Example : Find a subgrp of $\mathbb{Z}_{30} \oplus \mathbb{Z}_{12}$, which is isomorphic to $\mathbb{Z}_6 \oplus \mathbb{Z}_4$

(Solution) $o(\mathbb{Z}_6) = 6$
$o(\mathbb{Z}_4) = 4$

we have to find a subgrp of order 6 in $\mathbb{Z}_{30}$ and a subgrp of order 4 in $\mathbb{Z}_{12}$

$\mathbb{Z}_{30}$ is cyclic & $6 \mid 30$

Using! (for each divisor of order of cyclic grp, there is a subgrp of that order)

~~we get~~

$\Rightarrow \exists$ a subgrp H_1 of order 6 of form
$H_1 = \langle \frac{30}{6} \rangle = \langle 5 \rangle$

similarly, $4 \mid 12$ & $\mathbb{Z}_{12}$ is cyclic
$\Rightarrow \exists$ a subgrp H_2 of order 4
of form $H_2 = \langle \frac{12}{4} \rangle = \langle 3 \rangle$

Now $H_1 \oplus H_2 = \underbrace{\langle 5 \rangle}_{\text{cyclic grp of order 6}} \oplus \underbrace{\langle 3 \rangle}_{\text{cyclic grp of order 4}} \cong \mathbb{Z}_6 \oplus \mathbb{Z}_4$

Theorem: Criterion for $G \oplus H$ to be cyclic.

Let G & H be finite cyclic groups. Then $G \oplus H$ is cyclic if and only if $|G|$ and $|H|$ are relatively prime.

i.e $G \oplus H$ is cyclic $\Leftrightarrow \gcd(|G|, |H|) = 1$

(pf) To show: $G \oplus H$ is cyclic $\Leftrightarrow \gcd(|G|, |H|) = 1$

let assume that $G \oplus H$ is cyclic
and $|G| = m$ & $|H| = n$.
to show: $\gcd(m, n) = 1$

Suppose $\gcd(m,n) = d$
and $G \oplus H = \langle (g,h) \rangle$ where $g \in G$, $h \in H$ ($G \oplus H$ is cyclic)

Consider $(g,h)^{\frac{mn}{d}} = \left(g^{\frac{mn}{d}}, h^{\frac{mn}{d}}\right)$

$= \left((g^m)^{\frac{n}{d}}, (h^n)^{\frac{m}{d}}\right)$

$= \left(e^{\frac{n}{d}}, e^{\frac{m}{d}}\right)$

$= (e, e)$ — ①

(Using, let G be finite grp & $a \in G$, then $a^{O(G)} = e$)

Now, $|G \oplus H| = mn$ ($\because O(G \oplus H) = O(G) \cdot O(H)$)
and $G \oplus H = \langle (g,h) \rangle$

$\Rightarrow |(g,h)| = mn \le \frac{mn}{d}$ (using ①)

possible only if $d = 1$

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

Conversely, let $\gcd(m,n) = 1$, $|G| = m$, $|H| = n$
Let $G = \langle g \rangle$, $H = \langle h \rangle$ ($\because G$ & H are cyclic grps)
where $g \in G$, $h \in H$

Now, $|(g,h)| = \text{lcm}(|g|, |h|)$ (by theorem on order of elt in EDP)

$= \text{lcm}(m,n)$ (Using $G = \langle g \rangle \Rightarrow O(g) = m$)

$= mn$ ($\because \gcd(m,n) = 1 \Rightarrow \text{lcm}(m,n) = mn$)

$\therefore |(g,h)| = mn$
$= |G \oplus H|$

$\therefore G \oplus H$ is cyclic grp generated by (g,h)

Corollary (Extension of above theorem)
An external direct product $G_1 \oplus G_2 \oplus \cdots \oplus G_m$ of a finite number of finite cyclic groups is cyclic $\Leftrightarrow |G_i|$ & $|G_j|$ are relatively prime when $i \neq j$

$(|C_m|, |C_n|) = 1$

corollary ② Criterion for
$$Z_{n_1 n_2 \cdots n_k} \approx Z_{n_1} \oplus Z_{n_2} \oplus \cdots \oplus Z_{n_k}$$

Let $m = n_1 n_2 \cdots n_k$
then Z_m is isomorphic to $Z_{n_1} \oplus Z_{n_2} \oplus \cdots \oplus Z_{n_k}$ if and only if n_i & n_j are relatively prime when $i \neq j$

(e.g) $Z_2 \oplus Z_2 \oplus Z_3 \oplus Z_5 \approx Z_2 \oplus Z_6 \oplus Z_5$ (as $\gcd(2,3) = 1$)

$\approx Z_2 \oplus Z_{30}$ — ① (as $\gcd(6,5) = 1$)

Similarly

$Z_2 \oplus Z_2 \oplus Z_3 \oplus Z_5 \approx Z_2 \oplus Z_3 \oplus Z_2 \oplus Z_5$

