DOI: 10.1478/AAPP.1021A3

AAPP | Atti della Accademia Peloritana dei Pericolanti
Classe di Scienze Fisiche, Matematiche e Naturali
ISSN 1825-1242

Vol. 102, No. 1, A3 (2024)

ON THE ALGEBRAIC STRUCTURE OF PYTHAGOREAN TRIPLES

GIUSEPPINA ANATRIELLO [a] AND GIOVANNI VINCENZI [b*]

(communicated by Liliana Restuccia)

ABSTRACT. A Pythagorean triple is an ordered triple of integers $(a,b,c) \neq (0,0,0)$ such that $a^2+b^2=c^2$. It is well known that the set $\mathfrak{P}$ of all Pythagorean triples has an intrinsic structure of commutative monoid with respect to a suitable binary operation, $(\mathfrak{P},\star)$. In this article, we will introduce the "commensurability" relation $\mathfrak{R}$ among Pythagorean triples, and we will see that it induces a group quotient, $\mathfrak{P}/\mathfrak{R}$, which is isomorphic with the direct product of infinite (countable) copies of C_∞, the infinite cyclic group, and a cyclic group of order 4. As an application, we will see that the acute angles of Pythagorean triangles are irrational when measured in degrees.

1. Introduction

In literature by *Pythagorean tern* we usually mean a set of three non-negative integers such that the square of one of them is the sum of the squares of the other two. The trivial cases are:

$$a^2+0^2=a^2$$

Except for the trivial cases, the elements of a Pythagorean tern are three distinct positive integers. Usually, such a set is simply denoted by $\{a,b,c\}$; for example, $\{3,4,5\}$ is the *first Pythagorean tern*. A non-trivial Pythagorean tern (resp. a non-trivial Pythagorean triple) is said to be *primitive* if their terms are coprime. Pythagorean terns have been studied and enumerated since Babylonian times, and many mathematicians from Euclid, through Fibonacci, Fermat, Euler, and Gauss up to our contemporary mathematicians, have deeply studied this topic (see Alperin 2005; Maor 2007; Murray 2013, and references therein). Note that, if we put c to be the maximum of the three terms of a Pythagorean tern $\{a,b,c\}$, then c is positive and the following Pythagorean identities hold:

$$(\mp a)^2+(\mp b)^2=c^2.$$

A triple $(a,b,c) \in \mathbb{Z}\times\mathbb{Z}\times\mathbb{N}$ is said to be *Pythagorean* if $a^2+b^2=c^2$. Thus, given a non-trivial Pythagorean tern $\{a,b,c\}$ with the maximum term c we may associate eight ordered distinct Pythagorean triples:

$$(a,b,c),(-a,b,c),(a,-b,c),(-a,-b,c),(b,a,c),(-b,a,c),(b,-a,c),(-b,-a,c).$$

Conversely, if (a,b,c) is a Pythagorean triple, then $\{|a|,|b|,c\}$ defines a Pythagorean tern.

The aim of this article is to investigate, using elementary methods, the set

$$\mathfrak{P} = \{(a,b,c) \in \mathbb{Z}\times\mathbb{Z}\times\mathbb{N}: \quad a^2+b^2=c^2\}$$

of all Pythagorean triples, pointing out the main algebraic aspects and their consequences. As operation between triples, we will use a composition "$\star$" inspired by that introduced by Eckert (1984, p. 22, Eq. (2)) and Taussky (1970).

We highlight that our results are in line with and not dependent on those obtained by Eckert (1984, p. 24), and Jitman and Sangwisut (2022). In fact, Eckert focused his investigation on the collection $\mathfrak{P}_1$ of all *Pythagorean triangles*, which are right triangles with integer sides. He used geometric properties of the hypocycloids and results on the values that the trigonometric functions assume on angles that are rational in degrees (see Niven 1985) to prove that $\mathfrak{P}_1$ is an abelian torsion-free group. After he proved that $\mathfrak{P}_1$ is a free abelian group. In this way, he gave an indirect algebraic interpretation to the set of Pythagorean triples with all positive terms. Similarly, Jitman and Sangwisut considered the set $\mathfrak{P}_2$ of the primitive Pythagorean triples (a,b,c), such that a and c are odd positive integers and b is an even integer (which can be zero or negative). Then they introduced a binary operation different from those introduced by Eckert (1984, p. 22, Eq. (2)) and Taussky (1970). Thereafter, starting from the properties of hyperbolic numbers, they have provided a complete description of the structure of $\mathfrak{P}_2$ as a free abelian group.

The nature of our proofs are arithmetic and are based on elementary results on positive integers which are sums of two squares (see Section **3**). In Section **4**, we have introduced the "commensurability" relation $\mathfrak{R}$ among all Pythagorean triples, and than we have described the structure of $\mathfrak{P}/\mathfrak{R}$ (see Theorem **4.8**). As an application of our main result, we prove the so-called "Governor's theorem", which provides restrictions on the angle values of a Pythagorean triangle (see Theorem **5.1**). This shows another connection between Pythagorean triples and number theory.

The paper is suitable for a large audience.

2. Pythagorean terns and Pythagorean triples

Definition 2.1. A Pythagorean tern (resp. triple) $\{a,b,c\}$ with the maximum term c, is said to be *trivial* if either a or b is 0. Respectively, all trivial Pythagorean triples appear as follows:

$$(a,0,a),(0,b,b),(-a,0,a),(0,-b,b).$$

In order to produce non-trivial Pythagorean terns, and hence non-trivial Pythagorean triples, there is a very satisfactory classic result due to Euclid (see, for example, Joyce 1997, Book X , Proposition XXIX) or Maor (2007, Sec. 1):

Proposition 2.1 (Euclid's formula)**.** *Let m and n be positive integers, with $m>n$. Then $\{m^2-n^2,\ 2mn,\ m^2+n^2\}$ is a non-trivial Pythagorean tern.*

Remark **2.1**. Let $\{m^2-n^2,\ 2mn,\ m^2+n^2\}$ be a Pythagorean tern (m and n positive numbers). Note that m^2+n^2 is the maximum term among the three, moreover, $m^2-n^2 \neq 2mn$, and the greatest between them depends on the choice of m and n (see Table **2.1**).

TABLE **2.1**. Initial Pythagorean terns produced by Euclid's formula

m	n	m^2-n^2 , 2mn , m^2+n^2	
2	1	3, 4, 5	Primitive
3	1	8, 6, 10	Derivate
3	2	5, 12, 13	Primitive
4	1	15, 8, 17	Primitive
4	2	12, 16, 20	Derivate
4	3	7, 24, 25	Primitive
5	1	24, 10, 26	Derivate
5	2	21, 20, 29	Primitive
5	3	16, 30, 34	Derivate
5	4	9, 40, 41	Primitive

A Pythagorean tern that is not primitive is said to be *derivate*. Clearly, if $\{a,b,c\}$ is a Pythagorean tern, then for any positive integer $n>1$, $\{na,nb,nc\}$ is a derivate Pythagorean tern. Thus, the "relevant" Pythagorean terns are the primitive ones. How can we determine all primitive terns? Despite Euclid's formula does not produce all Pythagorean terns – for example, $\{9,12,15\}$ –, all primitive terns can be obtained by it (see Maor 2007, Appendix B):

Lemma 2.2. *For every primitive Pythagorean tern $\{a,b,c\}$ there exist two coprime positive integers $m>n$ such that $\{a,b,c\}=\{m^2-n^2,\ 2mn,\ m^2+n^2\}$.*

Remark **2.2**. We note that the most natural way to prove the Lemma **2.2** consists in solving a system of three "Diophantine" equations. Probably, this result was already known to Diophantus, but to the best of our knowledge its paternity is not established.

The following characterization of primitive terns holds (see Maor 2007, p. 11; Mollin 2008, Theorem 7.6; Moreno and Wagstaff Jr. 2005, Theorem 7.6).

