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

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

Corollary Sps $|a| = n$.

Then $\langle a^i \rangle = \langle a^j \rangle \Leftrightarrow \gcd(n,i) = \gcd(n,j)$

proof: exercise.

Ex In $\mathbb{Z}_{15}$,

$\langle 3 \rangle = \langle 6 \rangle = \langle 9 \rangle = \langle 12 \rangle \rightsquigarrow \gcd(15, x) = 3$

In $\mathbb{Z}_8$,

$\langle 2 \rangle = \langle 6 \rangle \rightsquigarrow \gcd(8,2) = \gcd(8,6)$.

$\{0, 1, 2, 3, 4, 5, 6, 7\}$

Corollary If G is cyclic order n and a is a generator of G, then the generators of G are exactly the elements a^k where $\gcd(n,k) = 1$.

↳ Note: since 1 is a generator of $\mathbb{Z}_n$, this tells us

$$\mathbb{Z}_n = \langle k \rangle \iff \gcd(n,k) = 1$$

$k \cdot 1$

Ex. Generators of $\mathbb{Z}_{12}$:

$$\mathbb{Z}_{12} = \langle 1 \rangle = \langle 5 \rangle = \langle 7 \rangle = \langle 11 \rangle .$$