

12.1 Pythagorean Triples

Recall the definition of a Pythagorean triple: positive integers x, y, z such that $x^2 + y^2 = z^2$. Two familiar examples are $(x, y, z) = (3, 4, 5)$ and $(x, y, z) = (5, 12, 13)$. Our goal is to describe all possible Pythagorean triples—to find a recipe or formula for them.

We begin with a lemma that we will need:

Lemma. Suppose a, b, c are positive integers such that $c^2 = ab$ and $\gcd(a, b) = 1$. Then a and b must be squares.

The proof of this is just: Write the prime factorizations of $a = p_1^{k_1} \cdots p_m^{k_m}$ and $b = q_1^{\ell_1} \cdots q_n^{\ell_n}$. Now we have $p_i \neq q_j$ for all i, j since $\gcd(a, b) = 1$. So the prime factorization of c^2 is $c^2 = p_1^{k_1} \cdots p_m^{k_m} \cdot q_1^{\ell_1} \cdots q_n^{\ell_n}$. But c^2 is a square, so we must have all of the exponents $k_1, \dots, k_m, \ell_1, \dots, \ell_n$ even. But this then forces a and b to both be squares.

So now we consider Pythagorean triples. Suppose x, y, z are positive integers such that $x^2 + y^2 = z^2$. We will assume x, y, z share no common factors; otherwise, we can divide each of them by a common factor and consider a triple that lacks a common factor. Then we realize that x and y cannot both be even, since then z would be even.

Less obvious is the fact that x and y cannot both be odd. But this is because any odd square is congruent to 1 mod 4, since $(2n + 1)^2 = 4(n^2 + n) + 1 \equiv 1 \pmod{4}$ but the sum of two odd squares will be congruent to $1 + 1 = 2 \pmod{4}$.

So we can assume that one of x and y are even, say x . So now we are assuming that x is even, y is odd, and therefore z is odd. We are also assuming these three numbers share no common factor.

Now from $x^2 + y^2 = z^2$, we can write $x^2 = z^2 - y^2 = (z + y)(z - y)$. Now $z + y$ and $z - y$ are both even, so we can write $z + y = 2a$ and $z - y = 2b$ for integers a and b . It turns out $\gcd(a, b) = 1$. Otherwise, suppose p is prime and suppose $p \mid a$ and $p \mid b$. Then p will divide $z = \frac{1}{2}(2a + 2b) = a + b$ and $y = \frac{1}{2}(2a - 2b) = a - b$. From $x^2 + y^2 = z^2$ it would follow that $p \mid x$, but we are supposing x, y, z have no common factors. So no prime p can divide both a and b .

Now since x is even, we can write $x = 2c$, so $x^2 = 4c^2$. So we have $4c^2 = (2a)(2b)$, or $c^2 = ab$ where $\gcd(a, b) = 1$. Therefore, by the lemma, we have $a = s^2$ and $b = t^2$ for integers s and t .

It follows that $x^2 = 4s^2t^2$, so $x = 2st$. Now since $z = a + b$ and $y = a - b$, we have $z = s^2 + t^2$ and $y = s^2 - t^2$. So to summarize, if we assume that $x^2 + y^2 = z^2$, with x even and x, y, z sharing no common factors, then there are relatively prime integers s and t such that

$$\begin{aligned}x &= 2st \\y &= s^2 - t^2 \\z &= s^2 + t^2\end{aligned}$$

Note s and t cannot be both odd, since that would make y and z both be even. (Or as Burton puts it, we cannot have $s \equiv t \pmod{2}$.)

It is easy to verify that for any integers s and t that are relatively prime and obey $s \not\equiv t \pmod{2}$, that x, y, z given by these three formulas are a Pythagorean triple which share no common factor. So we now have a complete description of all “primitive” Pythagorean triples (triples sharing no common factor larger than 1).

Theorem. All primitive Pythagorean triples x, y, z can be written as

$$\begin{aligned}x &= 2st \\y &= s^2 - t^2 \\z &= s^2 + t^2\end{aligned}$$

for positive integers s, t which are relatively prime and not both odd.

Example: Consider the Pythagorean triple 40, 9, 41. To find the numbers s and t , write $x^2 = z^2 - y^2 = 41^2 - 9^2 = (41+9)(41-9) = (50)(32)$. So $x^2 = 2(25) \cdot 2(16)$. So we pick up on the fact that $s = 5$ and $t = 4$. This works: $y = s^2 - t^2 = 25 - 16 = 9$ and $z = s^2 + t^2 = 25 + 16 = 41$.

Example: Let $s = 7$ and $t = 4$. This gives $x = 2st = 2(7)(4) = 56$, $y = s^2 - t^2 = 49 - 16 = 33$, and $z = s^2 + t^2 = 49 + 16 = 65$. And 56, 33, 65 is indeed a primitive Pythagorean triple.

12.2. Fermat's Last Theorem.

This famous theorem states that the equation $x^n + y^n = z^n$ has no solutions in positive integers x, y, z if n is an integer greater than 2. Fermat wrote in the margin of a book that he has a remarkable proof of this statement but not enough room to write it in the margin of the book. Given that he later published proofs of special cases of the theorem, and the difficulty of subsequent generations of mathematicians to find a proof, it is believed he was mistaken when he wrote that. It was not until the mid 1990s that the theorem was proved by Andrew Wiles.

Fermat did succeed in proving the theorem for $n = 4$. His technique of proof is known as "infinite descent": given that a solution exists, a new solution with smaller integers can be constructed. This cannot continue forever, so there is a contradiction.

Theorem (Fermat). The equation $x^4 + y^4 = z^2$ has no solution in positive integers x, y, z .

It follows immediately from this theorem that $x^4 + y^4 = z^4$ cannot have a solution in positive integers.

Proof of the theorem: Assume to the contrary that there is a solution x_0, y_0, z_0 . We may assume that $\gcd(x_0, y_0) = 1$. We construct a new solution x_1, y_1, z_1 as follows:

First notice that if $x_0^4 + y_0^4 = z_0^2$ then x_0^2, y_0^2, z_0 form a Pythagorean triple. So we can write

$$\begin{aligned}x_0^2 &= 2st \\ y_0^2 &= s^2 - t^2 \\ z_0 &= s^2 + t^2\end{aligned}$$

where s and t are relatively prime. The second equation forces t to be even and s to be odd. (Reduce the equation modulo 4 to see that.) So write $r = t/2$. Then

$$x_0^2 = 4sr,$$

which forces s and r to be squares, say $s = z_1^2$ and $r = w^2$.

Now $t^2 + y_0^2 = s^2$ implies

$$\begin{aligned}t &= 2uv \\y_0 &= u^2 - v^2 \\s &= u^2 + v^2\end{aligned}$$

with $u > v > 0$ and u, v relatively prime.

Now write $uv = t/2 = r = w^2$. So u and v must be squares, say $u = x_1^2$ and $v = y_1^2$. Then the equation

$$s = u^2 + v^2$$

becomes

$$z_1^2 = x_1^4 + y_1^4.$$

And we observe that

$$z_1 \leq z_1^2 = s \leq s^2 < s^2 + t^2 = z_0.$$

So given a solution x_0, y_0, z_0 in positive integers, we can always construct a new solution x_1, y_1, z_1 in positive integers, with $z_1 < z_0$. This is impossible, so there can be no solution to the equation.