PYTHAGOREAN TRIPLES

M. SUNIL R. KOSWATTA
HARPER COLLEGE, ILLINOIS

Abstract. This talk is based on a three week summer workshop (Los Angeles 2004) conducted by Professor Hung-Hsi Wu, University of California, Berkeley, on Algebra for K-12 teachers. Professor Wu has been conducting workshops for K-12 teacher in many parts of the country for several years. He is a member of the National Math Panal.

Three positive integers a, b, c form a **Pythagorean triple** $\{a, b, c\}$ if $a^2 + b^2 = c^2$. In other words, a, b and c are lengths of three sides of a right triangle. Almost everybody know that $\{3, 4, 5\}$, $\{5, 12, 13\}$, and $\{8, 15, 17\}$ are Pythagorean triples. But are there others?

Pythagorean triples can be produced at will by solving an extremely simple linear system of equations. It can be shown that this method produces *all* the Pythagorean triples.

"One would like to say that this method is due to Babylonians some 3800 years ago, but a more accurate statement would be that it is the algebraic rendition of the method one infers from a close reading of the cuneiform tablet, Plimpton 322[1] which listed fifteen Pythagorean triples. Lest you entertain for even a split second the idle thought that people couldn't have known such advanced mathematics thirty-eight centuries ago and that these triples were probably hit upon by trial and error, let it be noted that the largest triple (in Plimpton 322) is $\{12709, 13500, 18541\}$."[2] More amazingly, these were the work of a pupil probably doing his assigned homework from school.[3]

Theorem 1. *Let (u, v) be the solution of the linear system*

$$\begin{cases} u + v = \dfrac{t}{s} \\[2ex] u - v = \dfrac{s}{t} \end{cases}$$

where s and t are positive integers with $s < t$. If we write u and v as two fractions with the same denominator , $u = \dfrac{c}{b}$ and $v = \dfrac{a}{b}$, then $\{a, b, c\}$ is a Pythagorean triple.

[1]From the Plimpton collection of cuneiform tablets in the Colombia University
[2]Wu
[3]Robson

Proof of this theorem is very simple and should be accessible to any one with high school algebra background.

Proof. Multiply corresponding sides of the two equations in the theorem to get $(u+v)(u-v) = \frac{t}{s} \cdot \frac{s}{t}$ or $u^2 - v^2 = 1$. So with, $u = \frac{c}{b}$ and $v = \frac{a}{b}$, we have $\left(\frac{c}{b}\right)^2 - \left(\frac{a}{b}\right)^2 = 1$. Multiplying through both sides of this equality by b^2 gives $c^2 - a^2 = b^2$ and therefore, $a^2 + b^2 = c^2$. □

Let us use theorem 1 to produce some new Pythagorean triples.

EXAMPLE 1: Consider

$$\begin{cases} u + v = 2 \\ u - v = \frac{1}{2} \end{cases}$$

You get $2u = \frac{5}{2}$ so that $u = \frac{5}{4}$ by adding the two equations. Eliminating u (by subtracting) from the same two equations you get $2v = \frac{3}{2}$ so that $v = \frac{3}{4}$. Thus, the triple retrieved from this system of linear equations is $\{3, 4, 5\}$.

EXAMPLE 2: Consider

$$\begin{cases} u + v = \frac{3}{2} \\ u - v = \frac{2}{3} \end{cases}$$

Adding the two equations gives $u = \frac{13}{12}$. Substituting u in the second equation gives $v = \frac{5}{12}$. Therefore, by theorem 1, $\{5, 12, 13\}$ is a Pythagorean triple.

EXAMPLE 3: Consider

$$\begin{cases} u + v = \frac{4}{3} \\ u - v = \frac{3}{4} \end{cases}$$

Adding the two equations gives $u = \frac{25}{24}$. Substituting u in the second equation gives $v = \frac{7}{24}$. Therefore, by theorem 1, $\{7, 24, 25\}$ is a Pythagorean triple.

EXAMPLE 4: Consider

$$\begin{cases} u + v = \dfrac{69}{2} \\ \\ u - v = \dfrac{2}{69} \end{cases}$$

Adding the two equations gives $u = \frac{4765}{276}$. Substituting u in the second equation gives $v = \frac{4757}{276}$. theorem 1 guarantees that $\{276, 4757, 4765\}$ is a Pythagorean triple.

EXAMPLE 5: Consider

$$\begin{cases} u + v = \dfrac{179}{71} \\ \\ u - v = \dfrac{71}{179} \end{cases}$$

Adding the two equations gives $u = \frac{37082}{25418}$. Substituting u in the second equation gives $v = \frac{27000}{25418}$. theorem 1 guarantees that $\{27000, 25418, 37082\}$ is a Pythagorean triple.