Proposition 2.3. *Let $m>n$ be two positive integers. Then the tern $m^2-n^2,\ 2mn,\ m^2+n^2$ is primitive if and only if m and n are coprime and $m+n$ is an odd integer.*

3. Sums of two squares: recalls and technical lemmas

By Euclid's formula, studying Pythagorean triples is connected with the following problem:

which integers are the sum of two squares?

In this order, it will be useful to recall some basic results. The first one is the famous formula of Diophantus and Brahmagupta (see Moreno and Wagstaff Jr. 2005, p. 320, Eq. 8.1):

$$(a^2+b^2)(c^2+d^2)=(ac-bd)^2+(ad+bc)^2=(ac+bd)^2+(ad-bc)^2. \qquad \textbf{(3.1)}$$

Remark **3.1**. We note that the Diophantus - Brahmagupta identity (Eq.(**3.1**)) can be also derived by using complex numbers. Precisely, if $z = a + ib$ and $z' = c + id$, then $zz' = ac - bd + i(ad + bc)$, so that:

$$|z|^2 \left|z'\right|^2 = \left|zz'\right|^2 \iff (a^2+b^2)(c^2+d^2) = (ac-bd)^2 + (ad+bc)^2$$

This kind of problem was also studied by Fibonacci in the thirteenth century and Bachet in the seventeenth century (Dickson 2012). The first to correctly formulate necessary and sufficient conditions for an integer to be a sum of two squares (see next Theorem **3.1**) was Albert Girard (1595 –1632), and so the following is often referenced as the Girard's Theorem. Some years later on December 25, 1640, (so it is also referred to as *Christmas Theorem*), Fermat stated these conditions independently in a letter to Mersenne and claimed he had an iron-clad proof, which he did not publish. The first published proof was given by Euler in 1754 (see Mollin 2008, Theorem 6.1).

Theorem 3.1 (Euler)**.** *An odd prime $p = a^2 + b^2$ for $a, b \in \mathbb{N}$ if and only if $p \equiv 1 (mod 4)$. Moreover, when such a representation exists, it is unique (ignoring the order of the summands).*

Note that if $n \in \mathbb{N}$ admits a representation as the sum of two two integer squares, $n = a^2 + b^2$, then we may suppose that a and b are positive.

Definition 3.1. (See Mollin 2008, Definition 6.1, p. 247) A representation of $n \in \mathbb{N}$ as a sum of two integer squares, $n = a^2 + b^2$, is said to be *primitive* if $(a, b) = 1$.

Clearly, if a prime p admits a representation as a sum of two squares, then this representation must be primitive.

Remark **3.2**. Note that the prime $p = 2$, admits a trivial representation as the sum of two squares: $2 = 1 + 1$. If we force the Euclid's formula with $m = n = 1$, we see that this primitive representation produces a trivial Pythagorean tern: $\{0, 2, 2\}$.

The quoted Euler's result is a particular case of a general theorem that gives the number of primitive representations of a positive integer n as sums of two squares:

Theorem 3.2. *(See Mollin 2008, Theorem 6.3, p. 247) The number $r_2(n)$ of primitive representations of $n > 1$ as a sum of two integer squares is given by*

$$r_2(n) = \begin{cases} 0 & if\, 4 \text{ divides } n \text{ or if there is a prime } p \equiv 3 (mod\ 4) \text{ dividing } n; \\ 2^{d-1} & if\, 4 \text{ doesn't divide } n, \text{ there is no prime } p \equiv 3 (mod\ 4) \text{ dividing } n, \\ & \text{and } d \text{ is the number of distinct odd prime divisors of } n. \end{cases}$$

In particular, we have the following result:

Proposition 3.3. *Let p be an odd prime $p \equiv 1 (mod 4)$. Then for every positive integer h there exists a unique Pythagorean primitive triple (a, b, p^h) of the type $0 < a < b < p^h$.*

Proof. By hypothesis $p \equiv 1 (mod 4)$ and hence $p^h \equiv 1 (mod 4)$, then by Theorem **3.2**, p^h admits exactly one primitive representation as sum of two squares:

$$p^h = u^2 + v^2, \quad \text{where} \quad 0 < v < u \quad \text{and} \quad (u, v) = 1. \tag{**3.2**}$$

Now, put $a = min\{u^2 - v^2, 2uv\}$ and $b = max\{u^2 - v^2, 2uv\}$. Clearly, a and b are coprime, so that (a, b, p^h) is a primitive. Moreover, as $(p^h)^2 \equiv 1(mod 4)$, by Theorem **3.2**, $a^2 + b^2 = (p^h)^2$ is the unique representation of $(p^h)^2$ as sum of two squares, then (a, b, p^h) is the unique Pythagorean primitive triple of the type $0 < a < b < p^h$. □

Definition 3.2. In the following, when $p \equiv 1(mod\ 4)$, we will refer to the unique primitive triple $(a(p^h), b(p^h), p^h)$ of the type $0 < a(p^h) < b(p^h) < p^h$ as *the principal Pythagorean triple of the maximum term* p^h.

Remark **3.3**. Let $p \equiv 1(mod\ 4)$, and consider $(a(p), b(p), p^h)$ the principal Pythagorean triple with the maximum term p^h. Then we have exactly eight primitive triples with the maximum term p^h. They can be listed as follows:

$$(\mp a(p), \mp b(p), p^h), (\mp b(p), \mp a(p), p^h).$$

Remark **3.4**. We note that powers of prime numbers may be the third component of distinct Pythagorean triples. For example, $(15, 20, 25)$ and $(7, 24, 25)$ are Pythagorean triples. Note that the first one is not primitive.

The following technical results will be useful for our purpose:

Lemma 3.4. *Let p be a prime odd number, and* $h, k \in \mathbb{N}$. *If* $p^h = a^2 + b^2$ *and* $p^k = c^2 + d^2$ *with (a,b)=1 and (c,d)=1, then either* $(ac - bd)$ *is coprime with* $(ad + bc)$ *or* $(ac + bd)$ *is coprime with* $(ad - bc)$.

Proof. By Diophantus-Brahmagupta Identity (Eq. (**3.1**)) we have:

$$p^{h+k} = (a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2 = (ac + bd)^2 + (ad - bc)^2. \quad \textbf{(3.3)}$$

By contradiction, assume that the statement is false. Then, by Eq. (**3.3**) p divides both $(ac - bd)$ and $(ac + bd)$, hence p divides $2ac$. If p divides a, we have a contradiction, as $p^h = a^2 + b^2$ and $(a, b) = 1$; similarly, if p divides c, we have a contradiction, as $p^k = c^2 + d^2$ with and $(c, d) = 1$. □

Lemma 3.5. *Let* $(a, b) = 1$ *and* $(c, d) = 1$. *If* $c^2 + d^2$ *divides* $a^2 + b^2$ *and* $c^2 + d^2 = p^\alpha$, *with p prime and* $\alpha \in \mathbb{N}$, *then there exist m and n coprime integers, such that*

1) $a^2 + b^2 = (m^2 + n^2)(c^2 + d^2)$,
2) $b = mc + nd, \quad a = |md - nc|$.

