Hang Lung Mathematics Awards
Vol. 6 (2014)

Hang Lung Mathematics Awards 2014

Silver Award

Pseudo Pythagorean Triples Generator for Perpendicular Median Triangles

Team Members: Yan Lam Fan, Wai Pan Yik
Teacher: Mr. Ho Fung Lee
School: Pui Ching Middle School

Hang Lung Mathematics Awards
Vol. 6 (2014), pp. 69–100

PSEUDO PYTHAGOREAN TRIPLES GENERATOR FOR PERPENDICULAR MEDIAN TRIANGLES

TEAM MEMBERS
Yan Lam Fan, Wai Pan Yik

TEACHER
Mr. Ho Fung Lee

SCHOOL
Pui Ching Middle School

Abstract. The problem of finding all integral side length of a right-angled triangle is famous and the solution set is called the Pythagorean triple.

Now, instead of sides of a triangle, we concern the orthogonality of lines from vertices to their opposite sides. We want to generalize the problem to arbitrary rational ratio on the sides.

1. Introduction

The well-known Pythagoras's theorem and its converse show that the metric relations characterizes the orthogonality of the sides in a triangle. Furthermore, in number theory, a comprehensive investigation of Pythagorean triples is done by many mathematicians. The generator of primitive Pythagorean triples tells us how to find all the triples by equations in terms of parameters.

In this project, we wonder whether the above comprehensive investigation can be extended to different perpendicular lines in a triangle. Therefore, we consider the perpendicular medians in a triangle at the beginning and discover the governing equation, which characterizes the orthogonality of medians, in terms of the lengths of sides in a triangle.

Then, we investigate the properties of this type of Diophantine equations. The generator of this kind of triples is found similar to what we encounter in Pythagoras triples. Examples are given to illustrate our findings.

In third part, we modify our generator using a transformation of parameters to ensure that primitive triples are generated. Once we find all primitive triples, we can easily find all the triples by multiplying a factor. In this section, our investigation about the orthogonality of medians in a triangle is completed.

We know that a median cuts a side of triangle in the ratio 1 : 1. We further generalize our finding in an arbitrary rational ratio, say $p : q$. We tackle the problem by using the technique of transformation of parameters in the generator of triples. [See reviewer's comment (1)] In particular, we discuss the case $p = t$ and $q = 1$.

2. Introduction to Perpendicular Median Triangles

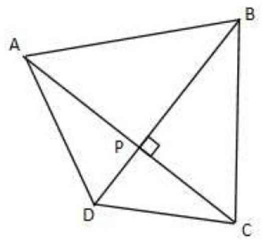
In this section, we are going to see the properties of a triangle which contains two perpendicular medians.

Lemma 1 is a metric relation characterizing the orthogonality of two lines.

Lemma 1. *Let $ABCD$ be a convex quadrilateral. $AC \perp BD$ if and only if*

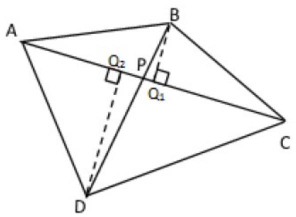
$$AB^2 + CD^2 = BC^2 + DA^2.$$

Proof. ($\Rightarrow$) Suppose $AC \perp BD$. Let P be the intersection of AC and BD.



$$\begin{aligned} AB^2 + CD^2 &= (AP^2 + PB^2) + (CP^2 + PD^2) \\ &= (BP^2 + PC^2) + (DP^2 + PA^2) \\ &= BC^2 + DA^2 \end{aligned}$$

($\Leftarrow$) Let P be the intersection of AC and BD, and Q_1 and Q_2 be the perpendicular foots of B and D onto AC, respectively.



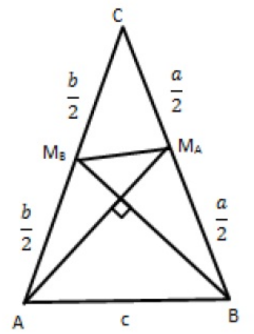
$$\begin{aligned}
AB^2 + CD^2 &= BC^2 + DA^2 \\
(AQ_1^2 + Q_1B^2) + (CQ_2^2 + Q_2D^2) &= (BQ_1^2 + Q_1C^2) + (DQ_2^2 + Q_2A^2) \\
AQ_1^2 + CQ_2^2 &= AQ_2^2 + CQ_1^2 \\
(AP + PQ_1)^2 + (CP + PQ_2)^2 &= (AP - PQ_2)^2 + (CP - PQ_1)^2 \\
AP \cdot (PQ_1 + PQ_2) + PC \cdot (PQ_1 + PQ_2) &= 0 \\
(AP + PC) \cdot (Q_1P + PQ_2) &= 0 \\
AC \cdot Q_1Q_2 &= 0 \\
Q_1Q_2 &= 0 \qquad (\because AC > 0)
\end{aligned}$$

$\because Q_1, P$ and Q_2 are the same point.

$\therefore AC \perp BD.$ □

Lemma 1 is in fact an extension of Pythagoras's theorem. If $A = D$, then the lemma becomes $AC \perp BA$ if and only if $AB^2 + AC^2 = BC^2$.

Lemma 2. *In $\triangle ABC$, let a, b and c be sides opposite to $\angle A, \angle B$ and $\angle C$, respectively. Let M_A, M_B and M_C be mid-points of BC, CA and AB, respectively. $AM_A \perp BM_B$ if and only if $a^2 + b^2 = 5c^2$.*



Proof. AM_BM_AB is a convex quadrilateral.

$$\begin{aligned}
& AM_A \perp BM_B \\
\Longrightarrow\ & AM_B^2 + M_AB^2 = M_BM_A^2 + BA^2 \qquad \text{(Lemma 1)} \\
\Longrightarrow\ & \left(\frac{b}{2}\right)^2 + \left(\frac{a}{2}\right)^2 = \left(\frac{c}{2}\right)^2 + (c)^2 \\
\Longrightarrow\ & a^2 + b^2 = 5c^2
\end{aligned}$$

□

$a^2+b^2=5c^2$ is the governing equation which reflects the orthogonality of medians. Then we prove the uniqueness in Lemma 3.

Lemma 3. *In $\triangle ABC$, if $AM_A \perp BM_B$, then neither*

$$BM_B \perp CM_C \quad \text{nor} \quad CM_C \perp AM_A.$$

Proof. If $AM_A \perp BM_B$, then $a^2+b^2=5c^2$. (Lemma 2)

Suppose $BM_B \perp CM_C$. We have $b^2+c^2=5a^2$. (Lemma 2)

$$\begin{aligned}(a^2+b^2)-(b^2+c^2)&=5c^2-5a^2\\ a^2&=c^2\\ a&=c\\ a^2+b^2&=5a^2\\ b&=2a\\ a+c=2a&=b\end{aligned}$$

It contradicts to triangle inequalities. Similarly, CM_C is not perpendicular to AM_A. □

Theorem 4 is the main result in this section. It characterizes the shortest side in this special type of triangles. [See reviewer's comment (2)]

Theorem 4. *In $\triangle ABC$, $a^2+b^2=5c^2$ if and only if there exists exactly one pair of medians which are perpendicular to each other (i.e. $AM_A \perp BM_B$). Also, we have $a>c$ and $b>c$, that is, c is the shortest side.*

Proof. ($\Rightarrow$) By Lemma 2, if $a^2+b^2=5c^2$ then $AM_A \perp BM_B$.

By Lemma 3, there exists exactly one pair of medians which are perpendicular to each other (i.e. $AM_A \perp BM_B$). By triangle inequalities,

$$\begin{array}{rcr} a+c>b & \text{and} & b+c>a\\ a^2+2ac+c^2>b^2 & \text{and} & b^2+2bc+c^2>a^2\\ a^2+2ac+c^2>5c^2-a^2 & \text{and} & b^2+2bc+c^2>5c^2-b^2\\ a^2+ac-2c^2>0 & \text{and} & b^2+bc-2c^2>0\\ (a+2c)(a-c)>0 & \text{and} & (b+2c)(b-c)>0\\ a>c & \text{and} & b>c\end{array}$$

($\Leftarrow$) There exists exactly one pair of medians which are perpendicular to each other.

Only one of the following statements is true:

(i) $AM_A \perp BM_B \iff a^2+b^2=5c^2$
(ii) $BM_B \perp CM_C \iff b^2+c^2=5a^2$

(iii) $CM_C \perp AM_A \iff c^2 + a^2 = 5b^2$

(ii) implies $a < c$, which contradicts to $a > c$.

(iii) implies $b < c$, which contradicts to $b > c$.

$\therefore$ Only (i) is true. i.e. $a^2 + b^2 = 5c^2$ $\square$

We illustrate our results by the following examples.

