CSCI 301 - Lecture 15: Modular Congruence, Proofs with sets

Modular Congruence (equivalence)

Definition: Given integers a, b and $n \in \mathbb{N}$, we say a and b are congruent modulo n if $n \mid (a-b)$.
We write this $a \equiv b \pmod{n}$.
If a and b are not congruent mod n, then we write $a \not\equiv b \pmod{n}$.

1.1. $\overset{a}{9} \equiv \overset{b}{1} \pmod{\overset{n}{4}}$ $\quad 4 \mid (9-1)$

$4 \mid 8$

1.2. $10 \equiv 20 \pmod{2}$ $\quad 2 \mid (10-20)$ $\quad 2 \mid -10$

1.5 $\forall x \in \mathbb{Z}, n \in \mathbb{N}$ $\quad x \equiv x \pmod{n}$ $\quad n \mid (x-x)$ $\quad n \mid 0$

1.6 $\forall n \in \mathbb{N}, 3n \equiv 0 \pmod{n}$ $\quad n \mid (3n-0)$ $\quad n \mid 3n$

Set Membership

$a \overset{?}{\in} \{x : P(x)\}$

Show $P(a)$

$a \overset{?}{\in} \{x \in S : P(x)\}$

Show $a \in S$ and $P(a)$

Subset Relationships.

How to Prove $A \subseteq B$ (Direct approach)

Proof. Suppose $a \in A$.

$\vdots$

Therefore $a \in B$.
Thus $a \in A$ implies $a \in B$,
so it follows that $A \subseteq B$. ■

How to Prove $A \subseteq B$ (Contrapositive approach)

Proof. Suppose $a \notin B$.

$\vdots$

Therefore $a \notin A$.
Thus $a \notin B$ implies $a \notin A$,
so it follows that $A \subseteq B$. ■

A is a subset of B

Set Equality

Show $A \overset{?}{=} B$

- Show $A \subseteq B$
- Show $B \subseteq A$

Then $A = B$

$A \times B = \{(a,b) : a \in A, b \in B\}$

<u>Example</u> Suppose A, B, C are sets and $C \neq \emptyset$.

If $A \times C = B \times C$, then $A = B$.

Suppose $A \times C = B \times C$.

First, show $A \subseteq B$.

Since $C \neq \emptyset$, there exists some $c \in C$.

For any $a \in A$, this means $(a, c) \in A \times C$.

Because $A \times C = B \times C$, this means $(a, c) \in B \times C$.

By definition of cartesian product, this means $a \in B$. Therefore $A \subseteq B$.

Next, show $B \subseteq A$

(proof is similar - see typed notes)