April 6–Pythagorean triples and Fermat's Last Theorem

We will prove a formula for generating Pythagorean triples. We will also prove some cases of Fermat's Last Theorem.

Pythagorean triples

From last time, we have that *primitive Pythagorean triples* are solutions to $x^2 + y^2 = z^2$ with $x, y, z > 0$ and $(x, y, z) = 1$. For a primitive Pythagorean triple (x, y, z), exactly one of x and y is even.

Theorem 1. 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.

Before proving this theorem, we illustrate it with some examples:

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 $x = 5, y = 12, z = 13$.

(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

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

Learning outcomes:
Author(s):

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 $d = 1$. ■

While this proof is not obvious, it does not use any concepts beyond chapter 1. Thus, this proof is considered *elementary*. Such elementary proofs often involve deep insights and intricate calculations, but no concepts beyond what we are learning in this course (and often not including things like divisor sums).

Fermat's Last Theorem

After the Diophantine equation $x^2 + y^2 = z^2$, one generalization is $x^n + y^n = z^n$ for $n \geq 3$. Fermat's Last Theorem was first conjectured in 1637 and proven in 1995 by Andrew Wiles. Attempts to solve this problem through the centuries have created new branches of mathematics.

Theorem 2 (Fermat's Last Theorem)**.** The Diophantine equation $x^n + y^n = z^n$ has no nonzero integer solutions for $n \geq 3$.

We will show that it suffices to prove Fermat's Last Theorem for the cases of n and odd prime and $n = 4$.

Theorem 3. The Diophantine equation $x^n + y^n = z^n$ has a solution no solutions for $n \geq 3$ if and only if there are no solutions for n and odd prime or $n = 4$.

Proof Let $n \in \mathbb{Z}$ and $n \geq 3$. Let $n = ab$ where $a, b \in \mathbb{Z}$ and b is either an odd prime or 4. If x, y, z is a solution to $x^n + y^n = z^n$, then x^a, y^a, z^a is a

solution to $x^b + y^b = z^b$. By contraposition, if $x^b + y^b = z^b$ has no solutions, then $x^n + y^n = z^n$ has no solutions. ■

We will prove the case where $n = 4$ using the *method of decent.* This is the only case that Fermat proved. The next 400+ years were spent proving the theorem for odd primes.

The idea of the method of decent for proving no solution exists for a Diophantine equation is to assume a solution exists. Then use this solution to construct one that has one component that is strictly smaller than the original solution. This process could be repeated indefinitely, but it is not possible to construct an infinitely decreasing list of positive integers. Thus, no solution exists.

Theorem 4. The Diophantine equation $x^4 + y^4 = z^2$ has not solutions in nonzero integers x, y, z.

Note: If x, y, z is a solution to $x^4 + y^4 = z^4$, then

Multiple Choice:

(a) x, y, z

(b) x, y, z^2 ✓

is a solution to $x^4+y^4 = z^4$. By contraposition, if $x^4+y^4 = z^2$ has no solutions, then $x^4 + y^4 = z^4$ has no solutions.

Proof Assume by way of contradiction, that $x^4 + y^4 = z^2$ has a solution x_1, y_1, z_1 nonzero integers. Without loss of generality, we may assume $x_1, y_1, z_1 > 0$ and $(x_1, y_1) = 1$. We will show that there is another solution x_2, y_2, z_2 positive integers such that $(x_2, y_2) = 1$ and $0 < z_2 < z_1$. Now, $(x_1)^2, (y_1)^2, z_1$ is a Pythagorean triple with $(x_1^2, y_1^2, z_1) = 1$, and without loss of generality, y_1^2 is even. Thus, by the first theorem of the day says that there exists $m, n \in \mathbb{Z}$ such that $(m, n) = 1, m > n > 0$, and exactly one of m and n is even such that $x_1^2 = m^2 - n^2, y_1^2 = 2mn, z_1 = m^2 + n^2$. Now, $x_1^2 = m^2 - n^2$ implies $x_1^2 + n^2 = m^2$ and x_1, m, n is a Pythagorean triple with $(x_1, m, n) = 1$ and n is even. Applying the same theorem again, we get that there exists $a, b \in \mathbb{Z}$ with $(a, b) = 1, a > b > 0$, exactly one of a and b is even, with $x_1 = a^2 - b^2, n = 2ab, m = a^2 + b^2$.

We want to show that m, a and b are perfect squares. Now, $y_1^2 = 2mn = m(2n)$ and $(m, 2n) = 1$, we have that

Select All Correct Answers:

(a) m ✓

(b) n

(c) 2n ✓

are perfect squares. Thus, there exists $c \in \mathbb{Z}$ such that $2n = 4c^2$ or, equivalently, $n = 2c^2$. Now, $n = 2ab$ and $(a, b) = 1$, we have that

Select All Correct Answers:

(a) a ✓

(b) b ✓

(c) 2b

are perfect squares.

There exists x_2, y_2, z_2 such that $m =$

Multiple Choice:

(a) x_2^2

(b) y_2^2

(c) z_2^2 ✓

$a =$

Multiple Choice:

(a) x_2^2 ✓

(b) y_2^2

(c) z_2^2

and $b =$

Multiple Choice:

(a) x_2^2

(b) y_2^2 ✓

(c) z_2^2.

Without loss of generality, we may assume $x_2, y_2, z_2 > 0$. Then $m^2 = a^2 + b^2$ implies $z_2^2 = x_2^4 + y_2^4$, so that x_2, y_2, z_2 is a solution with positive integers to $x^4 + y^4 = z^2$. Also $(x_2, y_2) = 1$ and $0 < z_2 \leq z_2^2 = m \leq m^2 < m^2 + n^2 = z_1$.

Thus, we have constructed another solution as desired. That is, we assumed the existence of a solution to $x^4 + y^4 = z^2$ in the positive integers, we can construct another solution with a strictly smaller value of z. This is a contradiction sine there are only finitely many positive integers between a given positive integer and zero. So $x64 + y^4 = z^2$ has no solutions on nonzero x, y, z. ■