Example 5. *Given a triangle $\triangle ABC$ with three known sides, we can check whether it has a pair of perpendicular medians.*
Suppose $a = 19, b = 22$ and $c = 13$.
$\because (19)^2 + (22)^2 = 5(13)^2$
$\therefore$ *$\triangle ABC$ has perpendicular medians AM_A and BM_B by Lemma 2. Also neither $BM_B \perp CM_C$ nor $CM_C \perp AM_A$.*

Example 6. *A triangle $\triangle ABC$ has a pair of perpendicular medians. If there are two known sides, we can solve for the remaining one.*
Suppose the two known sides are of lengths 19 and 22.
Case 1: $19^2 + 22^2 = 5c^2 \implies c = 13$
Case 2: $22^2 + c^2 = 5(19)^2 \implies c = \sqrt{1321} \approx 36.3$
Case 3: $c^2 + 19^2 = 5(22)^2 \implies c = \sqrt{2059} \approx 45.4$ *(rejected)*
By Theorem 4, Case 3 is rejected since c is not the shortest side, contradicting the triangle inequalities.
Note that other than 13, we have found another value of c. Hence, $\triangle ABC$ cannot be uniquely identified by two known sides, not knowing which side is the shortest.

Example 7. *Although $2^2 + 19^2 = 5(13)^2$ satisfies the equation $a^2 + b^2 = 5c^2$, these three sides cannot form a triangle because $a + c < b$, which cannot satisfy the triangle inequalities.* [See reviewer's comment (3)]

We are going to show that, after characterizing the shortest length, the solution of $a^2 + b^2 = 5c^2$ can form a triangle.

Theorem 8. *If $a^2 + b^2 = 5c^2$ with $a > c$ and $b > c$, then a, b and c satisfy the triangle inequalities.*

Proof.

$$\begin{aligned}
a &> c & \text{and} && b &> c \\
a - c &> 0 & \text{and} && b - c &> 0 \\
2(a+2c)(a-c) &> 0 & \text{and} && 2(b+2c)(b-c) &> 0 \\
2a^2 + 2ac - 4c^2 &> 0 & \text{and} && 2b^2 + 2bc - 4c^2 &> 0 \\
a^2 + 2ac + c^2 &> 5c^2 - a^2 & \text{and} && b^2 + 2bc + c^2 &> 5c^2 - b^2 \\
(a+c)^2 &> b^2 & \text{and} && (b+c)^2 &> a^2 \\
a + c &> b & \text{and} && b + c &> a
\end{aligned}$$

Also $a > c \implies a + b > c$
$\therefore$ a, b and c satisfy the triangle inequalities. $\square$

3. Pseudo-Pythagorean Triples

In this section, we study the finding in the previous section in the sense of number theory. To do so, we study the governing equation $a^2 + b^2 = 5c^2$. We attempt to find all its integral solutions.

Definition 9. *A triangle with a pair of perpendicular medians is called a "perpendicular median triangle"or a "PM triangle".*

Theorem 4 tells us that in a PM triangle, five times the square of the shortest side is equal to the sum of the squares of the other two sides. Conversely, any triangle for which five times the square of the shortest side is equal to the sum of the squares of the other two sides is a PM triangle. We are going to find all PM triangles which has integral side lengths, i.e. to find all triples of positive integers (a, b, c), satisfying the Diophantine equation

$$a^2 + b^2 = 5c^2 \tag{1}$$

$$\text{and} \quad a > b \quad \text{and} \quad b > c \tag{2}$$

[See reviewer's comment (4)]

Solving (1) involves the technique in number theory and (2) reflects the constraints in geometric aspect. By Theorem 8, (2) ensures that the solution of (1) forms a triangle. This is the main difference between our findings and Pythagorean triples because the solutions of $a^2 + b^2 = c^2$ automatically satisfy triangle inequalities but our triples do not.

Definition 10. *Triples of positive integers satisfying (1) and (2) are called "pseudo-Pythagorean triples", in short, "PPT".*

[See reviewer's comment (5)]

Example 11. *The triples* $(22, 19, 13)$, $(22, 31, 17)$ *and* $(38, 41, 25)$ *are PPT because they all satisfy (1) and (2).*

Definition 12. *A PPT* (a, b, c) *is called primitive if* $gcd(a, b, c) = 1$.

Example 13. $(19, 22, 13)$ *is a primitive PPT, whereas* $(44, 38, 26)$ *is not.*

Note that all PPTs can be found by forming integral multiples of primitive PPTs. Therefore, we only need to find all primitive PPTs if we want to find all PPTs.

Lemma 14 and Lemma 15 show some properties of primitive PPTs.

Lemma 14. *If* (a, b, c) *is a primitive PPT, then*

$$gcd(a, b) = gcd(b, c) = gcd(c, a) = 1.$$

Proof. Suppose $gcd(a, b) > 1$. There exists a prime p such that $p \mid a$ and $p \mid b$. So $p^2 \mid a^2$and $p^2 \mid b^2$. Hence, we have $p^2 \mid a^2 + b^2 = 5c^2$.

As 5 is a prime, $p \mid c^2 \implies p \mid c$. Therefore $p \mid a$, $p \mid b$ and $p \mid c$, contradicting $gcd(a, b, c) = 1$. Suppose $gcd(b, c) > 1$. There exists a prime p such that $p \mid b$ and $p \mid c$. So $p^2 \mid b^2$ and $p^2 \mid c^2$. Hence, we have $p^2 \mid 5c^2 - b^2 = a^2$. Therefore $p \mid a, p \mid b$ and $p \mid c$, contradicting $gcd(a, b, c) = 1$. Similarly, $gcd(c, a) = 1$. □

[See reviewer's comment (6)]

Lemma 15. *If* (a, b, c) *is a primitive PPT, then* a *and* b *have different parity and* c *is odd.*

Proof. a and b cannot be both even because $gcd(a, b) = 1$. Suppose a and b are both odd. $a^2 \equiv b^2 \equiv 1 \pmod 4$. $5c^2 = a^2 + b^2 \equiv 1 + 1 \equiv 2 \pmod 4$, which contradicts to $5c^2 \equiv c^2 \equiv 1 \text{ or } 0 \pmod 4$.

If a is odd and b is even, then a^2 is odd and b^2 is even. $5c^2 = a^2 + b^2$ is odd.

Therefore, c^2 is odd $\implies$ c is odd.

a is even and b is odd can be proved similarly.

c is odd in all cases. □

WLOG, we assume a is even and b is odd in the following.

Lemma 16. *If* r, s *and* t *are positive integers such that* $gcd(r, s) = 1$ *and* $rs = t^2$, *then there are integers* m *and* n *such that* $r = m^2$ *and* $s = n^2$.

Proof. If $r = 1$ or $s = 1$, then the lemma is trivial.

Suppose $r > 1$ and $s > 1$. Let $r = p_1^{a_1} \cdot p_2^{a_2} \cdot \cdots \cdot p_u^{a_u}$, $s = p_{u+1}^{a_{u+1}} \cdot p_{u+2}^{a_{u+2}} \cdot \cdots \cdot p_v^{a_v}$, where $p_1, p_2, \ldots, p_u, p_{u+1}, \ldots, p_v$ are distinct primes.

$t = q_1^{b_1} \cdots q_2^{b_2} \cdot \cdots \cdot q_k^{b_k}$, where $q_1, q_2, \ldots, q_k$ are distinct primes.

Since $rs = t^2$, $p_1^{a_1} \cdot p_2^{a_2} \cdot \cdots \cdot p_u^{a_u} \cdot p_{u+1}^{a_{u+1}} \cdot \cdots \cdot p_v^{a_v} = q_1^{2b_1} \cdots q_2^{2b_2} \cdot \cdots \cdot q_k^{2b_k}$

By the fundamental theorem of arithmetic,

$$p_i^{a_i} = q_j^{2b_j} \text{ for every } 1 \leq i \leq v \text{ and } 1 \leq j \leq k.$$

Therefore $a_i = 2b_j$ for every $1 \leq i \leq v$ and $1 \leq j \leq k$.

a_i is even so $\dfrac{a_i}{2}$ is an integer.

Therefore there exist integers m and n,

$$m = p_1^{\frac{a_1}{2}} \cdot p_2^{\frac{a_2}{2}} \cdot \cdots \cdot p_u^{\frac{a_u}{2}}, \quad n = p_{u+1}^{\frac{a_{u+1}}{2}} \cdot p_{u+2}^{\frac{a_{u+2}}{2}} \cdot \cdots \cdot p_v^{\frac{a_v}{2}},$$

such that $r = m^2$ and $s = n^2$.

[See reviewer's comment (7)]

$\square$

In the following theorem, we find a generator to express PPTs by using two parameters.

Theorem 17. *If there are relatively prime positive integers m and n, with m and n having different parity and $2n > m > n$ or $m > 3n$, such that for $2n > m > n$,*

$$\begin{cases} a &= 2m^2 + 2mn - 2n^2 \\ b &= n^2 + 4mn - m^2 \\ c &= m^2 + n^2 \end{cases} \tag{3}$$

for $m > 3n$,

$$\begin{cases} a &= 2m^2 - 2mn - 2n^2 \\ b &= m^2 + 4mn - n^2 \\ c &= m^2 + n^2 \end{cases} \tag{4}$$

then (a, b, c) is a primitive PPT or a PPT with $gcd(a, b, c) = 5$.

