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

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.

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

Thus, this contradicts Fermat's Last theorem implying $\sqrt[n]{2}$ is irrational for $n > 2$.

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 that for any $a, b, c \in \mathbb{Z}, \exists x, y \in \mathbb{Z} : a|bx + cy \impliedby a|b \wedge a|c$

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

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.