A RING OF PYTHAGOREAN TRIPLES

Bryan Dawson

Emporia State University

Abstract. A one–to–one correspondence between the set of all Pythagorean triples and $\mathbb{Z} \times \mathbb{Z}$ is established, resulting in a ring of Pythagorean triples.

A triple $\langle a, b, c \rangle$ is called a *Pythagorean triple* if $a, b,$ and c are integers such that $a^2 + b^2 = c^2$. It seems natural to ask whether operations can be defined on the set P of all Pythagorean triples in such a way as to give P a ring structure. In fact, since a Pythagorean triple is determined by any two of the three integers, one might attempt to obtain a ring structure isomorphic to $\mathbb{Z} \times \mathbb{Z}$ (where $\mathbb{Z}$ represents the set of integers and the operations on $\mathbb{Z} \times \mathbb{Z}$ are defined coordinatewise) by finding a one–to–one correspondence between P and $\mathbb{Z} \times \mathbb{Z}$. The establishment of such a correspondence and the resulting ring structure is the objective of this paper.

The Sets $\mathbf{P_n}$. Throughout this article, all variables will be assumed to represent integers unless otherwise stated. If r is a real number, the quantity $\lceil r \rceil$ will represent the smallest integer greater than or equal to r.

It is a sometimes overlooked fact that if $\langle a, b, c \rangle \in P$ and $c \neq b$, then

$$\langle a, b, c \rangle = \left\langle a, \frac{a^2 - n^2}{2n}, \frac{a^2 + n^2}{2n} \right\rangle, \qquad \text{where } n = c - b.$$

(The cases $n = 1$ and $n = 2$ appear in the exercise sets of some textbooks, e.g. [1].) We now have two parameters, a and n, which determine the triple; although the mapping given by $\langle a, b, c \rangle \mapsto (a, n)$ is not onto $\mathbb{Z} \times \mathbb{Z}$, a variant of this idea will yield the desired result.

For $n \in \mathbb{Z}$, let $P_n = \{ \langle a, b, c \rangle \in P : c - b = n \}$. The following lemma is helpful in the characterization of P_n.

<u>Lemma 1.1</u>. Let $a, n \in \mathbb{Z}$ with $n \neq 0$. Then

$$\left\langle a, \frac{a^2 - n^2}{2n}, \frac{a^2 + n^2}{2n} \right\rangle \in P$$

if and only if either n is odd, a is odd and $n|a^2$, or n is even, a is even and $2n|a^2$.

Proof. Suppose

$$\left\langle a, \frac{a^2-n^2}{2n}, \frac{a^2+n^2}{2n} \right\rangle \in P.$$

Suppose n is odd. We have that $2n|a^2+n^2$; thus a^2+n^2 is even. However, n^2 is odd, and thus a^2, and consequently a, are odd. Also, since $n|a^2+n^2$ and $n|n^2$, we have $n|a^2$. Next, suppose n is even. As above, a^2+n^2 is even. However, n^2 is even, and thus, a is even. Since $2n|n^2$, we have $2n|a^2$.

Conversely, if either (1) or (2) hold, both

$$\frac{a^2-n^2}{2n} \text{ and } \frac{a^2+n^2}{2n}$$

are integers. But,

$$a^2 + \left(\frac{a^2-n^2}{2n}\right)^2 = \left(\frac{a^2+n^2}{2n}\right)^2;$$

thus

$$\left\langle a, \frac{a^2-n^2}{2n}, \frac{a^2+n^2}{2n} \right\rangle \in P.$$

The next three propositions characterize P_n in its various cases.

Proposition 1.2. Let n be odd with $n = p_1^{a_1} p_2^{a_2} \cdots p_m^{a_m}$ its prime factorization. Then

$$P_n = \left\{ \left\langle a, \frac{a^2-n^2}{2n}, \frac{a^2+n^2}{2n} \right\rangle : a = dr, d \text{ odd} \right\},$$

where $r = p_1^{b_1} p_2^{b_2} \cdots p_m^{b_m}$ and $b_k = \left\lceil \frac{a_k}{2} \right\rceil$ for $k = 1, \ldots, m$.

