Diophantine Quotients and Remainders with Applications to Fermat and Pythagorean Equations

Kouadio Prosper Kouadio Kimou, François Emmanuel Tanoé

Scientific Research Publishing

American Journal of Computational Mathematics, 2023, 13, 199-210
https://www.scirp.org/journal/ajcm
ISSN Online: 2161-1211
ISSN Print: 2161-1203

Diophantine Quotients and Remainders with Applications to Fermat and Pythagorean Equations

Prosper Kouadio Kimou[1], François Emmanuel Tanoé[2]

[1]Department of Mathematics and Computer Science, Félix Houphouet-Boigny National Polytechnic Institute, Yamoussoukro, Ivory Coast
[2]UFR Mathematics of Computer Science, Université Félix Houphouet-Boigny, Abidjan, Ivory Coast
Email: kouadio.kimou@inphb.ci, aziz_marie@yahoo.fr

How to cite this paper: Kimou, P.K. and Tanoé, F.E. (2023) Diophantine Quotients and Remainders with Applications to Fermat and Pythagorean Equations. *American Journal of Computational Mathematics*, **13**, 199-210.
https://doi.org/10.4236/ajcm.2023.131010

Received: December 9, 2022
Accepted: March 28, 2023
Published: March 31, 2023

Abstract

Diophantine equations have always fascinated mathematicians about existence, finitude, and the calculation of possible solutions. Among these equations, one of them will be the object of our research. This is the Pythagoras'-Fermat's equation defined as follows.

$$x^n + y^n = z^n, n \geq 2 \text{ an integer} \quad (1)$$

when $n = 2$, it is well known that this equation has an infinity of solutions but has none (non-trivial) when $n > 2$. We also know that the last result, named Fermat-Wiles theorem (or FLT) was obtained at great expense and its understanding remains out of reach even for a good fringe of professional mathematicians. The aim of this research is to set up new simple but effective tools in the treatment of Diophantine equations and that of Pythagoras-Fermat. The tools put forward in this research are the properties of the quotients and the Diophantine remainders which we define as follows. Let (a,b,c) a non-trivial triplet ($abc \neq 0$) solution of Equation (1) such that $a < b < c$. (q_1, q_2) and (r_1, r_2) are called the Diophantine quotients and remainders of solution (a,b,c). We compute the remainder and the quotient of b and c by a using the division algorithm. Hence, we have: $b = aq_1 + r_1$ and et $c = aq_2 + r_2$ with $r_1, r_2 < a$. We prove the following important results. $q_2 = q_1$ if and only if $r_2 > r_1$ and $q_2 = q_1 + 1$ if and only if $r_2 < r_1$. Also, we deduce that $q_2 = q_1$ or $q_2 = q_1 + 1$ for any hypothetical solution (a,b,c). We illustrate these results by effectively computing the Diophantine quotients and remainders in the case of Pythagorean triplets using a Python program. In the end, we apply the previous properties to directly prove a partial result of FLT.

Keywords

Diophantine Equation, Modular Arithmetic, Fermat-Wiles Theorem, Pythagorean Triplets, Division Theorem, Division Algorithm, Python Program, Diophantine Quotients, Diophantine Remainders

MSC2020 Mathematical Sciences Classification System:
11A05-11A07-11D41-11D72-11D75.

1. Introduction

The subject we are dealing with is within the framework of Diophantine analysis [1]. A Diophantine equation is an equation that can be solved in the domain of natural integers or at most in the domain of rational numbers [1]. The study of this type of problem is recognized as being difficult [2]. Indeed, each equation or its special cases may require its own tools to deal with them. In most cases, these tools do not seem to fit into any general theory. The focus of our study is on the Diophantine equation $x^n + y^n = z^n$ with $n \geq 2$ an integer, which we name the Pythagoras'-Fermat's equation. When $n = 2$, we have the Pythagoras' equation which admits an infinite number of parametric solutions ([1] p. 462) [3].

Ancient Babylonian, Greek and Egyptian mathematicians were fascinated by Pythagorean triplets, and they discovered some of them. Today, they continue to be analyzed, classified, studied to bring out new properties or algorithms for cryptographic uses [4] [5] [6].

