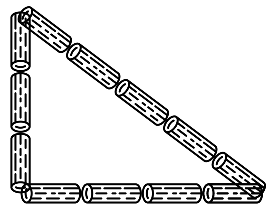
DEFINITION: A triple (a, b, c) of natural numbers is a **Pythagoran triple** if they form the side lengths of a right triangle, where c is the length of the hypotenuse.



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

Our goal today is to find all Pythagoran 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. □

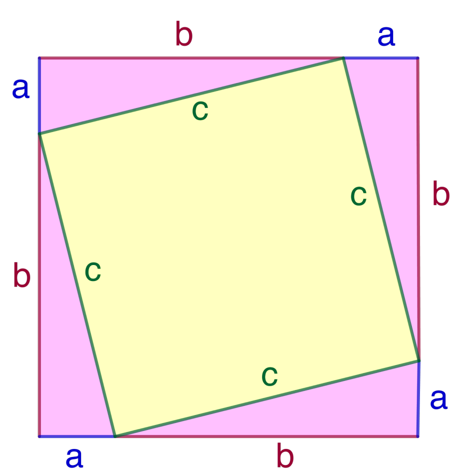
PROPOSITION: Let m, m', n, n' and K be natural numbers. Suppose that

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

Then

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

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



We calculate the area of the big square two ways. First, it is a square with side lengths $a+b$ so the area is

$$(a+b)^2 = a^2 + 2ab + b^2.$$

Second, it consists of a square with side length c and four right triangles with base a and height b, so the area is also

$$c^2 + 4(\frac{1}{2}ab) = c^2 + 2ab.$$

Equating the two and subtracting $2ab$, we get that $a^2 + b^2 = c^2$.

(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.

For (a), we assume that $a^2 + b^2 = c^2$ and test whether the new numbers (da, db, dc) satisfy the equation:

$$(da)^2 + (db)^2 = d^2a^2 + d^2b^2 = d^2(a^2 + b^2) = d^2c^2 = (dc)^2,$$

so they do! Part (b) is similar.

DEFINITION: A triple (a, b, c) of natural numbers is a **primitive Pythagoran 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 $a^2 \equiv 1 \pmod 4$.

First, suppose that a is even, so we can write $a = 2k$ for some integer k. Then $a^2 = (2k)^2 = 4k^2$, and $4k^2 - 0$ is a multiple of 4, so $a^2 \equiv 0 \pmod 4$. Now, suppose that a is odd, so we can write $a = 2k+1$ for some integer k. Then $a^2 = (2k+1)^2 = 4k^2 + 4k + 1$, and $(4k^2 + 4k + 1) - 1 = 4(k^2 + k)$ is a multiple of 4, so $a^2 \equiv 1 \pmod 4$.

(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.

If a and b are even then $a^2 \equiv 0 \pmod 4$ and $b^2 \equiv 0 \pmod 4$. To obtain a contradiction, suppose that c is odd. Then $c^2 \equiv 1 \pmod 4$, but since $a^2 \equiv 0 \pmod 4$ and $b^2 \equiv 0 \pmod 4$, we know that $a^2 + b^2 \equiv 0 \pmod 4$. The same number can't be equivalent to both 0 and 1 mod 4. This contradicts that $a^2 + b^2 = c^2$.

  (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.

If a and b are odd then $a^2 \equiv 1 \pmod 4$ and $b^2 \equiv 1 \pmod 4$. Then $a^2 + b^2 \equiv 2 \pmod 4$. However, c is either even or odd, so either $c^2 \equiv 0 \pmod 4$ or $c^2 \equiv 1 \pmod 4$. Either way, $a^2 + b^2 \equiv c^2$ is impossible!

(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.

We know that exactly one of a, b is even and the other odd since we ruled out the possibilities. Then c has to be odd, since $a^2 + b^2 \equiv 0 + 1 \equiv 1 \pmod 4$.

(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.

($\Rightarrow$): If n is a perfect square, say that $n = t^2$. Take a prime factorization for t:

$$t = p_1^{\ell_1} \cdots p_k^{\ell_k}.$$

Then

$$n = t^2 = p_1^{2\ell_1} \cdots p_k^{2\ell_k}$$

is a prime factorization of n, and the multiplicities $2\ell_i$ are all even.

($\Leftarrow$): Suppose that the multiplicity of every prime in the prime factorization of n is even. That means we can write

$$n = p_1^{2\ell_1} \cdots p_k^{2\ell_k}$$

for some primes p_i and natural numbers ℓ_i. Then

$$n = (p_1^{\ell_1} \cdots p_k^{\ell_k})^2$$

is a perfect square.

(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.

Take prime factorizations of m and n:

$$m = p_1^{e_1} \cdots p_k^{e_k}, \quad n = q_1^{f_1} \cdots q_s^{f_s};$$

by our assumption, the p's and q's are all different. Then

$$mn = p_1^{e_1} \cdots p_k^{e_k} q_1^{f_1} \cdots q_s^{f_s}$$

is a prime factorization of mn. Since mn is a square, each e_i and f_i is even. But, looking back and m and n, this implies that m and n are 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.

Suppose some prime p divides b and c, then it divides b^2 and c^2, and also $c^2 - b^2$, hence it divides a^2. If a prime p divides a^2, then it divides a. But we've assumed no number divides all three.

(b) Factor $c^2 - b^2$ as $(c-b)(c+b)$. Show that[1] there is no prime factor common to $c-b$ and $c+b$.

Suppose $c-b$ and $c+b$ have a common prime factor p. Then p divides $2c = (c-b)+(c+b)$ and $2b = (c+b)-(c-b)$. We know that b and c have no common prime factors, so the only possibility is $p = 2$. But $c+b$ is odd, so there are no common prime factors.

