International Journal of Pure and Applied Mathematics

Volume 35 No. 3 2007, 365-374

ON PYTHAGOREAN QUADRUPLES

Edray Goins[1], Alain Togbé[2] §

[1]Department of Mathematics
Purdue University
150 North University Street, West Lafayette, IN 47907, USA
e-mail: egoins@purdue.edu

[2]Department of Mathematics
Purdue University North Central
1401S, U.S. 421, Westville, IN 46391, USA
e-mail: atogbe@purdue.edu

Abstract: We consider the multplicative properties of integer quadruples (a, b, c, d) satisfying $a^2 + b^2 + c^2 = d^2$ as a generalization of Pythagorean triples. In the proces, we present a group structure on the rational points on the unit sphere minus the poles and discuss a factorization result.

AMS Subject Classification: 11E25, 11E20
Key Words: Pythagorean triples, ternary quadratic forms, sums of squares

1. Introduction

We are all familiar with the statement "given a right triangle with legs of length a and b and hypotenuse of length c, then $a^2 + b^2 = c^2$;" this is known as the Pythagorean Theorem. There are many such examples integral right triangles:

$$3^2 + 4^2 = 5^2, \qquad 5^2 + 12^2 = 13^2, \qquad 8^2 + 15^2 = 17^2. \tag{1}$$

Such integral triples (a, b, c) are called Pythagorean triples. Given such a triple, there exist relatively prime integers m and n such that

$$\frac{a}{c} = \frac{m^2 - n^2}{m^2 + n^2} \qquad \text{and} \qquad \frac{b}{c} = \frac{2\,m\,n}{m^2 + n^2}. \tag{2}$$

Received: January 8, 2007

§Correspondence author

To see why, let (a, b, c) be a Pythagorean triple, and choose integers m and n such that $b/(c+a) = n/m$. Then $b/(c-a) = (c+a)/b$, so that

$$\frac{a}{c} = \left(\frac{c+a}{b} - \frac{c-a}{b}\right) \Big/ \left(\frac{c+a}{b} + \frac{c-a}{b}\right) = \left(\frac{m}{n} - \frac{n}{m}\right) \Big/ \left(\frac{m}{n} + \frac{n}{m}\right) \qquad (3)$$

which simplifies to (2) (see for example [3], pp. 151-154).

The goal of this paper is to study a generalization to four variables, the so-called Pythagorean quadruples, where we consider integers a, b, c, d such that $a^2 + b^2 + c^2 = d^2$. There are many such examples:

$$\begin{aligned} & & & & 1^2 + 2^2 + 2^2 &= 3^2, \\ & & 2^2 + 5^2 + 14^2 &= 2^2 + 10^2 + 11^2 &= 15^2, \\ 1^2 + 6^2 + 18^2 &= 6^2 + 6^2 + 17^2 &= 6^2 + 10^2 + 15^2 &= 19^2. \end{aligned} \qquad (4)$$

Such quadruples have a parametrization similar to the well-known triples, as outlined in the following result.

Theorem 1. *For each Pythagorean quadruple (a, b, c, d) with $d \neq 0$, there exist relatively prime integers m, n, p such that*

$$\frac{a}{d} = \frac{2\,m\,p}{p^2 + m^2 + n^2}, \quad \frac{b}{d} = \frac{2\,n\,p}{p^2 + m^2 + n^2}, \quad \frac{c}{d} = \frac{p^2 - m^2 - n^2}{p^2 + m^2 + n^2}. \qquad (5)$$

There exist many similar formulas which give exact values for a, b, c, and d – but unfortunately there is not one parametrization for all Pythagorean quadruples (see for example [6], p. 1464). The result above circumvents this problem by considering ratios.

It is easy to show that the Pythagorean triples are closed under "multiplication." That is, given two such triples one generates a third through the operation

$$(a_1,\, b_1,\, c_1) \oplus (a_2,\, b_2,\, c_2) = (a_1\,a_2 - b_1\,b_2,\; a_1\,b_2 + a_2\,b_1,\; c_1\,c_2)\,. \qquad (6)$$

This operation induces an associative, commutative multiplicative structure on the Pythagorean triples; see for example [3], p. 116. In this paper, we consider the associative, commutative operation

$$\begin{aligned} &(a_1,\, b_1,\, c_1,\, d_1) \oplus (a_2,\, b_2,\, c_2,\, d_2) \\ &\qquad = (a_1\,a_2 - b_1\,b_2,\; a_1\,b_2 + a_2\,b_1,\; c_1\,d_2 + c_2\,d_1,\; c_1\,c_2 + d_1\,d_2) \end{aligned} \qquad (7)$$

and attempt to ask questions of factorization.

