Lagrange's Theorem.

Binary relation $E(x,y)$ on G.

$E(x,y) = x^{-1} * y \in H$.

Motivation

for $x = y \Rightarrow \frac{y}{x} = 1 \Rightarrow \frac{1}{x} * y = \underset{\varepsilon}{\underbrace{1}}$

Reflexivity

$E(x,x) = x^{-1} * x = \varepsilon \in H$.

Symmetry.

$E(x,y) \Rightarrow E(y,x)$

$x^{-1} * y = h \Rightarrow y^{-1} * x \in H$.

$(y^{-1} * x)^{-1} = x^{-1} * y$

Transitivity.

$E(x,y) \wedge E(y,z) \Rightarrow E(x,z)$.

$x^{-1} * y = h_1 \quad y^{-1} * z = h_2 \quad x^{-1} * z \in H$

$x^{-1} * z = \underline{x^{-1}} * y * y^{-1} * \underline{z} = h_1 * h_2 \in H$.

Claim: $(a * b)^{-1} = a^{-1} * b^{-1}$

Proof:

$(a * b)^{-1} = y$

$(a * b) * y = \varepsilon$.

$(a * b) * (a^{-1} * b^{-1}) = \varepsilon$

$a * a^{-1} * b * b^{-1}$

$= \varepsilon * b * b^{-1}$

$= b * b^{-1}$

$= \varepsilon$.

Any equivalence relation generate partitions.

Order of an element a is the smallest integer k such that

$a^k = \varepsilon$.

Example $2^{20} \pmod{15}$.

$G = 0, 1, 2, \cdots 13, 14$.

WT Find $2^k = \varepsilon$ $\Leftarrow$ such k would exist. & k should divide 15.

either $k = 3, 5, 15$.

$2^3 = 8 \equiv 8 \pmod{15}$

$2^5 = 32 \equiv 2 \pmod{15}$

Such that

$2^{15} \equiv \underset{\varepsilon.}{1} \pmod{15}$

$2^{20} = 2^{15} \cdot 2^5 = 1 \cdot 2 \pmod{15} = 2 \pmod{15}$

Given finite group G of order $|G| = n$.

for any a of G, if such order k exist, this k divides n.

$\Downarrow$

$\{\varepsilon, a, a^2, a^3 \cdots a^k\}$. $\quad k \mid n$.

Take a cyclic group generated by a

$\{a^m \mid m \in \mathbb{Z}\} = \{\varepsilon, a, a^2, a^3 \cdots a^k\}$