

UFRJ - Universidade Federal do Rio de Janeiro

Rio de Janeiro, 11 de Maio de 2017

TEOREMA: Se  $m$  e  $n$  são inteiros positivos tais que  $\text{MDC}(m, n) = 1$ , 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:

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

Monte e resolva o seguinte sistema:

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

Como  $\text{MDC}(m, n) = 1$ , esse sistema tem solução.

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

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

$\hookrightarrow m$  divide  $xy - 1$

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

$\hookrightarrow n$  divide  $xy - 1$

(a,b) = 1  $\Rightarrow$   $a \cdot x + b \cdot y = 1$

$$\left. \begin{array}{l} m \text{ divide } xy-1 \\ n \text{ divide } xy-1 \\ \text{MDC}(m,n)=1 \end{array} \right\} \begin{array}{l} mn \text{ divide } xy-1 \\ \Downarrow \\ xy \equiv 1 \pmod{mn} \end{array}$$

$\Downarrow$

$y$  é o inverso de  $x$

$\Downarrow$

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

(↓) 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  $n$ .

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

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

$\Downarrow$

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

$$\left. \begin{array}{l} mn \text{ divide } xx^{-1} - 1 \\ m \text{ divide } mn \end{array} \right\} \begin{array}{l} m \text{ divide } xx^{-1} - 1 \\ \Downarrow \\ xx^{-1} \equiv 1 \pmod{m} \end{array}$$

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

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

$\Downarrow$

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

$$\Downarrow \quad m \mid nm \quad \bar{b} \equiv \bar{y} \pmod{m}$$

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  $U(m)$  módulo  $n$ .

Mas existem  $\phi(m)$  elementos em  $U(m)$  e  $\phi(n)$  elementos de  $U(n)$ . (4)

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  $G$ .

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

Grupo { (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  $h * h^{-1} = e$ .

$\rightarrow$  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:

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

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

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

E  $H_2 = \{1, 3\}$ ? é subgrupo?

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

(1)  $H_2 \subseteq G$  OK

(2)  $1 \in H_2$  OK

(3)  $1 \cdot 1 = 1 \in H_2$

$1 \cdot 3 = 3 \in H_2$  OK

$3 \cdot 1 = 3 \in H_2$

$3 \cdot 3 = 9 = 1 \in H_2$

(4) Inverso de 1 é 1  $\in H_2$

Inverso de 3 é 3  $\in H_2$  OK

Sim,  $H_2$  é subgrupo.



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

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

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

$$(1) H_4 \subset G \quad \text{OK}$$

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

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

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

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

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

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

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

Sim,  $H_4$  é subgrupo.

OUTRO EXEMPLO:

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

ordem 8

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

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

$\left\{ \begin{array}{l} 1 \\ 2 \\ 4 \\ 8 \end{array} \right.$

$\Downarrow$

Divisores de 8  
(LAGRANGE)

Possíveis subgrupos de ordem 1

$\{1\}$

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  $a \in G$ .

$H = \{e, a, a^2, a^3, \dots\} \rightarrow$  Conjunto das potências de  $a$ .  
 $\hookrightarrow$  Elemento neutro

$$a^0 = e$$

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



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

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

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

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

Suponha que  $m > n$ .

$$a^m = a^n$$

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

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

$\Downarrow$

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

$$H = \{e, a, a^2, a^3, \dots, a^{k-1}\}$$

$k$  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)  $H \subseteq G$  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  $a$

$a^{K-1}$  é o inverso de  $a$

$$a^{K-1} * a = a^K = e.$$

$(H, *)$  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  $U(16) = \{1, 3, 5, 7, 9, 11, 13, 15\}$

$1^1 = 1$	$3^1 = 3$	$5^1 = 5$	$7^1 = 7$
$H_1 = \{1\}$	$3^2 = 9$	$5^2 = 25 = 9$	$7^2 = 49 = 1$
	$3^3 = 27 = 11$	$5^3 = 125 = 13$	$H_7 = \{1, 7\}$
	$3^4 = 81 = 1$	$5^4 = 625 = 1$	
	$H_3 = \{1, 3, 9, 11\}$	$H_5 = \{1, 5, 9, 13\}$	



