**Union** $S \cup T$: $\{x : x \in S \vee x \in T\}$

**Intersection** $S \cap T$: $\{x : x \in S \wedge x \in T\}$

**Difference** $S \setminus T$: $\{x : x \in S \wedge x \notin T\}$

**Complement** $S'$: $\{x : x \notin S \wedge x \notin T\}$

**Total (total)**: $\forall x \in A \implies f(x)$ is defined

**1 to 1 (injective)**: $\forall x, y \in X, \quad f(x) = f(y) \implies x = y$

**Onto (surjective)**: $f : X \to Y, \quad \forall y \in Y, \quad \exists x \in X \implies f(x) = y$

**Composition**: $(g \circ f)(x) = g(f(x))$

**Inverse**: $f^{-1}(x) : f \circ f^{-1} = f^{-1} \circ f = \mathrm{id}$

**Equivalence**: $\sim, \equiv \iff$ a relation is reflexive, symmetric (**partial**: antisymmetric), and transitive.

**Reflexive**: $\forall a \in X, \quad a \sim a$

**Symmetric**: $\forall a, b \in X, \quad a \sim b \iff b \sim a$

**Antisymmetric**: $\forall a, b \in X, \quad a \sim b, a \neq b \implies b \nsim a$ ...equiv... $a \sim b, b \sim a \implies a = b$

**Transitive**: $\forall a, b, c \in X, \quad : a \sim b, b \sim c \implies a \sim c$

**Direct**: using previous theorem or definition

**Contradiction**: assume false, find contradiction

**Contrapositive**: $A \implies B = \neg B \implies \neg A$

**Cases**: prove all possible cases.

**Generalization**: prove $\forall x$ pick arbitrary $x$. WLOG = swap variables same difference.

**Prove set**: $A = B \iff A \subseteq B \wedge B \subseteq A$

$$a, b, c, q, r, x, y \in \mathbb{Z} \Downarrow$$

$b = qa + r \impliedby \exists q, r : 0 \leq r < b$

$a \equiv b \bmod n \iff n | b - a$

$a | b \iff \exists q \implies b = qa$

**Theorem**: $a | b \wedge a | c \implies a | bx + cy$

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

**Theorem**: $a \equiv a \% n \bmod n, \quad n | qn$

---

Prove $\sqrt[n]{2}$ is irrational for $n > 2$

*Proof.*

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

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

*Proof.*

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

*Proof by contradiction.*

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

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

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

*Proof.*

$$\begin{aligned} a \% b = 0 &\implies a | b, \ \gcd(b, 0) = b \\ &\implies b = \delta, \ b = ca \\ &\implies \delta | b, \ \delta | ca \\ &\implies \delta | b \wedge \delta | a \end{aligned}$$

$$\begin{aligned} a \% b \neq 0 &\implies a \% b = r \quad \textit{by definition 2} \\ &\implies r | b - a \quad \textit{by definition 3} \\ &\implies r | a \wedge r | b \quad \textit{by question 3} \\ \delta | r &\implies \delta | a \wedge \delta | b \quad \blacksquare \end{aligned}$$

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

*Proof.*

$$\begin{aligned} a \% b = 0 &\implies a \leq b, \delta = \max(a, b) = b \quad \textit{by (a)} \\ a \% b \neq 0 &\implies \delta | r, 0 < r < a \leq b \quad \textit{by (a)} \\ &\implies \delta = \max(b, r) = b \quad \blacksquare \end{aligned}$$