When $n > 2$, it is the Fermat equation, and it is well known that this equation has no non-trivial solutions as demonstrated in 1995 by Wiles [1]. To achieve his proof, Wiles had to deploy "sophisticated" tools and difficult to access for the non-specialist [2] [7]. Even partial results like Abel's conjecture and the cases where $z = y + 1$ or even $y = x + 1$ in Fermat's equation have not been fully resolved [6]. Indeed, the second case, $xyz \equiv 0 \pmod{p}$ with $p > 2$ a prime, of these subproblems still awaits direct proof. Thus, the search for new ways that are accessible and comprehensible to most amateurs is still ongoing [8] [9] [10].

In 2021, Serdar Beji has numerically calculated solutions of a generalized form of Fermat's equation as a function of the number of terms and the degree of this equation [11]:

$$\sum_{i=1}^{m} z_i^n = Z^n,\ m, n \geq 2 \text{ integers} \tag{2}$$

This previous Diophantine equation, under certain conditions, does not admit solutions. Nevertheless, it should be noted that for

$$z_1^3 + z_2^3 + z_3^3 = Z^3 \left(\text{i.e } m = n = 3\right) \tag{3}$$

Scheinman L. J. found several non-trivial solutions based on relations between some known solutions or their elements [12]. He presented two different me-

thods for calculating some solutions of Equation (3) [12].

Let F_n be the set of proven or hypothetical non-trivial solutions of the Pythagoras-Fermat equation, the objective of this paper is to prove the following two main results.

Theorem 1. Let $n \geq 2$ be an integer, $(a,b,c) \in F_n$ such that $a < b < c$, (q_1, q_2) and (r_1, r_2) be its respective Diophantine quotients and remainders. We have:

$$q_2 = q_1 \Leftrightarrow r_2 > r_1 .$$

Theorem 2. Let $n \geq 2$ an integer, $(a,b,c) \in F_n$ such that $a < b < c$, (q_1, q_2) and (r_1, r_2) be its respective Diophantine quotients and remainders. We have:

$$q_2 = q_1 + 1 \Leftrightarrow r_2 < r_1 .$$

We apply these theorems to prove following result.

Theorem 3. Let $n \geq 2$ an integer, $(a,b,c) \in F_n$ such that $a < b < c$, (q_1, q_2) and (r_1, r_2) be its respective Diophantine quotients and remainders. We have:

$$c - b = 1 \Rightarrow q_2 = q_1 .$$

When $n > 2$, Theorem 3 directly proves that FLT is true in the case where $z = y + 1$ and $q_2 = q_1 + 1$.

To which must be added this important result:

Theorem 4. Let $n \geq 2$ a prime $(a,b,c) \in F_n$ such that $a < b < c$, (q_1, q_2) and (r_1, r_2) be its respective Diophantine quotients and remainders. We have:

$$q_1 = q_2 \text{ and } r_2 > r_1 \text{ or } q_2 = q_1 + 1 \text{ and } r_2 < r_1 .$$

2. Preliminaries

Definition 2.1 Let $n \geq 2$ be an integer, we call the subset of $\mathbb{N}^3$ defined as follows,

$$F_n = \left\{ (x,y,z) \in \mathbb{N}^3, x^n + y^n = z^n \text{ and } xyz \neq 0 \right\}$$

Pythagoras'-Fermat's domain.

The set F_n represents the set of non-trivial triplet solutions of the Pythagoras' or Fermat's equation. The Fermat-Wiles theorem shows that if $n > 2$ then $F_n = \varnothing$. In our study, we assume that a priori this set contains possible solutions.

Lemma 2.1. Let $n \geq 2$ be an integer, (a,b,c) an integer triplet such that $a < b < c$. We have.

$$(a,b,c) \in F_n \Rightarrow a > 1$$

Proof.

