Congruence

$m, a, b \in \mathbb{Z}$ $a \equiv b \bmod (m)$ if $m \mid (a-b)$

Congruence is an equivalence relation equivalence classes mod (m)

$[a] = [a]_m$ ← unique equivalence class $= \{a + qm \mid q \in \mathbb{Z}\}$.

$\mathbb{Z} = \bigcup_{x \in \mathbb{Z}} [x]_m$ disjoint union

Suppose $a \in [x]_m$ and $a \in [y]_m$ [i.e. $[x]_m \wedge [y]_m \neq \emptyset$]

$\exists q$ s.t. $a = x + qm$ $\exists p \in \mathbb{Z}$ s.t. $a = y + pm$

$a \in [x]_m \Leftrightarrow a \equiv x \bmod (m)$ $\Rightarrow$ (equivalence relation) $x \equiv y \bmod (m) \Leftrightarrow x \in [y]_m$

$a \in [y]_m \Leftrightarrow a \equiv y \bmod (m)$ $y \equiv x \bmod (m) \Leftrightarrow y \in [x]_m$

$\Rightarrow [x]_m \subseteq [y]_m$ and $[y]_m \subseteq [x]_m \Rightarrow [x]_m = [y]_m$

i.e. $[x] \wedge [y] \neq \emptyset \Rightarrow [x] = [y]$.

Find congruence classes mod (m)

(m) $a \in \mathbb{Z}$ Division Algorithm $\exists q, r \in \mathbb{Z}$ $0 \leq r < m$ s.t. $a = mq + r$

$\Rightarrow a \equiv r \bmod (m) \Rightarrow [a]_m = [r]_m \rightsquigarrow \exists m$ congruence classes.

Let's assume $r, r' < m$ and $[r] = [r']$ i.e. $r \equiv r' \bmod (m)$

$m \mid (r - r')$ and $|r - r'| < m \Rightarrow r - r' = 0 \Rightarrow r = r'$ hence.

Proposition 2.3: There are exactly m congruence classes modulo (m)

$[0]_m, [1]_m, \ldots, [m-1]_m$

Definition 2.4 Denote by $\mathbb{Z}_m$ the set of all congruence classes modulo m

e.g. $\mathbb{Z}_2 = \{[0], [1]\}$ (same as $\bar{0}, \bar{1}$) $\mathbb{Z}_3 = \{[0], [1], [2]\}$.

Binary operation. $[a]_m + [b]_m = [a+b]_m$

e.g. Mod (4) $[1]_4 = [5]_4$ $[2]_4 = [10]_4$ $[1] + [2] = [1+2] = [3]_4$ $[5] + [10] = [15] = [3]_4$

$a' \in [a]$, $b' \in [b]$ Show $[a+b] = [a'+b']$ or equivalently $a+b \equiv a'+b' \bmod (m)$.

$a' = a + mq$ some $q \in \mathbb{Z}$ $\Rightarrow b' = b + mp$ some $p \in \mathbb{Z}$.

$a' + b' = a + mq + b + mp = a + b + m(q+p) \Rightarrow a+b \equiv a'+b' \bmod (m)$

$\left[\bar{a}, \bar{b}\ (0 \leq a, b < m \quad \bar{a} + \bar{b} = \begin{cases} \overline{a+b} & \text{if } a+b < m \\ \overline{a+b-m} & \text{if } a+b > m \end{cases}\right]$

Proposition 2.5: The set $\mathbb{Z}_m$ with addition (as defined before) is a group.

Furthermore, $\mathbb{Z}_m$ is an abelian group

proof: we know addition is a binary operation

$+$ is commutative: $[a] + [b] = [a+b] \overset{=}{\text{in } \mathbb{Z}} [b+a] = [b] + [a]$.

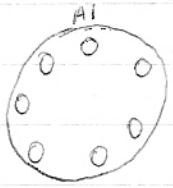
(G1): $([a] + [b]) + [c] = [a+b] + [c] = [(a+b)+c] \overset{=}{\mathbb{Z}} [a+(b+c)] = [a] + [b+c]$

$= [a] + ([b] + [c])$

(G2): $[0]$ is the identity element $[0] + [a] = [0+a] = [a]$

(G3): $[a]^{-1} = [-a]$: $[a] + [-a] = [a + (-a)] = [0]$.

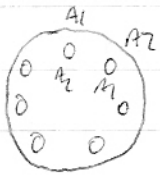
§ 3: PERMUTATIONS



How many ways are there to place 7 ambassadors around a round table (we have 7 seats).

Doesn't matter where A1 sits

A2 6 choices . A3 5 choices ... A7 1 choice } $6! = 720$.



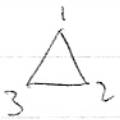
How many ways to place 7 ambassadors if 2 can't sit next to each other? Bad case: they sit next to each other

A3 5 choices, A4 4 choices ... A7 1 choice } $5! \times 2 = 240$.

⇝ Map $\mathcal{A} \longrightarrow \mathfrak{S}$ bijection

↑ set of ambassadors ↖ set of seats

Symmetries of equilateral triangle.



Set of vertices $V = \{1, 2, 3\}$.

r: $1 \to 2$, $2 \to 3$, $3 \to 1$ $\quad$ s: $1 \to 1$, $2 \to 3$, $3 \to 2$ $\quad$ etc...

Maps: $V \to V$ bijective maps.

Definition 3.1 $X \neq \emptyset$ set. A bijective function $\pi: X \to X$ is called a permutation.