"equivalent"

A binary relation $\equiv$ on S is called equivalence if and only if:

$\forall a \in S.\ a \equiv a$ — Reflexive

$\forall a,b \in S.\ (a \equiv b \Rightarrow b \equiv a)$ — Symmetric

$\forall a,b,c \in S.\ ((a \equiv b \wedge b \equiv c) \Rightarrow a \equiv c)$ — Transitive

$a \equiv b$ means $(a,b) \in R$

"precedes"

A binary relation $\prec$ on S is called partial order if and only if:

$\forall a \neq b \in S.\ (a \prec b \Rightarrow b \not\prec a)$ $(b,a) \notin R$ — Anti symmetric

$\forall a,b,c \in S.\ ((a \prec b \wedge b \prec c) \Rightarrow a \prec c)$ — Transitive

$\prec$ could be reflexive or not (strict partial order)

$a \prec b$ means $(a,b) \in R$

Example: $<$ or $\leqslant$ on $\mathbb{R}$

Equivalence relation partitions S into classes of equivalence

$$C_a = \{x \in S : a \equiv x\}$$

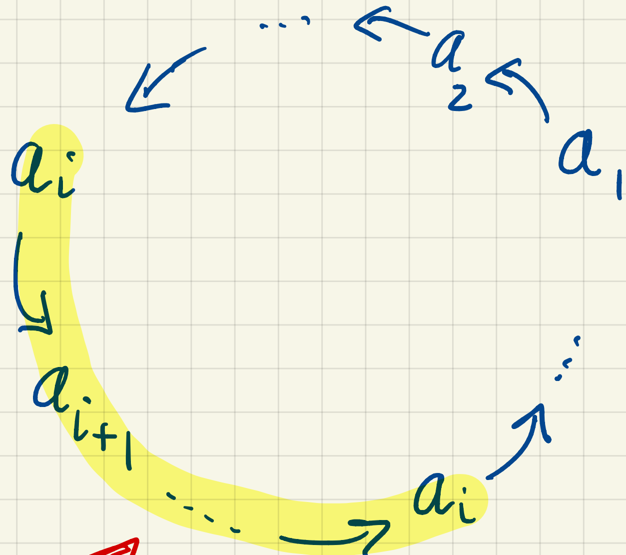
Partial order relation "orders" S. If S is finite $\preccurlyeq$ admits a minimum element

$$\exists e \in S. \left(\forall x \in S. (x \neq e \Rightarrow x \not\preccurlyeq e)\right)$$

Proof: Suppose e does not exists, then we can find an infinite sequence $\ldots a_n \preccurlyeq \ldots \preccurlyeq a_2 \preccurlyeq a_1$. (don't use reflexive steps)

Since S is finite, we must cycle.

So by transitivity, we have $a_i \preccurlyeq a_j$ and $a_j \preccurlyeq a_i$, a contradiction. (see below)



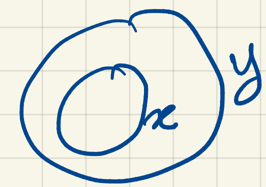
$a_j \neq a_i$

$a_j < a_i$ by transitivity

but $a_i < a_j$ by transitivity

Example 1: $S = \{a, b, c\}$

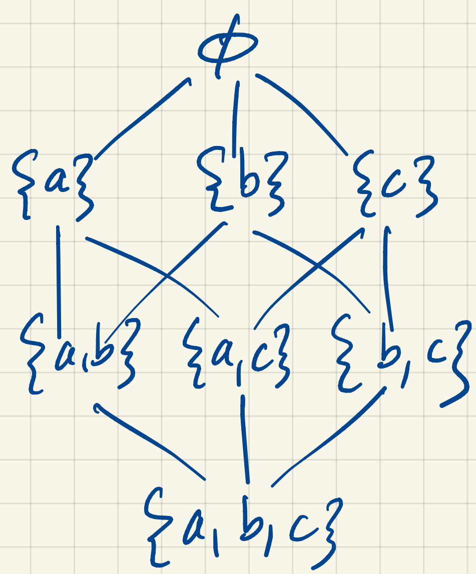
$$P(S) = \{\phi, \{a\}, \{b\}, \{c\}, \{a,b\}, \{a,c\}, \{b,c\}, \{a,b,c\}\}$$



Consider the proper subset relation:

- It's anti-symmetric: $x \subset y \Rightarrow y \not\subset x \quad (x \neq y)$
- It's transitive: $x \subset y,\ y \subset z \Rightarrow x \subset z$.

minimum element: ϕ



All "edges" that can be inferred by transitivity are omitted.