Furthermore, $\begin{cases} 5 \mid 2a - b & \text{if } 2n > m > n \\ 5 \mid 2a + b & \text{if } m > 3n \end{cases}.$

Proof.
<u>Case 1:</u> Suppose $2n > m > n$. (a, b, c) is defined by (3).

$$\begin{aligned} a^2 + b^2 &= (2m^2 + 2mn - 2n^2)^2 + (n^2 + 4mn - m^2)^2 \\ &= 5m^4 + 10m^2n^2 + 5n^4 \\ &= 5(m^2 + n^2)^2 \\ &= 5c^2 \end{aligned}$$

$$\begin{aligned} m > n &\implies (m + 3n)(m - n) > 0 \\ &\implies 2m^2 + 2mn - 2n^2 > m^2 + n^2 \\ &\implies a > c \\ 2n > m &\implies 2m(2n - m) > 0 \\ &\implies n^2 + 4mn - m^2 > m^2 + n^2 \\ &\implies b > c \end{aligned}$$

$\therefore$ (a, b, c) is a PPT by definition.

<u>Case 2:</u> Suppose $m > 3n$. (a, b, c) is defined by (4).

$$\begin{aligned} a^2 + b^2 &= (2m^2 - 2mn - 2n^2)^2 + (m^2 + 4mn - n^2)^2 \\ &= 5m^4 + 10m^2n^2 + 5n^4 \\ &= 5(m^2 + n^2)^2 \\ &= 5c^2 \end{aligned}$$

$$\begin{aligned} m > 3n &\implies (n + m)(m - 3n) > 0 \\ &\implies 2m^2 - 2mn - 2n^2 > m^2 + n^2 \\ &\implies a > c \\ 2m > n &\implies 2m(2m - n) > 0 \\ &\implies m^2 + 4mn - n^2 > m^2 + n^2 \\ &\implies b > c \end{aligned}$$

(a, b, c) is a PPT by definition. Next, we show that $gcd(a, b, c) = 1$ or 5.

Let $gcd(a, b, c) = d$. Since m and n have different parity, $c = m^2 + n^2$ is odd. Therefore $2 \nmid d$.

If $2n > m > n$, then $d \mid 5c + 2a - b = 10m^2$ and $d \mid 5c - 2a + b = 10n^2$.

If $m > 3n$, then $d \mid 5c + 2a + b = 10n^2$ and $d \mid 5c - 2a - b = 10m^2$.

$\because gcd(m, n) = 1$
$\therefore gcd(m^2, n^2) = 1$

Also since $2 \nmid d$, $d = 1$ or 5.
$\therefore gcd(a, b, c) = 1$ or 5

Suppose $2n > m > n$.

$$\begin{aligned} 2a - b &= 2(2m^2 + 2mn - 2n^2) - (n^2 + 4mn - m^2) \\ &= 5m^2 - 5n^2 \\ &= 5(m^2 - n^2) \end{aligned}$$

$\therefore 5 \mid 2a - b$

Suppose $m > 3n$.

$$\begin{aligned} 2a + b &= 2(2m^2 - 2mn - 2n^2) + (m^2 + 4mn - n^2) \\ &= 5m^2 - 5n^2 \\ &= 5(m^2 - n^2) \end{aligned}$$

$\therefore 5 \mid 2a + b$ □

Remark 18. *From the proof, if m and n do not satisfy $2n > m > n$ or $m > 3n$, then the generated (a, b, c) is not a PPT since c is not the shortest length. According to Theorem 17, we can use (3) or (4) to find some PPTs quickly.* [See reviewer's comment (8)] *For example, when $(m, n) = (3, 2)$, $2n > m > n$. Therefore by (3), $(a, b, c) = (22, 19, 13)$.*

It is natural to ask whether all primitive PPTs can be found by the generators. We are going to prove the existence of (m, n) for any primitive PPT (a, b, c).

Theorem 19. *If (a, b, c) is a primitive PPT, with a even, then there are relatively prime integers m and n, with m and n having different parity, such that*

for $5 \mid 2a - b$,

$$\begin{cases} a &= 2m^2 + 2mn - 2n^2 \\ b &= n^2 + 4mn - m^2 \\ c &= m^2 + n^2 \end{cases}$$

for $5 \mid 2a + b$,

$$\begin{cases} a &= 2m^2 - 2mn - 2n^2 \\ b &= m^2 + 4mn - n^2 \\ c &= m^2 + n^2 \end{cases}$$

Furthermore, $\begin{cases} 2n > m > n & \text{if } 5 \mid 2a - b \\ m > 3n & \text{if } 5 \mid 2a + b \end{cases}.$

Proof.
Case 1: Suppose $5 \mid 2a-b$.

$$\begin{aligned} a^2+b^2=5c^2 &\implies a^2+b^2<5a^2 \\ &\implies \quad 4a^2>b^2 \\ &\implies \quad 2a>b \\ &\implies 2a-b<0 \end{aligned}$$

$$\begin{aligned} a^2+b^2 &= 5c^2 \\ (2a-b)^2+(a+2b)^2 &= (5c)^2 \\ (a+2b)^2 &= (5c+2a-b)(5c-2a+b) \end{aligned}$$

$\because$ a is even, b is odd and c is odd.
$\therefore$ $a+2b, 5c+2a-b$ and $5c-2a+b$ are even.
$\because$ $5 \mid 2a-b$ and $5 \mid 5c$,
$\therefore$ $5 \mid a+2b, 5 \mid 5c+2a-b$ and $5 \mid 5c-2a+b$.

Therefore $10 \mid a+2b, 10 \mid 5c+2a-b$ and $10 \mid 5c-2a+b$.

$$\left(\frac{a+2b}{10}\right)^2 = \left(\frac{5c+2a-b}{10}\right)\left(\frac{5c-2a+b}{10}\right)$$

Let $r = \dfrac{5c+2a-b}{10} \in \mathbb{Z}^+, s = \dfrac{5c-2a+b}{10} \in \mathbb{Z}^+$, and $gcd(r,s)=d$.

$$\begin{aligned} & d^2 \mid rs = \left(\frac{a+2b}{10}\right)^2 \\ & d \mid \frac{a+2b}{10} \\ & d \mid r-s = \frac{2a-b}{5} \\ \therefore \quad & d \mid 2\left(\frac{2a-b}{5}\right)+2\left(\frac{a+2b}{10}\right)=a \\ & d \mid r+s=c \\ \therefore \quad & d \mid a \quad \text{and} \quad d \mid c \\ \because \quad & gcd(a,c)=1 \\ \therefore \quad & d = gcd(r,s) = 1 \end{aligned}$$

By Lemma 16, there are integers m and n such that $r = m^2, s = n^2$.

$$a = 2\left(\frac{2a-b}{5}\right) + 2\left(\frac{a+2b}{10}\right) = 2(r-s) + 2\sqrt{rs} = 2m^2 + 2mn - 2n^2$$
$$b = 4\left(\frac{a+2b}{10}\right) - \left(\frac{2a-b}{5}\right) = 4\sqrt{rs} - (r-s) = n^2 + 4mn - m^2$$
$$c = r + s = m^2 + n^2$$

$$\begin{array}{rcr} a > c & \text{and} & b > c \\ 2m^2 + 2mn - 2n^2 > m^2 + n^2 & \text{and} & n^2 + 4mn - m^2 > m^2 + n^2 \\ (m+3n)(m-n) > 0 & \text{and} & 2m(2n-m) > 0 \\ m > n & \text{and} & 2n > m \end{array}$$

$\therefore 2n > m > n$

<u>Case 2:</u> Suppose $5 \mid 2a + b$.

$$\begin{aligned} a^2 + b^2 = 5c^2 &\implies a^2 + b^2 < 5b^2 \\ &\implies 4b^2 > a^2 \\ &\implies 2b > a \\ &\implies 2b - a < 0 \end{aligned}$$

$$(2a-b)^2 = (5c + 2a + b)(5c - 2a - b)$$

In a similar manner, let $r = \dfrac{5c + 2a + b}{10} \in \mathbb{Z}^+, s = \dfrac{5c - 2a - b}{10} \in \mathbb{Z}^+$. Likewise, $gcd(r, s) = 1$.

By Lemma 16, there are integers m and n such that $r = m^2, s = n^2$.

$$a = 2\left(\frac{2a+b}{5}\right) - 2\left(\frac{2b-a}{10}\right) = 2(r-s) - 2\sqrt{rs} = 2m^2 - 2mn - 2n^2$$
$$b = 4\left(\frac{2b-a}{10}\right) + \left(\frac{2a+b}{5}\right) = 4\sqrt{rs} + (r-s) = m^2 + 4mn - n^2$$
$$c = r + s = m^2 + n^2$$

$$\begin{array}{rcr} a > c & \text{and} & b > c \\ 2m^2 - 2mn - 2n^2 > m^2 + n^2 & \text{and} & m^2 + 4mn - n^2 > m^2 + n^2 \\ (n+m)(m-3n) > 0 & \text{and} & 2n(2m-n) > 0 \\ m > 3n & \text{and} & 2m > n \end{array}$$

$\therefore m > 3n$ □

Now, given a primitive PPT (a, b, c), Theorem 19 ensures the existence of (m, n). How can we find (m, n)? We first check whether $5 \mid 2a - b$ or $5 \mid 2a + b$, then (m, n) can be found by solving the corresponding system of equations.

