/ /

UFRS - Universidade Federal do Rio de Janeiro

Rio de Janeiro, 11 de Maio de 2017

TEOREMA: Se m e n são inteiros positivos tais que $MDC(m,n) = 1$, então

$$\phi_{(mn)} = \phi_{(m)} \cdot \phi_{(n)}$$

Para provar este teorema preciso de um lema auxiliar.

LEMA: Seja $\bar{x} \in \mathbb{Z}_{mn}$ tal que $x \equiv a \pmod m$ e $x \equiv b \pmod n$. Então, $\bar{x} \in U_{(mn)}$ se e somente se $\bar{a} \in U_{(m)}$ e $\bar{b} \in U_{(n)}$

DEMONSTRAÇÃO:

($\Rightarrow$) Se $\bar{a} \in U_{(m)}$, existe a^{-1} tal que $a \cdot a^{-1} \equiv 1 \pmod m$. Se $\bar{b} \in U_{(n)}$, existe b^{-1} tal que $b \cdot b^{-1} \equiv 1 \pmod n$

Monto e resolvo o seguinte sistema:

$$\begin{cases} y \equiv a^{-1} \pmod m \\ y \equiv b^{-1} \pmod n \end{cases}$$

Como $MDC(m,n) = 1$, esse sistema tem solução.

Vamos mostrar que a solução y é o inverso de x módulo mn.

$xy \equiv a \cdot a^{-1} \equiv 1 \pmod m$

↳ m divide $xy - 1$

$xy \equiv b \cdot b^{-1} \equiv 1 \pmod n$

↳ n divide $xy - 1$

m divide $xy-1$
n divide $xy-1$
$MDC(m,n)=1$

$\Rightarrow$ mn divide xy^{-1}

$\Downarrow$

$xy \equiv 1 \pmod{mn}$

$\Downarrow$

y é o inverso de x

$\Downarrow$

$\bar{x} \in U(mn)$

($\Downarrow$) Seja x^{-1} o inverso de x módulo mn.

Suponha que $x^{-1} \equiv c \pmod{m}$ e $x^{-1} \equiv d \pmod{n}$

Vamos mostrar que c é o inverso de a módulo m e d é o inverso de b módulo n.

$a \cdot c \equiv x \cdot x^{-1} \equiv 1 \pmod{m}$ $\rightarrow \bar{a} \in U(m)$

Sei que $x \cdot x^{-1} \equiv 1 \pmod{mn}$

$\Downarrow$

mn divide $xx^{-1}-1$

mn divide $xx^{-1}-1$
m divide mn

$\Rightarrow$ m divide $xx^{-1}-1$

$\Downarrow$

$xx^{-1} \equiv 1 \pmod{m}$

Analogamente, $x \cdot x^{-1} \equiv 1 \pmod{n}$

b·d ≡ x·x⁻¹ ≡ 1 (mod n)

⇓

$\bar{b} \in U(n)$

Vamos agora demonstrar o teorema.

Pelo lema, cada elemento de $\mathbb{Z}_{mn}$ que tem inverso é congruente a um elemento de U(n) módulo m e a um elemento de U(n) módulo n.

Mas existem $\phi(m)$ elementos em U(m) e $\phi(n)$ elementos de em U(n).

Logo, a quantidade de elementos de $\mathbb{Z}_{mn}$ que tem inverso é o produto dessas duas quantidades:

$$\phi(mn) = \phi(m) \cdot \phi(n)$$

- SUBGRUPOS:

DEFINIÇÃO: Seja $(G, *)$ um grupo. Dizemos que $(H, *)$ é um subgrupo de $(G, *)$ se as seguintes propriedades são satisfeitas:

SUBGRUPO { (1) H é um subconjunto de G.

GRUPO {
(2) O Elemento Neutro de G pertence a H.

(3) Se $h_1, h_2 \in H$, então $h_1 * h_2 \in H$

(4) Se $h \in H$, então existe $h^{-1} \in H$ tal que $h * h^{-1} = e$.

↳ Elemento Neutro

/ /

- TEOREMA DE LAGRANGE:

Seja $(G, *)$ um grupo finito e $(H, *)$ um subgrupo de $(G, *)$. Então, a ordem de $(H, *)$ divide a ordem de $(G, *)$.

- EXEMPLO DE APLICAÇÃO:

$G = U(8) = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$

$H = \{\bar{1}, \bar{5}, \bar{7}\}$

(H, x) não pode ser subgrupo de (G, x) porque 3 não divide 4.

E $H_2 = \{\bar{1}, \bar{3}\}$? é subgrupo ?

2 divide 4. Então pode ser subgrupo. Preciso testar:

(1) $H_2 \subset G$ OK

(2) $\bar{1} \in H_2$ OK

(3) $\bar{1} \cdot \bar{1} = \bar{1} \in H_2$

$\bar{1} \cdot \bar{3} = \bar{3} \in H_2$ OK

$\bar{3} \cdot \bar{1} = \bar{3} \in H_2$

$\bar{3} \cdot \bar{3} = \bar{9} = 1 \in H_2$

(4) Inverso de $\bar{1}$ é $\bar{1} \in H_2$

Inverso de $\bar{3}$ é $\bar{3} \in H_2$ OK

Sim, H_2 é subgrupo.

/ /

E $H_3 = \{\bar{3}, \bar{5}\}$?

Não satizfaz a propriedade (2). Não é subgrupo.

E $H_4 = \{\bar{1}, \bar{5}\}$?