Example 2:

$$(a,b) \prec (c,d) \quad \text{iff} \quad a < c \;\&\; b \leq d$$

- Anti-symmetric: $(a,b) \prec (c,d)$ $\left.\begin{array}{l} a < c \\ b \leq d \end{array}\right\} \Rightarrow c \not< a$ so $(c,d) \not\prec (a,b)$

- Transitive: $\begin{array}{l} (a,b) \prec (c,d) \\ (c,d) \prec (e,f) \end{array}$ $\left.\begin{array}{l} a < c < e \\ b \leq d \leq f \end{array}\right\} \Rightarrow \begin{array}{l} a < e \\ b \leq f \end{array}$ so $(a,b) \prec (e,f)$

$$S = \{(1,1), (2,3), (2,0), (3,3)\}$$

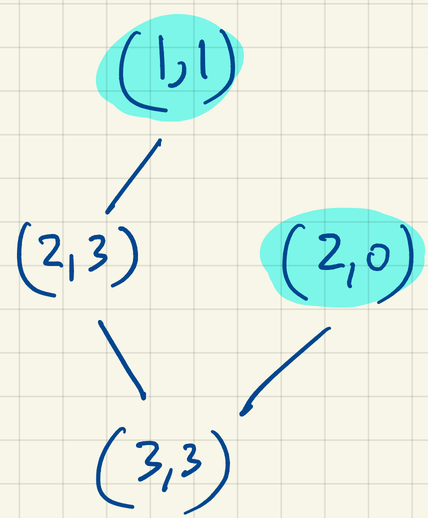
$(1,1) \prec (2,3)$

$(1,1) \prec (3,3)$

$(2,3) \prec (3,3)$

$(2,0) \prec (3,3)$

$(1,1)$ and $(2,0)$ are both minimum elements.



Congruence

$$a \equiv b \pmod{n} \iff n \mid a-b$$

(a & b have the same remainder in division by n)

Congruence "behaves like" equality (Equivalence relation)

Example:

$$\begin{array}{c} a \equiv b \pmod{n} \\ c \equiv d \pmod{n} \\ \hline a+c \equiv b+d \pmod{n} \end{array} \qquad \begin{array}{c} a = b \\ c = d \\ \hline a+c = b+d \end{array}$$

Proof: $n \mid a-b$ and $n \mid c-d \Rightarrow n \mid (a-b)+(c-d)$ (why?)

$$\Rightarrow n \mid (a+c)-(b+d) \Rightarrow a+c \equiv b+d \pmod{n}$$

$$a \equiv b \pmod{n} \Rightarrow n \mid a-b \Rightarrow a-b = k_1 n$$

$$c \equiv d \pmod{n} \Rightarrow n \mid c-d \Rightarrow c-d = k_2 n$$

$$(a-b)+(c-d) = (k_1+k_2)n$$

$$(a+c)-(b+d) = (k_1+k_2)n$$

$$n \mid (a+c)-(b+d)$$

$$a+c \equiv b+d \pmod{n}$$

$$\frac{\begin{array}{c} a \equiv b \pmod{n} \\ c \equiv d \pmod{n} \end{array}}{a+c \equiv b+d \pmod{n}}$$

$$\frac{\begin{array}{c} a \equiv b \pmod{n} \\ c \equiv d \pmod{n} \end{array}}{a-c \equiv b-d \pmod{n}}$$

We can even move from side to side

$$\frac{\begin{array}{c} a \equiv b \pmod{n} \\ c \equiv d \pmod{n} \end{array}}{a \times c \equiv b \times d \pmod{n}}$$

$$\frac{\begin{array}{c} a \equiv b \pmod{n} \\ b \equiv b \pmod{n} \end{array}}{a-b \equiv 0 \pmod{n}}$$

What about division ?

$$\begin{array}{l} a \equiv b \pmod{n} \\ c \equiv d \pmod{n} \\ \hline \end{array}$$

$\frac{a}{c} \equiv \frac{b}{d} \pmod{n}$? Is $\frac{a}{c}$ integer ?

Consider $a \equiv b \pmod{n}$

Can I say $1 \equiv \frac{b}{a} \pmod{n}$? [divide by a on both sides]

What is division in modular arithmetics ?

