X R is an equiv relation on X

R is reflexive $\forall x \in X$ xRx

symmetric $\forall x,y \in X$, $xRy \Rightarrow yRx$

transitive $\forall x,y,z$, xRy & yRz $\Rightarrow xRz$

If R is an ~~eq~~ ER on X, then
equiv Rel

R partitions X

A partition of a set X is a set of subsets of X, $X_1, \ldots, X_k$ s.t.
such that

(disjoint)

1) $X_i \cap X_j = \phi \quad \forall i \neq j$

2) $\bigcup_{i=1}^{k} X_i = X$

mod k

$R \Longrightarrow$ Partion. $\{[x] \mid x \in X\}$

$x \in X$, $[x] = \{y \mid xRy\}$ (equiv class of x)

$[x] \cap [y] = \phi$ or $[x]$

$[x] \neq \phi$ $\because$ xRx

$[x] \cap [y] \neq \phi \Rightarrow \exists z \in [x] \cap [y]$

$\Rightarrow xRz$ & yRz $\Rightarrow xRz$

$\Rightarrow xRz \,\&\, yRz \Rightarrow xRz$

	Reason
$xRz \,\&\, yRz$	$z \in [x] \cap [y]$
$xRz \,\&\, zRy$	R is symm
xRy	R is trans
yRx	R is symmetric
$[x] = [y]$	R trans xRy, yRx

Have partion, then get equiv relation?

$P = \{X_1, X_2, \ldots, X_K\}$, $X_i \cap X_j = \emptyset \ \forall i \neq j$

$\cup X_i = A$

xRy iff $\exists i$ s.t. $x, y \in X_i$

xRx $\because$ $\cup X_i = A$, $x \in X_i$ for some i

$xRy \Rightarrow yRx$? X_i unique

$xRy \,\&\, yRz \Rightarrow xRz$

mod 7

xRy iff $x \% 7 = y \% 7$

$x\%7 = x\%7$

$x\%7 = y\%7 \Rightarrow y\%7 = x\%7$

$x\%7 = y\%7 \,\&\, y\%7 = z\%7 \Rightarrow x\%7 = z\%7$

Equivalence Relations $\Longleftrightarrow$ Partitions

$n \times m$ Matrix $+$ $\times$

$\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix} \overset{+}{\times} \begin{bmatrix} 3 & 1 & 2 \\ 4 & 6 & 5 \end{bmatrix} = \begin{bmatrix} 3 & 2 & 6 \\ 16 & 30 & 30 \end{bmatrix}$

G is a group.

$|G|$ = order of G.

$|\mathbb{Z}| = \aleph_0$

$|\mathbb{Q}| = \aleph_0$

$|\mathbb{R}| = \aleph_1$

$g \in G$ order of g is the smallest n s.t. $g^n = e$ (if n exists) else $\text{order}(g) = \infty$

$(\mathbb{Z}, +)$ order $(1) = ?\ \infty$

$(\mathbb{Z}_9, +)$ order $(1) = 9$ order$(g) < \infty$

If $|G|$ is finite, & $g \in G$, Λ order$(g) \mid |G|$

$a|b \Rightarrow b \% a = 0$

$g, g*g = g^2, g^3 \ldots\ldots$ can't all be different.

so $\exists\, i, j$ $i \neq j$ s.t. $g^i = g^j$

assume $i < j$ $g^{-i} g^i = e$

$g^{-1} g = e$ $\quad \underbrace{g^{-1} g^{-1} \cdots g^{-1}}_{i}\ \underbrace{g\, g\, g \cdots}_{i} = e$

$g^{-i} g^i = g^{-i} g^j$

$e = g^{j-i}$ $\quad j - i \neq 0$

$$e = g^{j-i} \quad j-i \neq 0$$

$$\text{order}(g) = \text{order}(g^{-1})$$

G is <u>cyclic</u> iff $\exists\, g \in G$ s.t. $\text{order}(g) = |G|$

$$G = e, g, g^2, \ldots, g^{|G|-1}$$

<u>Thm</u> if G is cyclic then G is abelian

$$g^i \cdot g^j = g^{(i+j)\%|G|} \quad g^j \cdot g^i = g^{j+i} = g^{i+j}$$

If G is cyclic & $\text{order}(g) = |G|$, g is called a generator of G.

Are generators unique?

$\mathbb{Z}\ \%4$

1, 2, 3, 0	order 4
2, 0, 2, 0, . . .	order 2
3, 2, 1, 0	order 4
0	order 1

$\mathbb{Z}_{16}$ 1 order 16

$$(\mathbb{Z}_{16}^{\times} - \{0\}, *) \qquad (\mathbb{Z}_{16}^{\times}, *)$$

$$\mathbb{Z}_{16}^{\times} = \{ n \in \text{range}(16) \mid GCD(n, 16) = 1 \}.$$
$$= \{1, 3, 5, 7, 9, 11, 13, 15\}$$
$$1^{-1} = 1 \quad 7^{-1} = 7$$

$3^{-1} = 11 \quad 9^{-1} = 9$

$5^{-1} = 13$

$(\mathbb{Z}/\mathbb{Z}_{16})^*$

order of $\mathbb{Z}_k^*$ is $\phi(k)$

Euler ϕ function.

if p is prime $\phi(p) = p-1$

How to compute $\phi(k)$?