(1) $H_4 \subset G$ OK

(2) $\bar{1} \in H_4$ OK

(3) $\bar{1}\cdot\bar{1} = \bar{1} \in H_4$

$\bar{1}\cdot\bar{5} = \bar{5} \in H_4$ OK

$\bar{5}\cdot\bar{1} = \bar{5} \in H_4$

$\bar{5}\cdot\bar{5} = \overline{25} = \bar{1} \in H_4$

(4) O inverso de $\bar{1}$ é $\bar{1}$.

O inverso de $\bar{5}$ é $\bar{5}$. OK

Sim, H_4 é subgrupo.

OUTRO EXEMPLO:

$G = U(16) = \underbrace{\{\bar{1}, \bar{3}, \bar{5}, \bar{7}, \bar{9}, \bar{11}, \bar{13}, \bar{15}\}}_{\text{ORDEM } 8}$

$\phi(16) = \phi(2^4) = 2^3(2-1) = 8$

Possíveis Ordens para Subgrupos de $U(16)$?

- 1
- 2
- 4
- 8

⇓

Divisores de 8 (Lagrange)

Possíveis subgrupos de ordem 1

$\{\bar{1}\}$

Possíveis Subgrupos de ordem 8.

$U(16)$

Observação: Se um grupo tem ordem K, ele sempre tem um único subgrupo de ordem 1 e um único subgrupo de ordem K.

⇓

Definição: Seja $(G,*)$ um grupo de ordem K e $(H,*)$ um subgrupo de $(G,*)$. Dizemos que $(H,*)$ é um subgrupo próprio se a sua ordem é diferente de 1 e K.

- Grupos e Subgrupos Cíclicos

Seja $(G,*)$ um grupo finito. Seja $a \in G$.

$H = \{e, a, a^2, a^3 \dots\}$ → Conjunto das potências de a.

↳ Elemento neutro

$a^0 = e$

$a^K = \underbrace{a * a * \dots * a}_{K \text{ vezes}}$

11

Existem a princípio, infinitas potências de a, então H é aparentemente um conjunto infinito.

Mas G é um conjunto finito e $H \subset G$. Logo, H precisa ser finito.

Isso significa que vão existir expoentes $m \neq n$ tais que

$$a^m = a^n.$$

Suponha que $m > n$.

$$a^m = a^n$$

$$a^m * (a^{-1})^n = a^m * (a^{-1})^n = e$$

$$a^{m-n} = e$$

⇓

Vai existir uma potência a^k tal que $a^k = e$.

$$H = \underbrace{\{e, a, a^2, a^3, \ldots, a^{k-1}\}}_{k \text{ elementos}}$$

Seja $(G,*)$ um grupo e $a \in G$. Definimos a ordem de a como o menor inteiro positivo k, tal que $a^k = e$ em G.

$(H,*)$ é um subgrupo de $(G,*)$

(1) $H \subset G$ OK

(2) $e \in H$ OK

/ /

(3) A operação entre duas potências de a resulta em uma potência de a, logo, pertence a H.

(4) Seja K a ordem de a

a^{K-i} é o inverso de a^i

$a^{K-i} * a^i = a^K = e$.

$(H, *)$ é chamado de subgrupo cíclico gerado por a.

a é chamado de gerador do subgrupo $(H, *)$

Se a tem ordem K, o subgrupo cíclico gerado por a também tem ordem K.

$$H = \underbrace{\{e, a, a^2, a^3, \dots, a^{K-1}\}}_{K \text{ elementos}}$$

Qualquer grupo que admite um gerador, ou seja, que pode ser escrito como potências de um dado elemento é chamado de grupo cíclico.

EXEMPLO: Vamos calcular todos os subgrupos cíclicos de $U(16) = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}, \bar{9}, \bar{11}, \bar{13}, \bar{15}\}$

$\bar{1}^1 = \bar{1}$	$\bar{3}^1 = \bar{3}$	$\bar{5}^1 = \bar{5}$	$\bar{7}^1 = \bar{7}$
$H_1 = \{\bar{1}\}$	$\bar{3}^2 = \bar{9}$	$\bar{5}^2 = \overline{25} = \bar{9}$	$\bar{7}^2 = \overline{49} = \bar{1}$
	$\bar{3}^3 = \overline{27} = \overline{11}$	$\bar{5}^3 = \overline{45} = \overline{13}$	$H_7 = \{\bar{1}, \bar{7}\}$
	$\bar{3}^4 = \overline{33} = \bar{1}$	$\bar{5}^4 = \overline{65} = \bar{1}$	
	$H_3 = \{\bar{1}, \bar{3}, \bar{9}, \overline{11}\}$	$H_5 = \{\bar{1}, \bar{5}, \bar{9}, \overline{13}\}$	

/ /

$\overline{9}^1 = \overline{9}$	$\overline{11}^1 = \overline{11}$	$\overline{13}^1 = \overline{13}$	$\overline{15}^1 = \overline{15}$
$\overline{9}^2 = \overline{81} = \overline{1}$	$\overline{11}^2 = \overline{121} = \overline{9}$	$\overline{13}^2 = \overline{169} = \overline{9}$	$\overline{15}^2 = \overline{1}$
$H_9 = \{\overline{1}, \overline{9}\}$	$\overline{11}^3 = \overline{99} = \overline{8}$	$\overline{13}^3 = \overline{117} = \overline{5}$	$H_{15} = \{\overline{1}, \overline{15}\}$
	$\overline{11}^4 = \overline{33} = \overline{1}$	$\overline{13}^4 = \overline{65} = \overline{1}$	
	$H_{\overline{11}} = \{\overline{1}, \overline{3}, \overline{9}, \overline{11}\} =$	$H_{13} = \{\overline{1}, \overline{5}, \overline{9}, \overline{13}\} =$	
	$= H_3$	$= H_5$	

$U(16)$ não é cíclico.