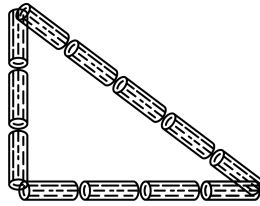


## PYTHAGOREAN TRIPLES

DEFINITION: A triple  $(a, b, c)$  of natural numbers is a **Pythagorean triple** if they form the side lengths of a right triangle, where  $c$  is the length of the hypotenuse.



$(3, 4, 5)$  is a Pythagorean triple.

*Our goal today is to find all Pythagorean triples.* We will use a couple of tools that whose relevance might not be clear at first:

FUNDAMENTAL THEOREM OF ARITHMETIC: Every natural number  $n \geq 1$  can be written as a product of prime numbers:

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}.$$

This expression is unique up to reordering. □

We call the number  $e_i$  the **multiplicity** of the prime  $p_i$  in the prime factorization of  $n$ .

DEFINITION: Let  $m, n$  be integers and  $K \geq 1$  be a natural number. We say that  $m$  **is congruent to  $n$  modulo  $K$** , written as  $m \equiv n \pmod{K}$ , if  $m - n$  is a multiple of  $K$ .

THEOREM: Let  $n$  be an integer and  $K \geq 1$  a natural number. Then  $n$  is congruent to exactly one nonnegative integer between 0 and  $K - 1$ : this number is the “remainder” when you divide  $n$  by  $K$ . □

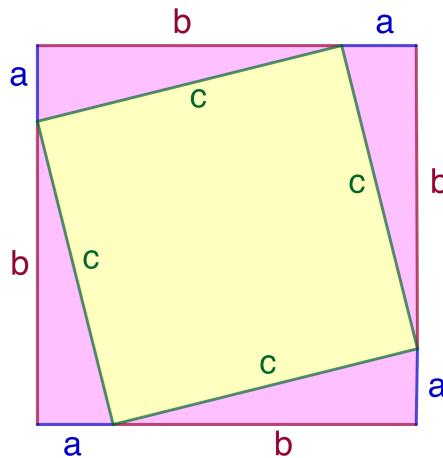
PROPOSITION: Let  $m, m', n, n'$  and  $K$  be natural numbers. Suppose that

$$m \equiv m' \pmod{K} \quad \text{and} \quad n \equiv n' \pmod{K}.$$

Then

$$m + n \equiv m' + n' \pmod{K} \quad \text{and} \quad mn \equiv m'n' \pmod{K}. \quad \text{□}$$

- (1) Without writing too much, use the picture below to deduce the  
 PYTHAGOREM THEOREM: If  $a, b, c$  are the side lengths of a right triangle, where  $c$  is the length of the hypotenuse, then  $a^2 + b^2 = c^2$ .



(2) Creating Pythagorean triples from others:

- (a) Show that if  $(a, b, c)$  is a Pythagorean triple and  $d$  is a natural number, then  $(da, db, dc)$  is a Pythagorean triple. Deduce that there are infinitely many Pythagorean triples.
- (b) Show that if  $(a, b, c)$  is a Pythagorean triple and  $d$  is a common factor of  $a$ ,  $b$ , and  $c$ , then  $(a/d, b/d, c/d)$  is a Pythagorean triple.

**DEFINITION:** A triple  $(a, b, c)$  of natural numbers is a **primitive Pythagorean triple (PPT)** if  $a^2 + b^2 = c^2$ , and there is no common factor of  $a, b, c$  greater than 1; equivalently,  $a, b, c$  have no common prime factor.

Based on (1) and (2), finding all Pythagorean triples boils down to finding all PPTs.

- (3) Let  $a$  be a natural number. Show that if  $a$  is even, then  $a^2 \equiv 0 \pmod{4}$ , and if  $a$  is odd, then  $a^2 \equiv 1 \pmod{4}$ .
- (4) Suppose that  $(a, b, c)$  is a Pythagorean triple. We want to examine the parity (even vs. odd) of the numbers  $a, b, c$ .
  - (a) Suppose that  $a$  and  $b$  are both even. Show that  $c$  is even too. Deduce that there are no PPTs with  $a$  and  $b$  both even.
  - (b) Suppose now that  $a$  and  $b$  are both odd. Consider the equation  $a^2 + b^2 = c^2$  modulo 4, and use the problem (3) to get a contradiction.
  - (c) Conclude that if  $(a, b, c)$  is a PPT, then one of  $a, b$  is odd, and the other is even, and that  $c$  is odd.
- (5) Let  $m$  and  $n$  be natural numbers.
  - (a) Show that  $n$  is a perfect square if and only if the multiplicity of each prime in its prime factorization is even.
  - (b) Suppose that  $m$  and  $n$  have no common prime factors. Show that if  $mn$  is a perfect square, then  $m$  and  $n$  are both perfect squares.
- (6) Consider a PPT  $(a, b, c)$ . Following (4c), without loss of generality we can assume that  $a$  is odd and  $b$  is even. Rewrite the equation  $a^2 + b^2 = c^2$  as  $a^2 = c^2 - b^2$ .
  - (a) By definition, there is no prime factor common to all three of  $a, b$ , and  $c$ . Show that there is no prime factor common to just  $b$  and  $c$ .
  - (b) Factor  $c^2 - b^2$  as  $(c - b)(c + b)$ . Show that<sup>1</sup> there is no prime factor common to  $c - b$  and  $c + b$ .
  - (c) Show that  $c - b$  and  $c + b$  are perfect squares.
  - (d) Show<sup>2</sup> that any PPT can be written in the form
 
$$(a, b, c) = \left( st, \frac{s^2 - t^2}{2}, \frac{s^2 + t^2}{2} \right)$$
 for some odd integers  $s > t \geq 1$  with no common factors.
  - (e) Check the other direction: show that any triple of the form  $(st, \frac{s^2 - t^2}{2}, \frac{s^2 + t^2}{2})$  where  $s, t \in \mathbb{N}$  with no common factors is a PPT.