Proof. In order to find pairs (m, n) as required, we first solve the following systems:

$$\begin{cases} cx + dy &= b \\ dx - cy &= a \end{cases}, \quad \text{and} \quad \begin{cases} cx + dy &= b \\ -dx + cy &= a \end{cases}. \quad \textbf{(3.4)}$$

As $c^2 + d^2 \neq 0$, each of the above systems has just one solution. Respectively:

$$(m_1, n_1) = \left(\frac{bc + ad}{c^2 + d^2}, \frac{ac - bd}{c^2 + d^2} \right) \quad \text{and} \quad (m_2, n_2) = \left(\frac{bc - ad}{c^2 + d^2}, \frac{ac + bd}{c^2 + d^2} \right). \quad \textbf{(3.5)}$$

Clearly, both (m_1, n_1) and (m_2, n_2) satisfy the second requirement of the statement. On the other hand, an easy computation shows that

$$m_1^2+n_1^2=m_2^2+n_2^2=(a^2+b^2)/(c^2+d^2)\in\mathbb{N}. \tag{3.6}$$

Thus, to complete the proof it suffices to prove that either (m_1,n_1) or (m_2,n_2) is composed of coprime integers. In this order, note that by hypothesis $p^\alpha=c^2+d^2$ divides both $c^2a^2+c^2b^2$ and $c^2a^2+d^2a^2$, so that p^α divides $b^2c^2-a^2d^2=(bc+ad)(bc-ad)$. By hypothesis $(c,d)=1$, thus $p\nmid c$ and $p\nmid d$. Now suppose that p divides both the factors $(bc+ad)$ and $(bc-ad)$, then p divides $2bc$ and $2ad$, and hence p divides both a and b. This contradicts the hypothesis, as $(a,b)=1$. Then p^α either divides $(bc+ad)$ or $(bc-ad)$. Therefore, by Eq. (**3.5**), either m_1 or m_2 must be an integer.

If m_1 is an integer, then, by Eq. (**3.6**), n_1 is a rational number whose square is an integer, thus n_1 is likewise an integer. We have proved that (m_1,n_1) is a pair of integers that is a solution of the first system of (**3.4**). In particular, every common divisor of m_1 and n_1 must divide both a and b. By hypothesis, $(a,b)=1$, then m_1 and n_1 are coprime.

Similarly, also in the case that m_2 is an integer, we can prove that m_1 and n_1 are coprime. The proof is complete. □

4. The group of primitive Pythagorean triples

In this section, according to Eckert (1984), we will see that the set of all Pythagorean triples

$$\mathfrak{P}:=\{(a,b,c)\in\mathbb{Z}\times\mathbb{Z}\times\mathbb{N}:a^2+b^2=c^2\}$$

has a proper natural algebraic structure. Note that by Eq. (**3.1**), if $(a,b,c),(a',b',c')$ belongs to $\mathfrak{P}$, then also $(aa'-bb',ba'+b'a,cc')$ lies in $\mathfrak{P}$, therefore, we may consider the following operation:

$$\star:((a,b,c),(a',b',c'))\in\mathfrak{P}\times\mathfrak{P}\to(a,b,c)\star(a',b',c'):=(aa'-bb',ba'+b'a,cc')\in\mathfrak{P},$$

Theorem 4.1. $(\mathfrak{P},\star)$ *is a commutative monoid.*

Proof. It is easy to check that $\star$ is a commutative operation and that $(1,0,1)$ is the identity of $\mathfrak{P}$.

Now we check that $\star$ is associative. Let $(a,b,c),(a',b',c'),(a'',b'',c'')\in\mathfrak{P}$.

Then

$$\big((a,b,c)\star(a',b',c')\big)\star(a'',b'',c'')=(a,b,c)\star\big((a',b',c')\star(a'',b'',c'')\big).$$

In fact

$$\begin{aligned}&\big((a,b,c)\star(a',b',c')\big)\star(a'',b'',c'')=(aa'-bb',ba'+b'a,cc')\star(a'',b'',c'')\\&=((aa'-bb')a''-(ba'+b'a)b'',(ba'+b'a)a''+b''(aa'-bb'),cc'c'')\\&=(aa'a''-bb'a''-ba'b''-b'ab'',\ ba'a''+b'aa''+b''aa'-b''bb',cc'c'').\end{aligned}$$

$$\begin{aligned}&(a,b,c)\star((a',b',c')\star(a'',b'',c''))=(a,b,c)\star(a'a''-b'b'',b'a''+b''a',c'c'')\\&=(a(a'a''-b'b'')-b(b'a''+b''a'),\ b(a'a''-b'b'')+a(b'a''+b''a'),cc'c'')\\&=(aa'a''-ab'b''-bb'a''-bb''a',\ ba'a''-bb'b''+ab'a''+ab''a',cc'c'').\end{aligned}$$

□

The above theorem allows us to produce Pythagorean triples as the product of two given Pythagorean triples. See the next examples:

Example **4.1**.

$$(4,3,5)\star(5,12,13)=(-16,63,65).$$

Special cases are the powers of a triple. Below there are the first 5 powers of $(3,4,5)$:

$$(3,4,5)^2=(3,4,5)\star(3,4,5)=(-7,24,25),$$

$$(3,4,5)^3=(3,4,5)\star(-7,24,25)=(-117,44,125),$$

$$(3,4,5)^4=(-7,24,25)\star(-7,24,25)=(-527,-336,625),$$

$$(3,4,5)^5=(-7,24,25)\star(-117,44,125)=(-237,-3116,3125).$$

Remark **4.1**. Note that $(\mathfrak{P},\star)$ is not a group, as it contains only the following units:

$$(1,0,1),\ (0,1,1)\ (-1,0,1),\ (0,-1,1),$$

for which, the following composition rules yield:

i) $(0,1,1)\star(0,1,1)=(-1,0,1)$;
ii) $(0,1,1)\star(-1,0,1)=(0,-1,1)$;
iii) $(0,1,1)\star(0,-1,1)=(1,0,1)$.

Remark **4.2**. By Remark **4.1**, $C=\langle(0,1,1)\rangle=\{(1,0,1),(0,1,1),(-1,0,1),(0,-1,1)\}$ is a finite cyclic subgroup of $\mathfrak{P}$ of order 4. In $(\mathfrak{P},\star)$ the following composition rules yield:

i) $(a,b,c)\star(1,0,1)=(a,b,c)$;
ii) $(a,b,c)\star(-1,0,1)=(-a,-b,c)$;
iii) $(a,b,c)\star(0,-1,1)=(+b,-a,c)$;
iv) $(a,b,c)\star(0,1,1)=(-b,a,c)$.

In $(\mathfrak{P},\star)$ it is natural to consider the following equivalence relation $\mathfrak{R}$:

$$(a,b,c)\mathfrak{R}(a_1,b_1,c_1)\iff\exists n,m\in\mathbb{Z}\setminus\{0\}:ma=na_1,mb=nb_1,mc=nc_1.$$

In this case we will say that (a,b,c) and (a_1,b_1,c_1) are *commensurable*.

Example **4.2**.

i) $(6,-8,10)\mathfrak{R}(3,-4,5)$; and $(6,-8,10)\mathfrak{R}(9,-12,15)$;
ii) $(6,-8,10)\ \not\mathfrak{R}(3,4,5)$ and $(6,-8,10)\ \not\mathfrak{R}(9,12,15)$;
iii) $[(10,-24,26)]_{\mathfrak{R}}=[(5,-12,13)]_{\mathfrak{R}}$.

Lemma 4.2. *For every class $X\in\mathfrak{P}/\mathfrak{R}$ there exists a unique primitive triple of $\mathfrak{P}$ that belongs to X.*

Proof. Let $[(a',b',c')]]_{\mathfrak{R}}\in\mathfrak{P}/\mathfrak{R}$, and let d be the positive greater common divisor of $\{a',b',c'\}$. Put

$$a:=\frac{a'}{d},\qquad b:=\frac{b'}{d},\qquad c:=\frac{c'}{d}.$$

Then (a,b,c) is a primitive triple that belongs to X.

Now, let $(e,f,g) \in X$ be a primitive triple, then there exists $m/n \in \mathbb{Q}$ such that $(n,m) = 1$ and $m(e,f,g) = n(a,b,c)$. It follows that n divides e, f and g and m divides a, b and c. Thus, $m = n = 1$, and $(e,f,g) = (a,b,c)$. □

Remark **4.3**. Note that if a triple (a',b',c') is commensurable to a primitive triple (a,b,c), that is (a',b',c') belongs to $[(a,b,c)]_{\mathfrak{R}}$, then a divides a', b divides b', and c divides c'.

