Finite Cycle Group Structure

Theorem

$$\forall\, a \in \mathbb{Z}_n, \langle a \rangle = \langle d \rangle, d = (a, n)$$

Proof

Assume $a \in \mathbb{Z}_n$
Let $d = (a, n)$

$\exists\, r, s \in \mathbb{Z}, ra + sn = d$
But $sn = 0$
$ra = d$
$a \mid d$
$d \in \langle a \rangle$
$\langle d \rangle \subseteq \langle a \rangle$

$d \mid a$
$a \in \langle d \rangle$
$\langle a \rangle \subseteq \langle d \rangle$

$\therefore \langle a \rangle = \langle d \rangle$

Corollary

$$\forall\, a \in \mathbb{Z}_n, |\langle a \rangle| = \frac{n}{d}, d = (a, n)$$

Proof

Assume $a \in \mathbb{Z}_n$
Let $d = (a, n)$
Let k be the smallest positive integer such that $kd = n = 0 \pmod n$
$k = \frac{n}{d}$
But $k = |\langle d \rangle|$ and $\langle a \rangle = \langle d \rangle$
$\therefore |\langle a \rangle| = \frac{n}{d}$

Corollary

$$\forall\, a \in \mathbb{Z}_n, \langle a \rangle = \mathbb{Z}_n \iff (a, n) = 1$$

Proof

Assume $a \in \mathbb{Z}_n$
Let $d = (a, n)$

$\Longrightarrow$ Assume $\langle a \rangle = \mathbb{Z}_n$
$|\langle a \rangle| = \frac{n}{d}$
But $|\langle a \rangle| = |\mathbb{Z}_n| = n$
$n = \frac{n}{d}$
$\therefore d = 1$

$\Longleftarrow$ Assume $d = 1$
$\langle a \rangle = \langle 1 \rangle = \mathbb{Z}_n$

Corollary

$$\forall\, h, k \in \mathbb{Z}_n, \langle h \rangle = \langle k \rangle \iff (h, n) = (k, n)$$

Proof

Assume $h, k \in \mathbb{Z}_n$
Let $d_h = (h, n)$ and $d_k = (k, n)$

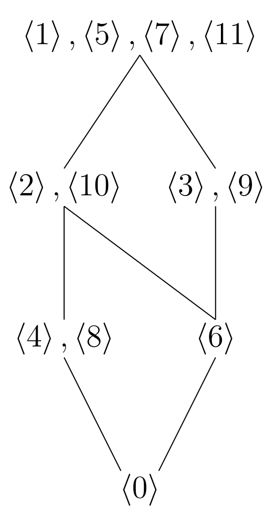
$\implies$ Assume $d_h \neq d_k$ (CP)
AWLOG: $d_h < d_k$
d_k is the smallest positive integer in $\langle d_k \rangle$
But $d_h \in \langle d_h \rangle$
$d_h \notin \langle d_k \rangle$
$\therefore \langle h \rangle \neq \langle k \rangle$

$\impliedby$ Assume $d_h = d_k = d$
$\langle h \rangle = \langle d \rangle$
$\langle k \rangle = \langle d \rangle$
$\therefore \langle h \rangle = \langle k \rangle$

Example

Z_{12}:

$\langle 1 \rangle$	=	$\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 0\}$	$(12, 1) = 1$	$\frac{12}{1} = 12$
$\langle 2 \rangle$	=	$\{2, 4, 6, 8, 10, 0\}$	$(12, 2) = 2$	$\frac{12}{2} = 6$
$\langle 3 \rangle$	=	$\{3, 6, 9, 0\}$	$(12, 3) = 3$	$\frac{12}{3} = 4$
$\langle 4 \rangle$	=	$\{4, 8, 0\}$	$(12, 4) = 4$	$\frac{12}{4} = 3$
$\langle 5 \rangle$	=	$\{5, 10, 3, 8, 1, 6, 11, 4, 9, 2, 7, 0\}$	$(12, 5) = 1$	$\frac{12}{1} = 12$
$\langle 6 \rangle$	=	$\{6, 0\}$	$(12, 6) = 6$	$\frac{12}{6} = 2$
$\langle 7 \rangle$	=	$\langle 5 \rangle$	$(12, 7) = 1$	$\frac{12}{1} = 12$
$\langle 8 \rangle$	=	$\langle 4 \rangle$	$(12, 8) = 4$	$\frac{12}{4} = 3$
$\langle 9 \rangle$	=	$\langle 3 \rangle$	$(12, 9) = 3$	$\frac{12}{3} = 4$
$\langle 10 \rangle$	=	$\langle 2 \rangle$	$(12, 10) = 2$	$\frac{12}{2} = 6$
$\langle 11 \rangle$	=	$\langle 1 \rangle$	$(12, 11) = 1$	$\frac{12}{1} = 12$



Corollary

Let $G = \langle a \rangle$ and $|G| = n$:

$$\forall\, a^m \in G, \langle a^m \rangle = \left\langle a^d \right\rangle, d = (m, n)$$

Corollary

Let $G = \langle a \rangle$ and $|G| = n$:

$$\forall\, a^m \in G, |\langle a^m \rangle| = \frac{n}{d}, d = (m, n)$$

Corollary

Let $G = \langle a \rangle$ and $|G| = n$:

$$\forall\, a^m \in G, \langle a^m \rangle = G \iff (m, n) = 1$$

Corollary

Let $G = \langle a \rangle$ and $|G| = n$:

$$\forall\, a^h, a^k \in G, \left\langle a^h \right\rangle = \left\langle a^k \right\rangle \iff (h, n) = (k, n)$$