Let us prove by the absurd by assuming that $(a,b,c) \in F_n$ and $a = 1$.

$$(a,b,c) \in F_n \text{ and } a = 1 \Rightarrow 1 = c^n - b^n$$

$$\Rightarrow 1 = (c-b) T_n (b,c) \text{ where } T_n (b,c) = \frac{c^n - b^n}{c-b}$$

$$\Rightarrow 1 = c - b = 1 \text{ and } T_n(b,c) = 1 \text{ because } c \neq b$$
$$\Rightarrow T_n(b,c) = c^{n-1} + bc^{n-2} + \cdots + b^{n-1}$$
$$\Rightarrow \square \text{ because } c^{n-1} + bc^{n-2} + \cdots + b^{n-1} > 1$$

where the symbol $\square$ designates the logic empty clause. It means absurd. So $a > 1$.

Lemma 2.2. Let $n \geq 2$ be an integer, (a,b,c) an integer triplet such that $a < b < c$. So, there are unique pairs of natural numbers (q_1, r_1) and (q_2, r_2) such that:

$$(a,b,c) \in F_n \Rightarrow b = aq_1 + r_1 \text{ and } c = aq_2 + r_2.$$

Proof. Let $(a,b,c) \in F_n$, according to Lemma 2.1. and the division theorem, we have: $a < b < c_1 \Rightarrow a > 1$

$$\Rightarrow \exists (q_1, r_1), (q_2, r_2) \in \mathbb{N}^2,\ b = aq_1 + r_1, c = aq_2 + r_2 \text{ and } r_1, r_2 < a$$

Remark 2.1. (q_1, r_1) and (q_2, r_2) are unique. If $(a,b,c) \in F_n$ then $q_1 < \frac{b}{2}$ and $q_2 < \frac{c}{2}$. Because, for example $b = aq_1 + r_1 > aq_1$ as a result $b > 2q_1$ because of lemma 2.1.

Definition 2.2. The pair of unique integer numbers (q_1, r_1) and (q_2, r_2) appearing in Lemma 2.1 define the Diophantine quotient (q_1, q_2) and the Diophantine remainders (r_1, r_2) of triplet solution (a,b,c) of the Pythagoras'-Fermat's equation. When $n = 2$, the triplet solution is a Pythagorean triplet and (q_1, q_2), (r_1, r_2) are calls Pythagorean quotients and remainders of this solution.

The Definition 2.2 relies on the division theorem or algorithm ([3], p.334).

Lemma 2.3. Let $n \geq 2$ be an integer and (a,b,c) an integer triplet such as $a < b < c$. We have

$$(a,b,c) \in F_n \Rightarrow c < \frac{a}{n} + b.$$

Proof.

$$(a,b,c) \in F_n \Rightarrow a^n + b^n = c^n$$
$$\Rightarrow a^n = c^n - b^n \Rightarrow a^n = (c-b)\sum_{k=0}^{n-1} c^{n-1-k} b^k$$
$$\Rightarrow (c-b)\sum_{k=0}^{n-1} b^{n-1-k} b^k < a^n$$
$$\Rightarrow (c-b) b^{n-1} \sum_{k=0}^{n-1} 1 < a^n$$
$$\Rightarrow n(c-b) b^{n-1} < a^n \Rightarrow n(c-b) < a \frac{a^{n-1}}{b^{n-1}}$$
$$\Rightarrow n(c-b) < a \Rightarrow c < \frac{a}{n} + b$$

Remark 2.2. We have $a > n$ otherwise $c < \frac{a}{n} + b < 1 + b$ which implies $c \leq b$, which is absurd.

Lemma 2.4. Let $n \geq 2$ be an integer, $(a,b,c) \in F_n$ such that $a < b < c$. We have:

$$c < a + b .$$

Proof.

$$(a,b,c) \in F_n \Rightarrow c < \frac{a}{n} + b < a + b \Rightarrow c < a + b$$

Remark 2.3: This property is also found in ([4], p. 100).