We end this section by giving the examples of PPT using the generators. [See reviewer's comment (9)]

m	**n**	**(a,b,c)**	**gcd(a,b,c)**
3	2	(22,19,13)	1
4	3	(38,41,25)	1
5	4	(58,71,41)	1
6	5	(82,109,61)	1
7	4	(122,79,65)	1
7	6	(110,155,85)	5
8	5	(158,121,89)	1
8	7	(142,209,113)	1
9	8	(178,271,145)	1
10	7	(242,229,149)	1
10	9	(218,341,181)	1
11	6	(302,179,157)	1
11	8	(290,295,185)	5

$2n > m > n$

m	**n**	**(a,b,c)**	**gcd(a,b,c)**
4	1	(22,31,17)	1
6	1	(58,59,37)	1
7	2	(62,101,53)	1
8	1	(110,95,65)	5
9	2	(118,149,85)	1
10	1	(178,139,101)	1
10	3	(122,211,109)	1
11	2	(190,205,125)	5
12	1	(262,191,145)	1
13	2	(278,269,173)	1
13	4	(202,361,185)	1
14	1	(362,251,197)	1
14	3	(290,355,205)	5

$m > 3n$

[See reviewer's comment (10)]

4. Further Study on the Generators by Transformation

From Theorem 17 and Theorem 19, we can generate all primitive PPTs but we observe from the table that some non-primitive PPTs with $gcd(a, b, c) = 5$ are produced too. It suggests that we should study the generators and see what kinds of m and n can form primitive PPT. We tackle this problem by taking transformations on (m, n).

Let m and n be two relatively prime integers, with m and n having different parity.

For $2n > m > n$, denote m' and n' by the transformation

$$\begin{pmatrix} m' \\ n' \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ -1 & 2 \end{pmatrix} \begin{pmatrix} m \\ n \end{pmatrix}$$

and define (a, b, c) by

$$\begin{cases} a = 2m^2 + 2mn - 2n^2 \\ b = n^2 + 4mn - m^2 \\ c = m^2 + n^2 \end{cases}$$

For $m > 3n$, define m' and n' by the transformation

$$\begin{pmatrix} m' \\ n' \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} m \\ n \end{pmatrix}$$

and define (a, b, c) by

$$\begin{cases} a = 2m^2 - 2mn - 2n^2 \\ b = m^2 + 4mn - n^2 \\ c = m^2 + n^2 \end{cases}$$

Theorem 20. *m' and n' are relatively prime, with m' and n' having different parity, if and only if (a, b, c) is a primitive PPT.*

Proof. $(\Rightarrow)$ By Theorem 17, $gcd(a, b, c) = 1$ or 5. Assume $gcd(a, b, c) = 5$.

Define a', b' and c' by m' and n', such that

for $2n > m > n$,

$$5m > 5n \implies 2m + n > 3(2n - m) \implies m' > 3n'$$

$$a' = 2m'^2 - 2m'n' - 2n'^2$$
$$b' = n'^2 + 4m'n' - m'^2$$
$$c' = m'^2 + n'^2$$

$$\begin{aligned}
a' &= 2(2m+n)^2 - 2(2n-m)(2m+n) - 2(2n-m)^2 \\
&= 10m^2 + 10mn - 10n^2 \\
&= 5a \\
b' &= (2m+n)^2 + 4(2n-m)(2m+n) - (2n-m)^2 \\
&= 5n^2 + 20mn - 5m^2 \\
&= 5b \\
c' &= (2n-m)^2 + (2m+n)^2 \\
&= 5m^2 + 5n^2 \\
&= 5c
\end{aligned}$$

for $m > 3n$,

$$\begin{aligned}
&5n > 0 \implies 2(m+2n) > 2m-n \implies 2n' > m' \\
&m > 3n \implies 2m-n > m+2n \implies m' > n' \\
&2n' > m' > n'
\end{aligned}$$

$$\begin{aligned}
a' &= 2m'^2 + 2m'n' - 2n'^2 \\
b' &= m'^2 + 4m'n' - n'^2 \\
c' &= m'^2 + n'^2
\end{aligned}$$

$$\begin{aligned}
a' &= 2(2m-n)^2 - 2(2m-n)(2n+m) - 2(2n+m)^2 \\
&= 10n^2 - 10mn - 10m^2 \\
&= 5a \\
b' &= (2n+m)^2 + 4(2m-n)(2n+m) - (2m-n)^2 \\
&= 5m^2 + 20mn - 5n^2 \\
&= 5b \\
c' &= (2m-n)^2 + (2n+m)^2 \\
&= 5m^2 + 5n^2 \\
&= 5c
\end{aligned}$$

Since $gcd(a, b, c) = 5$, $gcd(a', b', c') = 25$.

But by Theorem 17, $gcd(a', b', c') = 1$ or 5 because m' and n' are relatively prime and have different parity. $gcd(a, b, c) \neq 5$, $gcd(a, b, c) = 1$, (a, b, c) is a primitive PPT.

($\Leftarrow$) We only prove for $5 \mid 2a - b$. The proof for $5 \mid 2a + b$ is similar.
Since m and n have different parity,

Case 1: m is even and n is odd, $2n - m = m'$ is even and $2m + n = n'$ is odd.
Case 2: m is odd and n is even, $2n - m = m'$ is odd and $2m + n = n'$ is even.
$\therefore m'$ and n' have different parity.

Let $gcd(m', n') = d$.

$d \mid m'$ and $d \mid n'$

$\therefore d \mid 2n' - m' = 5m$ and $d \mid 2m' + n' = 5n$

$\because gcd(m, n) = 1$

$\therefore d = 1$ or 5

Assume $gcd(m', n') = d = 5$.

$5 \mid m'$ and $5 \mid n'$

$$\begin{aligned} 25 \mid m'^2 + 4m'n' - n'^2 &= (2m+n)^2 + 4(2m+n)(2n-m) - (2n-m)^2 \\ &= 5n^2 + 2mn - 5m^2 \\ &= 5b \end{aligned}$$

and

$$\begin{aligned} 25 \mid m'^2 + n'^2 &= (2m+n)^2 + (2n-m)^2 \\ &= 5m^2 + 5n^2 \\ &= 5c \end{aligned}$$

$\therefore 5 \mid b$ and $5 \mid c$. But $gcd(b, c) = 1$ by Lemma 15. Contradiction.

$\therefore gcd(m', n') = 1$. ☐

Theorem 21. *There is a unique representation of a primitive PPT (a, b, c) by m and n, where*

for $5 \mid 2a - b$,

$$\begin{cases} a = 2m^2 + 2mn - 2n^2 \\ b = n^2 + 4mn - m^2 \\ c = m^2 + n^2 \end{cases}$$

for $5 \mid 2a + b$,

$$\begin{cases} a = 2m^2 - 2mn - 2n^2 \\ b = m^2 + 4mn - n^2 \\ c = m^2 + n^2 \end{cases}$$

Proof. Assume the representation is not unique. By Theorem 19,

$$\exists m, n, m_1, n_1 \in \mathbb{Z}^+ \text{ , such that}$$

for $5 \mid 2a - b$,

$$\begin{aligned} a &= 2m^2 + 2mn - 2n^2 = 2m_1^2 + 2m_1n_1 - 2n_1^2 \\ b &= n^2 + 4mn - m^2 = n_1^2 + 4m_1n_1 - m_1^2 \\ c &= m^2 + n^2 = m_1^2 + n_1^2 \end{aligned}$$

$$\begin{aligned} 5c + 2a - b = 10m^2 = 10m_1^2 &\implies m = m_1 \\ 5c - 2a + b = 10n^2 = 10n_1^2 &\implies n = n_1 \end{aligned}$$

Similarly, we can prove the result by considering $5c + 2a + b$ and $5c - 2a - b$.

$\therefore$ The representation of (a, b, c) is unique. □

m	**n**	**m'**	**n'**	**(a,b,c)**	**gcd(a,b,c)**
3	2	8	1	(22,19,13)	1
4	1	7	6	(22,31,17)	1
4	3	11	2	(38,41,25)	1
5	4	14	3	(58,71,41)	1
6	1	11	8	(58,59,37)	1
6	5	17	4	(82,109,61)	1
7	2	12	11	(62,101,53)	1
7	4	18	1	(122,79,65)	1
8	5	21	2	(158,121,89)	1
8	7	23	6	(142,209,113)	1
9	2	16	13	(118,149,85)	1
9	8	26	7	(178,271,145)	1
10	1	19	12	(178,139,101)	1

Note that all m' and n' in the above table are relatively prime and have different parity. The produced (a, b, c) are all primitive. This asserts the result in Theorem 20.

We conclude this section by the language of set theory.

