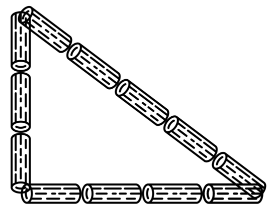
DEFINITION: A triple (a, b, c) of natural numbers is a **Pythagoran triple** if they form the side lengths of a right triangle, where c is the length of the hypotenuse.



$(3, 4, 5)$ 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. □

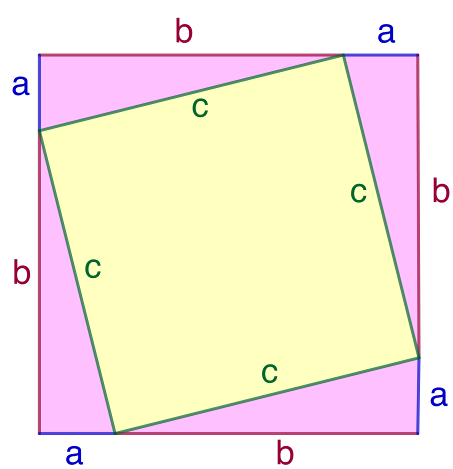
PROPOSITION: Let m, m', n, n' and K be natural numbers. Suppose that

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

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 $a \equiv 0 \pmod 4$, and if a is odd, then $a \equiv 1 \pmod 4$.

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.