Observe: In $\mathbb{Z}_{30}$, it's easy to calculate

$$\langle 2 \rangle = \{2, 4, 6, 8, \ldots, 28, 0\}$$

or $$\langle 5 \rangle = \{5, 10, 15, 20, 25, 0\}$$

or $\langle k \rangle$ when $k \mid 30$.

Note orders:

$$|\langle 2 \rangle| = \frac{30}{2} = 15$$

$$|\langle 5 \rangle| = \frac{30}{5} = 6$$

$$|\langle k \rangle| = \frac{30}{k}$$

what about

$$\langle 23 \rangle = ?$$

$$\langle 26 \rangle = ?$$

$$\langle 18 \rangle = ?$$

Thm Let $a \in G$ have order n. Let k be a positive integer. Then

a divisor of n.

$$\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle \quad \text{and} \quad |a^k| = \frac{n}{\gcd(n,k)}.$$

i.e. $|\langle a^k \rangle|$

What is this saying?

generator of $\mathbb{Z}_{30}$

Ex. In $\mathbb{Z}_{30}$, $26 = 26 \cdot 1$

like a^{26}, but with additive notation when $a = 1$.

Thm says

$$\underbrace{\langle 26 \cdot 1 \rangle}_{\langle a^k \rangle} = \underbrace{\langle \gcd(30,26) \cdot 1 \rangle}_{\langle a^{\gcd(n,k)} \rangle} = \langle 2 \rangle = \{2, 4, 6, \ldots, 28, 0\}.$$

Idea: $\underbrace{\langle 26 \rangle}_{\text{hard to calculate}}$ vs. $\underbrace{\langle 2 \rangle}_{\text{easy to calculate}}$

Also: in $\mathbb{Z}_{30}$,

$$|26| = |\langle 26 \rangle| = |\langle 2 \rangle| = \frac{30}{2}$$

n

$\gcd(n,k)$

$4 = \gcd(12,8)$

<u>Ex.</u> In $\mathbb{Z}_{12}$, $\langle 8 \rangle = \langle 4 \rangle$

$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$

Also: $|8| = |\langle 8 \rangle| = \frac{12}{\gcd(12,8)} = \frac{12}{4} = 3.$

Play with all of this to develop intuition! :)