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 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.

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

Then $n|(a - b)$.

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

The division algorithm states that:

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

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

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.

So, $ny = r_1 - r_2$.

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: $r = r_1 = r_2$.

Continuing,

$a = nq_1 + r$

$b = nq_2 + r$

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 $n = n'p$ and $r = r'p$.

Make note that $p|a$, $p|b$, and $p|n$.

Lemma: If n' and r' are coprime, then $\gcd(n'q + r', n') = 1$ where $q \in \{q_1, q_2\}$.

Suppose $\gcd(n'q + r', n') \neq 1$.

Then $\gcd(n'q + r', n') > 1$.

So, $n'q + r'$ and n' share some common divisor d.

It follows that $d|n'q + r'$ and $d|n'$.

Expanded, this is $dm_1 = n'q + r'$ and $dm_2 = n'$.

Substituting n', $dm_1 = n'q + r' \implies dm_1 = dm_2q + r'$.

Isolation r', we get $r' = dm_1 - dm_2q \implies r' = d(m_1 - m_2q)$.

Thus, $dm_3 = r'$ where m_3 is the integer $m_1 - m_2q$.

So, $d|r'$.

Because $d|r'$ and $d|n'$ for some $d > 0$. r' and n' cannot be coprime.

Therefore, $\gcd(n'q + r', n') = 1$ where q equals q_1 or q_2, because n' and r' are coprime.

Because $n'q + r'$ and n' share no more common factors and $p(n'q + r')$ is equal to a or b, $\gcd(a, n) = p$ and $\gcd(b, n) = p$.

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

$\square$