Remark **4.4**. $\mathfrak{R}$ is a congruence in $(\mathfrak{P},\star)$, in fact, if $(a,b,c)\mathfrak{R}(a_1,b_1,c_1)$ and $(a',b',c')\mathfrak{R}(a'_1,b'_1,c'_1)$, then $(a,b,c) = z(a_1,b_1,c_1)$ and $(a',b',c') = z'(a'_1,b'_1,c'_1)$ where $z,z' \in \mathbb{Q}$. So we have

$$(aa'-bb',ba'+ba',cc') = zz'(a_1a'_1-b_1b'_1,b_1a'_1+b_1a'_1,c_1c'_1).$$

It follows that

$$[(aa'-bb',ba'+b'a,cc')]_{\mathfrak{R}} = [(a_1a'_1-b_1b'_1,b_1a'_1+b'_1a_1,c_1c'_1)]_{\mathfrak{R}},$$

and so that

$$(a,b,c)\star(a',b',c') \quad \mathfrak{R} \quad (a_1,b_1,c_1)\star(a'_1,b'_1,c'_1).$$

Thus, we may consider the induced quotient operation in $G := \mathfrak{P}/\mathfrak{R}$:

$$\star : ([(a,b,c)]_{\mathfrak{R}},[(a',b',c')]_{\mathfrak{R}}) \in G\times G \to [(a,b,c)]_{\mathfrak{R}}\star[(a',b',c')]_{\mathfrak{R}} \in G,$$

defined by $[(a,b,c)]_{\mathfrak{R}}\star[(a',b',c')]_{\mathfrak{R}} := [(aa'-bb',ba'+b'a,cc')]_{\mathfrak{R}}$.

As a quotient of $(\mathfrak{P},\star)$, G is likewise a monoid. Indeed, it turns out that G is a group.

Theorem 4.3. *$(G,\star)$ is an abelian group.*

Proof. We have just to check that every element of G is invertible. For, let $[(a,b,c)]_{\mathfrak{R}} \in G$, then $[(a,b,c)]_{\mathfrak{R}}\star[(a,-b,c)]_{\mathfrak{R}} = [(aa+bb,0,cc)]_{\mathfrak{R}} = [(c^2,0,cc)]_{\mathfrak{R}} = [(1,0,1)]_{\mathfrak{R}}$. In other terms $[(a,b,c)]^{-1}_{\mathfrak{R}} = [(a,-b,c)]_{\mathfrak{R}}$. □

Definition 4.1. As every element of G can be represented by a unique primitive Pythagorean triple (see Lemma **4.2**), we will call G as *the group of primitive Pythagorean triples*.

We highlight the following properties of $(G,\star)$ that are inherited from $(\mathfrak{P},\star)$.

Remark **4.5**. By Remark **4.1** and Remark **4.2** we have that

$C_4 := \langle[(0,1,1)]_{\mathfrak{R}}\rangle = \{[(1,0,1)]_{\mathfrak{R}},[(0,1,1)]_{\mathfrak{R}},[(-1,0,1)]_{\mathfrak{R}},[(0,-1,1)]_{\mathfrak{R}}\}$ is a cyclic subgroup of G of finite order 4. Moreover, the following rules yield:

i) $[(a,b,c)]_{\mathfrak{R}}\star[(1,0,1)]_{\mathfrak{R}} = [(a,b,c)]_{\mathfrak{R}}$,
ii) $[(a,b,c)]_{\mathfrak{R}}\star[(-1,0,1)]_{\mathfrak{R}} = [(-a,-b,c)]_{\mathfrak{R}}$,
iii) $[(a,b,c)]_{\mathfrak{R}}\star[(0,-1,1)]_{\mathfrak{R}} = [(+b,-a,c)]_{\mathfrak{R}}$,
iv) $[(a,b,c)]_{\mathfrak{R}}\star[(0,1,1)]_{\mathfrak{R}} = [(-b,a,c)]_{\mathfrak{R}}$,
v) $[(a,b,c)]^{-1}_{\mathfrak{R}}\star[(1,0,1)]_{\mathfrak{R}} = [(a,-b,c)]_{\mathfrak{R}}\star[(1,0,1)]_{\mathfrak{R}} = [(a,-b,c)]_{\mathfrak{R}}$,
vi) $[(a,b,c)]^{-1}_{\mathfrak{R}}\star[(-1,0,1)]_{\mathfrak{R}} = [(a,-b,c)]_{\mathfrak{R}}\star[(-1,0,1)]_{\mathfrak{R}} = [(-a,b,c)]_{\mathfrak{R}}$,
vii) $[(a,b,c)]^{-1}_{\mathfrak{R}}\star[(0,-1,1)]_{\mathfrak{R}} = [(a,-b,c)]_{\mathfrak{R}}\star[(0,-1,1)]_{\mathfrak{R}} = [(-b,-a,c)]_{\mathfrak{R}}$,
viii) $[(a,b,c)]^{-1}_{\mathfrak{R}}\star[(0,1,1)]_{\mathfrak{R}} = [(a,-b,c)]_{\mathfrak{R}}\star[(0,1,1)]_{\mathfrak{R}} = [(+b,a,c)]_{\mathfrak{R}}$.

In particular, for every Pythagorean triple (a,b,c) the subgroup $\langle[(a,b,c)]_{\mathfrak{R}}\rangle \cdot \langle[(0,1,1)]_{\mathfrak{R}}\rangle$ contains all the eight elements:

$$[(a,b,c)]_{\mathfrak{R}}, [(a,-b,c)]_{\mathfrak{R}}[(-a,b,c)]_{\mathfrak{R}}, [(-a,-b,c)]_{\mathfrak{R}},$$
$$[(b,a,c)]_{\mathfrak{R}}, [(b,-a,c)]_{\mathfrak{R}}, [(-b,a,c)]_{\mathfrak{R}}, [(-b,-a,c)]_{\mathfrak{R}}.$$

Remark **4.6**. Every trivial Pythagorean triple, $(a,0,a)$, $(0,b,b)$, $(-a,0,a)$, $(0,-b,b)$, belongs to one of the following class:

$$[(1,0,1)]_{\mathfrak{R}}, [(0,1,1)]_{\mathfrak{R}}, [(-1,0,1)]_{\mathfrak{R}}, [(0,-1,1)]_{\mathfrak{R}}.$$

In other terms, the class represented by a trivial Pythagorean triple is one of the elements of the finite cyclic group $C_4 = \langle[(0,1,1)]_{\mathfrak{R}}\rangle$.

Lemma 4.4. *Let p be a prime number such that $p \equiv 1 (mod\, 4)$, and let (a,b,p) be a primitive Pythagorean triple. Then for every positive integer h, there exists a unique primitive triple of the type (a_h,b_h,p^h) that belongs to $[(a,b,p)]^h_{\mathfrak{R}}$. In particular, $\langle[(a,b,p)]_{\mathfrak{R}}\rangle$ is an infinite cyclic subgroup of G.*

Proof. We show that every positive power of $[(a,b,p)]^h_{\mathfrak{R}}$ can be represented by a primitive triple of the type (a_h,b_h,p^h) then the uniqueness follows by Lemma **4.2**.

By hypothesis,(a,b,p) is a primitive Pythagorean triple, so that if $h=1$ it is enough to choose $a_1 = a$ and $b_1 = b$.

If $h=2$ we have $[(a,b,p)]_{\mathfrak{R}} \star [(a,b,p)]_{\mathfrak{R}} = [(a^2-b^2, 2ab, p^2)]_{\mathfrak{R}}$. On the other hand, a and b are coprime, so that $(a^2-b^2, 2ab, p^2)$ is likewise a primitive triple.

