Fundamental Theorem of Cyclic Groups:

Statement: Every subgroup of a cyclic group is cyclic. Moreover, if $|\langle a\rangle| = n$, then the order of any subgroup of $\langle a\rangle$ is a divisor of n and for each positive divisor k of n, the group $\langle a\rangle$ has exactly one subgroup of order k - namely $\langle a^{n/k}\rangle$.

$G = \mathbb{Z}_6 = \langle 1\rangle$.
$\quad = \langle 5\rangle$

$G = \langle a\rangle$, $|G| = n$

$|\langle 1\rangle| = 6$

$H_1 = \{0\}$, $H_2 = \mathbb{Z}_6 = \langle 1\rangle$

$H_3 = \{0, 2, 4\} = \langle 2\rangle$

$H_4 = \{0, 3\} = \langle 3\rangle$.

$1, 2, 3, 6$

Note: 1 and $(n-1)$ are always generator of $\mathbb{Z}_n$.

$\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$

$k=1$, $\langle a^{6/1}\rangle = \langle 1^6\rangle = \langle 6\rangle = \langle 0\rangle = H_1$

$k=2$, $\langle 1^{6/2}\rangle = \langle 1^3\rangle = \langle 3\rangle = H_4$

$k=3$, $\langle 1^{6/3}\rangle = \langle 1^2\rangle = \langle 2\rangle = H_3$

$k=6$, $\to H_2$.

Proof: Let $G = \langle a\rangle$ and suppose that H is a subgroup of G

TS H is a cyclic subgroup.

If $H = \{e\}$, then $H = \langle e\rangle$.

we are done.

If $H \neq \{e\}$. Then we claim that H contains an element of the form a^t, where t is positive.

$H \subseteq G = \langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$

If t is negative, then $-t$ is positive and $a^t \in H \Rightarrow a^{-t} \in H$ [$\because H$ is a subgroup]

Now let m be the smallest positive integer such that $a^m \in H$

Now we will show that $H = \langle a^m \rangle$.

Now let $b \in H$ be an arbitrary element of H.

Now $b \in H \subseteq G = \langle a \rangle$

$\Rightarrow b = a^k$ for some $k \in \mathbb{Z}$

By division algorithm, $\exists\, q$ & r such that

$k = mq + r$, where $0 \leq r \leq m-1$ — (1)

$$a^k = a^{mq+r} = a^{mq} \cdot a^r$$

$$\Rightarrow a^{-mq} \cdot a^k = a^{-mq} \cdot a^{mq}\, a^r$$

$$\Rightarrow a^r = a^{-mq} \cdot a^k \quad \text{— (2)}$$

$\Rightarrow \quad a^{r} = a^{-mq} \cdot a^{k}$ ——— (2)

$\because \quad a^{k} = b \in H$

and $a^{-mq} = (a^{m})^{-q} \in H$ [$\because$ H is a subgroup]

from eqn (2), $a^{r} \in H$, where $0 \le r \le m-1$

$\Rightarrow \quad r = 0.$

from eqn (2), $a^{0} = a^{-mq} \cdot a^{k}$

$\Rightarrow \quad a^{-mq} \cdot a^{k} = e$

$\Rightarrow \quad a^{k} = a^{mq}$

$\Rightarrow \quad a^{k} = (a^{m})^{q}$

$\Rightarrow \quad a^{k} \in \langle a^{m} \rangle$

$\Rightarrow \quad b \in \langle a^{m} \rangle$

$\because$ b is an arbitrary element of H

$\therefore$ every element of H is an element of $\langle a^{m} \rangle$.

$\therefore \quad H \subseteq \langle a^{m} \rangle$ ——— (3)

Now, $a^{m} \in H$

$\Rightarrow \quad \langle a^{m} \rangle \subseteq H$ ——— (4)

from eqn ③ & ④,

$$H = \langle a^m \rangle$$

$\therefore$ every subgroup of $G = \langle a \rangle$ is cyclic.

Suppose that $|G| = |\langle a \rangle| = n$ and let H be the subgroup of G.

then $H = \langle a^m \rangle$ for some m.

Now, $(a^m)^n = a^{mn} = (a^n)^m = e^m = e$

$|a| = n$ & $a^k = e$ then n divides k.

$\Rightarrow |a^m|$ divides n

$\Rightarrow |H|$ divides n. $[\because |H| = |a^m|]$

Now, let k be any divisor of n.

TS The group $G = \langle a \rangle$ has exactly one subgroup of order k, namely $\langle a^{n/k} \rangle$.

$\because k$ is the divisor of n.

clearly, $(a^{n/k})^k = a^n = e$.

and $(a^{n/k})^t \neq e$ for any positive $t < k$.

$t < k$.

$(\cdot)^t \; {}^{nt}/_k$

$|a^{n/k}| = k$

$t < k$.

$a^{(n/k)t} = a^{nt/k}$

$= a^m = e \mid m < n$.

$\therefore \; |a^{n/k}| = k$.

$\Rightarrow |\langle a^{n/k} \rangle| = k$ —— (5)

We need to ~~IS~~ show

$\langle a^{n/k} \rangle$ is the only subgroup of order k.

Let H be any other subgroup of order k.

then $H = \langle a^m \rangle$, where m is the smallest positive integer such that $a^m \in H$

Now, by division algorithm, $\exists q$ & r such that

$n = mq + r$, where $0 \le r \le m-1$ —— (6)

Now, $a^n = a^{mq+r}$

$\Rightarrow e = a^{mq} \cdot a^r$

$\Rightarrow a^r = a^{-mq}$

$\Rightarrow a^r = (a^m)^{-q} \in H$

and $0 \le r \le m-1$.

$\therefore r = 0$.

from eqn (6), $n = mq$

$|a^m| = n/m$

$(a^m)^{n/m} = a^n = e.$

$|a| = n$

$|a| = ?$

$a^n = e.$

$\therefore k = |H| = |\langle a^m \rangle| = n/m$

$\therefore k = n/m \Rightarrow m = n/k$

$\therefore H = \langle a^m \rangle = \langle a^{n/k} \rangle$

$\therefore \langle a^{n/k} \rangle$ is the only subgroup of order k.

"Hence Proved".

Example:

$|a| = 12.$

$G = \langle a \rangle = \{a, a^2, a^3, \dots, a^{11}, e = a^{12}\}$ order 12.

$\langle a^{n/k} \rangle$ for each divisor k.

$\langle a^{n/k} \rangle \to$ order k.

divisors of 12 are 1, 2, 3, 4, 6, 12.

$\langle a^{12/12} \rangle = \langle a \rangle = G \to$ order 12

$\langle a^{12/6} \rangle = \langle a^2 \rangle = \{a^2, a^4, a^6, a^8, a^{10}, e\} \to$ order 6

$\langle a^{12/4} \rangle = \langle a^3 \rangle = \{a^3, a^6, a^9, e\} \to$ order 4

$\langle a^{12/3} \rangle = \langle a^4 \rangle = \{a^4, a^8, e\} \to$ order 3

$\langle a^{12/2} \rangle = \langle a^6 \rangle = \{a^6, e\} \to$ order 2

$\langle a^{12/1} \rangle = \langle a^{12} \rangle = \{e\} \to$ order 1.