111

$$\bar{q}^1 = \bar{q}$$

$$\bar{q}^2 = \bar{q}1 = 1$$

$$H_9 = \{1, \bar{q}\}$$

$$\bar{1}1^1 = \bar{1}1$$

$$\bar{1}1^2 = \bar{1}21 = \bar{q}$$

$$\bar{1}1^3 = \bar{q}q = \bar{q}$$

$$\bar{1}1^4 = \bar{q}3 = 1$$

$$H_{11} = \{1, \bar{q}, \bar{q}, \bar{1}1\} = H_3$$

$$\bar{1}3^1 = \bar{1}3$$

$$\bar{1}3^2 = \bar{1}6q = \bar{q}$$

$$\bar{1}3^3 = \bar{1}11 = 5$$

$$\bar{1}3^4 = \bar{q} = 1$$

$$H_{13} = \{1, 5, \bar{q}, \bar{1}3\} = H_6$$

$$\bar{1}5^1 = \bar{1}5$$

$$\bar{1}5^2 = 1$$

$$H_{15} = \{1, \bar{1}5\}$$

$U(16)$  não é cíclico.

$$\left\{ \begin{matrix} 1 & 5 & 9 & 13 & 17 & 21 & 25 & 29 & 33 & 37 & 41 & 45 & 49 & 53 & 57 & 61 & 65 & 69 & 73 & 77 & 81 & 85 & 89 & 93 & 97 & 101 & 105 & 109 & 113 & 117 & 121 & 125 & 129 & 133 & 137 & 141 & 145 & 149 & 153 & 157 & 161 & 165 & 169 & 173 & 177 & 181 & 185 & 189 & 193 & 197 & 201 & 205 & 209 & 213 & 217 & 221 & 225 & 229 & 233 & 237 & 241 & 245 & 249 & 253 & 257 & 261 & 265 & 269 & 273 & 277 & 281 & 285 & 289 & 293 & 297 & 301 & 305 & 309 & 313 & 317 & 321 & 325 & 329 & 333 & 337 & 341 & 345 & 349 & 353 & 357 & 361 & 365 & 369 & 373 & 377 & 381 & 385 & 389 & 393 & 397 & 401 & 405 & 409 & 413 & 417 & 421 & 425 & 429 & 433 & 437 & 441 & 445 & 449 & 453 & 457 & 461 & 465 & 469 & 473 & 477 & 481 & 485 & 489 & 493 & 497 & 501 & 505 & 509 & 513 & 517 & 521 & 525 & 529 & 533 & 537 & 541 & 545 & 549 & 553 & 557 & 561 & 565 & 569 & 573 & 577 & 581 & 585 & 589 & 593 & 597 & 601 & 605 & 609 & 613 & 617 & 621 & 625 & 629 & 633 & 637 & 641 & 645 & 649 & 653 & 657 & 661 & 665 & 669 & 673 & 677 & 681 & 685 & 689 & 693 & 697 & 701 & 705 & 709 & 713 & 717 & 721 & 725 & 729 & 733 & 737 & 741 & 745 & 749 & 753 & 757 & 761 & 765 & 769 & 773 & 777 & 781 & 785 & 789 & 793 & 797 & 801 & 805 & 809 & 813 & 817 & 821 & 825 & 829 & 833 & 837 & 841 & 845 & 849 & 853 & 857 & 861 & 865 & 869 & 873 & 877 & 881 & 885 & 889 & 893 & 897 & 901 & 905 & 909 & 913 & 917 & 921 & 925 & 929 & 933 & 937 & 941 & 945 & 949 & 953 & 957 & 961 & 965 & 969 & 973 & 977 & 981 & 985 & 989 & 993 & 997 \end{matrix} \right\} = H$$

$$\{1, \bar{q}, \bar{q}, \bar{1}1\} = H_3$$

$$\bar{q} = \bar{q}$$

$$\bar{q} = \bar{q}$$

$$\bar{q} = \bar{q}$$

$$\bar{q} = \bar{q}$$

$$\bar{q} = \bar{q}$$

$$\bar{q} = \bar{q}$$

$$\bar{q} = \bar{q}$$

$$\bar{q} = \bar{q}$$

$$\bar{q} = \bar{q}$$

$$\bar{q} = \bar{q}$$

$$\bar{q} = \bar{q}$$

$$\bar{q} = \bar{q}$$

$$\bar{q} = \bar{q}$$

$$\{1, \bar{q}, \bar{q}, \bar{1}1\} = H_3$$

$$\{1, \bar{q}, \bar{q}, \bar{1}1\} = H_3$$