Suppose now that $h > 2$. By induction, we may assume that the statement is true for all positive integers i such that $1 \leq i < h$, thus there exist two pairs of integers numbers, (a_{h-1}, b_{h-1}) and (a_{h-2}, b_{h-2}), such that

$$[(a,b,p)]^{h-1}_{\mathfrak{R}} = [(a_{h-1}, b_{h-1}, p^{h-1})]_{\mathfrak{R}}, \quad \text{and} \quad [(a,b,p)]^{h-2}_{\mathfrak{R}} = [(a_{h-2}, b_{h-2}, p^{h-2})]_{\mathfrak{R}}$$

and the triples $(a_{h-1}, b_{h-1}, p^{h-1})$ and $(a_{h-2}, b_{h-2}, p^{h-2})$ are primitive. Now, we note that

$$[(a,b,p)]^h_{\mathfrak{R}} = [(a,b,p)]_{\mathfrak{R}} \star [(a,b,p)]^{h-1}_{\mathfrak{R}} = [(a_1,b_1,p)]_{\mathfrak{R}} \star [(a_{h-1}, b_{h-1}, p^{h-1})]_{\mathfrak{R}}$$
$$= [(a_1a_{h-1} - b_1b_{h-1},\ a_1b_{h-1} + b_1a_{h-1},\ p^h)]_{\mathfrak{R}}.$$

By contradiction, suppose that the triple $(a_1a_{h-1} - b_1b_{h-1},\ a_1b_{h-1} + b_1a_{h-1},\ p^h)$ is not primitive, then by Lemma **3.4** the triple $(a_1a_{h-1} + b_1b_{h-1},\ a_1b_{h-1} - b_1a_{h-1},\ p^h)$ is primitive. On the other hand

$$[(a,b,p)]^{h-2}_{\mathfrak{R}} = [(a,b,p)]_{\mathfrak{R}}{}^{-1} \star [(a,b,p)]^{h-1}_{\mathfrak{R}} = [(a_1,-b_1,p)]_{\mathfrak{R}} \star [(a_{h-1}, b_{h-1}, p^{h-1})]_{\mathfrak{R}}$$
$$= [(a_1a_{h-1} + b_1b_{h-1},\ a_1b_{h-1} - b_1a_{h-1},\ p^h)]_{\mathfrak{R}}.$$

It follows that both $(a_1a_{h-1} + b_1b_{h-1},\ a_1b_{h-1} - b_1a_{h-1},\ p^h)$ and $(a_{h-2}, b_{h-2}, p^{h-2})$ are two distinct primitive triples representing the same element $[(a,b,p)]^{h-2}_{\mathfrak{R}}$. This is a contradiction by Lemma **4.2**. We have proved that for every positive h, the h-power $[(a,b,p)]^h_{\mathfrak{R}}$ admits a primitive representation of the type:

$$[(a,b,p)]^h_{\mathfrak{R}} = [(a_1a_{h-1} - b_1b_{h-1},\ a_1b_{h-1} + b_1a_{h-1},\ p^h)]_{\mathfrak{R}}.$$

The first part of the proof shows that for every $h>1$, $[(a,b,p)]^h_{\mathfrak{R}} = [(a_h,b_h,p^h)]_{\mathfrak{R}} \neq 1_G = [(1,0,1)]_{\mathfrak{R}}$. Then $\langle [(a,b,p)]_{\mathfrak{R}} \rangle$ is an infinite cyclic subgroup of G. □

The above lemma can be extended as follows:

Corollary 4.5. *Let p be a prime number such that $p \equiv 1 (mod\ 4)$, and let (a,b,p) be a primitive Pythagorean triple. Then any non-trivial element of $\langle [(a,b,p)]_{\mathfrak{R}} \rangle$ is of the type (a_h,b_h,p^h) for suitable coprime integers a_h,b_h and $h \in \mathbb{N}$.*

Proof. Any non-trivial element of $\langle [(a,b,p)]_{\mathfrak{R}} \rangle$, is of the type $X = [(a,b,p)]^k_{\mathfrak{R}}$, where $0 \neq k \in \mathbb{Z}$.

If $k>0$, then the statement follows from Lemma **4.4**.
Let $k<0$, and put $h=-k$. Then

$$[(a,b,p)]^k_{\mathfrak{R}} = [(a,b,p)]^{(-1)(-k)}_{\mathfrak{R}} = [(a,-b,p)]^h_{\mathfrak{R}},$$

and the statement follows again by Lemma **4.4**. □

Remark **4.7**. Applying the Lemma **4.4** to an element of G represented by a principal triple $(a(p),b(p),p)$ of the maximum term p (see Definition **3.2**), we have:

i) $\langle [(a(p),b(p),p)]_{\mathfrak{R}} \rangle \cap C_4 = 1$, where $C_4 = [(0,1,1)]_{\mathfrak{R}}$ (see Remark **4.6**). It follows that the product $\langle [(a(p),b(p),p)]_{\mathfrak{R}} \rangle \star C_4 \leq G$ generated by $[(0,1,1)]_{\mathfrak{R}}$ and $[(a(p),b(p),p)]_{\mathfrak{R}}$ is a direct product: $\langle [(a(p),b(p),p)]_{\mathfrak{R}} \rangle \times C_4$.
ii) By Remark **3.3**, and Remark **4.5**, the subgroup $\langle [(a,b,p)]_{\mathfrak{R}} \rangle \times C_4$ contains all classes represented by one of the eight primitive triples of the maximum term p: $[(u,v,p)]_{\mathfrak{R}} \in \langle [(a,b,p)]_{\mathfrak{R}} \rangle \times C_4$.

Example **4.3**. It is easy to see that $[(3,4,5)]^2{}_{\mathfrak{R}} = [(-7,24,25)]_{\mathfrak{R}}$ and $[(7,24,25)]_{\mathfrak{R}} = [(4,3,5)]^2{}_{\mathfrak{R}}$, so that $[(7,24,25)]_{\mathfrak{R}}$ is not a power of $[(3,4,5)]_{\mathfrak{R}}$. Therefore, a Pythagorean triple of the type (u,v,p^h) may be not a power of the principal triple $(a(p),b(p),p)$. On the other hand, by Remark **4.7** both $[(7,24,25)]_{\mathfrak{R}}$ and $[(-7,24,25)]_{\mathfrak{R}}$ belong to $\langle [(3,4,5)]_{\mathfrak{R}} \rangle \times C_4$, where $C_4 = \langle [(0,1,1)]_{\mathfrak{R}} \rangle$. This suggests a more general result, in which the principal triples play a crucial role.

As the following two results show, if u and v are coprime integers, such that $u^2+v^2=p^{2h}$, then each of the eight classes of triples derived from the tern $\{u,v,p^h\}$:

$$[(u,v,p^h)]_{\mathfrak{R}}, \quad [(-u,v,p^h)]_{\mathfrak{R}}, \quad [(u,-v,p^h)]_{\mathfrak{R}}, \quad [(-u,-v,p^h)]_{\mathfrak{R}},$$

$$[(v,u,p^h)]_{\mathfrak{R}}, \quad [(-v,u,p^h)]_{\mathfrak{R}}, \quad [(v,-u,p^h)]_{\mathfrak{R}}, \quad [(-v,-u,p^h)]_{\mathfrak{R}}$$

lies in $\langle [(a(p),b(p),p)]_{\mathfrak{R}} \rangle \times C_4$.