Proof. First note that

$$\frac{a^2+n^2}{2n} - \frac{a^2-n^2}{2n} = n.$$

Let
$$\left\langle a, \frac{a^2-n^2}{2n}, \frac{a^2+n^2}{2n} \right\rangle \in P_n.$$

Then by Lemma 1.1, $n|a^2$, i.e., $p_1^{a_1}p_2^{a_2}\cdots p_m^{a_m}|a^2$. Consequently, with b_k as defined above, $p_1^{b_1}p_2^{b_2}\cdots p_m^{b_m}|a$. Therefore, $a = dr$ for some $d \in \mathbb{Z}$ where r is as defined above. Also by Lemma 1.1, a must be odd; hence, d must also be odd.

Conversely, suppose a is an odd multiple of r. Then a is odd and a^2 is a multiple of $p_1^{2b_1}p_2^{2b_2}\cdots p_m^{2b_m}$. Hence, $n|a^2$. By Lemma 1.1,

$$\left\langle a, \frac{a^2-n^2}{2n}, \frac{a^2+n^2}{2n} \right\rangle \in P_n.$$

<u>Proposition 1.3</u>. Let n be even such that $n \neq 0$ with $n = 2^{a_0}p_1^{a_1}p_2^{a_2}\cdots p_m^{a_m}$ its prime factorization. Then
$$P_n = \left\{ \left\langle a, \frac{a^2-n^2}{2n}, \frac{a^2+n^2}{2n} \right\rangle : a = dr, d \in \mathbb{Z} \right\}$$

where $r = 2^{b_0}p_1^{b_1}p_2^{b_2}\cdots p_m^{b_m}$, $b_0 = \left\lceil \frac{a_0+1}{2} \right\rceil$, and $b_k = \left\lceil \frac{a_k}{2} \right\rceil$ for $k = 1, \ldots, m$.

The proof is analagous to the proof of Proposition 1.2. The only significant difference is that when Lemma 1.1 is applied, we have $2n|a^2$, causing b_0 to be defined as stated.

Finally, we have the case $n = 0$, whose proof is omitted.

<u>Proposition 1.4</u>. $P_0 = \{ \langle 0, x, x \rangle : x \in \mathbb{Z} \}$.

A Ring Structure for P. The results of the previous section make it clear how to proceed with the problem at hand. The rest of this paper consists of the formalization of this process.

<u>Definition 2.1</u>. Define $r' : \mathbb{Z}^+ \to \mathbb{Z}^+$ by $r'(x) = 2^{b_0}p_1^{b_1}p_2^{b_2}\cdots p_m^{b_m}$, where x has prime factorization $x = 2^{a_0}p_1^{a_1}p_2^{a_2}\cdots p_m^{a_m}$, $b_k = \left\lceil \frac{a_k}{2} \right\rceil$ for $k = 1, \ldots, m$, and

$$b_0 = \begin{cases} 0, & \text{if x is odd} \\ \left\lceil \frac{a_0+1}{2} \right\rceil, & \text{if x is even.} \end{cases}$$

This is the r, depending on n, of Propositions 1.2 and 1.3.

Definition 2.2. Define $d' : P \to \mathbb{Z}$ by

$$d'(\langle a,b,c\rangle) = \begin{cases} \frac{a}{r'(c-b)}, & \text{if } c-b \text{ even, } n \neq 0 \\ \frac{\frac{a}{r'(c-b)}-1}{2}, & \text{if } c-b \text{ odd} \\ \text{b}, & \text{if } c-b=0. \end{cases}$$

This is the d (modified for the case n odd) of Propositions 1.2 and 1.3, and the x of Proposition 1.4.

Putting these together, we have

Theorem 2.3. The mapping $\varphi : P \to \mathbb{Z} \times \mathbb{Z}$ given by

$$\varphi(\langle a,b,c\rangle) = (c-b, d'(\langle a,b,c\rangle))$$

is both injective and surjective. Consequently, $\langle P, \oplus, \odot\rangle$ is a commutative ring with identity where $\oplus$ and $\odot$ are operations on P defined by

$$\langle a,b,c\rangle \oplus \langle d,e,f\rangle = \varphi^{-1}(\varphi(\langle a,b,c\rangle) + \varphi(\langle d,e,f\rangle))$$

and

$$\langle a,b,c\rangle \odot \langle d,e,f\rangle = \varphi^{-1}(\varphi(\langle a,b,c\rangle) \cdot \varphi(\langle d,e,f\rangle)).$$

Proof. Propositions 1.2, 1.3, and 1.4 with Definitions 2.1 and 2.2. Note that $+$ and $\cdot$ represent coordinatewise addition and multiplication on $\mathbb{Z} \times \mathbb{Z}$. The operations on P are really those of $\mathbb{Z} \times \mathbb{Z}$ interpreted through the correspondence φ.