Our main result may be stated as follows. Let $P = (a, b, c, d)$ be a Pythagorean quadruple, and denote n as the greatest common divisor of a, b, c, d; then $P_0 = \left(\frac{a}{n}, \frac{b}{n}, \frac{c}{n}, \frac{d}{n}\right)$ is also a Pythagorean quadruple, and we say that $h(P) = |d/n|$ is the height of P. Define the "conjugacy class" $[P]$ as the collection of all scalar multiples of P_0, where we allow sign changes and permutations $a \leftrightarrow b$, $a \leftrightarrow c$, $b \leftrightarrow c$ as well. This set corresponds to the identity $a^2 + b^2 + c^2 = d^2$. We will prove the following result.

Theorem 2. *Let P be a Pythagorean quadruple with $h(P) > 3$. Then there exist Pythagorean quadruples P_1, P_2 with $h(P_1)$, $h(P_2) < h(P)$ such that $[P] = [P_1 \oplus P_2]$.*

As an example, consider the identity $3^2+4^2 = 5^2$. Viewed as a Pythagorean quadruple, we have the factorization

$$[(0,\, 3,\, 4,\, 5)] = [(0,\, 8,\, 6,\, 10)] = [(2,\, 2,\, 1,\, 3) \oplus (2,\, 2,\, 1,\, 3)]\,. \tag{8}$$

In a sense, the identity $3^2+4^2 = 5^2$ is "generated" by the identity $1^2+2^2+2^2 = 3^2$.

The paper is organized as follows. First, we use stereographic projection to define a group structure on the points on the unit sphere. Next, we discuss "factorization" of the rational points by introducing the notions of height and irreducibility. Finally, we apply these results to Pythagorean quadruples. Our proofs ultimately rely on the composition

$$(a,\, b,\, c,\, d) \quad \mapsto \quad \left(\frac{a}{d},\, \frac{b}{d},\, \frac{c}{d}\right) \quad \mapsto \quad \frac{a + i\, b}{c + d}\,, \tag{9}$$

where the multiplicative properties of the complex numbers induce the multiplicative properties of the Pythagorean quadruples.

2. Multiplication on the Unit Sphere

Ultimately we wish to study Pythagorean quadruples (a, b, c, d), but we note that through the map

$$(a,\, b,\, c,\, d) \mapsto \left(\frac{a}{d},\, \frac{b}{d},\, \frac{c}{d}\right), \quad \text{where} \quad \left(\frac{a}{d}\right)^2 + \left(\frac{b}{d}\right)^2 + \left(\frac{c}{d}\right)^2 = 1\,, \tag{10}$$

it suffices to consider rational points on the unit sphere. To this end, we begin with a discussion of the real points.

Recall that the unit sphere $S^2(\mathbb{R}) = \{ (x_1,\, x_2,\, x_3) \in \mathbb{R}^3 \,\big|\, x_1^2 + x_2^2 + x_3^2 = 1\}$ is isomorphic with the extended complex numbers under the "stereographic projection" map $(x_1,\, x_2,\, x_3) \mapsto (x_1 + i\, x_2)/(1 + x_3)$ (see [2], p. 8-9 for details, our formulas are different in that we map the north pole $(0, 0, 1) \mapsto 0$ and the south pole $(0,\, 0,\, -1) \mapsto \infty$). The multiplicative structure of the complex numbers induces a corresponding structure on the unit sphere.