Lemma 2.5. Let $n \geq 2$ be an integer, $(a,b,c) \in F_n$ such that $a < b < c$, q_1 and q_2 be its Diophantine quotients. We have:

$$q_2 \geq q_1 .$$

Proof

On the one hand,

(a,b,c) is an increasingly ordered triplet so $a < b < c$. Moreover, this triplet is a solution of Pythagoras'-Fermat's equation, so by lemma 2.1 $a > 1$. We can therefore apply the division algorithm. There are therefore unique pairs of integers (q_1, r_1) and (q_2, r_2) such that $b = aq_1 + r_1$ and $c = aq_2 + r_2$ such that $0 \leq r_1, r_2 < a$.

On the other hand,

$$\begin{aligned}(a,b,c) \in F_n \text{ and } q_2 < q_1 &\Rightarrow c - b = a(q_2 - q_1) + r_2 - r_1 \text{ and } a < b < c \\ &\Rightarrow c - b = r_2 - r_1 - a(q_1 - q_2) \\ &\Rightarrow c - b < 0 \text{ because } |r_2 - r_1| < a \\ &\Rightarrow c < b \\ &\Rightarrow \square\end{aligned}$$

Hence $q_2 \geq q_1$

Remark 2.3. Note that q_1 and q_2 are non-zero. Otherwise, *b* or *c* would be less than *a*.

The following lemma is important for what follows. It will be used as a basis for the proof of the two theorems.

Lemma 2.6. Let $n \geq 2$ be an integer, $(a,b,c) \in F_n$ such that $a < b < c$ and (q_1, q_2) and (r_1, r_2), its Diophantine quotients and remainders associates. We have:

$$\frac{r_1 - r_2}{a} < q_2 - q_1 < 1 + \frac{r_1 - r_2}{a}$$

Proof. We know that: $b = aq_1 + r_1, c = aq_2 + r_2$. According to lemmas 2.4 and 2.5, we have

$$\begin{aligned}(a,b,c) \in F_n &\Rightarrow c < a + b \text{ and } q_2 \geq q_1 \\ &\Rightarrow 0 < c - b < a \text{ and } q_2 \geq q_1 \\ &\Rightarrow 0 < a(q_2 - q_1) + r_2 - r_1 < a \\ &\Rightarrow 0 < q_2 - q_1 + \frac{r_2 - r_1}{a} < 1 \\ &\Rightarrow -\frac{r_2 - r_1}{a} < q_2 - q_1 < 1 - \frac{r_2 - r_1}{a} \\ &\Rightarrow \frac{r_1 - r_2}{a} < q_2 - q_1 < 1 + \frac{r_1 - r_2}{a}\end{aligned}$$

Proposition 2.1. Let $n \geq 2$ be an integer, $(a,b,c) \in F_n$ such that $a < b < c$ and (q_1, q_2) and (r_1, r_2) be its Diophantine quotients and remainders associates. We have

$$r_2 \neq r_1 .$$

Proof. By absurd suppose that $r_2 = r_1$. According to lemma 2.6

$$\begin{aligned}(a,b,c) \in F_n \text{ and } r_2 = r_1 &\Rightarrow 0 < q_2 - q_1 < 1\\ &\Rightarrow q_2 - q_1 \in]0,1[\\ &\Rightarrow \square \text{ because } q_2 - q_1 \in \mathbb{N}\end{aligned}$$

Lemma 2.7. Let $n \geq 2$ be an integer, $(a,b,c) \in F_n$ such that $a < b < c$. We have:

$$c - b = 1 \text{ and } q_2 = q_1 + 1 \Rightarrow a = 1 + r_1 - r_2 .$$

Lemma 2.8. Let $n \geq 2$ be an integer, $(a,b,c) \in F_n$ such that $a < b < c$. We have:

$$c - b = 1 \text{ and } q_2 = q_1 + 1 \Rightarrow r_1 < a - 1 .$$

Lemma 2.9. Let $n \geq 2$ be an integer, $(a,b,c) \in F_n$ such that $a < b < c$. We have:

$$c - b = 1 \Rightarrow \gcd(b,c) = 1 .$$

Proof. According to Euclid algorithm, we have,

$$c - b = 1 \Rightarrow \gcd(b,c) = \gcd(b,b+1) = \gcd(b,1) = 1$$

Lemma 2.10. Let $n \geq 2$ be an integer, $(a,b,c) \in F_n$ such that $a < b < c$. We have:

$$c - b = 1 \Rightarrow \gcd(a,c) = \gcd(b,c) = 1 .$$

Proof. Let $(a,b,c) \in F_n$ and $c - b = 1$. We have on the one hand.