Lemma 4.6. *Let p be a prime number such that $p \equiv 1 (mod\ 4)$, and let $(a(p),b(p),p)$ be the principal Pythagorean triple with the maximum term p. Let h be a positive integer and (u,v,p^h) be a primitive Pythagorean triple. Then $[(u,v,p^h)]_{\mathfrak{R}}$ has infinite order and belongs to $\langle [(a(p),b(p),p)]^h_{\mathfrak{R}} \rangle \times \langle [(0,1,1)]_{\mathfrak{R}} \rangle$.*

Proof. By Lemma **4.4** there exists a (unique) primitive triple of the type (a_h, b_h, p^h) such that $[(a(p), b(p), p)]^h_{\mathfrak{R}} = [(a_h, b_h, p^h)]_{\mathfrak{R}}$. Note that, by Remark **4.5**,

$$\langle [(a(p), b(p), p)]^h_{\mathfrak{R}} \rangle \times \langle [(0,1,1)]_{\mathfrak{R}} \rangle = [(a_h, b_h, p^h)]_{\mathfrak{R}} \times \langle [(0,1,1)]_{\mathfrak{R}} \rangle,$$

contains all the following elements, and each of them has infinite order, by Lemma **4.4**:

$$[(a_h, b_h, p^h)]_{\mathfrak{R}},\ [(a_h, -b_h, p^h)]_{\mathfrak{R}},\ [(-a_h, b_h, p^h)]_{\mathfrak{R}},\ [(-a_h, -b_h, p^h)]_{\mathfrak{R}},$$

$$[(b_h, a_h, p^h)]_{\mathfrak{R}},\ [(b_h, -a_h, p^h)]_{\mathfrak{R}},\ [(-b_h, a_h, p^h)]_{\mathfrak{R}},\ [(-b_h, -a_h, p^h)]_{\mathfrak{R}}.$$

On the other hand, by Proposition **3.3** there exists a unique primitive tern with the maximum term p^h, so that each element of G represented by a primitive Pythagorean triple of the type (u, v, p^h) must coincide with one of the above 8 elements. □

Lemma 4.7. *Let P_n be the set of the first n prime numbers p such that $p \equiv 1 (mod 4)$. For every $p \in P_n$, let $(a(p), b(p), p)$ be the principal Pythagorean triple of the maximum term p. Then the subgroup A_n of G generated by $[(a(p_1), b(p_1), p_1)]_{\mathfrak{R}}, \ldots, [(a(p_n), b(p_n), p_n)]_{\mathfrak{R}}$, where $p_i \in P_n$, is isomorphic with the direct product of n copies of an infinite cyclic group:*

$$Dr_{p \in P_i} \langle [(a(p), b(p), p)]_{\mathfrak{R}} \rangle \simeq \underbrace{C_\infty \times \ldots \times C_\infty}_{n}.$$

Proof. By Lemma **4.4**, for every $p \in P_i$, the subgroup $\langle [(a(p), b(p), p)]_{\mathfrak{R}} \rangle$ is isomorphic with a cyclic infinite group. Thus, it is enough to show:

$$A_n = Dr_{p \in P_n} \langle [(a(p), b(p), p)]_{\mathfrak{R}} \rangle.$$

If $n = 1$, it is trivial.

Let $n > 1$ and proceeding by induction suppose that $A_{n-1} = Dr_{p \in P_{n-1}} \langle [(a(p), b(p), p)]_{\mathfrak{R}} \rangle$. By contradiction suppose that X is a non-trivial element lying in $A_{n-1} \cap \langle [(a(p_n), b(p_n), p_n)]_{\mathfrak{R}} \rangle$. By Corollary **4.5**, for every $i = 1, \ldots, n$, any non-trivial element of $\langle [(a(p_i), b(p_i), p_i)]_{\mathfrak{R}} \rangle$is of the type $[(a_{i,h_i}, b_{i,h_i}, p_i^{h_i})]_{\mathfrak{R}}$ for suitable coprime integers a_{i,h_i} and b_{i,h_i} and $h_i \in \mathbb{N}$. In particular, $X = [(a_{n,h_n}, b_{n,h_n}, p_n^{h_n})]_{\mathfrak{R}}$. On the other hand, by a computation, we have

$$X = [(a_{1,h_1}, b_{1,h_1}, p_1^{h_1})]_{\mathfrak{R}} \cdots [(a_{n-1,h_{n-1}}, b_{n-1,h_{n-1}}, p_{n-1}^{h_{n-1}})]_{\mathfrak{R}} = [(u, v, p_1^{h_1} \cdots p_{n-1}^{h_{n-1}})]_{\mathfrak{R}},$$

for suitable integers u and v, so that

$$[u, v, p_1^{h_1} \cdots p_{n-1}^{h_{n-1}}]_{\mathfrak{R}} = [(a_{n,h_n}, b_{n,h_n}, p_n^{h_n})]_{\mathfrak{R}}.$$

It follows that p^{h_n} divides $p_1^{h_1} \cdots p_{n-1}^{h_{n-1}}$, by Remark **4.3**. This contradiction shows that

$$A_{n-1} \cap \langle [(a(p_n), b(p_n), p_n)]_{\mathfrak{R}} \rangle = [(1,0,1)]_{\mathfrak{R}},$$

and hence

$$A_n = A_{n-1} \star \langle [(a(p_n), b(p_n), p_n)]_{\mathfrak{R}} \rangle = A_{n-1} \times \langle [(a(p_n), b(p_n), p_n)]_{\mathfrak{R}} \rangle. \qquad \square$$

We are now in a position to describe the structure of the group G.

Theorem 4.8. *Let $G = \mathfrak{P}/\mathfrak{R}$ be the group of primitive Pythagorean triples. Then G is a direct product of a free abelian group and a finite cyclic group of order 4. Precisely:*

$$G = (Dr_{p\in P}\langle[(a(p),b(p),p)]_{\mathfrak{R}}\rangle) \times \langle[(0,1,1)]_{\mathfrak{R}}\rangle \simeq (C_\infty \times \ldots \times C_\infty \times \ldots) \times C_4,$$

where P is the set of prime (positive) numbers p such that $p \equiv 1(mod\ 4)$, and $(a(p),b(p),p)$ is the principal triple with the maximum term p.

Moreover, for every non-trivial triple $(a,b,c,)$ the element $[(a,b,c,)]_{\mathfrak{R}}$ has infinite order.

Proof. Let A be the subgroup of G generated by all elements of the type $[(a(p),b(p),p)]_{\mathfrak{R}}$, where p is a prime such that $p \equiv 1(mod\ 4)$, and let $X \in A$. Then X lies in some subgroup of the type

$$A_n = \left\langle [(a(p_1),b(p_1),p_1)]_{\mathfrak{R}}, \ldots, [(a(p_n),b(p_n),p_n)]_{\mathfrak{R}} \right\rangle,$$

where P_n is the set of the first n prime numbers p such that $p \equiv 1(mod 4)$. By Lemma **4.7**

$$A_n = \langle[(a(p_1),b(p_1),p_1)]_{\mathfrak{R}}\rangle \times \ldots \times \langle[(a(p_n),b(p_n),p_n)]_{\mathfrak{R}}\rangle \simeq \underbrace{C_\infty \times \ldots \times C_\infty}_{n}.$$

Thus X can be written in a unique way as the product of finitely many elements of the type $[(a(p),b(p),p)]_{\mathfrak{R}}$ In other terms A is a direct product of infinitely many countable copies of infinite cyclic groups:

$$A = Dr_{p\in P}\langle[(a(p),b(p),p)]_{\mathfrak{R}}\rangle.$$

Put $H := A \times \langle[(0,1,1)]_{\mathfrak{R}}\rangle$. We will show that $G = H$.

By Lemma **4.2** any element $x \in G$ can be represented by a primitive triple (u,v,r), so that $x = [(u,v,r)]_{\mathfrak{R}}$. Clearly, $\{|u|,|v|,r\}$ is a primitive Pythagorean tern, and hence, by Lemma **2.2**, there exist two coprime positive integers $a > b$ such that $\{|u|,|v|,r\} = \{a^2-b^2,\ 2ab,\ a^2+b^2\}$; in particular, $r = a^2+b^2$ is an odd integer.

