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 $4z^2$ respectfully.

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 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.

$\square$

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. $\square$

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 $a \equiv b(\text{mod } n)$.

Then $n|(a - b)$.

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

So $a = nx + b$.

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

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, $dm_1 = \alpha x + \beta \implies dm_1 = dm_2 x + \beta$.

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.

Case 1: $\gcd(a, n) = 1$

Case 2: $\gcd(a, n) \neq 1$

Then we can invoke the lemma established above.

Because $\gcd(nx + b, n) \neq 1$, n and b are not coprime.

So there is some d_1 that $d_1|n$ and $d_1|b$.

Additionally, because $\gcd(a, n) \neq 1$, there is some d_2 that $d_2|a$ and $d_2|n$.

$\square$