

Prove the following propositions. Format your proof so each step of the proof is on its own line; each line should still be a complete sentence. Below, I have entered a nonsensical proof as a model.

**Proposition 1.** Suppose  $a, b, c \in \mathbb{Z}$ . If  $a^2 + b^2 = c^2$ , then  $a$  or  $b$  is even.

*Proof.*

Suppose  $a^2 + b^2 = c^2$  and it's not the case that  $a$  or  $b$  is even.

Therefore,  $a$  and  $b$  are both odd.

So  $a = 2x + 1$  and  $b = 2y + 1$  for some integers  $x$  and  $y$ .

Either  $c$  is even or odd.

**Case 1:**  $c$  is even.

Then  $c = 2z$  for some integer  $x$ .

The expression  $a^2 + b^2 = c^2$  becomes  $(2x + 1)^2 + (2y + 1)^2 = 4z^2$ .

Expanding the expression yields  $4x^2 + 4x + 1 + 4y^2 + 4y + 1 = 4z^2$ .

Factoring yields  $4(x^2 + y^2 + x + y) + 2 = 4z^2$ .

Simplifying the expression shows  $4k + 2 = 4j$  where  $k$  and  $j$  are the integers  $x^2 + y^2 + x + y$  and  $4z^2$  respectfully.

Observe that  $2 = 4(k - j)$ , thus  $4|2$ .

We have arrived at contradiction.

**Case 2:**  $c$  is odd.

Then  $c = 2z + 1$  for some integer  $x$ .

The expression  $a^2 + b^2 = c^2$  becomes  $(2x + 1)^2 + (2y + 1)^2 = (2z + 1)^2$ .

Expanded and factored yields  $2(2x^2 + 2x + 2y^2 + 2y + 1) = 2(2z^2 + 2z) + 1$

Simplifying the expression shows that  $2k = 2j + 1$  for integers  $k$  and  $j$ .

Therefore, an even number equals an odd number. We have arrived at contradiction.

□

**Proposition 2.** Suppose  $x, y \in \mathbb{Z}$ . If  $x + y$  is even, then  $x$  and  $y$  have the same parity.

*Proof.*

Suppose  $x + y$  is even.

Assume  $x$  and  $y$  do not have the same parity.

Then  $x$  is even and  $y$  odd without loss of generality.

So  $x = 2a$  and  $y = 2b + 1$  for some integers  $a$  and  $b$ .

The expression  $x + y$  becomes  $2a + 2b + 1 = 2(a + b) + 1$ .

Therefore  $x + y = 2m + 1$  where  $m$  is the integer  $a + b$ .

So,  $x + y$  is odd. But,  $x + y$  is even.

We have arrived at contradiction.

□

**Proposition 3.** If  $a \equiv b \pmod{n}$ , then  $\gcd(a, n) = \gcd(b, n)$ .

*Proof.*

Suppose  $a \equiv b \pmod{n}$ .

Congruent modulo means two integers share the same remainder when the division algorithm is applied with the same divisor.

The division algorithm tells us that:

$a = q_1n + r$  and  $b = q_2n + r$ , where  $q_1, q_2, r \in \mathbb{Z}$  and  $0 \leq r < n$ .

For all  $x$  where  $x|a$

□