$$\begin{aligned}\gcd(a,b) > 1 &\Rightarrow a^n + b^n = (b+1)^n \text{ and } (b+1)^n \equiv 0[d]\\ &\Rightarrow \square \text{ because } b \equiv 0[d] \text{ and } \gcd\left(b,(b+1)^n\right) = 1\end{aligned}$$

Hence $\gcd(a,b) = 1$.

On the other hand,

$$\begin{aligned}\gcd(a,c) > 1 &\Rightarrow a^n + b^n = (b+1)^n \text{ and } b^n \equiv 0 \pmod d\\ &\Rightarrow \square \text{ because } b+1 \equiv 0 \pmod d \text{ and } \gcd\left(b^n, b+1\right) = 1\end{aligned}$$

Hence $\gcd(a,c) = 1$.

Proposition 2.2. Let $n \geq 2$ be an integer, $(a,b,c) \in F_n$ such that $a < b < c$. We have:

$$c - b = 1 \Rightarrow (a,b,c) \text{ is a primitive triplet.}$$

3. Proof of Theorems

In this section, we prove Theorems 1 and 2 stated in our introduction.

3.1. Proof of Theorem 1

To prove Theorem 1, we proceed by implication.

Proof. Let $n \geq 2$ an integer and $(a,b,c) \in F_n$. On the one hand, let's prove that: if $q_1 = q_2$ then $r_2 > r_1$. We have:

$$\begin{aligned} q_1 = q_2 &\Rightarrow \frac{r_1 - r_2}{a} < q_2 - q_1 < 1 + \frac{r_1 - r_2}{a} \\ &\Rightarrow \frac{r_1 - r_2}{a} < 0 < 1 + \frac{r_1 - r_2}{a} \Rightarrow \frac{r_1 - r_2}{a} < 0 \\ &\Rightarrow r_2 - r_1 > 0 \Rightarrow r_2 > r_1 \end{aligned}$$

Reciprocally

$$\begin{aligned} r_2 > r_1 &\Rightarrow \frac{r_1 - r_2}{a} < q_2 - q_1 < 1 + \frac{r_1 - r_2}{a} \text{ et } r_2 - r_1 > 0 \\ &\Rightarrow -\frac{r_2 - r_1}{a} < q_2 - q_1 < 1 - \frac{r_2 - r_1}{a} \\ &\Rightarrow -1 < -\frac{r_2 - r_1}{a} < q_2 - q_1 < 1 - \frac{r_2 - r_1}{a} < 1 \\ &\Rightarrow -1 < q_2 - q_1 < 1 \\ &\Rightarrow |q_2 - q_1| < 1 \Rightarrow q_2 - q_1 = 0 \\ &\Rightarrow q_2 = q_1 \end{aligned}$$

3.2. Proof of Theorem 2

We use the same approach as before to prove Theorem 2.

Proof. Let $n \geq 2$ be an integer and $(a,b,c) \in F_n$. On the one hand,

$$\begin{aligned} q_2 = q_1 + 1 &\Rightarrow \frac{r_1 - r_2}{a} < q_2 - q_1 < 1 + \frac{r_1 - r_2}{a} \\ &\Rightarrow \frac{r_1 - r_2}{a} < 1 < 1 + \frac{r_1 - r_2}{a} \\ &\Rightarrow 1 < 1 + \frac{r_1 - r_2}{a} \Rightarrow \frac{r_1 - r_2}{a} > 0 \\ &\Rightarrow r_1 - r_2 > 0 \Rightarrow r_1 > r_2 \end{aligned}$$

On the other hand, we prove the reciprocal of the previous result.