Let $r = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_t^{e_t}$ be the primary decomposition of r ($p_1,\ldots,p_t$ are distinct primes and $e_1,\ldots,e_t$ are positive integers). By Theorem **3.2**, for every $i = 1\ldots t$ we have $p_i \not\equiv 3(mod\ 4)$, and hence $p_i \equiv 1(mod\ 4)$. In particular, by Theorem **3.2**, $p_1^{e_1} = c^2+d^2$, for suitable coprime integers c and d. We will prove that

$$[(u,v,r)]_{\mathfrak{R}} \in \left(Dr_{i=1}^{t}\langle[(a(p_i),b(p_i),p_i)]_{\mathfrak{R}}\rangle\right) \times \langle[(0,1,1)]_{\mathfrak{R}}\rangle \leq H.$$

If $t = 1$, then $[(u,v,r)]_{\mathfrak{R}} = [(u,v,p_1^{e_1})]_{\mathfrak{R}}$ and applying Lemma **4.6** we have

$$[(u,v,p_1^{e_1})]_{\mathfrak{R}} \in \langle[(a(p_1),b(p_1),p_1)]_{\mathfrak{R}}^{e_1}\rangle \times \langle[(0,1,1)]_{\mathfrak{R}}\rangle \leq \langle[(a(p_1),b(p_1),p_1)]_{\mathfrak{R}}\rangle \times \langle[(0,1,1)]_{\mathfrak{R}}\rangle.$$

Suppose now that $t > 1$ and proceed by induction.

Clearly, $p_1^{e_1} = c^2+d^2$ divides $r = a^2+b^2$ so that, if we put $w = \dfrac{r}{p_1^{e_1}}$, by Lemma **3.5** one of the following holds:

i) There exist m and n coprime integers such that $w = m^2+n^2$, and $b = mc+nd, \quad a = md-nc$. In particular, in this case

$$a^2-b^2 = (d^2-c^2)(m^2-n^2) - 4cdmn, \quad \text{and} \quad 2ab = (d^2-c^2)2mn + (m^2-n^2)2cd.$$

ii) There exist m and n coprime integers such that $w = m^2 + n^2$, and $b = mc + nd, \quad a = -md + nc$. In particular, in this case

$$a^2 - b^2 = (d^2 - c^2)(m^2 - n^2) - 4cdmn, \quad \text{and} \quad -2ab = (d^2 - c^2)2mn + (m^2 - n^2)2cd.$$

Clearly, $(d^2 - c^2, 2dc, p^{e_1})$ is a primitive triple, and both in the above cases, by Proposition **2.3** $(m^2 - n^2, 2mn, w)$ is likewise a primitive triple. Now, we note that the number of primes that appears in the primary decomposition of w is less than t. Thus, by induction we may suppose that the elements $[(d^2 - c^2, 2dc, p^{e_1})]_{\mathfrak{R}}$ and $[(m^2 - n^2, 2mn, w)]_{\mathfrak{R}}$ belong to H. Now we may compose them taking into account the two possible cases:

i) In this case, we have:
$$\begin{aligned}&[(d^2 - c^2, 2dc, p^{e_1})]_{\mathfrak{R}} \star [(m^2 - n^2, 2mn, w)]_{\mathfrak{R}} \\ &= [((d^2 - c^2)(m^2 - n^2) - 2dc2mn,\ (d^2 - c^2)2mn + (m^2 - n^2)2dc,\ p^{e_1}w))]_{\mathfrak{R}} \\ &= [(a^2 - b^2, 2ab, r)]_{\mathfrak{R}} \in H.\end{aligned}$$
On the other hand $\{|u|, |v|, r\} = \{|a^2 - b^2|, |2ab|, p^{e_1}w\}$, so that, by Remark **4.5**, $[(u, v, r)]_{\mathfrak{R}} \in \langle [(a^2 - b^2, 2ab, p^{e_1}w)]_{\mathfrak{R}} \rangle \star \langle [(0, 1, 1)]_{\mathfrak{R}} \rangle \leq H$.

ii) In this case, we have: $[(d^2 - c^2, 2dc, p^{e_1})]_{\mathfrak{R}} \star [(m^2 - n^2, 2mn, w)]_{\mathfrak{R}}$
$$\begin{aligned}&= [((d^2 - c^2)(m^2 - n^2) - 2dc2mn,\ (d^2 - c^2)2mn + (m^2 - n^2)2dc,\ p^{e_1}w))]_{\mathfrak{R}} \\ &= [(a^2 - b^2, -2ab, r)]_{\mathfrak{R}} \in H.\end{aligned}$$
On the other hand, $\{|u|, |v|, r\} = \{|a^2 - b^2|, |2ab|, p^{e_1}w\}$, so that, by Remark **4.5**,
$[(u, v, r)]_{\mathfrak{R}} \in \langle [(a^2 - b^2, -2ab, p^{e_1}w)]_{\mathfrak{R}} \rangle \star \langle [(0, 1, 1)]_{\mathfrak{R}} \rangle \leq H$.

We have proved that every element $[(u, v, r)]_{\mathfrak{R}} \in G$ belongs to H. Thus, $G = H$.

Let now (a, b, c) be a non-trivial triple. Then $[(a, b, c)]_{\mathfrak{R}} \notin C_4$. On the other hand, the first part of the proof shows that

$$[(a, b, c)]_{\mathfrak{R}} = X \star Y, \quad \text{where } X \in A \text{ and } Y \in C_4.$$

It follows that $X \neq 1$, and by Lemma **4.7** it has infinite order so that $[(a, b, c)]_{\mathfrak{R}} = X \star Y$, has infinite order, too. □

5. The geometric interpretation

In the introduction, we have recalled that a Pythagorean triangle is a right triangle with integer side lengths. In this section, we highlight how an interesting property referred to Pythagorean triangles may be obtained via the algebraic properties of Pythagorean triples. Precisely, as a consequence of Theorem **4.8** we obtain an elementary proof of the "Governor Theorem" (see Garibaldi 2008, p. 191; Scarpis 1903):

Theorem 5.1 (The Governor Theorem)**.** *If a right triangle has integer side lengths, then the acute angles are irrational, when measured in degrees.*

Proof. Let $\mathscr{T}$ be a Pythagorean triangle whose hypotenuse has length c and whose legs have lengths a and b. Clearly, $\mathscr{T}$ may be associated with a non-trivial triple (a, b, c): $\mathscr{T} = \mathscr{T}_{(a,b,c)}$ (see Fig. **5.1**). Note that $a = c\cos(\beta)$ e $b = c\sin(\beta)$, where β is the angle between the sides a and c.

Now we prove that for every positive integer n, both $\cos(n\beta)$ and $\sin(n\beta)$ are integers, moreover the following identity holds:

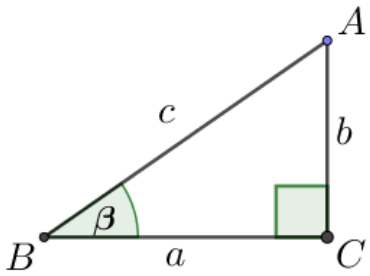

FIGURE **5.1**. The Pythagorean triple (a,b,c) associated with a Pythagorean triangle $\mathscr{T}_{(a,b,c)}$

$$[(a,b,c)]^n_{\mathfrak{R}} = [c(\cos(n\beta), c\sin(n\beta), c)]_{\mathfrak{R}}. \tag{5.1}$$

The statement is trivially true for $n = 1$. Let $n > 1$ and proceeding by induction assume that $\cos((n-1)\beta)$ and $\sin((n-1)\beta)$ are integers and the following identity holds:

$$[(a,b,c)]^{n-1}_{\mathfrak{R}} = [(c\cos((n-1)\beta), c\sin((n-1)\beta), c)]_{\mathfrak{R}}.$$