Theorem 3. *Let k be a field contained in $\mathbb{R}$, and denote the "poleless" unit sphere by*

$$\begin{aligned} G(k) &= S^2(k) - \{(0, 0, \pm 1)\} \\ &= \left\{ (x_1,\, x_2,\, x_3) \in k^3 \,\big|\, x_1^2 + x_2^2 + x_3^2 = 1,\ x_3 \neq \pm 1 \right\} \end{aligned} \tag{11}$$

and define the operation $\circledast : G(k) \times G(k) \to G(k)$ as

$$\begin{aligned} &(x_1,\, x_2,\, x_3) \circledast (y_1,\, y_2,\, y_3) \\ &\qquad = \left(\frac{x_1\, y_1 - x_2\, y_2}{1 + x_3\, y_3},\, \frac{x_1\, y_2 + x_2\, y_1}{1 + x_3\, y_3},\, \frac{x_3 + y_3}{1 + x_3\, y_3} \right). \end{aligned} \tag{12}$$

This makes $G(k)$ into a commutative group, where the identity is $\mathcal{O} = (1, 0, 0)$ and the inverse of a point $P = (x_1,\, x_2,\, x_3)$ is $[-1]\, P = (x_1,\, -x_2,\, -x_3)$.

The reader should keep in mind that although these formulas may seem a bit odd, the underlying structure is closely tied to that of the complex numbers. This construction is equivalent to $G(\mathbb{R}) \cong \mathbb{C}^\times$ with stereographic projection the group isomorphism.

Proof. Given two points (x_1, x_2, x_3), $(y_1, y_2, y_3) \in G(k)$ we define the expression $(x_1, x_2, x_3) \circledast (y_1, y_2, y_3) = (z_1, z_2, z_3)$ based on the product

$$\frac{x_1 + i\, x_2}{1 + x_3} \cdot \frac{y_1 + i\, y_2}{1 + y_3} = \frac{z_1 + i\, z_2}{1 + z_3}, \qquad \text{where} \qquad (z_1,\, z_2,\, z_3) \in G(k). \tag{13}$$

Noting that

$$\left| \frac{z_1 + i\, z_2}{1 + z_3} \right|^2 = \frac{z_1^2 + z_2^2}{(1 + z_3)^2} = \frac{1 - z_3^2}{(1 + z_3)^2} = \frac{1 - z_3}{1 + z_3}, \tag{14}$$

we may take norms of both sides to aid in solving for z_3:

$$\frac{1 - x_3}{1 + x_3} \cdot \frac{1 - y_3}{1 + y_3} = \frac{1 - z_3}{1 + z_3} \qquad \Longrightarrow \qquad z_3 = \frac{x_3 + y_3}{1 + x_3\, y_3} \tag{15}$$

(showing in particular that $z_3 \neq \pm 1$), while considering real and imaginary parts to aid in solving for z_1 and z_2:

$$z_1 = \frac{x_1\, y_1 - x_2\, y_2}{1 + x_3\, y_3} \qquad \text{and} \qquad z_2 = \frac{x_1\, y_2 + x_2\, y_1}{1 + x_3\, y_3}. \tag{16}$$

The statements about $\circledast$ associativity and commutativity follow from well-known multiplicative properties of the complex numbers. The point $(1, 0, 0) \mapsto 1$ under stereographic projection, and

$$(x_1,\, -x_2,\, -x_3) \mapsto \frac{x_1 - i\, x_2}{1 - x_3} = \frac{x_1^2 + x_2^2}{x_1 + i\, x_2}\ \frac{1 + x_3}{1 - x_3^2} = \left(\frac{x_1 + i\, x_2}{1 + x_3}\right)^{-1} \tag{17}$$

thereby verifying the statements about the identity and the inverse. □

3. Factorization on the Rational Unit Sphere

We now focus on the case $k = \mathbb{Q}$. We give some examples of the operation defined in the previous section. Both $\left(0,\, \frac{4}{5},\, \frac{3}{5}\right)$ and $\left(\frac{2}{11},\, \frac{6}{11},\, \frac{9}{11}\right)$ are such rational points on the unit sphere. We find that

$$\begin{aligned} \left(0,\, \frac{4}{5},\, \frac{3}{5}\right) &= \left(\frac{2}{3},\, \frac{2}{3},\, \frac{1}{3}\right) \circledast \left(\frac{2}{3},\, \frac{2}{3},\, \frac{1}{3}\right), \\ \left(\frac{2}{11},\, \frac{6}{11},\, \frac{9}{11}\right) &= \left(\frac{2}{3},\, \frac{1}{3},\, \frac{2}{3}\right) \circledast \left(\frac{2}{3},\, \frac{2}{3},\, \frac{1}{3}\right). \end{aligned} \tag{18}$$

This motivates the concept of "factorization" but first we need a way to measure when one point is "larger" than another.