(c) Show that $c-b$ and $c+b$ are perfect squares.

This follows from (5b) and (6b).

(d) Show[2] 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.

By (6c), we can write $c + b = s^2$, $c - b = t^2$ for some integers with no common factors. These have to be odd because $c+b$ and $c-b$ are odd, and clearly $s > t$. Then

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

$$\text{and} \quad a = \sqrt{(c+b)(c-b)} = \sqrt{s^2t^2} = st.$$

(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 $s > t \geq 1$ are odd integers with no common factors, is a PPT.

To check it is a Pythagorean triple, note first that $s^2 - t^2$ is always even, so these things are integers (which was at risk of failing with the division); then just plug into the formula and chug. To check it is primitive, if a prime p divides $\frac{s^2-t^2}{2}$ and $\frac{s^2+t^2}{2}$, it divides s^2 and t^2, hence s and t, which we assumed to share no factors.

You have proven the following:

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

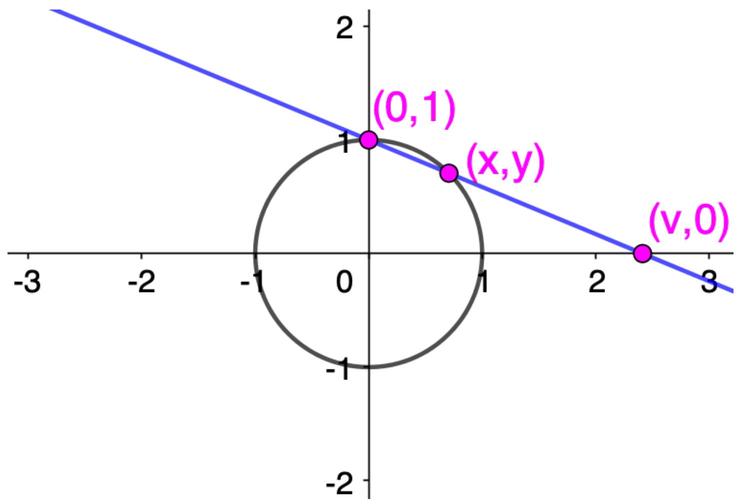
$$a = st, \quad b = \frac{s^2 - t^2}{2}, \quad c = \frac{s^2 + t^2}{2},$$

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

These mysterious formulas have a geometric explanation.

[1] Hint: If there is a (prime) number that divides these, it divides their sum and difference too.

[2] Hint: Start with writing $c + b = s^2$, $c - b = t^2$ and solve for a, b, c.



(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.

$$y = \frac{-1}{v}x + 1$$

(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.

$$x^2 + \left(\frac{-1}{v}x + 1\right)^2 = 1$$
$$\left(1 + \frac{1}{v^2}\right)x^2 + \left(\frac{-2}{v}\right)x = 0$$
$$\left(v^2 + 1\right)x + (-2v) = 0$$
$$x = \frac{2v}{v^2 + 1}$$
$$y = \frac{v^2 - 1}{v^2 + 1}$$

(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.

$$y = \frac{-1}{v}x + 1$$
$$vy = 1 - x$$
$$y = \frac{1 - x}{y}$$

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.

$$(x, y) = \left(\frac{2st}{s^2+t^2}, \frac{s^2-t^2}{s^2+t^2} \right)$$

(f) Plug these expressions back into $x^2 + y^2 = 1$, clear denominators, and divide through by 4. What do you notice?

$$(2st)^2 + (s^2 - t^2)^2 = (s^2 + t^2)^2$$
$$(st)^2 + \left(\frac{s^2-t^2}{2} \right)^2 = \left(\frac{s^2+t^2}{2} \right)^2$$

This is our formula from before.

(8) Use similar techniques[3] 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 $x^2 + y^2 = 3$.

We show (a) and leave the rest for you. The point $(1, 1)$ is on this circle. We will use the same trick of taking the line between $(1, 1)$ and a point on the x-axis to parametrize solutions. Following the hint, set $x' = x - 1$ and $y' = y - 1$. If $(v, 0)$ is a point on the x-axis, let's even set $v' = v - 1$. Then the line through $(1, 1)$ and $(0, v)$ in (x, y)-coordinates is the line through $(0, 0)$ and $(v', -1)$ in (x', y')-coordinates, so $y' = -1/v' \cdot x$, and $x' = -v'y'$. Then the equation of the circle is

$$(x' + 1)^2 + (y' + 1)^2 = 2 \rightsquigarrow x'^2 + 2x' + y'^2 + 2y' = 0$$
$$\rightsquigarrow y'^2(v'^2 + 1) + 2y'(1 - v') = 0 \rightsquigarrow y' = \frac{v'-1}{v'^2+1} \rightsquigarrow x' = -v'\frac{v'-1}{v'^2+1}$$

We need to switch back to (x, y)-coordinates (but it doesn't really matter whether we switch back with v or not, so we won't):

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

(9) Use this to find integer solutions (a, b, c) to the equations:
(a) The circle $a^2 + b^2 = 2c^2$.

[3]Hint: You many 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).

(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?

Plug in s/t and clear denominators. For (a), we get the formula

$$(a, b, c) = (t^2 + 2st - s^2, s^2 + 2st - t^2, s^2 + t^2).$$

However, it's not clear whether this accounts for every integer solution: we might have an integer solution that only has a multiple of the form above. This happened when we investigated Pythagorean triples using this method; we have to unexpectedly divide through by 4! I'll leave it to you to investigate if anything is missing here.

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.