The following proposition contains interesting observations about $\langle P, \oplus, \odot\rangle$, the proofs of which are left as exercises for the reader.

Proposition 2.4.

If $\langle a,b,c\rangle, \langle e,f,g\rangle \in P$ then

$$\langle a,b,c\rangle \oplus \langle e,f,g\rangle = \begin{cases} \left\langle h, \frac{h^2-n^2}{2n}, \frac{h^2+n^2}{2n}\right\rangle, & \text{for } n \neq 0 \text{ even} \\ \left\langle k, \frac{k^2-n^2}{2n}, \frac{k^2+n^2}{2n}\right\rangle, & \text{for } n \text{ odd} \\ \langle 0, j, j\rangle, & \text{for } n = 0, \end{cases}$$

where

$$\begin{aligned}
h &= \left[d'\left(\langle a,b,c\rangle\right) + d'\left(\langle e,f,g\rangle\right)\right] r'(n)\\
n &= c-b+g-f\\
k &= \left[2\left[d'\left(\langle a,b,c\rangle\right) + d'\left(\langle e,f,g\rangle\right)\right]+1\right] r'(n)\\
j &= d'\left(\langle a,b,c\rangle\right) + d'\left(\langle e,f,g\rangle\right).
\end{aligned}$$

If $\langle a,b,c\rangle, \langle e,f,g\rangle \in P$ then

$$\langle a,b,c\rangle \odot \langle e,f,g\rangle = \begin{cases} \left\langle h, \frac{h^2-n^2}{2n}, \frac{h^2+n^2}{2n}\right\rangle, & \text{for } n \neq 0 \text{ even}\\ \left\langle k, \frac{k^2-n^2}{2n}, \frac{k^2+n^2}{2n}\right\rangle, & \text{for } n \text{ odd}\\ \langle 0,j,j\rangle, & \text{for } n=0, \end{cases}$$

where

$$\begin{aligned}
h &= d'\left(\langle a,b,c\rangle\right) d'\left(\langle e,f,g\rangle\right) r'(n)\\
n &= (c-b)(g-f)\\
k &= \left[2d'\left(\langle a,b,c\rangle\right) d'\left(\langle e,f,g\rangle\right)+1\right] r'(n)\\
j &= d'\left(\langle a,b,c\rangle\right) d'\left(\langle e,f,g\rangle\right).
\end{aligned}$$

The additive identity in $\langle P,\oplus,\odot\rangle$ is $\langle 0,0,0\rangle$.
The multiplicative identity in $\langle P,\oplus,\odot\rangle$ is $\langle 3,4,5\rangle$.
The additive inverse $I(\langle a,b,c\rangle)$ of $\langle a,b,c\rangle$ is given by

$$I(\langle a,b,c\rangle) = \begin{cases} \langle a,-b,-c\rangle, & \text{if } c-b \text{ even, } c-b\neq 0\\ \left\langle h, \frac{h^2-m^2}{2m}, \frac{h^2+m^2}{2m}\right\rangle, & \text{if } c-b \text{ odd}\\ \langle 0,-b,-c\rangle, & \text{if } c-b=0, \end{cases}$$

where $h = a - 2r'(c-b)$and $m = b-c$.
The units in $\langle P,\oplus,\odot\rangle$ are $\langle 3,4,5\rangle$, $\langle -3,-4,-5\rangle$, $\langle -1,0,1\rangle$, and $\langle 1,0,-1\rangle$.

The fact that P is partitioned into the sets P_n leaves an interesting avenue for further exploration. Also, it may be possible to define other operations in a natural way under which P is essentially a different ring. This is left as an open problem.

Acknowledgement. The author wishes to thank Elwyn Davis (Pittsburg State University) and the referee for their helpful comments and suggestions.

Reference

1. D. M. Burton, *Elementary Number Theory*, Wm. C. Brown Publishers, Dubuque, Iowa, 1989.