Then,

$$\begin{aligned}[(a,b,c)]^n_{\mathfrak{R}} &= [(c\cos((n-1)\beta), c\sin((n-1)\beta), c)]_{\mathfrak{R}} \star [c(\cos(\beta), c\sin(\beta), c)]_{\mathfrak{R}} \\ &= [(\cos((n-1)\beta)(\cos(\beta)c^2 - \sin((n-1)\beta)\sin(\beta)c^2, \cos((n-1)\beta)\sin(\beta)c^2 + \\ &\qquad \sin(n-1\beta)\cos(\beta)c^2, c^2)]_{\mathfrak{R}} \\ &= [(\cos(n\beta)c^2, \sin(n\beta)c^2, c^2)]_{\mathfrak{R}} = [(\cos(n\beta)c, \sin(n\beta)c, c)]_{\mathfrak{R}}.\end{aligned}$$

Thus, $\cos(n\beta)$ and $\sin(n\beta)$ are integers, and (**5.1**) holds. By contradiction, suppose now that β is rational in degrees, and put $\beta = m/n\ 360^\circ$. Then $(n\beta) = m\pi$, and two cases appear:

m even) In this case, $[(c\cos(n\beta), c\sin(n\beta), c)]_{\mathfrak{R}} = [(1,0,1)]_{\mathfrak{R}} = 1_G$.

m odd) In this case, $[(c\cos(n\beta), c\sin(n\beta), c)]_{\mathfrak{R}} = [(-1,0,1)]_{\mathfrak{R}}$ that is a periodic element of G (see Remark **4.5**).

So that, by Eq.(**5.1**), in both cases $[(a,b,c)]$ is a periodic element of G. On the other hand (a,b,c) is a non-trivial triple, so that, by Theorem **4.8** it has infinite order. This contradiction completes the proof. □

6. Conclusions

The study of Pythagorean triples has deep historical roots, dating back to the most ancient Assyrian-Babylonian civilizations and the Pythagorean theorem. It is closely tied to number theory, as it provides an entry point for discussions on prime numbers, divisibility, and modular arithmetic. Pythagorean triples are a specific case of Diophantine equations, which involve finding integer solutions to polynomial equations. This connects the study of Pythagorean triples to broader algebraic concepts (see Jannamorelli 2013).

FIGURE **6.1**. Plimpton 322 XIX sec. B.C. (see *Plimpton 322* 2024): a Babylonian clay tablet, containing a significant list of Pythagorean triples.

Moreover, Pythagorean triples have a clear geometric interpretation. In physics, these triples are relevant to problems involving vectors and forces, where right-angled triangles often arise. Understanding these triples lays the groundwork for applications in physics and engineering. It should also be noted that they also have a certain relevance in computer science. For example, some cryptographic algorithms involve the use of Pythagorean triples. Exploring these applications shows the intersection of number theory and modern technology, showcasing the ongoing relevance of these mathematical concepts. Besides these scientific aspects, we also highlight relevant didactic perspective derived from:

- Concrete Exploration of Number Theory: exploring Pythagorean triples offers a concrete and visual way to introduce and understand number theory concepts.
- Geometric Visualization: connection with Pythagorean theorem.
- Pattern Recognition: investigating Pythagorean triples encourages students to recognize patterns and relationships between numbers. This can lead to discussions about symmetry, the role of odd and even numbers, and the impact of scaling on the triples.
- Problem-Solving Skills: investigating Pythagorean triples encourages students to recognize patterns and relationships between numbers. This can lead to discussions about symmetry, the role of odd and even numbers, and the impact of scaling on the triples.

As we have said in the introduction, the set $\mathfrak{P}$ of all Pythagorean triples has an intrinsic structure of commutative monoid with respect to a suitable binary operation, $(\mathfrak{P}, \star)$. Eckert and Vestergaard (1989), Jitman and Sangwisut (2022), and Mariani (1962) considered different points of view and proved that special subsets of Pythagorean triples can be regarded as torsion free groups. On the other hand, their investigations appear somehow technical and sometimes by means of non-elementary concepts (see Jitman and Sangwisut 2022). This could affect the applications of their results.

We conclude by noting that our investigation approach could be adapted to a larger set of triples. This provides new insights and ideas for further research.

References

Alperin, R. C. (2005). "The modular tree of Pythagoras". *The American Mathematical Monthly* **112**(9), 807–816. URL: http://www.jstor.org/stable/30037602.

Dickson, L. E. (2012). *History of the Theory of Numbers. Volume I: Divisibility and Primality*. Mineola, New York: Dover Publications, Inc.

Eckert, E. J. (1984). "The group of primitive Pythagorean triangles". *Mathematics Magazine* **57**(1), 22–27. DOI: 10.1080/0025570X.1984.11977070.

Eckert, E. J. and Vestergaard, P. D. (1989). "Groups of integral triangles". *Fibonacci Quarterly* **27**(5), 458–464. URL: https://www.fq.math.ca/Scanned/27-5/eckert.pdf.

Garibaldi, S. (2008). "Somewhat more than governors need to know about trigonometry". *Mathematics Magazine* **81**(3), 191–200. DOI: 10.1080/0025570X.2008.11953548.

Jannamorelli, B. (2013). "Terne pitagoriche, numero d'oro e successione di Fibonacci". *Progetto Alice* **14**(40) (I), 65–98.

Jitman, S. and Sangwisut, E. (2022). "The group of primitive Pythagorean triples and perplex numbers". *Mathematics Magazine* **95**(4), 285–293. DOI: 10.1080/0025570X.2022.2092383.

Joyce, D. E. (1997). *Euclid's Elements*. Clark University, Worcester, MA, USA. URL: http://aleph0.clarku.edu/~djoyce/java/elements/toc.html.

Maor, E. (2007). *The Pythagorean Theorem : A 4,000-Year History*. Princeton, USA: Princeton University Press. URL: https://press.princeton.edu/books/paperback/9780691196886/the-pythagorean-theorem.

Mariani, J. (1962). "The group of the Pythagorean numbers". *The American Mathematical Monthly* **69**(2), 125–128. URL: http://www.jstor.org/stable/2312540.

Mollin, R. A. (2008). *Fundamental Number Theory with Applications*. 2nd ed. New York: Chapman and Hall/CRC. DOI: 10.1201/b15895.

Moreno, C. J. and Wagstaff Jr., S. S. (2005). *Sums of Squares of Integers*. Ed. by K. H. Rosen. 1st ed. Discrete Mathematics and Its Applications. New York: Chapman and Hall/CRC. DOI: 10.1201/9781420057232.

Murray, W. (2013). "Torsion in groups of integral triangles". *Advances in Pure Mathematics* **3**(1), 116–120. DOI: 10.4236/apm.2013.31015.

Niven, I. (1985). *Irrational Numbers*. 1st ed. Vol. 11. The Carus Mathematical Monographs. The Mathematical Association of America. URL: http://www.jstor.org/stable/10.4169/j.ctt5hh8zn.

Plimpton 322 (2024). URL: https://en.wikipedia.org/wiki/Plimpton_322 (visited on 02/03/2024).

Scarpis, U. (1903). "Una proprietà degli archi le cui funzioni goniometriche sono razionali". *Periodico di Matematiche*. 2nd ser. **5**, 280–284.

Taussky, O. (1970). "Sums of squares". *The American Mathematical Monthly* **77**(8), 805–830. URL: http://www.jstor.org/stable/2317016 (visited on 02/03/2024).

[a] Università degli Studi di Napoli,
Dipartimento di Architettura,
Via Monteoliveto 3, 80134 Napoli, Italy

[b] Università degli Studi di Salerno,
Dipartimento di Matematica,
Via Giovanni Paolo II 132, 84084 Fisciano (SA), Italy

* To whom correspondence should be addressed | email: vincenzi@unisa.it

Communicated 27 November 2023; manuscript received 6 December 2023; published online 10 February 2024