$$\begin{aligned} r_2 < r_1 &\Rightarrow \frac{r_1 - r_2}{a} < q_2 - q_1 < 1 + \frac{r_1 - r_2}{a} \\ &\Rightarrow \frac{r_1 - r_2}{a} < q_2 - q_1 < 1 + \frac{r_1 - r_2}{a} \text{ et } r_1 - r_2 > 0 \\ &\Rightarrow 0 < \frac{r_1 - r_2}{a} < q_2 - q_1 < 1 + \frac{r_1 - r_2}{a} < 2 \\ &\Rightarrow 0 < q_2 - q_1 < 2 \Rightarrow 0 < q_2 - q_1 \leq 1 \\ &\Rightarrow q_2 - q_1 = 1 \Rightarrow q_2 = 1 + q_1 \end{aligned}$$

Proposition 3.1. Let $n \geq 2$ be an integer, $(a,b,c) \in F_n$ such that $a < b < c$ and (q_1, q_2) its Diophantine quotients. Then

$$q_2 = q_1 \text{ or } q_2 = q_1 + 1$$

Proof. Let $(a,b,c) \in F_n$

$$a < b < c \Rightarrow b = aq_1 + r_1 \text{ et } b = aq_2 + r_2 \text{ and } r_1, r_2 < a$$

On the one hand, according to Theorem 1, we have

$$r_2 > r_1 \Rightarrow q_2 = q_1$$

On the other hand, according to Theorem 2, we have

$$r_2 < r_1 \Rightarrow q_2 = q_1 + 1$$

Hence the result.

Example 3.1. Table 1 illustrates the values of Diophantine quotients and remainders in the case of the Pythagorean equation. This table, obtained by the python program calculates the Diophantine quotients and remainders of some Pythagorean triplets. The algorithm of the program in Figure 1 is based on the Definition 2.2

Table 1. Examples of Diophantine quotients and remainders of some Pythagorean triplets.

$(a,b,c) \in F_2$			q_1	q_2	r_1	r_2
5	12	13	2	2	2	3
7	24	25	3	3	3	4
20	21	29	1	1	1	9
28	45	53	1	1	17	25
36	77	85	2	2	5	13
39	80	89	2	2	2	11
276	493	565	1	2	217	13
287	816	865	2	3	242	4
300	589	661	1	2	289	61

Remark 3.1. The data in Table 1 were extracted from the results of the Calc_pythaQ_R(5, 39) and Calc_pythaQ_R(287, 300) commands. The first three columns identify a Pythagorean triplet, columns 4 and 5 respectively identify the Diophantine quotients q_1 and q_2 (note that either $q_1 = q_2$ or $q_1 = q_2 + 1$) the last two columns identify r_1 and r_2. They confirm the results of Theorems 1 and 2 as well as that of Proposition 3.2.

```
import math
def Calc_pythaQ_R(M,N):
    for a in range(M,N):
        for b in range(a,math.floor((a/2+1)*a)):
            for c in range(b+1, a+b+1):
                if (math.gcd(a,b)==1 and math.gcd(a,c)==1) and a*a+b*b==c*c:
                    q1=b//a; q2=c//a; r1=b%a; r2=c%a;
                    print(a, b, c, q1, q2, r1, r2)
```

Figure 1. Python program to compute Pythagorean triples and their Diophantine quotients and remainders.

4. Applications

We apply the previous results to prove theorems 3 and 4. Theorem 3 gives a partial proof of FLT and gives new properties of Pythagorean triplets when Equation (1) becomes:

$$x^n + y^n = (y+1)^n, n \geq 2 \tag{4}$$

Let us denote by $\mathcal{F}_n$ the set of hypothetical solution of the Equation (4). According to Proposition 3.1, we can write

$$\mathcal{F}_n = \mathcal{F}_{n/q_1=q_2} \bigcup \mathcal{F}_{n/q_2=q_1+1} \text{ and } \mathcal{F}_{n/q_1=q_2} \bigcap \mathcal{F}_{n/q_2=q_1+1} = \varnothing$$

with

$$\mathcal{F}_{n/q_1=q_2} = \left\{(a,b,c) \in \mathcal{F}_n, E\left(\frac{b}{a}\right) = E\left(\frac{c}{a}\right)\right\} \text{ and}$$

$$\mathcal{F}_{n/q_2=q_1+1} = \left\{(a,b,c) \in \mathcal{F}_n, E\left(\frac{b}{a}\right) = E\left(\frac{c}{a}\right)+1\right\}$$

where $E(\,)$ is the integer part function.