Definition 1. Write $\vec{x} = \left(\frac{a}{d},\, \frac{b}{d},\, \frac{c}{d}\right) \in G(\mathbb{Q})$ with a, b, c, d integers. We define the height of $\vec{x}$ as the integer

$$h(\vec{x}) = \frac{|d|}{\gcd(a, b, c, d)}. \tag{19}$$

Write $\vec{x} = \vec{x}_1 \circledast \vec{x}_2$ with $\vec{x}_1$, $\vec{x}_2 \in G(\mathbb{Q})$. We say that $\vec{x}$ is reducible if $h(\vec{x}_1)$, $h(\vec{x}_2) < h(\vec{x})$; and irreducible if no such $\vec{x}_1$, $\vec{x}_2$ exist.

As $G(\mathbb{Q})$ is a group under $\circledast$, we can always find $\vec{x}_2$ such that $\vec{x} = \vec{x}_1 \circledast \vec{x}_2$ given $\vec{x}$ and $\vec{x}_1$. The importance of reducibility is in bounding the heights of $\vec{x}_1$ and $\vec{x}_2$.

Proposition 1. *Write* $\vec{x} = \left(\frac{a}{d}, \frac{b}{d}, \frac{c}{d}\right) \in G(\mathbb{Q})$ *for integers* a, b, c, *and* d.
(a) $h(\vec{x})$ *is odd.*
(b) If $h(\vec{x}) \leq 3$ *then* $\vec{x}$ *is irreducible.*
(c) If $h(\vec{x}) > 3$ *and* $\frac{c+d}{gcd(a,b,c,d)}$ *is a multiple of 4 then* $\vec{x}$ *is reducible.*

Given an odd integer $d = 2\,m+1$, we can always find a point $\vec{x} \in G(\mathbb{Q})$ such that $h(\vec{x}) = |d|$. This is equivalent to expressing $d^2 = 8\,\frac{m^2+m}{2} + 1 = a^2 + b^2 + c^2$ as the sum of three integral squares, a result which was known to Legendre, see [3], p. 127 and [4], article 291.

Proof. (a) Assume to the contrary, that $\vec{x} = \left(\frac{a}{d}, \frac{b}{d}, \frac{c}{d}\right) \in G(\mathbb{Q})$ has even height $|d|$ for relatively prime integers a, b, c, and d. Then $a^2 + b^2 + c^2 = d^2$, where d^2 now is a multiple of 4. It is well-known that this happens only when a, b, c are even as well, which contradicts the assumption that a, b, c, and d are relatively prime. Hence, $h(\vec{x})$ must be odd.

(b) Assume that $\vec{x}$ is reducible with $h(\vec{x}) \leq 3$. From the definitions, if $h(\vec{x}) = 1$, then $\vec{x}$ is irreducible; and from (a) the value $h(\vec{x}) = 2$ is not possible; so $h(\vec{x}) = 3$. By our assumption, there exist $\vec{x}_1$, $\vec{x}_2 \in G(\mathbb{Q})$, each of height $h(\vec{x}_1) = h(\vec{x}_2) = 1$ such that $\vec{x} = \vec{x}_1 \circledast \vec{x}_2$. But the only points of height 1 are in the form

$$(\pm 1,\, 0,\, 0)\,, \qquad (0,\, \pm 1,\, 0)\,, \qquad \text{or} \qquad (0,\, 0,\, \pm 1)\,, \tag{20}$$

and so the product $\vec{x}_1 \circledast \vec{x}_2$ is of the same form. These points have height 1, and so $\vec{x}$ must have height 1 as well. Again, this is a contradiction.