Let

$$\mathcal{M} = \left\{ (m,n) \in \mathbb{Z}^+ \times \mathbb{Z}^+ \;\middle|\; \begin{array}{l} 1.\ 2n > m > n \text{ or } m > 3n, \\ 2.\ gcd(m,n) = 1,\ m \text{ and } n \text{ have different parity,} \\ 3.\ gcd(m',n') > 1,\ m' \text{ and } n' \text{ have different parity.} \end{array} \right\}$$

$$\mathcal{P} = \{(a,b,c) \in \mathbb{Z}^+ \times \mathbb{Z}^+ \times \mathbb{Z}^+ : (a,b,c) \text{ is a primitive PPT.}\}$$

We have shown that there exists a well-defined bijective mapping $f : \mathcal{M} \to \mathcal{P}$ defined by (3) and (4). [See reviewer's comment (11)]

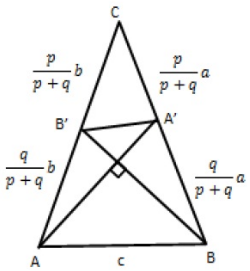
5. Extension to Rational Ratios

Instead of studying the orthogonality of medians, we extend the study on medians to lines which cut the sides of a triangle in rational ratios.

Lemma 22. *In $\triangle ABC$, let a, b and c be sides opposite to $\angle A, \angle B$ and $\angle C$, respectively. Let A' and B' be points on BC and AC respectively such that*

$$CB' : B'A = CA' : A'B = p : q,$$

where p and q are positive integers and relatively prime.



$AA' \perp BB'$ if and only if $q^2a^2 + q^2b^2 = \lambda c^2$, where $\lambda = 2p^2 + 2pq + q^2$.

Proof. $AB'A'B$ is a conves quadrilateral.

$$\begin{aligned} & AA' \perp BB' \\ \iff\quad & AB'^2 + A'B^2 = B'A'^2 + AB^2 \\ \iff\quad & \left(\frac{q}{p+q}b\right)^2 + \left(\frac{q}{p+q}a\right)^2 = \left(\frac{p}{p+q}c\right)^2 + c^2 \\ \iff\quad & q^2a^2 + q^2b^2 = p^2c^2 + (p+q)^2c^2 \\ \iff\quad & q^2a^2 + q^2b^2 = (2p^2 + 2pq + q^2)c^2 \end{aligned}$$

[See reviewer's comment (12)] $\square$

Instead of $a^2+b^2=5c^2$ in Lemma 2, the governing equation becomes

$$q^2a^2+q^2b^2=\lambda c^2.$$

Since the equation is determined by the ratio $p:q$, some properties for the orthogonality of medians (i.e. the case where $p=1$ and $q=1$) may not hold. [See reviewer's comment (13)] As some properties change, we need Theorem 23 on metric relations of a, b and c to help us extend the definition on PPT. For simplicity, we set $\lambda=2p^2+2pq+q^2$ later on.

Theorem 23. *In $\triangle ABC$, $q^2a^2+q^2b^2=\lambda c^2$ if and only if $AA'\perp BB'$ and $qa>pc$ and $qb>pc$, where p and q are relatively prime positive integers.*

Proof. By Lemma 22,

$$q^2a^2+q^2b^2=\lambda c^2 \iff AA'\perp BB'$$

By triangle inequalities,

$$\begin{aligned}
& a+c>b\\
\iff\quad & a^2+2ac+c^2>b^2\\
\iff\quad & q^2(a^2+2ac+c^2)>(2p^2+2pq+q^2)c^2-q^2a^2\\
\iff\quad & (qa+(p+q)c)(qa-pc)>0\\
\iff\quad & qa>pc
\end{aligned}$$

and

$$\begin{aligned}
& b+c>a\\
\iff\quad & b^2+2bc+c^2>a^2\\
\iff\quad & q^2(b^2+2bc+c^2)>(2p^2+2pq+q^2)c^2-q^2b^2\\
\iff\quad & (qb+(p+q)c)(qb-pc)>0\\
\iff\quad & qb>pc
\end{aligned}$$

□

Now, we can extend the definition of PPT from medians to the lines which cut the sides of a triangle in rational ratios.

Definition 24. *Triples of positive integers satisfying*

$$q^2a^2+q^2b^2=\lambda c^2 \tag{5}$$

$$\textit{and}\quad qa>pc \quad \textit{and}\quad qb>pc \tag{6}$$

where $\lambda=2p^2+2pq+q^2$, are called "pseudo-Pythagorean triples", in short "PPT".

[See reviewer's comment (14)]

Still, the definition is composed by two parts. (5) ensures the orthogonality and (6) ensures it forms a triangle.

Example 25. *The triple* $(27, 31, 26)$ *is a PPT because it satisfies (5) and (6) for* $p = 1$ *and* $q = 2$.

Next, similar to Theorem 17 and Theorem 19, we find a generator to express PPT by using two parameters, in terms of p and q. [See reviewer's comment (15)]

Theorem 26. *If there are relatively prime integers* m *and* n, *and*

$$(p+q)n > pm > pn \quad \text{or} \quad qm > (2p+q)n,$$

such that

for $(p+q)n > pm > pn$,

$$\begin{cases} a = (p+q)m^2 + 2pmn - (p+q)n^2 \\ b = pn^2 + 2(p+q)mn - pm^2 \\ c = qm^2 + qn^2 \end{cases} \tag{7}$$

for $qm > (2p+q)n$,

$$\begin{cases} a = (p+q)m^2 - 2pmn - (p+q)n^2 \\ b = pm^2 + 2(p+q)mn - pn^2 \\ c = qm^2 + qn^2 \end{cases} \tag{8}$$

then (a, b, c) *is a PPT with* $gcd(a, b, c) \mid q\lambda$.

Furthermore, $\begin{cases} \lambda \mid (p+q)a - pb & \text{if } (p+q)n > pm > pn \\ \lambda \mid (p+q)a + pb & \text{if } qm > (2p+q)n \end{cases}.$

Proof.
Case 1: Suppose $(p+q)n > pm > pn$. (a, b, c) is defined by (7).

$$\begin{aligned} & q^2a^2 + q^2b^2 \\ &= q^2((p+q)m^2 + 2pmn - (p+q)n^2)^2 + q^2(pn^2 + 2(p+q)mn - pm^2)^2 \\ &= q^2(2p^2 + 2pq + q^2)m^4 + 2q^2(2p^2 + 2pq + q^2)m^2n^2 + q^2(2p^2 + 2pq + q^2)n^4 \\ &= (2p^2 + 2pq + q^2)(qm^2 + qn^2)^2 \\ &= (2p^2 + 2pq + q^2)c^2 \end{aligned}$$

$$\begin{aligned} & m > n \\ \Longrightarrow\ & q(qm + (2p+q)n)(m-n) > 0 \\ \Longrightarrow\ & q(p+q)m^2 + 2pqmn - q(p+q)n^2 > pqm^2 + pqn^2 \\ \Longrightarrow\ & qa > pc \end{aligned}$$

and

$$\begin{aligned} & (p+q)n > pm \\ \Longrightarrow \quad & 2qm((p+q)n-pm) > 0 \\ \Longrightarrow \quad & pqn^2 + 2p(p+q)mn - pqm^2 > pqm^2 + pqn^2 \\ \Longrightarrow \quad & qb > pc \end{aligned}$$

$\therefore$ (a,b,c) is a PPT by definition.

<u>Case 2:</u> Suppose $qm > (2p+q)n$, (a,b,c) is defined by (8).

$$\begin{aligned} & q^2a^2 + q^2b^2 \\ & = q^2((p+q)m^2 - 2pmn - (p+q)n^2)^2 + q^2(pm^2 + 2(p+q)mn - pn^2)^2 \\ & = q^2(2p^2+2pq+q^2)m^4 + 2q^2(2p^2+2pq+q^2)m^2n^2 + q^2(2p^2+2pq+q^2)n^4 \\ & = (2p^2+2pq+q^2)(qm^2+qn^2)^2 \\ & = (2p^2+2pq+q^2)c^2 \end{aligned}$$

$$\begin{aligned} & qm > (2p+q)n \\ \Longrightarrow \quad & q(qm-(2p+q)n)(m-n) > 0 \\ \Longrightarrow \quad & q(p+q)m^2 - 2pqmn - q(p+q)n^2 > pqm^2 + pqn^2 \\ \Longrightarrow \quad & qa > pc \end{aligned}$$

and

$$\begin{aligned} & (p+q)m > pn \\ \Longrightarrow \quad & 2qn((p+q)m-pn) > 0 \\ \Longrightarrow \quad & pqm^2 + 2p(p+q)mn - pqn^2 > pqm^2 + pqn^2 \\ \Longrightarrow \quad & qb > pc \end{aligned}$$

$\therefore$ (a,b,c) is a PPT by definition.