Remark 4.1. $\mathcal{F}_n = \{(x,y,z) \in F_n, z = y+1\}$ and $\mathcal{F}_n \subset F_n$.

We have, the following result.

Proposition 4.1. Let $n \geq 2$ an integer and $\mathcal{F}_{n/q_2=q_1+1}$ as previously defined. We have:

$$\mathcal{F}_{n/q_2=q_1+1} = \varnothing$$

Proof. We proceed by absurd, supposing that $\mathcal{F}_{n\setminus q_1=q_2} \neq \varnothing$. So, we have:

$$\begin{aligned}
\mathcal{F}_{n/q_2=q_1+1} = \varnothing &\Rightarrow \exists (a,b,c) \in F_n, c-b=1 \text{ and } q_2 = q_1+1 \\
&\Rightarrow a = 1 + r_1 - r_2 \text{ with } r_1, r_2 < a \text{ according to Lemma 2.7.} \\
&\Rightarrow a < 1 + a - 1 - r_2 \text{ according to Lemma 2.8} \\
&\Rightarrow r_2 < 0 \Rightarrow \square
\end{aligned}$$

Hence the result.

Proof of **Theorem 3.** Theorem 3 is an immediate consequence of Proposition 4.1.

Remark 4.2. When $n=2$, the following Python program calculates Pythagorean triplets that verify whether Theorem 3. The program also tests this proposition.

Indeed, the program of **Figure 2** calculates respectively the number of Pythagorean triplets such that $c-b=1$ and ($c-b=1$ and $q_1 = q_2$). Then, it compares these two numbers to check the theorem 3: if there is equality the theorem 3 is checked otherwise it is not. This program also computes Pythagorean triplets (a,b,c) such that $c-b=1$ and it's Pythagorean quotients and remainders. The results in **Table 2** show that the theorem 3 is verified for the range of Pythagorean triplets tested.

The OK in the last row of **Table 2** means that in the defined range, the Pythagorean triples such that $c-b=1$ are of the same number as the triplets satisfying $c-b=1$ and $q_2 = q_1$.

```
Import math
def verify_theo3(M,N):
    k=0; l=0 ;
    for a in range(M,N):
        for b in range(a+1,math.floor(a*(a/2+1))):
            for c in range(b,b+a):
                if a*a+b*b==c*c:
                    if c==b+1:
                        k=k+1
                        q1=b//a; q2=c//a
                        if q1==q2:
                            l=l+1
                            print(a,b,c,q1,q2)
    if k==l: print("OK")
```

Figure 2. Python program compute Pythagorean triplets such as $c-b=1$ or $q_1=q_2$ and verify theorem 3.

Table 2. Result of very_theo3(3, 16) showing that theorem 3 is true for Pythagorean triplets (a,b,c) where $3\le a<16$.

$(a,b,c)\in F_2$			q_1	q_2
3	4	5	1	1
5	12	13	2	2
7	24	25	3	3
9	40	41	4	4
11	60	61	5	5
13	84	85	6	6
15	112	113	7	7
OK				

Proof of **Theorem 4.**

On the one hand, suppose that $q_1=q_2$ and $r_1>r_2$. We have

$q_1=q_2$ and $r_1>r_2\Rightarrow r_2>r_1$ because of Theorem 1

$\Rightarrow\square$

Hence $q_1=q_2$ and $r_2>r_1$

On the other hand, suppose that $q_1+1=q_2$ and $r_1<r_2$. We have

$q_1+1=q_2$ and $r_2>r_1\Rightarrow r_2<r_1$ because of Theorem 2

$\Rightarrow\square$

Hence $q_2=q_1+1$ and $r_1>r_2$.

Remark. When n = 2, theorem 4 becomes the Pythagorean Quotients and Remainders Theorem (PQR Theorem). In this case, the Quotients and Remainders are said Pythagorean and we can compute them (see Table 1).