(c) Choose $\vec{x} = \left(\frac{a}{d}, \frac{b}{d}, \frac{c}{d}\right) \in G(\mathbb{Q})$ in terms of relatively prime integers a, b, c, and d. Assume that $h(\vec{x}) = |d| > 3$ and $c + d = 4\,n$ for some integer n. Since

$$(a+b)^2 = 2\,a\,b + d^2 - c^2 = 2\,a\,b + 4\,n\,(d-c), \tag{21}$$

the sum $a + b = 2\,m$ is even as well. Define the rational points

$$\vec{x}_1 = \left(\frac{2}{3}, \frac{2}{3}, \frac{1}{3}\right) \quad \text{and} \quad \vec{x}_2 = \left(\frac{m}{d-n}, \frac{m-a}{d-n}, \frac{3\,n-d}{d-n}\right) \qquad \text{in } G(\mathbb{Q}). \tag{22}$$

It is easy to see that $\vec{x} = \vec{x}_1 \circledast \vec{x}_2$. The first point has height $h(\vec{x}_1) = 3 < h(\vec{x})$. Since $c^2 < d^2$ we have the inequality

$$h(\vec{x}_2) \leq |d-n| = \left|\frac{3\,d-c}{4}\right| \leq \frac{3\,|d| + |c|}{4} < |d| = h(\vec{x}). \tag{23}$$

Hence $\vec{x}$ is reducible. □

The condition that $\frac{c+d}{\gcd(a,b,c,d)}$ be a multiple of 4 is a bit strong. In fact, there are irreducible points $\vec{x} \in G(\mathbb{Q})$, where $h(\vec{x}) > 3$; take for example $\vec{x} = (\frac{2}{7}, \frac{3}{7}, \frac{6}{7})$. To remedy this, we consider instead a "conjugacy class" which can always be factored.

Definition 2. Let $\vec{x} = (x_1, x_2, x_3) \in G(\mathbb{Q})$. Denote the conjugacy class of $\vec{x}$ as the set

$$[\vec{x}] = \left\{ \left(\pm x_{\sigma(1)}, \pm x_{\sigma(2)}, \pm x_{\sigma(3)}\right) \;\middle|\; \sigma \in \mathrm{Sym}\,(3) \right\} \subseteq G(\mathbb{Q}). \tag{24}$$

We say that $[\vec{x}]$ is reducible if there is a representative $\vec{x}_0 \in [\vec{x}]$ such that $\vec{x}_0$ is reducible; and irreducible if no such $\vec{x}_0$ exists.

For instance, while $\vec{x} = (\frac{2}{7}, \frac{3}{7}, \frac{6}{7})$ is irreducible as a point, $[\vec{x}] = \left[(\frac{2}{7}, \frac{3}{7}, \frac{6}{7})\right]$ is reducible as a conjugacy class:

$$\left[\left(\frac{2}{7}, \frac{3}{7}, \frac{6}{7}\right)\right] = \left[\left(\frac{2}{7}, \frac{6}{7}, -\frac{3}{7}\right)\right] = \left[\left(\frac{2}{3}, \frac{1}{3}, -\frac{2}{3}\right) \circledast \left(\frac{2}{3}, \frac{2}{3}, \frac{1}{3}\right)\right]. \tag{25}$$

This motivates the main result of this section.

Theorem 4. *Let $\vec{x} \in G(\mathbb{Q})$.*
(a) $h(\vec{x})$ is independent of choice of representative $\vec{x}_0 \in [\vec{x}]$.
(b) $h(\vec{x}) \leq 3$ if and only if $[\vec{x}]$ is irreducible.
(c) $h(\vec{x}) > 3$ if and only if $[\vec{x}]$ is reducible.

Proof. For the following, write $\vec{x} = \left(\frac{a}{d}, \frac{b}{d}, \frac{c}{d}\right)$ in terms of relatively prime integers a, b, c, and d, so that $h(\vec{x}) = |d|$.

(a) $[\vec{x}]$ simply consists of permutations and sign changes of the coordinates, and each representative $\vec{x}_0 \in [\vec{x}]$ has the same denominator d. Hence $h(\vec{x}_0) = |d|$ as well.

(b) ($\Longrightarrow$) If $h(\vec{x}) \leq 3$ then $h(\vec{x}_0) \leq 3$ for each representative $\vec{x}_0 \in [\vec{x}]$. Each $\vec{x}_0$ is irreducible by Proposition 1, so $[\vec{x}]$ is irreducible.

