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

a divisor of $n$.

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

ie. $|\langle a^k \rangle|$

proof: Let $d = \gcd(n,k)$ and sps $k = dp$.

WTS: $\langle a^k \rangle = \langle a^d \rangle$.

First, $\langle a^k \rangle \subseteq \langle a^d \rangle$ because for any integer $m$,

integer

$$\underbrace{a^{mk}}_{\text{generic elt. of } \langle a^k \rangle} = a^{mdp} = (a^d)^{mp} \in \langle a^d \rangle.$$

$d = \gcd(n, k)$

OTOH, to show $\langle a^d \rangle \leq \langle a^k \rangle$, write $d = ks + nt$ for some $s, t \in \mathbb{Z}$.

Then
$$\underbrace{a^{md}}_{\text{generic elt of } \langle a^d \rangle} = a^{m(ks+nt)}$$
$$= (a^k)^{ms} (\underbrace{a^n}_{e})^{mt}$$
$$= (a^k)^{ms} e \quad \leftarrow |a| = n.$$
$$= (a^k)^{ms} \in \langle a^k \rangle.$$

So $\langle a^d \rangle \leq \langle a^k \rangle$.

Thus $\langle a^k \rangle = \langle a^d \rangle$.

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

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

Now : NTS : $|a^k| = \dfrac{n}{\gcd(n,k)}$.

Recall $d = \gcd(n,k)$, so $d \mid n$. Sps $n = d\ell$. for some $\ell \in \mathbb{Z}$.

Notice that if $|a| = n$ and $n = d\ell$, then $|a^d| = \ell$ because

$$(a^d)^\ell = a^{d\ell} = a^n = e.$$

smallest pos. power s.t. $a^n = e$.

and if $0 \leq s < \ell$ then $ds < d\ell = n$ so $a^{ds} \neq e$.

↳ $s$ can't be order of $a^d$.

Thus $|a^d| = \ell$.

Then

a divisor of $n$

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

part 1 of thm