5. Conclusions

In this paper we have shown that if (a,b,c) is a solution of the Fermat equation and (q_1,q_2) and (r_1,r_2) are its Diophantine quotients and remainders, then $q_2 = q_1$ if and only if $r_2 - r_1 > 0$ and $q_2 = q_1 + 1$ if and only if $r_2 - r_1 < 0$. These new properties used efficiently allowed us to find new properties verified by the Pythagorean triplets and to prove algebraically an important partial result of the FLT. This study opens new perspectives in the study of Diophantine equations and their applications. Here are some issues that can arise: Let (a,b,c) be a solution of Pythagoras'-Fermat's equation with (q_1,q_2) and (r_1,r_2) its Diophantine quotients and remainders:

1) In the case of Pythagorean triplets, we must solve the following questions.

a) q_1 is it increased or not (study the evolution of q_1)?

b) Which is new expression of r_2 when $q_2 = 1$?

c) New classification of (a,b,c) use Diophantine quotients and remainders properties and possible cryptographic applications.

2) In the case of FLT being false, we have the following conjectures:

a) If $n = p$ is a prime and $q_2 = 1$ then $\begin{cases} r_2 = \dfrac{e^p}{p} \text{ if } b \equiv 0[p] \\ r_2 = e^p \text{ otherwise} \end{cases}$ with e is Fermat principal divisor of b [10].

b) If $n = p$ is a prime then p is bounded ($p < N, N \in \mathbb{N}$).

c) If $n = p$ is a prime then $q_1 = 1$ and $r_1 = 1$ or 2.

3) Generalize Diophantine quotients and remainders to variants of Fermat's equation such as Equations (2) and (3).

Conflicts of Interest

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

References

[1] Planet Maths (2004) Free Encyclopedia of Mathematics 0.0.1. 459-462. https://documents.pub/document/free-encyclopaedia-of-mathematics-vol1.html

[2] Davenport, H. (2008) The Higher Arithmetic: An Introduction to the Theory of Numbers. 8th Edition, Cambridge University Press, London, 137-164. https://doi.org/10.1017/CBO9780511818097

[3] Tanoé, F.E. and Kimou, P.K. (2023) Pythagorician Divisors and Applications to Somme Diophantine Equations. *Advances in Pure Mathematics*, **13**, 35-70. https://doi.org/10.4236/apm.2023.132003

[4] Arthan, L. and Bujur, R. (2014) Data Encryption and Decryption Using New Pythagorean Triple Algorithm. *Proceeding of the World Congress on Engineering*, London, UK, 2-4 July 2014.

[5] Trivedi, R.A. and Bhanotar, S.A. (2015) Pythagorean Triplets—Views, Analysis and Classification. *IOSR Journal of Mathematics*, **11**, 54-63.

[6] Delahaye, J.-P. (2020) Dans les arcanes des triplets pythagoriciens. *Pour la science*, 80-85. https://doi.org/10.3917/pls.514.0080

[7] Paulo, R. (1999) Fermat's Last Theorem for Amateurs. Springer-Verlag New-York Inc., New-York.

[8] Nag. B.B. (2021) An Elementary Proof of Fermat's Last Theorem for Epsilon. *Advanced in Pures Mathematics*, **11**, 735-740. https://doi.org/10.4236/apm.2021.118048

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

[10] Kimou, P.K. (2023) On Fermat Last Theorem: The new Efficient Expression of a Hypothetical Solution as a function of its Fermat Divisors. *American Journal of Computational Mathematics*, **13**, 82-90. https://doi.org/10.4236/ajcm.2023.131002

[11] Beji, S. (2021) A Variant of Fermat's Diophantine Equation. *Advances in Pure Mathematics*, **11**, 929-936. https://doi.org/10.4236/apm.2021.1112059

[12] Scheinman, L.J. (2006) On the Solution of the Cubic Pythagorean Diophantine Equation $x^3 + y^3 + z^3 = a^3$. *Missouri Journal of Mathematical Sciences*, **18**, 3-16. https://doi.org/10.35834/2006/1801003