Unit-2

The Group of units Modulo n as an External Direct product

Date: 12.04.20

Defn: Let n be a positive integer. The set of all congruence classes of integer modulo n is denoted by $\mathbb{Z}_n$. Define addition '+' of the congruence classes $[a], [b] \in \mathbb{Z}_n$ by $[a] + [b] = [a+b]$ $\forall [a], [b]$ in $\mathbb{Z}_n$.

Then $(\mathbb{Z}_n, +)$ is a commutative group.

In $\mathbb{Z}_n$, $[0], [1], [2], \ldots [n-1]$ are n distinct congruence classes. The number of elements of $\mathbb{Z}_n$ is n. Also we know $(\mathbb{Z}_n, +)$ is cyclic group.

Again $(\mathbb{Z}_n^*, \cdot)$ is not a group, because inverse of some element doesn't exists.

We know $\bar{a} \in \mathbb{Z}_n$ has multiplicative inverse modulo n iff $g.c.d(a, n) = 1$.

We define $U(n)$ to be the set of all possitive integer less than n and prime to n.

i.e $U(n) = \{ a \in \mathbb{Z}^+ : 1 < a \leq n-1, g.c.d(a, n) = 1 \}$.

i.e, $U(n)$ is a set of all multiplicative inverse of $\mathbb{Z}_n$.

Then $U(n)$ is a group under multiplication modulo n.

$\therefore U(n) = \{ [a] \in \mathbb{Z}_n^* \mid g.c.d(a, n) = 1 \}$.

which is also denoted by U_n.

$\therefore (U(n), \cdot)$ is a commutative group. $[a][b] = [ab]$ $\forall [a], [b] \in \mathbb{Z}_n^*$

The U-grops provide a convenient way to illustrate the preceding ideas.

Defn: Let K is a divisor of n. Then

$$U_K(n) = \{ x \in U(n) \mid x \bmod K = 1 \}$$

Ex: $U_7(30) = \{1, 23, 29\}$.

$U(30) = \{1, 7, 11, 13, 17, 19, 23, 27, 29\}$

Th: Show that $U_k(n)$ is a subgroup of $U(n)$. (HT).

Th: Suppose s and t are relatively prime. Then $U(st)$ is isomorphic to the external direct product of $U(s)$ and $U(t)$. i.e, $U(st) \simeq U(s) \oplus U(t)$.

Moreover, $U_s(st) \simeq U(t)$ and $U_t(st) \simeq U(s)$.

Proof: Let us define $\varphi : U(st) \to U(s) \oplus U(t)$ by

$\varphi(x) = (x \bmod s, x \bmod t)$. $\forall x \in U(st)$.

Clearly φ is well define.

one-one: Let $x, y \in U(st)$ and $\varphi(x) = \varphi(y)$

$\Rightarrow (x \bmod s, x \bmod t) = (y \bmod s, y \bmod t)$

$\Rightarrow x \bmod s = y \bmod s \mid x \bmod t = y \bmod t$.

$\Rightarrow s \mid x-y$ and $t \mid x-y$

$\Rightarrow x \equiv y \pmod s$

$x \equiv y \pmod t$.

$\Rightarrow x \equiv y \pmod{st}$ $\because$ g.c.d $(s,t) = 1$.

$\Rightarrow st \mid x-y$.

$\Rightarrow x \bmod st = y \bmod st$.

$\Rightarrow x = y$.

onto: Let $(x \bmod s, y \bmod t) \in U(s) \oplus U(t)$

Since g.c.d $(s,t) = 1$. $\exists\ S, T \in \mathbb{Z}$

$sS + tT = 1$

$\Rightarrow tT - 1 = sS$

$\Rightarrow tT \equiv 1 \pmod s$

Similarly $sS \equiv 1 \pmod t$

Then $xtT \equiv x \pmod s$

$ysS \equiv y \pmod t$.

Thus $\varphi(xtT + ysS) = (x \bmod s, y \bmod t)$

$\therefore xtT + ysS$ is preimage of φ

$\therefore \varphi$ is onto

clearly φ is homomorphism.

$\therefore U(st) \simeq U(s) \oplus U(t)$.

for second part: to show $U_s(st) \simeq U(T)$ define.

$\psi(x) = x \bmod T$

Test ψ is isomorphism ($s \perp T$).

corollary: Let $m = n_1 n_2 \cdots n_k$, where $g.c.d(n_i, n_j) = 1$ for $i \neq j$

Then $U(m) \simeq U(n_1) \oplus U(n_2) \oplus \cdots \oplus U(n_k)$.

prob: Show that $U(105) \simeq U(3) \oplus U(5) \oplus U(7)$.

Show $U_{15}(105) \simeq ?$

Note: Among all groups, surely the cyclic groups Z_n have the simplest structures, and, at the same time, are the easiest groups with which to compute. Direct products of groups of the form Z_n are only slightly more complicated in structure and computability. Because of this, algebraists endeavor to describe a finite Abelian group as such a direct product. We shall soon see that every finite Abelian group can be so represented.

Some result:

$U(2) \simeq \{0\}$, $U(2^2) \simeq Z_2$

$U(2^n) \simeq Z_2 \oplus Z_{2^{n-2}}$ $\forall n > 3$

$U(p^n) \simeq Z_{p^n - p^{n-1}}$ for p an odd prime.

Prob: ① $U(720) \simeq ?$ ⑤ prove or disprove $U(40) \oplus Z_6 \simeq U(72) \oplus Z_4$

② $U(105) \simeq ?$

③ find number of element of order 7 in $U(21)$.

④ find number of 5 order subgroup of $U(35)$