Definitions

(1) $a|b \iff \exists c \in \mathbb{Z} \implies b = ca$

(2) $a\%b = r \impliedby \frac{a}{b}$ has remainder r

(3) $a \equiv b \bmod n \iff n|b - a$

Theorem 4.1: if n is even then n^2 is even. (source: lecture)

---

1. Prove that $n^2 \neq 2 \bmod 3, \quad \forall n \in \mathbb{Z}$

   Proof.

$$\forall n \in E, 2|n \implies 2|n^2 \quad \textit{by theorem 4.1}$$
$$2|n^2 = 2 \bmod 0 \neq 2 \bmod 3 \qquad \blacksquare$$

2. Fermat's Last theorem is a famous theorem in Math that was unproven for 200 years. The theorem says $\forall n > 2,\ a, b, c \in \mathbb{N} \implies a^n + b^n \neq c^n$. Another way to state this is $a^n + b^n = c^n$ has no integer solutions for n larger than 2. Use this theorem to prove that $\sqrt[n]{2}$ is irrational for n larger than 2.

   Proof.

$$\sqrt[n]{2} \in \mathbb{Q} \implies \exists a, b \in \mathbb{Z} : \gcd(a, b) = 1$$
$$\implies \sqrt[n]{2} = \frac{a}{b} \implies a^n = 2b^n$$
$$\implies a^n = b^n + b^n \qquad \blacksquare$$

Note: this is essentially zscoder's proof. No real credit here; I couldn't figure it out myself at first. It's pretty simple though, so I couldn't formulate something else that was better without adding unnecessary steps (originally completed in hw3).

3. Prove $\forall a, b, c \in \mathbb{Z} : a|b \wedge a|c \implies a|bx + cy \quad \forall x, y \in \mathbb{Z}$

Proof.

$$b = qa, \quad c = qa \quad \text{by definition 1}$$
$$\implies a|qax + qay = a|a(qx + qy) = a|qa \quad \blacksquare$$

4. Prove $\forall n, a, b \in \mathbb{Z}, n|a - b \iff a\%n = b\%n$

Proof.

$$a\%n = b\%n \iff \exists q \in \mathbb{Z} : \frac{a}{n} = \frac{qb}{n}$$
$$\implies a = qb$$
$$\implies n|qb - b = n|b(q - 1) \quad \blacksquare$$

Proof by contradiction.

$$a\%n \neq b\%n \implies \exists q \notin \mathbb{Z} : \frac{a}{n} = \frac{qb}{n}$$
$$\implies a \neq qb \quad \blacksquare$$

Thus, if $a\%n = b\%n$ then one integer is guaranteed to be a multiple of the other, which must be true for $a - b$ to be divisible by n. Alternatively, a contradiction arises because every integer should be able to represented as a multiple of some other integer.

5. Let $a, b \in \mathbb{Z}, n \in \mathbb{N}$. Prove that

$$a \sim b \impliedby a \equiv b \bmod n$$

is a n equivalence relation for any n.

6. The greatest common divisor of natural numbers a, b; $\gcd(a, b)$, is the largest number δ such that $\delta | a \wedge \delta | b$

   (a) Let $\delta = \gcd(b, a\%b)$, prove that $\delta | a \wedge \delta | b$

   (b) Use part (a) to show that $\gcd(a, b) = \gcd(b, a\%b)$

7. We defined the identity function

$$\mathrm{id} : A \to A, \quad \mathrm{id}(x) = x, \quad \text{has property: } \forall f : A \to A,\ \mathrm{id} \circ f = f \circ \mathrm{id} = f$$

Prove that id is the only function that can have this property.