.P.F. (1965) Notes on Elliptic Curves. II. *Journal für die reine und angewandte Mathematik*, **1965**, 79-108. https://doi.org/10.1515/crll.1965.218.79

[11] Dujella, A. (2021) Number Theory. Texbook of the University of Zagreb, Školska knjiga, Masarykova.

[12] Lagrange, J. (1975) Nombres congruents et courbes elliptiques. *Séminaire Delange-Pisot-Poitou*, **16**, 1-17.

[13] Keuméan, L.D. (2020) Diviseurs pythagoriciens appliqués à la résolution du problème de certains nombres congruents. Mémoire de Master 2, Université Félix Houphouet Boigny, Abidjan.

[14] Tanoé, F.E. and Kimou, P.K. (2023) Pythagorician Divisors and Applications to

Some Diophantine Equations. *Advances in Pure Mathematics*, **13**, 35-70. https://doi.org/10.4236/apm.2023.132003

[15] Hemenway, B.R. (2006) On Recognizing Congruent Prime. Master Thesis, Simon Fraiser University, Burnaby. http://summit.sfu.ca/item/6418

[16] Coates, J. and Wiles A. (1977) On the Conjecture of Birch and Swinnerton-Dyer. *Inventiones Mathematicae*, **39**, 223-251. https://doi.org/10.1007/BF01402975

[17] Evink, T., Top, J. and Top, J.D. (2021) A Remarque on Prime (non)Congruent Numbers. *Quaestiones Mathematicae*, **45**, 1841-1853. https://www.tandfonline.com/loi/tqma20 https://doi.org/10.2989/16073606.2021.1977410

[18] Lucas, E. (1877) Recherches sur plusieurs ouvrages de Léonard de Pise et sur diverses questions d'Arithmétiques supérieures. *Extrait du Bullettino di bibliografia di storia delle scienze mathematiche e fisiche*, **10**, 124. https://upload.wikimedia.org/wikipedia/commons/5/51/Recherches_Sur_Plusieurs_Ouvrages_De_L%C3%A9onard_De_Pise_Et_Sur_Diverses_Questions_D%E2%80%99Arithm%C3%A9tique_Sup%C3%A9rieure%2C_%C3%89douard_Lucas_%281877%29.pdf

[19] Euler, L. (1738) Theorematum quorundam arithmeticorum demonstrations. *Novi Commentarii academiae scientiarum Petropolitanae*, **10**, 125-146.

[20] Rimbeboim, P. (1999) Fermat's Last Theorem for Amateurs. Springer-Verlag New York Inc., New York.

[21] Mouanda, J. (2022) On Fermat's Last Theorem and Galaxies of Sequences of Positive Integers. *American Journal of Computational Mathematics*, **12**, 162-189. https://doi.org/10.4236/ajcm.2022.121009

[22] Bhanota, S.A. and Kaabar, M.K.A. (2022) On Multiple Primitive Pythagorean Triplets. *Palestine Journal of Mathematics*, **11**, 119-129.

[23] Monsky, P. (1990) Mock Heegner Points and Congruent Numbers. *Mathematische Zeitschrift*, **204**, 45-67. https://doi.org/10.1007/BF02570859

[24] Stephens, N.M. (1975) Congruence Properties of Congruent Numbers, *Bulletin of the London Mathematical Society*, **7**, 182-184. https://doi.org/10.1112/blms/7.2.182