Next, we show that $gcd(a,b,c) \mid q\lambda$.
Let $gcd(a,b,c) = d$.
If $(p+q)n > pm > pn$,

$$d \mid \lambda c + q(p+q)a - pqb = 2\lambda qm^2$$
$$d \mid \lambda c - q(p+q)a + pqb = 2\lambda qn^2$$

If $qm > (2p+q)n$, then

$$d \mid \lambda c + q(p+q)a + pqb = 2\lambda qm^2$$
$$d \mid \lambda c - q(p+q)a - pqb = 2\lambda qn^2$$

$\because$ $gcd(m,n) = 1$
$\therefore$ $gcd(m^2,n^2) = 1$
$\because$ m and n have different parity.

$\therefore$ We can prove that $2 \nmid d$ by considering the parity of p and q.
$\therefore d \mid \lambda q$ $\square$

Remark 27. *Note that some PPTs generated will have a common factor d, where $d \mid q$, and their corresponding primitive PPT cannot be found by the generator. However, after reducing all PPTs to a primitive PPT by dividing them by d, we can find all primitive PPTs.*

It is possible to have intersection of the solution set formed by the two inequalities. Therefore it yields two sets of triple (a, b, c) from the same (m, n). [See reviewer's comment (16)]

We illustrate our results by the following examples.

Example 28. *When $p = 1$ and $q = 2$,*

$$4(a^2 + b^2) = (2(1)^2 + 2(1)(2) + 2^2)c^2$$
$$2(a^2 + b^2) = 5c^2$$

for $3n > m > n$,

$$\begin{cases} a = 3m^2 + 2mn - 3n^2 \\ b = n^2 + 6mn - n^2 \\ c = 2m^2 + 2n^2 \end{cases} \tag{1}$$

for $m > 2n$,

$$\begin{cases} a = 3m^2 - 2pmn - 3n^2 \\ b = m^2 + 6mn - n^2 \\ c = 2m^2 + 2n^2 \end{cases} \tag{2}$$

For $m = 5$ and $n = 2$, m and n lie on both $3n > m > n$ and $m > 2n$. Therefore there are two sets of (a, b, c): $(43, 81, 58)$ and $(39, 83, 58)$.

Now we study the generators and see what kinds of m and n can form primitive PPT. We tackle the problem of the non-primitive PPTs generated by the generator by taking the transformation on (m, n).

Let m and n be two relatively prime integers, with m and n having different parity.

For $(p + q)n > pm > pn$, denote m' and n' by the transformation

$$\begin{pmatrix} m' \\ n' \end{pmatrix} = \begin{pmatrix} p + q & p \\ -p & p + q \end{pmatrix} \begin{pmatrix} m \\ n \end{pmatrix}$$

and define (a, b, c) by

$$\begin{cases} a = (p + q)m^2 + 2pmn - (p + q)n^2 \\ b = pn^2 + 2(p + q)mn - pm^2 \\ c = qm^2 + qn^2 \end{cases}$$

For $qm > (2p+q)n$, define m' and n' by the transformation

$$\begin{pmatrix} m' \\ n' \end{pmatrix} = \begin{pmatrix} p+q & -p \\ p & p+q \end{pmatrix} \begin{pmatrix} m \\ n \end{pmatrix}$$

and define (a,b,c) by

$$\begin{cases} a = (p+q)m^2 - 2pmn - (p+q)n^2 \\ b = pm^2 + 2(p+q)mn - pn^2 \\ c = qm^2 + qn^2 \end{cases}$$

Theorem 29. *Given that λ is a prime, m' and n' are relatively prime, with m' and n' having different parity, if and only if (a,b,c) is a PPT with $gcd(a,b,c) \neq q\lambda$.*

Proof. ($\Rightarrow$) By Theorem 26, (a,b,c) is a PPT with $gcd(a,b,c) \mid q\lambda$.
Assume $gcd(a,b,c) = q\lambda$.
Denote a', b' and c' by m' and n', such that
for $(p+q)n > pm > pn$,

$$\begin{aligned} m > n &\implies (2p^2+2pq+q^2)m > (2p^2+2pq+q^2)n \\ &\implies \; q((p+q)m+pn) > (2p+q)((p+q)n-pm) \\ &\implies \qquad qm' > (2p+q)n' \end{aligned}$$

$$\begin{aligned} a' &= (p+q)m'^2 - 2pm'n' - (p+q)n'^2 \\ b' &= pm'^2 + 2(p+q)m'n' - pn'^2 \\ c' &= qm'^2 + qn'^2 \end{aligned}$$

By the substitution of m' and n',

$$\begin{aligned} a' &= (2p^2+2pq+q^2)((p+q)m^2+2pmn-(p+q)n^2) = \lambda a \\ b' &= (2p^2+2pq+q^2)(pn^2+2(p+q)mn-pm^2) = \lambda b \\ c' &= (2p^2+2pq+q^2)(qm^2+qn^2) = \lambda c \end{aligned}$$

for $qm > (2p+q)n$,

$$\begin{aligned} (2p^2+2pq+q^2)n > 0 &\implies (p+q)(pm+(p+q)n) > p((p+q)m-pn) \\ &\implies \qquad (p+q)n' > pm' \end{aligned}$$

and

$$\begin{aligned} qm > (2p+q)n &\implies (p+q)m - pn > pm + (p+q)n \\ &\implies \qquad m' > n' \end{aligned}$$

$$(p+q)n' > pm' > pn'$$

$$\begin{aligned} a' &= (p+q)m'^2 - 2pm'n' - (p+q)n'^2 \\ b' &= pn'^2 + 2(p+q)m'n' - pm'^2 \\ c' &= qm'^2 + qn'^2 \end{aligned}$$

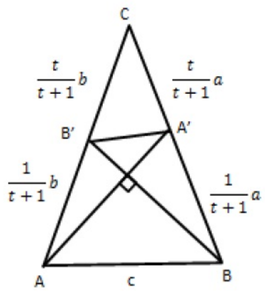
By the substitution of m' and n',

$$a' = (2p^2 + 2pq + q^2)((p+q)m^2 - 2pmn - (p+q)n^2) = \lambda a$$
$$b' = (2p^2 + 2pq + q^2)(pm^2 + 2(p+q)mn - pn^2) = \lambda b$$
$$c' = (2p^2 + 2pq + q^2)(qm^2 + qn^2) = \lambda c$$

Since $gcd(a,b,c) = q\lambda, gcd(a',b',c') = q\lambda^2$.
But by Theorem 26, $gcd(a',b',c') \neq q\lambda^2$ because m' and n' are relatively prime and have different parity. $gcd(a,b,c) \neq q\lambda$
($\Leftarrow$) We only prove for $\lambda \mid (p+q)a - pb$. The proof for $\lambda \mid (p+q)a + pb$ is similar. Since m and n have different parity, by trial and error, m' and n' have different parity. [See reviewer's comment (17)] Assume $gcd(m',n') = d > 1$.
$d \mid m'$ and $d \mid n'$
$d^2 \mid (p+q)m'^2 - 2pm'n' - (p+q)n'^2 = \lambda a$
$d^2 \mid pm'^2 + 2(p+q)m'n' - pn'^2 = \lambda b$
$d^2 \mid qm'^2 + qn'^2 = \lambda c$
$\therefore d^2 \mid \lambda a, d^2 \mid \lambda b$ and $d^2 \mid \lambda c$
$\because gcd(a,b,c) = 1$
$\therefore d^2 \mid \lambda$
But λ is a prime. Contradiction.
$\therefore gcd(m',n') = 1.$ □

6. The Special Case: $p = t$ and $q = 1$

We want to look at the case where $CB' : B'A = CA' : A'B = t : 1$.



Note that it is a special case where $p = t$ and $q = 1$.

Hence by substitution, $\lambda = 2t^2 + 2t + 1$. $a^2 + b^2 = \lambda c^2$ if and only if $AA' \perp BB'$. Also, $a > tc$ and $b > tc$.

By Theorem 26, if there are relatively prime integers m and n, with m and n having different parity, and $(t+1)n > tm > tn$ or $m > (2t+1)n$, such that for $(t+1)n > tm > tn$,

$$\begin{cases} a = (t+1)m^2 + 2tmn - (t+1)n^2 \\ b = tn^2 + 2(t+1)mn - tm^2 \\ c = m^2 + n^2 \end{cases}$$

for $m > (2t+1)n$,

$$\begin{cases} a = (t+1)m^2 - 2tmn - (t+1)n^2 \\ b = tm^2 + 2(t+1)mn - tn^2 \\ c = m^2 + n^2 \end{cases}$$

then (a, b, c) is a primitive PPT or a PPT with $gcd(a, b, c) \mid \lambda$.

Similar to Theorems 20 and 21, when λ is a prime, let m and n be two relatively prime integers, with m and n having different parity.

