Recall

- $\varphi(n) = \#\{ i \in \mathbb{N},\ 0 \leq i \leq n,\ \gcd(i,n) = 1 \}$

- if $g \in G$ of order n the generators of $\langle g \rangle$ are the powers g^i w/ $\gcd(i,n) = 1$

Thm:

- any subgroup of a cyclic group is cyclic

- if $|\langle g \rangle| = \mathrm{ord}(g)$ is n, then $\mathrm{ord}(g^2) = \dfrac{n}{\gcd(n,i)}$
  and in particular if $i | n$ (i divs. n)
  then $\mathrm{ord}(g^i) = \dfrac{n}{i}$

- the subgroups of $\langle g \rangle$ all have size dividing n.

- if $k | n$ then there is exactly one subgroup of size k (generated by $g^{(n/k)}$)

- The number of elements in $\langle g \rangle$ that have order k, is exactly $\varphi(k)$. Also, any such k must divide n.
- $n = \sum_{d|n} \varphi(k)$

<u>Ex</u> $\mathbb{Z}/12\mathbb{Z}$

- $\langle \bar{1} \rangle = \langle \bar{11} \rangle = \langle \bar{5} \rangle = \langle \bar{7} \rangle$ size 12
- $\langle \bar{2} \rangle = \langle \bar{10} \rangle$ 6
- $\langle \bar{3} \rangle = \langle \bar{9} \rangle$ 4
- $\langle \bar{4} \rangle = \langle \bar{8} \rangle$ 3
- $\langle \bar{6} \rangle$ 2
- $\langle \bar{0} \rangle$ 1

$$12 = \underset{12}{4} + \underset{6}{2} + \underset{4}{2} + \underset{3}{2} + \underset{2}{1} + \underset{1}{1} = 12$$

Products + Cyclicity

<u>Ex</u> : $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ has 6 elements and it is a group.

$\bar{0}, \bar{1}$ $\quad\quad$ $\bar{0}, \bar{1}, \bar{2}$

is it cyclic?

$$\langle(\bar{0},\bar{0})\rangle = \{(\bar{0},\bar{0})\}$$

$$\langle(\bar{1},\bar{1})\rangle = \underbrace{\{(\bar{1},\bar{1}), \overset{(\bar{0},\bar{2})}{(\bar{2},\bar{2})}, \overset{(\bar{1},\bar{0})}{\overset{\shortparallel}{(\bar{3},\bar{3})}}, \overset{(\bar{0},\bar{1})}{(\bar{4},\bar{4})}, \overset{(\bar{1},\bar{2})}{(\bar{5},\bar{5})}, \overset{(\bar{0},\bar{0})}{\overset{\shortparallel}{(\bar{6},\bar{6})}}\}}_{\text{size 6 (the whole group)}}$$

so $(\bar{1},\bar{1})$ is a generator of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, so this group is cyclic.

if we try $(\bar{a},\bar{b})$, we get

$(\bar{a},\bar{b}), (\overline{2a},\overline{2b}), (\overline{3a},\overline{3b}), (\overline{4a},\overline{4b}), (\overline{5a},\overline{5b}), (\overline{6a},\overline{6b})$

In order for the elts. to be different, we need

$\gcd(a,2) = 1$ & $\gcd(b,3) = 1$

$\bar{a} = \bar{1}$ $\quad\quad\quad$ $\bar{b} = 1$ or $\bar{b} = 2$

Check:

$$(\bar{1},\bar{2}),\ (\bar{2},\bar{4}),\ (\bar{3},\bar{6}),\ (\bar{4},\bar{8}),\ (\bar{5},\overline{10}),\ (\bar{6},\overline{12})$$

$$(\bar{2},\bar{4}) = (\bar{0},\bar{1}),\quad (\bar{3},\bar{6}) = (\bar{1},\bar{0}),\quad (\bar{4},\bar{8}) = (\bar{0},\bar{2}),\quad (\bar{5},\overline{10}) = (\bar{1},\bar{1}),\quad (\bar{6},\overline{12}) = (\bar{0},\bar{0})$$

Ex: $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$

$\bar{0},\bar{1}$ $\qquad$ $\bar{0},\bar{1},\bar{2},\bar{3}$

$(\bar{a},\bar{b})$ gives,

$(\bar{a},\bar{b}), (\overline{2a},\overline{2b}), \ldots, (\overline{8a},\overline{8b})$ these are not all different because

$(\overline{8a},\overline{8b}) = (\bar{0},\bar{0})$

$(\overline{4a},\overline{4b}) = (\bar{0},\bar{0})$

$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ $\quad (\bar{a},\bar{b}) \ldots (\overline{12a},\overline{12b})$

Thm: $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ is cyclic

$\iff \operatorname{lcm}(m,n) = m \cdot n \iff \gcd(m,n) = 1$

Suppose $\gcd(m,n)=1$

then $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ is a cyclic group,

with $m \times n$ elts.

so $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/_{mn}\mathbb{Z}$

How does this work?

<u>Ex</u>: $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \overset{?}{=} \mathbb{Z}/6\mathbb{Z}$

		Preserve addition	
	$(\bar{0},\bar{0})$		$\bar{0}$
	$(\bar{1},\bar{1})$		$\bar{1}$
$(\bar{0},\bar{2})=$	$(\bar{2},\bar{2})$		$\bar{2}$
$(\bar{1},\bar{0})=$	$(\bar{3},\bar{3})$		$\bar{3}$
$(\bar{0},\bar{1})=$	$(\bar{4},\bar{4})$		$\bar{4}$
$(\bar{1},\bar{2})$	$(\bar{5},\bar{5})$		$\bar{5}$

Could have:

sent $(\bar{1})$ to any

generator of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/_{3}\mathbb{Z}$

So, we also could have sent the generator $\bar{1}$,

to the generator $(\bar{1},\bar{2})$

(This <u>is</u> a generator, because it was matched

with the generator $(\bar{5})$)

$$(\bar{0},\bar{0}) \longleftrightarrow \bar{0}$$

$$(\bar{1},\bar{2}) \longleftrightarrow \bar{1}$$

$$(\bar{0},\bar{1}) = (\bar{2},\bar{4}) \qquad \bar{2}$$

$$(\bar{1},\bar{0}) = (\bar{3},\bar{6}) \qquad \bar{3}$$

$$(\bar{0},\bar{2}) = (\bar{4},\bar{8}) \qquad \bar{4}$$

$$(\bar{1},\bar{1}) = (\bar{5},\overline{10}) \qquad \bar{5}$$