Defn: Let G be any group, and choose $g \in G$

the cyclic subgroup of G generated by g is

$\{\ldots, g^{-2}, g^{-1}, 1, g, g^2, \ldots\} =: \langle g \rangle$

2 possibilities

$|\langle g \rangle| < \infty$

then $\exists\ k \neq l \in \mathbb{N}$

w/ $g^k = g^l$

then also

$1 = g^{-k} g^k = g^{-k} g^l = g^{l-k}$

$\Rightarrow \operatorname{ord}(g) < \infty$

$|\langle g \rangle| = \infty$

"translation"

$\langle g \rangle \qquad \mathbb{Z}$

$g^i \longleftrightarrow i$

$g^i \cdot g^j \longleftrightarrow i+j$

We see

$|\langle g \rangle| < \infty \iff \operatorname{ord}(g) < \infty$

Ex: $G = (\mathbb{Z}/_{12}\mathbb{Z}, +)$

study orders, subgroups, etc

g	$\langle g \rangle$	$\frac{n}{\langle g \rangle}$	$\lvert\langle g \rangle\rvert$
$\bar{0}$	$\{\bar{0}\}$	12	1
$\bar{1}$, $\bar{5}, \bar{11}, \bar{7}$	$\{\bar{0}, \bar{1}, \ldots, \bar{11}\}$	1	12
$\bar{2}, \bar{10}$	$\{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \bar{10}\}$	2	6
$\bar{3}, \bar{9}$	$\{\bar{0}, \bar{3}, \bar{6}, \bar{9}\}$	3	4
$\bar{4}, \bar{8}$	$\{\bar{0}, \bar{4}, \bar{8}\}$	4	3
$\bar{6}$	$\{\bar{0}, \bar{6}\}$	6	2

Facts:

- inside $\mathbb{Z}/n\mathbb{Z}$, $\lvert\langle \bar{g} \rangle\rvert = \dfrac{n}{\gcd(n,g)}$
- $\langle \bar{g}^i \rangle = \langle \bar{g}^j \rangle \iff \gcd(i,n) = \gcd(j,n)$

Note: The subgroup of $\langle \bar{g}^i, \bar{g}^j \rangle$ is cyclic

Ex: $\mathbb{Z}/12\mathbb{Z}$ look at $\langle \bar{4}, \bar{6} \rangle$

$$\langle \bar{4}, \bar{6} \rangle = \{ \bar{4}, \bar{6}, \bar{2}, \overline{10}, \bar{8}, \bar{0} \} = \langle 2 \rangle$$

Namely: let a be the gcd of $i, j, \operatorname{ord}(g)$

Euclid: $\exists\ x, y \in \mathbb{Z}$ w/ $\gcd(i,j) = xi + yj$

Euclid: $\exists\ r, s \in \mathbb{Z}$ w/ $\gcd(\gcd(i,j), \operatorname{ord}(g))$

$$= r \cdot \gcd(i,j) + s \cdot \operatorname{ord}(g)$$

So, there are u, v, w w/

$\gcd(i, j, \operatorname{ord}(g)) = u \cdot i + v \cdot j + w \cdot \operatorname{ord}(g)$

then:

$$g^{\gcd(i,j,\operatorname{ord}(g))} = g^{u \cdot i + v \cdot j + w \cdot \operatorname{ord}(g)}$$

$$= (g^i)^u \cdot (g^j)^v \underbrace{(g^{\operatorname{ord}(g)})^w}_{1G}$$

is an element of $\langle g^i, g^j \rangle$

and also some power of g.

O.T.O.H, $\gcd(i, j, \mathrm{ord}(g)) \mid i$

$\Rightarrow g^i$ is a power of $g^{\gcd(i,j,\mathrm{ord}(g))}$

conclusion: $\langle g^i, g^j \rangle = \langle g^{\gcd(i,j,\mathrm{ord}(g))} \rangle$

So, any subgroup of $\langle g \rangle$ is cyclic

Ex: $\mathbb{Z}/12\mathbb{Z}$, we found

$\langle \bar{1} \rangle = \langle \bar{5} \rangle = \langle \bar{7} \rangle = \langle \bar{11} \rangle = \{\bar{0}, \dots, \bar{11}\}$

$\langle \bar{0} \rangle = \{\bar{0}\}$

$\langle \bar{2} \rangle = \langle \bar{10} \rangle = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \bar{10}\}$

$\langle \bar{3} \rangle = \langle \bar{9} \rangle = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}\}$

$\langle \bar{4} \rangle = \langle \bar{8} \rangle = \{\bar{0}, \bar{4}, \bar{8}\}$

$\langle \bar{6} \rangle = \{\bar{0}, \bar{6}\}$

Next, in $\mathbb{Z}/n\mathbb{Z}$, which (and how many) elements in g produce $\langle g \rangle = \mathbb{Z}/n\mathbb{Z}$?

A: $\langle g \rangle = \mathbb{Z}/n\mathbb{Z} \iff \gcd(g, n) = 1$

Def^n: Given $n \in \mathbb{N}$, the number of numbers i, on the list $0, \ldots, n-1$, w/ $\gcd(i, n) = 1$ is the Euler φ-function $\varphi(n)$

Ex: $\varphi(12) = 4$