For $(t+1)n > tm > tn$, define m' and n' by the transformation

$$\begin{pmatrix} m' \\ n' \end{pmatrix} = \begin{pmatrix} t+1 & t \\ -t & t+1 \end{pmatrix} \begin{pmatrix} m \\ n \end{pmatrix}$$

and define (a, b, c) by

$$\begin{cases} a = (t+1)m^2 + 2tmn - (t+1)n^2 \\ b = tn^2 + 2(t+1)mn - tm^2 \\ c = m^2 + n^2 \end{cases}$$

For $m > (2t+1)n$, define m' and n' by the transformation

$$\begin{pmatrix} m' \\ n' \end{pmatrix} = \begin{pmatrix} t+1 & -t \\ t & t+1 \end{pmatrix} \begin{pmatrix} m \\ n \end{pmatrix}$$

and define (a, b, c) by

$$\begin{cases} a = (t+1)m^2 - 2tmn - (t+1)n^2 \\ b = tm^2 + 2(t+1)mn - tn^2 \\ c = m^2 + n^2 \end{cases}$$

m' and n' are relatively prime, with m' and n' having different parity, if and only if (a, b, c) is a primitive PPT.

Example 30. *When $t = 2$,*

$$a^2 + b^2 = 13c^2$$

For $3n > 2m > 2n$,

$$\begin{cases} a = 3m^2 + 4mn - 3n^2 \\ b = 2n^2 + 6mn - 2m^2 \\ c = m^2 + n^2 \end{cases}$$

For $m > 5n$,

$$\begin{cases} a = 3m^2 - 4mn - 3n^2 \\ b = 2m^2 + 6mn - 2n^2 \\ c = m^2 + n^2 \end{cases}$$

When $m = 6$ *and* $n = 1$, $(a, b, c) = (81, 106, 37)$ *is a primitive PPT.*

After the transformation of m *and* n,

$$\begin{pmatrix} m' \\ n' \end{pmatrix} = \begin{pmatrix} 3 & -2 \\ 2 & 3 \end{pmatrix} \begin{pmatrix} 6 \\ 1 \end{pmatrix} = \begin{pmatrix} 16 \\ 15 \end{pmatrix}$$

$$3m'^2 + 4m'n' - 3n'^2 = 1053 = 13 \times 81$$
$$2n'^2 + 6m'n' - 2m'^2 = 1378 = 13 \times 106$$
$$m'^2 + n'^2 = 481 = 13 \times 3$$

$(1053, 1378, 481)$ *is a PPT with* $gcd(a, b, c) = 13 \neq 1$.

When λ is not a prime, some PPTs generated will have a common factor $d > 1$, where $d \mid \lambda$, and their corresponding primitive PPT cannot be found by the generator.

Example 31. *When* $t = 6$,

$$a^2 + b^2 = 85c^2$$

For $7n > 6m > 6n$,

$$\begin{cases} a = 7m^2 + 12mn - 7n^2 \\ b = 6n^2 + 14mn - 6m^2 \\ c = m^2 + n^2 \end{cases}$$

For $m > 13n$,

$$\begin{cases} a = 7m^2 - 12mn - 7n^2 \\ b = 6m^2 + 14mn - 6n^2 \\ c = m^2 + n^2 \end{cases}$$

When $m = 12$ *and* $n = 11$,

$$a = 1745 = 5 \times 349$$
$$b = 1710 = 5 \times 342$$
$$c = 265 = 5 \times 53$$

$(349, 342, 53)$ *is a PPT, but it cannot be found by the generator. Therefore, we should divide* $(1745, 1710, 265)$ *by* 5 *in order to obtain the corresponding primitive PPT.*

It is natural to ask why it is only applicable to a prime λ. By Thue's Lemma, since $\lambda = 2t^2 + 2t + 1$ is of the form $4k+1$, if λ is a prime, it can be uniquely represented by the sum of two squares (i.e. $\lambda = t^2 + (t+1)^2$). The transformation for m and

n is unique when λ is a prime. Otherwise, if λ is a composite number, there are other ways to write down λ as sum of two squares.

We use α and β to denote the aforementioned form, i.e. $\lambda = \alpha^2 + \beta^2$, where $\alpha < t$ and $\beta > t + 1$.

$$\begin{aligned}
a > tc &\implies a > \alpha c \implies a^2 > \alpha^2 c^2 \implies (\alpha^2 + \beta^2)a^2 > \alpha^2(\alpha^2 + \beta^2)c^2 \\
&\implies \beta^2 a^2 > \alpha^2((\alpha^2 + \beta^2)c^2 - a^2) \implies \beta^2 a^2 > \alpha^2 b^2 \implies \beta a > \alpha b \\
b > tc &\implies b > \alpha c \implies b^2 > \alpha^2 c^2 \implies (\alpha^2 + \beta^2)b^2 > \alpha^2(\alpha^2 + \beta^2)c^2 \\
&\implies \beta^2 b^2 > \alpha^2((\alpha^2 + \beta^2)c^2 - b^2) \implies \beta^2 b^2 > \alpha^2 a^2 \implies \beta b > \alpha a
\end{aligned}$$

$$\begin{aligned}
a^2 + b^2 &= \lambda c^2 \\
(\alpha^2 + \beta^2)(a^2 + b^2) &= ((\alpha^2 + \beta^2)c)^2 \\
(\alpha a + \beta b)^2 + (\beta a - \alpha b)^2 &= ((\alpha^2 + \beta^2)c)^2 \qquad \text{(i)} \\
\text{or} \quad (\beta b - \alpha a)^2 + (\beta a + \alpha b)^2 &= ((\alpha^2 + \beta^2)c)^2 \qquad \text{(ii)}
\end{aligned}$$

[See reviewer's comment (18)]

By Pythagorean triples,

$$\text{Case I: } \begin{cases} \alpha a + \beta b = 2(\alpha^2 + \beta^2)mn \\ \beta a - \alpha b = (\alpha^2 + \beta^2)(m^2 - n^2) \end{cases} \implies \begin{cases} a = \beta m^2 + 2\alpha mn - \beta n^2 \\ b = \alpha n^2 + 2\beta mn - \alpha m^2 \end{cases}$$

$$\text{Case II: } \begin{cases} \beta b - \alpha a = 2(\alpha^2 + \beta^2)mn \\ \beta a + \alpha b = (\alpha^2 + \beta^2)(m^2 - n^2) \end{cases} \implies \begin{cases} a = \beta m^2 - 2\alpha mn - \beta n^2 \\ b = \alpha m^2 + 2\beta mn - \alpha n^2 \end{cases}$$

$$\text{Case III: } \begin{cases} \beta b - \alpha a = (\alpha^2 + \beta^2)(m^2 - n^2) \\ \beta a + \alpha b = 2(\alpha^2 + \beta^2)mn \end{cases} \implies \begin{cases} a = \alpha n^2 + 2\beta mn - \alpha m^2 \\ b = \beta m^2 + 2\alpha mn - \beta n^2 \end{cases}$$

$$\text{Case IV: } \begin{cases} \alpha a + \beta b = (\alpha^2 + \beta^2)(m^2 - n^2) \\ \beta a - \alpha b = 2(\alpha^2 + \beta^2)mn \end{cases} \implies \begin{cases} a = \alpha m^2 + 2\beta mn - \alpha n^2 \\ b = \beta m^2 - 2\alpha mn - \beta n^2 \end{cases}$$

Note that since a and b are symmetric to each other, Case III is equivalent to Case I and Case IV is equivalent to Case II. We may reject Cases III and IV. Moreover, $c = m^2 + n^2$ for all cases.

<u>Case I</u>:

$$\begin{aligned}
&a > tc \quad \text{and} \quad b > tc \\
\iff &\beta m^2 + 2\alpha mn - \beta n^2 > t(m^2 + n^2) \quad \text{and} \quad \alpha n^2 + 2\beta mn - \alpha m^2 > t(m^2 + n^2) \\
\iff &\frac{t + 1 - \alpha}{\beta - t} < \frac{m}{n} < \frac{\beta + t + 1}{\alpha + t}
\end{aligned}$$

<u>Case II</u>:

$$\begin{aligned} & a > tc \quad \text{and} \quad b > tc \\ \iff & \beta m^2 - 2\alpha mn - \beta n^2 > t(m^2+n^2) \quad \text{and} \quad \alpha n^2 + 2\beta mn - \alpha n^2 > t(m^2+n^2) \\ \iff & \frac{\alpha+t+1}{\beta-t} < \frac{m}{n} < \frac{\beta+t+1}{t-\alpha} \end{aligned}$$

Therefore, we have the following conclusion:

for $\dfrac{t+1-\alpha}{\beta-t} < \dfrac{m}{n} < \dfrac{\beta+t+1}{\alpha+t}$,

$$\begin{cases} a = \beta m^2 + 2\alpha mn - \beta n^2 \\ b = \alpha n^2 + 2\beta mn - \alpha m^2 \\ c = m^2 + n^2 \end{cases}$$

for $\dfrac{\alpha+t+1}{\beta-t} < \dfrac{m}{n} < \dfrac{\beta+t+1}{t-\alpha}$,

$$\begin{cases} a = \beta m^2 - 2\alpha mn - \beta n^2 \\ b = \alpha m^2 + 2\beta mn - \alpha n^2 \\ c = m^2 + n^2 \end{cases}$$

Let m and n be two relatively prime integers, with m and n having different parity.