$\approx Z_6 \oplus Z_{10}$ — ②

Thus, $Z_2 \oplus Z_{30} \approx Z_6 \oplus Z_{10}$.
(from ① & ②)

But $Z_2 \oplus Z_{30} \not\approx Z_{60}$ ($\because \gcd(2,30) \neq 1$)

GROUP OF UNITS MODULO n as an EDP (External Direct Product)

$U(n)$ is group of units modulo n

$U(n) = \{1 \leq x < n \mid \gcd(x,n) = 1\}$

Now, we define subset $U_k(n)$ of $U(n)$ provided k is a divisor of n.

i.e $U_k(n) = \{x \in U(n) \mid x \equiv 1 \bmod k\}$

(e.g) $U(15) = \{1, 2, 4, 7, 8, 11, 13, 14\}$

Now, $U_3(15) = \{x \in U(15) \mid x \equiv 1 \mod 3\}$ (as $3 \mid 15$)

$= \{1, 4, 7, 13\} \subseteq U(15)$

(Exercise)

Remark: $U_k(n)$ is subgrp of $U(n)$, where $k \mid n$

(Theorem) $U(n)$ as an EDP

Suppose s & t are relatively prime. Then $U(st)$ is isomorphic to the external direct product of $U(s)$ & $U(t)$.

i.e $U(st) \approx U(s) \oplus U(t)$

Moreover, $U_s(st) \approx U(t)$

& $U_t(st) \approx U(s)$

(proof) $U(st) \approx U(s) \oplus U(t)$

$x \longmapsto (x \mod s, x \mod t)$

(show: isomorphism)

$U_s(st) \approx U(t)$

$x \longmapsto x \mod t$ (show: isomorphism)

$U_t(st) \approx U(s)$

$x \longmapsto x \mod s$ (show: isomorphism)

(Do as exercise)

Corollary: Let $m = n_1 n_2 \cdots n_k$ where $\gcd(n_i, n_j) = 1$ for $i \neq j$. Then

$U(m) \approx U(n_1) \oplus U(n_2) \oplus \cdots \oplus U(n_k)$

(e.g) $U(15) = \{1, 2, 4, 7, 8, 11, 13, 14\}$

Now, $U_3(15) = \{x \in U(15) \mid x \equiv 1 \bmod 3\}$ (as $3 \mid 15$)

$= \{1, 4, 7, 13\} \subseteq U(15)$

Remark: (Exercise) $U_k(n)$ is subgrp of $U(n)$, where $k \mid n$

(Theorem) $U(n)$ as an EDP

Suppose s & t are relatively prime. Then $U(st)$ is isomorphic to the external direct product of $U(s)$ & $U(t)$.

i.e $U(st) \approx U(s) \oplus U(t)$

Moreover, $U_s(st) \approx U(t)$

& $U_t(st) \approx U(s)$

(proof) $U(st) \approx U(s) \oplus U(t)$

$x \longmapsto (x \bmod s, x \bmod t)$

(show: isomorphism)

$U_s(st) \approx U(t)$

$x \longmapsto x \bmod t$ (show: isomorphism)

$U_t(st) \approx U(s)$

$x \longmapsto x \bmod s$ (show: isomorphism)

(Do as exercise)

Corollary: let $m = n_1 n_2 \cdots n_k$ where $\gcd(n_i, n_j) = 1$ for $i \neq j$. Then

$U(m) \approx U(n_1) \oplus U(n_2) \oplus \cdots \oplus U(n_k)$

Application:

$U(105)$

$105 = 3 \times 5 \times 7$

$U(105) \approx U(3) \oplus U(5) \oplus U(7)$

$\approx U(15) \oplus U(7)$

$\approx U(3) \oplus U(35)$

$\approx U(21) \oplus U(5)$

Remark:

U(n) as product of Z_n

① $U(2) \approx \{0\}$

② $U(2^2) \approx U(4) \approx Z_2$

③ $U(2^n) \approx Z_2 \oplus Z_{2^{n-2}}$ for $n \geq 3$

and $U(p^n) \approx Z_{p^n - p^{n-1}}$ for p is odd prime

example:

$U(105) = U(3 \cdot 5 \cdot 7)$

$\approx U(3) \oplus U(5) \oplus U(7)$

$\approx Z_2 \oplus Z_4 \oplus Z_6$

$U(720) = U(16 \cdot 9 \cdot 5) = U(2^4 \cdot 9 \cdot 5)$

$\approx U(16) \oplus U(9) \oplus U(5)$

$\approx U(2^4) \oplus U(3^2) \oplus U(5)$

$\approx Z_2 \oplus Z_4 \oplus Z_6 \oplus Z_4$

Exercise: what can be order of elements of $U(720)$?

and find number of elements of order 12 in $U(720)$.