Nonlinear Diophantine equations and 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.

Reading None

0.1 Nonlinear Diophantine equations

Definition 1. A Diophantine equation is *nonlinear* if it is not linear.

Example 1. (a) The Diophantine equation $x^2 + y^2 = z^2$ is our next section. Solutions are called Pythagorean triples.

(b) Let $n \in \mathbb{Z}$ with $n \geq 3$. The Diophantine equation $x^n + y^n = z^n$ is the subject of the famous Fermat's Last Theorem. We will also prove one case of this.

(c) Let $n \in \mathbb{Z}$. The Diophantine equation $x^2 + y^2 = n$ tells us which integers can be represented as the sum of two squares.

(d) Let $d, n \in \mathbb{Z}$. The Diophantine equation $x^2 - dy^2 = n$ is known as Pell's equation.

Sometimes we can use congruences to show that a particular nonlinear Diophantine equation has no solutions.

Example 2. Prove that $3x^2 + 2 = y^2$ is not solvable.

Solution: Assume that there is a solution. Then any solution to the Diophantine equation is also a solution to the congruence $3x^2 + 2 \equiv y^2 \mod 3$, which implies $2 \equiv y^2 \mod 3$, which we know is false. Thus there are no integer solutions to $3x^2 + 2 = y^2$.

Note: viewing the same equation modulo 2 says $x^2 \equiv y^2 \mod 2$, which does not give us enough information to prove a solution does not exist–it also is not enough information to conclude a solution exists.

0.2 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 2. 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:

Learning outcomes:
Author(s): Claire Merriman

(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

$$x = m^2 - n^2$$
$$y = 2mn$$
$$z = m^2 + n^2$$

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

Example 3. (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 $x = 5, y = 12, z = 13$.

(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 $d = 1$. ■

0.3 Sums of Squares

The first result will prove which primes can be written as the sum of two squares. Note $1^2 + 1^2 = 2$, and if a is a positive integer such that $a \equiv 3 \pmod 4$, then a cannot be written as the sum of two squares.

Proposition (Proposition 6.5)**.** Let $m, n \in \mathbb{Z}$ with $m, n > 0$. If m and n can be written as the sums of two squares of integers, then mn can be written as the sum of two squares of integers.

Proof Let $m, n \in \mathbb{Z}$ with $m, n > 0$ and assume that there exists $a, b, c, d \in \mathbb{Z}$ such that $m = a^2 + b^2$ and $n = c^2 + d^2$. Then

$$
\begin{aligned}
mn = (a^2 + b^2)(c^2 + d^2) &= a^2c^2 + b^2c^2 + a^2d^2 + b^2d^2 \\
&= a^2c^2 + 2abcd + b^2d^2 + a^2d^2 - 2abcd + b^2c^2 \\
&= (ac + bd)^2 + (ad - bc)^2.
\end{aligned}
$$

■