

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.

Let $a, b, c \in \mathbb{Z}$.

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 z .

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 $4z^2$ respectively.

Observe that $2 = 4(k - j) \implies 2 = 4l$ where l is the integer $k - j$, thus $4|2$.

We have arrived at contradiction.

Case 2: c is odd.

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

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.

Let $x, y \in \mathbb{Z}$.

Suppose 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. □

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

Proof.

Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$.

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

Then $n \mid (a - b)$.

Then $nx = a - b$ for some integer x .

The division algorithm states that:

$$a = nq_1 + r_1 \text{ where } q_1, r_1 \in \mathbb{Z} \text{ where } 0 \leq r_1 < n.$$

$$b = nq_2 + r_2 \text{ where } q_2, r_2 \in \mathbb{Z} \text{ where } 0 \leq r_2 < n.$$

$$\text{So, } nx = nq_1 + r_1 - nq_2 - r_2$$

$$= n(q_1 - q_2) + r_1 - r_2$$

Observe that $r_1 - r_2$ must be some multiple of n in order for the equality to hold.

$$\text{So, } nx = r_1 - r_2.$$

However, $-n < r_1 - r_2 < n$, so the only possible multiple is 0.

So, $n(0) = 0 = r_1 - r_2 \implies r_1 = r_2$.

Therefore they share the same remainder. Moving forward: Let $r = r_1 = r_2$.

If $r = 0$, then both a and b are multiples of n . So the greatest shared divisor between a and n and between b and n will simply be n itself.

So, $\gcd(a, n) = \gcd(b, n)$ when $r = 0$.

If $r \neq 0$, then n and r may share prime factors, we can factor these out and replace them with their product p :

$$a = p(n'q_1 + r')$$

$$b = p(n'q_2 + r')$$

Where $n = pn'$ and $r = pr'$.

Lemma: Let $\alpha, \beta \in \mathbb{N}$, $x \in \mathbb{Z}$. If α and β are coprime, then $\gcd(\alpha x + \beta, \alpha) = 1$.

Suppose $\gcd(\alpha x + \beta, \alpha) \neq 1$.

Then $\gcd(\alpha x + \beta, \alpha) > 1$.

So, $\alpha x + \beta$ and α share some common divisor d .

It follows that $d|\alpha x + \beta$ and $d|\alpha$.

Expanded, this is $dm_1 = \alpha x + \beta$ and $dm_2 = \alpha$.

Substituting α , $dm_1 = \alpha x + \beta \implies dm_1 = dm_2x + \beta$.

Isolation β , we get $\beta = dm_1 - dm_2x \implies \beta = d(m_1 - m_2x)$.

Thus, $dm_3 = \beta$ where m_3 is the integer $m_1 - m_2x$.

So, $d|\beta$.

Because $d|\beta$ and $d|\alpha$ for some $d > 0$, β and α cannot be coprime.

So, $\gcd(n'q + r', n') = 1$ when $q \in \{q_1, q_2\}$, because n' and r' are coprime.

So, $n'q + r'$ and n' share no prime factors.

Since $a = p(n'q_1 + r')$, $n = pn'$, and $n'q_1 + r'$ and n' share no more common factors, it follows that $\gcd(a, n) = p$.

Similarly, since $b = p(n'q_2 + r')$, $n = pn'$, and $n'q_2 + r'$ and n' share no more common factors, it follows that $\gcd(b, n) = p$.

So, $\gcd(a, n) = \gcd(b, n)$ when $r \neq 0$.