($\Longleftarrow$) Now assume that $h(\vec{x}) > 3$. By Proposition 1, $d = 2\,m + 1$ is odd, and not all of a, b, c, are even. We may choose a representative $\vec{x}_0 = \left(\frac{a}{d}, \frac{b}{d}, \frac{c}{d}\right)$ with $c = 2\,n + 1$ odd as well. Note that

$$c + d = 2\,(m + n + 1) \qquad \text{and} \qquad -c + d = 2\,(m + n) - 4\,n, \tag{26}$$

so choose the sign of c so that $c + d$ is a multiple of 4; this can be done because either $m + n$ or $m + n + 1$ is even. Then by Proposition 1 again, $\vec{x}_0$ is reducible, so by definition $[\vec{x}]$ is reducible.

(c) This is the contrapositive of (b). ∎

4. Factorization of Pythagorean Quadruples

We now consider the composition of maps

$$(a,\, b,\, c,\, d) \qquad \mapsto \qquad \left(\frac{a}{d},\, \frac{b}{d},\, \frac{c}{d}\right) \qquad \mapsto \qquad \frac{a+i\,b}{c+d} \tag{27}$$

to gain more information about the multiplicative nature of Pythagorean quadruples. For the sake of completeness, we show how to parametrize all such quadruples.

Theorem 5. *For each Pythagorean quadruple (a, b, c, d) with $d \neq 0$, there exist relatively prime integers m, n, p such that*

$$\frac{a}{d} = \frac{2\,m\,p}{p^2+m^2+n^2}, \qquad \frac{b}{d} = \frac{2\,n\,p}{p^2+m^2+n^2}, \qquad \frac{c}{d} = \frac{p^2-m^2-n^2}{p^2+m^2+n^2}. \tag{28}$$

In [1], one can see that some Pythagorean quadruples are in the form

$$\begin{aligned} a &= 2\,\alpha\,\beta + 2\,\gamma\,\delta, \qquad & c &= \alpha^2 - \beta^2 - \gamma^2 + \delta^2, \\ b &= 2\,\alpha\,\gamma - 2\,\beta\,\delta, \qquad & d &= \alpha^2 + \beta^2 + \gamma^2 + \delta^2; \end{aligned} \tag{29}$$

for α, β, γ, and δ integers. Our formulas are related by setting

$$m = \alpha\,\beta + \gamma\,\delta, \qquad n = \alpha\,\gamma - \beta\,\delta, \qquad p = \alpha^2 + \delta^2. \tag{30}$$

Compare the above formulas to those in [5] and [6].

Proof. There exist relatively prime integers m, n, p such that

$$p\,(a + i\,b) = (c+d)\,(m + i\,n). \tag{31}$$

Considering real and imaginary parts and using the fact that $a^2 + b^2 + c^2 = d^2$ we find that

$$\frac{a}{d} = \frac{2\,m\,p}{p^2+m^2+n^2}, \qquad \frac{b}{d} = \frac{2\,n\,p}{p^2+m^2+n^2}, \qquad \frac{c}{d} = \frac{p^2-m^2-n^2}{p^2+m^2+n^2} \tag{32}$$

as desired. □

Now that we know how to factor points on the rational unit sphere, we discuss factorizations of Pythagorean quadruples. We begin by discussing "conjugacy classes."

Definition 3. Let $P = (a, b, c, d)$ be a nontrivial Pythagorean quadruple i.e. integers such that $a^2 + b^2 + c^2 = d^2$ but $c^2 \neq d^2$. Denote the conjugacy class of P as the set

$$[P] = \left\{ (a_0,\, b_0,\, c_0,\, d_0) \in \mathbb{Z}^4 \;\middle|\; d_0 \neq 0,\; \left(\frac{a_0}{d_0},\, \frac{b_0}{d_0},\, \frac{c_0}{d_0} \right) \in [\vec{x}] \right\}, \tag{33}$$

where $\vec{x} = \left(\frac{a}{d},\, \frac{b}{d},\, \frac{c}{d}\right)$. For any representative $P_0 \in [P]$ define the height $h(P_0)$ as the height of a representative $P_0 \in [P]$. We say that $[P]$ is reducible (irreducible, respectively) if $[\vec{x}]$ is reducible (irreducible, respectively).