We define a Pythagorean triple $\{a, b, c\}$ to be **primitive** if the integers a, b and c have no common divisor other than 1. We say that a Pythagorean triple is a **multiple** of anther Pythagorean triple $\{a', b', c'\}$ if there is a positive integer n so that $a = na'$, $b = nb'$ and $c = nc'$. In this terminology, a given Pythagorean triple is either primitive, or is a multiple of a primitive Pythagorean triple.

EXAMPLE 6: Consider

$$\begin{cases} u + v = 5 \\ \\ u - v = \dfrac{1}{5} \end{cases}$$

Adding the two equations you get $2u = \frac{26}{5}$ so that $u = \frac{26}{10}$. Eliminating u (by subtracting) from the same two equations you get $2v = \frac{24}{5}$ so that $v = \frac{24}{10}$. Thus, by

Theorem 3, $\{10, 25, 26\}$ is a Pythagorean triple. This is not primitive because it is a multiple of the primitive Pythagorean triple $\{5, 12, 13\}$.

However, if we have taken the trouble to reduce $u = \dfrac{26}{10}$ to its lowest terms, then we would obtain $u = \dfrac{13}{5}$ and the primitive triple $\{5, 12, 13\}$ would be the result. Thus we see that different values of s and t do not always lead to distinct primitive Pythagorean triples.

We now explain the genesis of Theorem 1. We assume that we already have a Pythagorean triple $\{a, b, c\}$ and proceed to find what it must be. By assumption, $a^2 + b^2 = c^2$. By dividing this equation through by b^2, we get

$$\left(\frac{a}{b}\right)^2 + 1 = \left(\frac{c}{b}\right)^2. \tag{1}$$

Let $u = \dfrac{c}{b}$ and $v = \dfrac{a}{b}$. Thus u and v are both fractions and $u > v$. Now (1) becomes $v^2 + 1 = u^2$ and therefore,

$$u^2 - v^2 = 1. \tag{2}$$

Since $u^2 - v^2 = (u + v)(u - v)$, we get $(u + v)(u - v) = 1$. Since both $(u + v)$ and $(u - v)$ are known fractions, let s, t be two positive integers with $s < t$ so that $u + v = \dfrac{t}{s}$. Because $(u + v)(u - v) = 1$, necessarily, $u - v = \dfrac{s}{t}$. Therefore, we have:

$$\begin{cases} u + v = \dfrac{t}{s} \\[2ex] u - v = \dfrac{s}{t} \end{cases} \tag{3}$$

where s and t are positive integers with $s < t$. From this point of view, Theorem 1 is inevitable.

We can refine Theorem 1 by directly solving system (3).

Adding the two equations, we get $2u = \frac{t}{s} + \frac{s}{t} = \frac{t^2+s^2}{st}$, and therefore,

$$u = \frac{t^2+s^2}{2st}.$$

By substituting u in the second equation of (3), we get,

$$v = \frac{t^2-s^2}{2st}.$$

A simple computation gives,

$$\left(\frac{t^2-s^2}{2st}\right)^2 + 1 = \left(\frac{t^2+s^2}{2st}\right)^2.$$

Multiplying both sides by $(2st)^2$, we get

$$(t^2-s^2)^2 + (2st)^2 = (t^2+s^2)^2.$$

This shows that if s, t are positive integers and $t > s$, then

$$\{2st, t^2-s^2, t^2+s^2\} \text{ is a Pythagorean triple.}$$

We say that two integers x and y are **relatively prime** if x and y have no common divisors other than ± 1. We will use the notation $(x, y) = 1$ to indicate that x and y are relatively prime. We use the notation $(x, y) = z$ to indicate that z is the greatest common divisor of x and y.

If $\{a, b, c\}$ is a Pythagorean triple and if $(a, b) = n$ then n divides c. Therefore, if $a = a'n$, $b = b'n$ and $c = c'n$ then $\{a', b', c'\}$ is a triple with $(a', b') = 1$.

In other words, $\{a', b', c'\}$ is a primitive triple and $\{a, b, c\}$ is a multiple of $\{a', b', c'\}$. Therefore, we will consider $\{a, b, c\}$ to be a primitive triple for the rest of the discussion.

Both a and b cannot be even because if so, then $(a, b) \neq 1$. We claim that both a and b cannot be odd either. We can establish this claim by using proof by contradiction method. Assume that both a and b are odd. That is, $a = n + 1$ and $b = m + 1$ for two even integers n and m. Then

$$a^2 + b^2 = (n + 1)^2 + (m + 1)^2 = n^2 + m^2 + 2n + 2m + 2 = c^2$$

That is,

$$c^2 - 2 = n^2 + m^2 + 2n + 2m$$

Since n and m are even, 4 divides $(c^2 - 2)$. Now this is the contradiction we sought. c is a positive integer. Therefore, it is either even or odd. If c is even the c^2 is divisible by 4. Therefore, $c^2 - 2$ is not divisible by 4. If c is odd, then $c^2 - 1$ is divisible by 4. (Assume $c = k + 1$ for some even integer k. Then $c^2 = k^2 + 2k + 1$ and $c^2 - 1 = k^2 + 2k$.) Therefore, $c^2 - 2$ is not divisible by 4. Therefore, if $\{a, b, c\}$ is primitive then a and b are of opposite parity. Without loss of generality, lets assume that a is even.

