Ex We know the order of every element of a cyclic group must divide the order of the group.

Q: If $|a| = 12$, how many elements of order 12 are there in $\langle a \rangle$?

how many generators?

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

Recall: $|a^k| = 12 \Leftrightarrow \gcd(12, k) = 1$ So there are 4 elts. of order 12.

Q: How many elts of order 6 are there in $\langle a \rangle$?

Note: $|a^2| = 6$

$\{(a^2)^0, (a^2)^1, (a^2)^2, (a^2)^3, (a^2)^4, (a^2)^5\}$

* By FTCG, this is the only subgroup order 6, and it's cyclic. So any elt. of order 6 must be a generator of this group.

$|(a^2)^k| = 6 \Leftrightarrow \gcd(6, k) = 1$. So there are 2 elts order 6 in $\langle a \rangle$.

Q : How many elts of order 4 are there in $\langle a \rangle$?

Note: $|a^3| = 4$

$$\{(a^3)^0, (a^3)^1, (a^3)^2, (a^3)^3\}$$

* By FTCG, this is the only subgroup order 4, and it's cyclic. So any elt. of order 4 must be a generator of this group.

$|(a^3)^k| = 4 \iff \gcd(4,k) = 1$. So there are 2 elts order 4 in $\langle a \rangle$.

Q : How many elts of order 3 are there in $\langle a \rangle$?

Note: $|a^4| = 3$

$$\{(a^4)^0, (a^4)^1, (a^4)^2\}$$

* By FTCG, this is the only subgroup order 3, and it's cyclic. So any elt. of order 3 must be a generator of this group.

$|(a^4)^k| = 3 \iff \gcd(3,k) = 1$. So there are 2 elts order 3 in $\langle a \rangle$.

Q : How many elts of order 2 are there in $\langle a \rangle$?

Note: $|a^6| = 2$

$\{ (a^6)^0, (a^6)^1 \}$

* By FTCG, this is the only subgroup order 2, and it's cyclic. So any elt. of order 2 must be a generator of this group.

$|(a^6)^k| = 2 \iff \gcd(2,k) = 1$, So there is 1 elt order 2 in $\langle a \rangle$.

Q : How many elts of order 1 are there in $\langle a \rangle$?

One : a^0, the identity.

φ

Defn The Euler phi function

$$\varphi : \{\text{pos. integers}\} \longrightarrow \{\text{pos. integers}\}$$

given by

$$\varphi(1) = 1 \quad \text{and}$$

for $d > 1$, $\quad \varphi(d) =$ number positive integers $m < d$ s.t.

$$\gcd(m, d) = 1$$

Thm Sps G cyclic of order n. Sps $d \mid n$. The number of elts of order d in G is $\varphi(d)$.

Ex. Number of elements of order 5 in $\mathbb{Z}_{30}$? In $\mathbb{Z}_{25}$? in $\mathbb{Z}_{17}$?

In $\mathbb{Z}_{30}$, it's $\varphi(5) = 4$.

In $\mathbb{Z}_{25}$, it's $\varphi(5) = 4$.

In $\mathbb{Z}_{17}$, it's 0 b/c $5 \nmid 17$.

proof: By FTCG, G has exactly one subgroup of order d, and it is cyclic. Sps $H = \langle b \rangle$. Then b is an elt. order d and any other elt. of order d must also generate H, since H is the only subgroup order d.

But $\langle b \rangle = \langle b^k \rangle \Leftrightarrow \gcd(d,k) = 1$, so number of elements of order d is $\varphi(d)$.