We present a more intuitive way to view this definition of conjugacy class. If $P = (a, b, c, d)$ is a Pythagorean qudruple, set

$$P_0 = \left(\frac{a}{n},\, \frac{b}{n},\, \frac{c}{n},\, \frac{d}{n} \right), \qquad \text{where} \qquad n = \gcd(a, b, c, d). \tag{34}$$

Then $[P]$ is the collection of all scalar multiples of P_0, where we allow sign changes and permutations $a \leftrightarrow b$, $a \leftrightarrow c$, $b \leftrightarrow c$ as well. For example, the Pythagorean quadruples with height either 3, 5, or 7 generate the classes $[(1, 2, 2, 3)]$, $[(0, 3, 4, 5)]$, and $[(2, 3, 6, 7)]$, respectively. This fact corresponds to the identities

$$1^2 + 2^2 + 2^2 = 3^2, \quad 3^2 + 4^2 = 5^2, \quad \text{and} \quad 2^2 + 3^2 + 6^2 = 7^2, \tag{35}$$

respectively.

We may now state the main result of the paper.

Theorem 6. *Let $P = (a,\, b,\, c,\, d)$ be a nontrivial Pythagorean quadruple, and define the operation $\oplus$ as*

$$\begin{aligned} &(a_1,\, b_1,\, c_1,\, d_1) \oplus (a_2,\, b_2,\, c_2,\, d_2) \\ &= (a_1\, a_2 - b_1\, b_2,\, a_1\, b_2 + a_2\, b_1,\, c_1\, d_2 + c_2\, d_1,\, c_1\, c_2 + d_1\, d_2)\,. \end{aligned} \tag{36}$$

(a) This makes such quadruples into a commutative monoid, with identity $\mathcal{O} = (1, 0, 0, 1)$.

(b) $[P]$ is irreducible if and only if $h(P) \leq 3$.

(c) $[P]$ is reducible if and only if $h(P) > 3$.

The operation $\oplus$ may also be realized through the map defined by

$$\varphi :\; \mathbb{Z}^4 \to \mathrm{Mat}_4(\mathbb{Z}), \qquad (a,\, b,\, c,\, d) \mapsto \begin{pmatrix} a & -b & 0 & 0 \\ b & a & 0 & 0 \\ 0 & 0 & d & c \\ 0 & 0 & c & d \end{pmatrix}. \tag{37}$$

Then $\varphi(P_1 \oplus P_2) = \varphi(P_1) \cdot \varphi(P_2)$ is the product of the matrices, $\varphi(\mathcal{O})$ is the identity matrix, and the nontrivial Pythagorean quadruples correspond to the submonoid of the image defined by $\det \begin{pmatrix} a & -b \\ b & a \end{pmatrix} = \det \begin{pmatrix} d & c \\ c & d \end{pmatrix} \neq 0$.

Proof. The results follow directly from Theorems 3 and 4 via the mapping $(a, b, c, d) \mapsto \left(\frac{a}{d}, \frac{b}{d}, \frac{c}{d}\right)$. □

Acknowledgments

The second author is grateful Purdue University North Central for the support.

References

[1] Robert D. Carmichael, *The Theory of Numbers and Diophantine Analysis*, Dover Publications Inc., New York (1959).

[2] John B. Conway, *Functions of one Complex Variable*, Springer-Verlag, New York, Second Edition (1978).

[3] H. Davenport, *The Higher Arithmetic*, Cambridge University Press, Cambridge, seventh edition (1999); *An Introduction to the Theory of Numbers*, Chapter VIII by J.H. Davenport.

[4] Carl Friedrich Gauss, *Disquisitiones Arithmeticae*, Springer-Verlag, New York (1986); Translated and with a preface by Arthur A. Clarke, Revised by William C. Waterhouse, Cornelius Greither and A. W. Grootendorst and with a preface by Waterhouse.

[5] L.J. Mordell, *Diophantine Equations*, Academic Press, London (1969).

[6] Eric W. Weisstein, *CRC Concise Encyclopedia of Mathematics*, CRC Press, Boca Raton, FL (1999).