For $\dfrac{t+1-\alpha}{\beta-t} < \dfrac{m}{n} < \dfrac{\beta+t+1}{\alpha+t}$, define m' and n' by the transformation

$$\begin{pmatrix} m' \\ n' \end{pmatrix} = \begin{pmatrix} \beta & \alpha \\ -\alpha & \beta \end{pmatrix} \begin{pmatrix} m \\ n \end{pmatrix}$$

and define (a, b, c) by

$$\begin{cases} a = \beta m^2 + 2\alpha mn - \beta n^2 \\ b = \alpha n^2 + 2\beta mn - \alpha m^2 \\ c = m^2 + n^2 \end{cases}$$

For $\dfrac{\alpha+t+1}{\beta-t} < \dfrac{m}{n} < \dfrac{\beta+t+1}{t-\alpha}$, define m' and n' by the transformation

$$\begin{pmatrix} m' \\ n' \end{pmatrix} = \begin{pmatrix} \beta & -\alpha \\ \alpha & \beta \end{pmatrix} \begin{pmatrix} m \\ n \end{pmatrix}$$

and define (a, b, c) by

$$\begin{cases} a = \beta m^2 - 2\alpha mn - \beta n^2 \\ b = \alpha m^2 + 2\beta mn - \alpha n^2 \\ c = m^2 + n^2 \end{cases}$$

If m' and n' are relatively prime, with m' and n' having different parity, then (a, b, c) is a primitive PPT.

We can prove it with a similar approach to Theorem 20 by assuming
$$gcd(a,b,c) = \lambda = \alpha^2 + \beta^2.$$

Example 32. *When* $t = 6, \alpha = 2$ *and* $\beta = 9$.

For $\frac{5}{3} < \frac{m}{n} < 2$,
$$\begin{cases} a = 9m^2 + 4mn - 9n^2 \\ b = 2n^2 + 18mn - 2m^2 \\ c = m^2 + n^2 \end{cases}$$
For $3 < \frac{m}{n} < 4$,
$$\begin{cases} a = 9m^2 - 4mn - 9n^2 \\ b = 2m^2 + 18mn - 2n^2 \\ c = m^2 + n^2 \end{cases}$$
When $m = 7$ *and* $n = 2, 3 < \frac{m}{n} < 4$, $(a,b,c) = (349, 342, 53)$.
When $m = 15$ *and* $n = 8, \frac{5}{3} < \frac{m}{n} < 2$, $(a,b,c) = (1929, 1838, 289)$.
When $m = 23$ *and* $n = 6, 3 < \frac{m}{n} < 4$, $(a,b,c) = (3885, 3470, 565)$.
Since $gcd(3885, 3470, 565) = 5$, *we should divide the triple by* 5 *in order to obtain* $(777, 694, 113)$, *the corresponding primitive PPT.*

7. Conclusion

In the first part, we have found that for the orthogonality of medians, we have the metric relation $a^2 + b^2 = 5c^2$ as the governing equation. [See reviewer's comment (19)] We define PPT as the integral triple which satisfies the governing equation and triangle inequalities. Based on the findings and with reference to the Pythagorean triples, we then create a PPT generator. Different from the Pythagorean triple generator, it generates not only primitive PPTs but also PPTs with common factor. Therefore the transformations of the parameters is introduced to tackle the problem as we want to classify primitive PPTs from all PPTs.

Then, we extend and redefine the concept of PPT and have further investigation on the orthogonality of lines which cut the sides in a rational ratio $p : q$. Similar to the previous part, we find that the governing equation becomes $q^2(a^2 + b^2) = \lambda c^2$, and it also has a generator in terms of p and q. [See reviewer's comment (20)] There is also a problem of generating non-primitive PPTs, so a transformation on the parameters is also introduced. This is a more general solution.

In the third part, we focus on the special case that $p = t$ and $q = 1$. The governing equation becomes $a^2 + b^2 = (2t^2 + 2t + 1)c^2$. This has special properties as we can make use of Thue's Lemma to show that it has the same properties as median does when $2t^2 + 2t + 1$ is a prime. Otherwise, if it is not the case that $2t^2 + 2t + 1$ is a prime, we find another way to express the generator and transformation.

Acknowledgement

We deeply thank Mr. Lee Kwok Chu and Mr. So Pak Yeung for guiding us and giving us inspiring questions.

REFERENCES

[1] Wladimir G. Boskoff, L. Homentcovschi and B. D. Suceav, *Some theorems about perpendicular lines, proved using an extension of Pythagoras' theorem*, Mathematical Gazette **93** (2009), no. 526, p.119-125, Note 93.15.
[2] Kenneth H. Rosen, *Elementary Number Theory and its Applications*, Fifth Edition, Pearson, Addison-Wesley, 2005.

Reviewer's Comments

General Comments

The flow of this report was generally well. The report had literature review, and state the aim of each section clearly. The linkage between sections was also found. The organization of the report was good, but one needs some clarifications at certain parts.

The writing of abstract was unsatisfactory, and especially the last sentence in the abstract was quite strange. In the first sentence of abstract, one would be better if we change *solution set* to *solution*, and we may rephrase the last sentence as *In view of the Pythagorean triple. we device some generalizations to the lines from vertices to their opposite sides at any arbitrary rational ratios.*

Section 1 is about introduction. Usually we write in the form: *In Section 2, we define..., In Sections 3 & 4, we investigate...* rather than only use such words 'at the beginning', 'Then' and 'In the third part'. The word 'metric', which first appeared in Section 1, may need more elaborations.

One may expect that before each lemmas and theorems, some illustrations should be introduced.

The writing of proofs can be improved. A lot of isolated equations in the proofs without explaining the logical relationship between them were found, for example, Lemma 1, Lemma 3, Theorem 4, Theorem 8, Theorem 19 and Theorem 29. Symbols $\Rightarrow$, $\Leftarrow$ and $\Leftrightarrow$ were used repeatedly, please check there is any abuses in the report. The proofs of Theorems 20, 26 and 29 are rather unclear, please try to say a few words on the outline of proof at the beginning. One may change 'Contradiction.' to 'Contradiction occurs.' in the proofs of Theorems 20 and 29. Pay special attention on Theorem 19, it seems that these two conditions $5|2a-b$ and $5|2a+b$ can be obtained from $a^2+b^2=5c^2$. The proofs of Theorems 19 and 26 were badly written. Case 1 and Case 2 should not be used in this way. It would be better if one writes *set* $r=m^2$ *and* $s=n^2$ instead of 'there are integers m and n such that $r=m^2$ and $s=n^2$' The proofs of Theorems 20 and 29 were quite disorganised. Near the end of the only if part in the proof of Theorem 20, the logical dependence of each line was not clear. In the if part of the proof of Theorem 20, the reason why we need to show that m' and n' have different parity is not clear and at the starting point one may not need case by case. In the proof of Theorem 20, one may rewrite the part proving $gcd(m',n')=1$ as follows: *Let* $d=gcd(m',n')$, *then* d *divides* m' *and* n'. *By linearity,* $d|2n'-m'=5m$ *and* $d|2m'-n'=5n$, *and hence* $d|\gcd(5m,5n)=5\gcd(m,n)$. *Since* $\gcd(m,n)=1$, $d=1$ *or* 5. *Suppose* $d=5$, *one gets* $25|m'^2+4m'n'-n'^2=5b$ *and* $25|m'^2+n'^2=5c$. *So we have that* 5 *divides both* b *and* c. *On the other hand, by Lemma 15,* b *and* c *are coprime. Contradiction occurs so* $d=1$. *Therefore* $gcd(m',n')=1$. The proof of Theorem 29 carries the similar situation.

It would be better if the report have a detailed normal citation system.

For a report of such large number of pages, some typographical and minor mistakes are unavoidable. In the next section some spotted mistakes will be marked.

<u>Comments</u>

1. 'using the technique of transformation of parameters' is rather unclear.
2. 'special type of triangles' is rather unclear.
3. Example 7 has some mistakes in calculation.
4. We may add a big left brace on the left.
5. Definition can be rewritten as *A triple of positive integers satisfying (1) and (2) is called "pseudo-Pythagorean triple", in short, "PPT".*
6. The fundamental theorem of arithmetic was implicitly used.
7. $\gcd(r, s) = 1$ was implicitly used.
8. 'quickly' was used strangely.
9. Change 'the examples of PPT' to 'two tables of examples of PPTs'.
10. Two tables should have names.
11. 'We have shown that...' is rather unclear.
12. Lemma 1 was used implicitly.
13. The sentence 'Since the equation ... hold.' is rather unclear
14. Rewrite as *For positive integers p and q, a triple of positive integers satisfying*
$$\begin{cases} q^2a^2 + q^2b^2 = \lambda c^2 & ...(5) \\ qa > pc \text{ and } qb > pc & ...(6), \end{cases}$$
where $\lambda = 2p^2 + 2pq + q^2$, is called "pseudo-Pythagorean triple", in short, "PPT".
15. Change 'express PPT' to 'express all PPTs'.
16. The whole paragraph is rather unclear.
17. How does the method by trial and error come in?
18. Equations (i) and (ii) haven't appeared once defined.
19. 'In the first part,...' is rather unclear.
20. 'it also has...' is rather unclear.