Pythagorean triples

Learning Objectives. By the end of class, students will be able to:

- Define a nonlinear Diophantine equation
- Define a primitive Pythagorean triple
- Prove the formula for generating primitive Pythagorean triples .

One of the most famous math equations is $x^2 + y^2 = z^2$, probably because we learn it in high school. We are going to classify all integer solutions to the equation.

Definition 1. A triple (x, y, z) of positive integers satisfying the Diophantine equation $x^2 + y^2 = z^2$ is called *Pythagorean triple.*

Select the Pythagorean triples:

Select All Correct Answers:

(a) 3,4,5 ✓

(b) 5,12,13 ✓

(c) -3,4,5

(d) 6,8,10 ✓

(e) 0,1,1

It is actually possible to classify all Pythagorean triples, just like we did for linear Diophantine equations in two variables. To simplify this process, we will work with $x, y, z > 0$, and $(x, y, z) = 1$. For any given solution of this form, we have that $(-x, y, z), (x, -y, z), (x, y, -z), (-x, -y, z), (x, -y, -z), (-x, y, -z)$, and $(-x, -y, -z)$ are also solutions to the Diophantine equation, as is (nx, ny, nz) for any integer n. Thus, we call such a solution a *primitive Pythagorean triple*. We call $(0, n, \pm n)$ and $(n, 0, \pm n)$ the *trival solutions*.

Theorem 1. For a primitive Pythagorean triple (x, y, z), exactly one of x and y is even.

Proof If x and y are both even, then z must also be even, contradicting that $(x, y, z) = 1$.

If x and y are both odd, then z is even. Now we can work modulo 4 to get a contradiction. Since x and y are odd, we have that $x^2 \equiv y^2 \equiv 1 \pmod 4$. Since z is even, we have that $z^2 \equiv 0 \pmod 4$, but $x^2 + y^2 \equiv 2 \pmod 4$.

Thus, the only remaining option is exactly one of x and y is even. ■

Theorem 2 (Theorem 6.3)**.** There are infinitely many primitive Pythagorean triples x, y, z with y even. Furthermore, they are given precisely by the equations

$$\begin{aligned} x &= m^2 - n^2 \\ y &= 2mn \\ z &= m^2 + n^2 \end{aligned}$$

where $m, n \in \mathbb{Z}, m > n > 0, (m, n) = 1$ and exactly one of m and n is even.

Example 1. (a) $m = 2$ and $n = 1$ satisfy the conditions of m and n in the theorem. This gives $x = 3, y = 4, z = 5$.

(b) $m = 3$ and $n = 2$ gives $x = 5, y = 12, z = 13$.

Learning outcomes:
Author(s): Claire Merriman

(c) Try with your own values of m and n.

Proof We first show that given a primitive Pythagorean triple with y even, there exist m and n as described. Since y is even, y and z are both odd. Moreover, $(x, y) = 1, (y, z) = 1$, and $(x, z) = 1$. Now,

$$y^2 = z^2 - x^2 = (x + z)(z - x)$$

implies that

$$\left(\frac{y}{2}\right)^2 = \frac{(x+z)}{2}\frac{(z-x)}{2}.$$

To show, $\left(\frac{(x+z)}{2}, \frac{(z-x)}{2}\right) = 1$, let $\left(\frac{(x+z)}{2}, \frac{(z-x)}{2}\right) = d$. Then $d \mid \frac{z+x}{2}$ and $d \mid \frac{z-x}{2}$. Thus, $d \mid \frac{z+x}{2} + \frac{z-x}{2} = z$ and $d \mid \frac{z+x}{2} - \frac{z-x}{2} = x$. Since $(x, z) = 1$, we have that $d = 1$. Thus, $\frac{(x+z)}{2}$ and $\frac{(z-x)}{2}$ are perfect squares. Let

$$m^2 = \frac{(x+z)}{2}, \quad n^2 = \frac{(z-x)}{2}.$$

Then $m > n > 0, (m, n) = 1, m^2 - n^2 = x, 2mn = y$, and $m^2 + n^2 = z$. Also, $(m, n) = 1$ implies that not both m and n are both even. If both m and n are odd, we have that z and x are both even, but $(x, z) = 1$. This proves that every primitive Pythagorean triple has this form.

Now we prove that given any such m and n, we have a primitive Pythagorean triple. First, $(m^2 - n^2)^2 + (2mn)^2 = m^4 - 2m^2n^2 + n^4 + 4m^2n^2 = (m^2 + n^2)^2$. We need to show that $(x, y, z) = 1$. Let $(x, y, z) = d$. Since exactly one of m and n is even, we have that x and z are both odd. Then d is odd, and thus $d = 1$ or d is divisible by some odd prime p. Assume that $p \mid d$. Thus, $p \mid x$ and $p \mid z$. Thus, $p \mid z + x$ and $p \mid z - x$. Thus, $p \mid (m^2 + n^2) + (m^2 - n^2) = 2m^2$ and $p \mid (m^2 + n^2) - (m^2 - n^2) = 2n^2$. Since p is odd, we have that $p \mid m^2$ and $p \mid n^2$, but $(m, n) = 1$, so $d = 1$. ■