Theorem 2. *If a, b, and c are positive integers, then the most general solution of the equation $a^2 + b^2 = c^2$, satisfying the conditions, $(a, b) = 1$, and a is even is*

$$a = 2st, b = t^2 - s^2, c = t^2 + s^2$$

where s, t are integers of opposite parity and $(s, t) = 1$ and $t > s > 0$. Moreover there is a 1-1 correspondence between different values of s, t and different values of a, b, c.[4]

Proof. First assume that $\{a, b, c\}$ is a primitive Pythagorean triple and a is even and b is odd.

Since b is odd, let $b = m + 1$ for some even integer m. Then $c^2 = a^2 + m^2 + 2m + 1$ and therefore, c^2 is odd and hence, c is odd. Also, $(b, c) = 1$. If not, then $(b, c) = n$ for some positive integer $n \neq 1$. That means, $c = nc'$ and $b = nb'$ and $c^2 - b^2$ is divisible by n^2 and therefore, a is divisible by n. This contradicts the fact that $(a, b) = 1$.

Since both b and c are odd, $\frac{1}{2}(c - b)$ and $\frac{1}{2}(c + b)$ are positive integers. Also, $\left(\frac{1}{2}(c - b), \frac{1}{2}(c + b)\right) = 1$. If not, then $\left(\frac{1}{2}(c - b), \frac{1}{2}(c + b)\right) = d$, for some positive integer $d \neq 1$. That is, $\frac{c+b}{2} = dx$ and $\frac{c-b}{2} = dy$ for some positive integers x and y and $x > y$. That means, $c = d(x + y)$ and $b = (x - y)$. This contradicts the fact that $(b, c) = 1$.

Now $\left(\frac{a}{2}\right)^2 = \left(\frac{c - b}{2}\right) \cdot \left(\frac{c + b}{2}\right)$.

The two factors on the right, being relatively prime, must both be squares.

Let $\frac{c - b}{2} = s^2$ and $\frac{c + b}{2} = t^2$. Clearly, $t > s > 0$. Also, $(s, t) = 1$. If not, then $(s, t) = u$ for some postive integer $u \neq 1$. That is $s = us'$ and $t = ut'$ for some positive integers s' and t'. Then $(s^2, t^2) \neq 1$ and this is a contradiction.

[4]Hardy and Wright

Since $(t, s) = 1$, both t and s cannot be even. If both t and s are odd, say $t = n + 1$ and $s = m + 1$ for positive even integers n and m and $n > m$, then $b = t^2 - s^2 = (n - m)(n + m + 2)$ being product of two even integers is even and that is a contradiction. Therefore, s and t are of opposite parity.

Now assume that s and t are two positive integers of opposite parity, $(s, t) = 1$ and $t > s > 0$ so that $a = 2st, b = t^2 - s^2, c = t^2 + s^2$. Then $a^2 + b^2 = 4s^2t^2 + (t^2 - s^2)^2 = (t^2 + s^2)^2 = c^2$. Hence, $\{a, b, c\}$ is a Pythagorean triple, a is even and b is odd. If $(a, b) = d$ for some positive integer $d \geq 1$, then d divides a, b and hence c and therefore, d divides $t^2 - s^2$ and $t^2 + s^2$. That is, $t^2 - s^2 = dm$ and $t^2 + s^2 = dn$ for some positive integers m and n and $m > n$. That means, $2t^2 = d(n + m)$ and $2s^2 = d(n - m)$. Therefore, d divides both $2t^2$ and $2s^2$. But, clearly, $(t^2, s^2) = 1$ since $(t, s) = 1$. Therefore, d must be either 1 or 2. But d divides b and b is odd. Therefore, d is 1 and $(a, b) = 1$.

Finally, if b and c are given then s^2, and t^2 are uniquely determined and as a consequence s and t are uniquely determined. □

References

[1] Hung-Hsi Wu, *"Introduction to School Algebra [DRAFT]"* , http://math.berkeley.edu/ wu/, June 2006.

[2] G.H. Hardy and E.M. Wright *"An Introduction to the Theory of Numbers"*, Oxford University Press.

[3] O. Neugebauer *"The Exact Sciences in Antiquity"*, Brown University Press.

[4] R. Creighton Buck *"Sherlock Holmes in Babylon"*, The American Mathematical Monthly, Vol. 87, No. 5. (May, 1980), pp. 335-345.

[5] Eleanor Robson *"Neither Sherlock Holmes nor Babylon": A reassessment of Plimpton 322"*, Historia Mathematica, 28 (2001), 167-206.

[6] Eleanor Robson *"Words and Pictures: New Light on Plimpton 322"*, The American Mathematical Monthly, February (2002), 105-120.

e-mail: skoswatt@harpercollege.edu