$n = 7$

Example 1: $\frac{2}{3} \equiv x \pmod 7 \Rightarrow 2 \equiv 3.x \pmod 7$

Is there x when multiplied by 3 gives 2 ?

$$3.3 \equiv 2 \pmod 7$$

So $\frac{2}{3} \equiv 3 \pmod 7$

What about $\frac{3}{2} \equiv ?5 \pmod 7$

is there an x such that

$x.2 \equiv 3$

$x = 5$

$$\frac{2}{3} \times \frac{3}{2} \equiv 3 \times 5 \equiv 15 \equiv 1 \pmod 7$$

For division to be well defined, we need to find <u>inverses</u>

$\frac{b}{a} \equiv b \times \frac{1}{a} \equiv b \times a^{-1}$ where $a a^{-1} \equiv 1 \pmod{n}$

Problem: Given a and n, find a^{-1} such that

$$a a^{-1} \equiv 1 \pmod{n}$$

a^{-1} is the inverse of a modulo n.

$n=7$

a	1	2	3	4	5	6
a^{-1}	1	4	5	2	3	6

(1) • $\gcd(a,n)=1 \iff \exists\ a^{-1} \in \{1,\dots,n-1\}.\ aa^{-1} \equiv 1 \pmod{n}$

(2) • When a^{-1} exists, it's <u>UNIQUE</u>.

Proof(1): • $\gcd(a,n)=1 \Rightarrow ar-ns=1 \Rightarrow ar = ns+1 \Rightarrow ar \equiv 1 \pmod{n}$

$\Rightarrow$ $r \bmod n$ is a^{-1}! (here mod is used as operator)

• $aa^{-1} \equiv 1 \pmod{n} \Longrightarrow aa^{-1} = nk+1 \Rightarrow aa^{-1} - nk = 1 \Rightarrow \gcd(a,n)=1.$

Proof (2):

To prove uniqueness, assume $ab \equiv ac \pmod{n}$

where $b < n$, $c < n$, $b > c$

$$a(b-c) \equiv 0 \pmod{n} \Rightarrow a(b-c) = kn$$

since $\gcd(a,n) = 1 \Rightarrow$ all factors of n come from $(b-c)$

(uniqueness of prime factorization)

so $(b-c)$ is a multiple of n, contradiction since $b < n$

$c < n$.

so $b - c < n$.

$n=8$

$$\begin{array}{cccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{array}$$

$\times 3$

$a=3.$

$$\begin{array}{cccccccc} 0 & 3 & 6 & 1 & 4 & 7 & 2 & 5 \end{array}$$

$$\gcd(3,8)=1 \Rightarrow 3x \not\equiv 3y \pmod{8}$$

$3x$ are all different $\Rightarrow$ Permutation.

Euclidean alg. can find inverses.

<u>Example:</u> Find inverse of 13 modulo 21.

First observe that $\gcd(21,13)=1$.

Now perform Euclidean Alg. (not to find gcd but to find the linear combination)

21	13	8	5	3	2	1	0
1	0	1	-1	2	-3	5	
0	1	-1	2	-3	5	-8	

$$\gcd(21,13) = 21(5) + 13(-8) = 21(5) - 13(8) = 1$$

So -8 is the inverse of 13 mod 21

$$-8 \equiv 13 \pmod{21}$$

$$13 \cdot 13 \equiv 1 \pmod{21}$$

Similarly: 5 is inverse of 21 mod 13.

$$21 \cdot 5 \equiv 1 \pmod{13}$$

Find the inverse of 15 mod 26

($\gcd(15,26) = 1$)

Find x s.t

$15 . x \equiv 1 \pmod{26}$

$\uparrow 15^{-1}$

26	15	11	4	3	1	0
1	0	1	-1	3	-4	
0	1	-1	2	-5	7	

We can write $26(-4) + 15(7) = 1$

So $15^{-1} \equiv 7 \mod 26$

Also, $26(-4+15) + 15(7-26) = 1$

So $26^{-1} \equiv 11 \mod 15$

- We can even solve equations modulo n when inverses exist for instance when n is prime

$$ax \equiv b \pmod{n}$$

$$\underbrace{a^{-1}a}_{1}x \equiv a^{-1}b \pmod{n}$$

$$x \equiv a^{-1}b \pmod{n}$$

It's like dividing by a on both sides!

- We can solve a system of equations as well.

$$\left.\begin{aligned} ax + by &\equiv c \pmod{n} \\ dx + ey &\equiv f \pmod{n} \end{aligned}\right\} \text{eliminate } y \text{ as usual}$$

get $Ax \equiv B \pmod{n}$