<sup>1</sup>Hint: If there is a (prime) number that divides these, it divides their sum and difference too.

<sup>2</sup>Hint: Start with writing  $c + b = s^2$ ,  $c - b = t^2$  and solve for  $a, b, c$ .

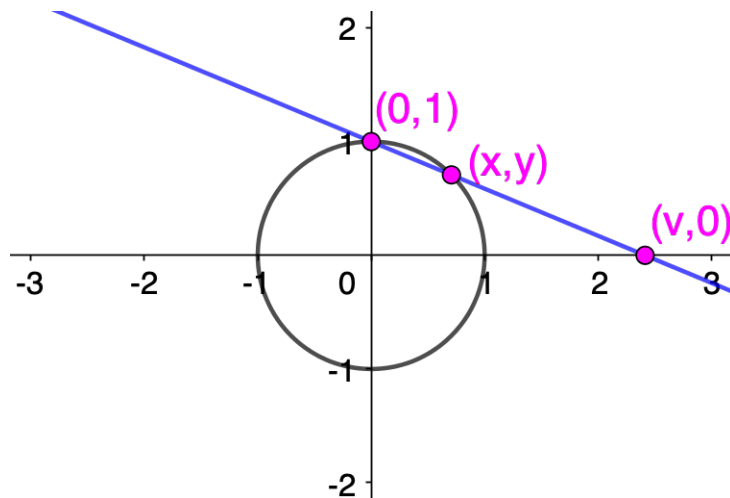
You have proven the following:

**THEOREM:** The set of primitive Pythagorean triples  $(a, b, c)$  with  $a$  odd is given by the formula

$$a = st, \quad b = \frac{s^2 - t^2}{2}, \quad c = \frac{s^2 + t^2}{2},$$

where  $s > t \geq 1$  are odd integers with no common factors.

These mysterious formulas have a geometric explanation.



- (7) (a) Show that if  $(a, b, c)$  is a Pythagorean triple, then  $\left(\frac{a}{c}, \frac{b}{c}\right)$  is a point on the circle with positive rational coordinates, and vice versa.
- (b) Given a rational number  $v > 1$ , the line  $L$  through  $(0, 1)$  and  $(v, 0)$  intersects the unit circle in two points (one of which is  $(0, 1)$ ). As a first step towards finding this point, find an equation for  $L$ .
- (c) Use the equation you found in (7b) and the equation for the unit circle to solve for  $x$  and  $y$  in terms of  $v$ .
- (d) Use (b) to solve for  $v$  in terms of  $x$  and  $y$  and this to show that if  $x$  and  $y$  are rational, then  $v$  is rational.

Conclude the following theorem:

**THEOREM:** The set of points on the unit circle  $x^2 + y^2 = 1$  with positive rational coordinates is given by the formula

$$(x, y) = \left( \frac{2v}{v^2 + 1}, \frac{v^2 - 1}{v^2 + 1} \right)$$

where  $v$  ranges through rational numbers greater than one.

- (e) Take the expressions for  $x$  and  $y$  from the Theorem above in terms of  $v$ , and plug in  $v = s/t$  and simplify each expression for  $x$  and  $y$  into a single fraction.
- (f) Plug these expressions back into  $x^2 + y^2 = 1$ , clear denominators, and divide through by 4. What do you notice?

- (8) Use similar techniques<sup>3</sup> to find rational points on:
- (a) The circle  $x^2 + y^2 = 2$ .
  - (b) The hyperbola  $x^2 - y^2 = 1$ .
  - (c) The hyperbola  $x^2 - 2y^2 = 1$ .
  - (d) The circle  $x^2 + y^2 = 3$ .
- (9) Use this to find integer solutions  $(a, b, c)$  to the equations:
- (a) The circle  $a^2 + b^2 = 2c^2$ .
  - (b) The hyperbola  $a^2 - b^2 = c^2$ .
  - (c) The hyperbola  $a^2 - 2b^2 = c^2$ .
  - (d) The circle  $a^2 + b^2 = 3c^2$ .

Are these all of the integer solutions?

**Key Points:**

- Using the Fundamental Theorem of Arithmetic for basic divisibility arguments.
- Definition of congruence, and using congruences to rule out solutions of equations.
- Using geometry to find rational points.

---

<sup>3</sup>Hint: You may have to change your starting point and/or target line. You might find it useful to take new coordinates in which your starting point is the origin, i.e.,  $x' = x - a$ ,  $y' = y - b$  if your starting point is  $(a, b)$ .