UFRS - Universidade Federal do Rio de Janeiro

Rio de Janeiro, 18 de Maio de 2017

- SUBGRUPOS CÍCLICOS

$U(20) = \{\bar{1}, \bar{3}, \bar{7}, \bar{9}, \overline{11}, \overline{13}, \overline{17}, \overline{19}\}$

$\phi(20) = \phi(2^2 \cdot 5) = \phi(2^2) \cdot \phi(5) = 2 \cdot (2-1) \cdot (5-1) = 2 \cdot 4 = 8$

$\bar{1}^1 = 1$	$\bar{3}^1 = \bar{3}$	$\bar{7}^1 = \bar{7}$	$\bar{9}^1 = \bar{9}$	$\overline{11}^1 = \overline{11}$
$H_1 = \{\bar{1}\}$	$\bar{3}^2 = \bar{9}$	$7^2 = \overline{49} = \bar{9}$	$\bar{9}^2 = \overline{81} = \bar{1}$	$\overline{11}^2 = \overline{121} = \bar{1}$
	$\bar{3}^3 = \bar{7}$	$7^3 = \overline{63} = \bar{3}$	$H_9 = \{\bar{1}, \bar{9}\}$	$H_{11} = \{\bar{1}, \overline{11}\}$
	$3^4 = \bar{1}$	$7^4 = \overline{21} = \bar{1}$		
	$H_3 = \{\bar{1}, \bar{3}, \bar{7}, \bar{9}\}$	$H_7 = \{\bar{1}, \bar{3}, \bar{7}, \bar{9}\}$		
		$H_7 = H_3$		

$\overline{13}^1 = \overline{13}$	$\overline{17}^1 = \overline{17}$	$\overline{19}^1 = \overline{19}$
$\overline{13}^2 = \overline{169} = \bar{9}$	$\overline{17}^2 = \overline{289} = \bar{9}$	$\overline{19}^2 = \overline{361} = \bar{1}$
$\overline{13}^3 = \overline{117} = \overline{17}$	$17^3 = \overline{153} = \overline{13}$	$H_{19} = \{\bar{1}, \overline{19}\}$
$\overline{13}^4 = \overline{221} = \bar{1}$	$17^4 = \overline{221} = \bar{1}$	
$H_{13} = \{\bar{1}, \bar{9}, \overline{13}, \overline{17}\}$	$H_{17} = \{\bar{1}, \bar{9}, \overline{13}, \overline{17}\}$	
	$H_{17} = H_{13}$	

- TEOREMA DE EULER:

Sejam a e n inteiros positivos tais que $n \geq 2$ e $MDC(a,n) = 1$. Então,

$$a^{\phi(n)} \equiv 1 \pmod n$$

OBSERVAÇÃO: Este teorema é uma generalização do teorema de Fermat, pois, se n é primo, $\phi(n) = n-1$.

/ /

Se $MDC(a,n)=1$, então $\bar{a} \in U(n)$

$\phi(n)$ é a ordem de $U(n)$.

Seja k a ordem de $\bar{a}$.

$$a^k \equiv 1 \pmod{n}$$

$\bar{a}$ é o gerador de um subgrupo cíclico de ordem k de $U(n)$.

Pelo teorema de Lagrange, a ordem de qualquer subgrupo deve dividir a ordem do grupo.

$$\Downarrow$$

k divide $\phi(n)$

$$\Downarrow$$

$$\phi(n) = k \cdot t$$

$$a^{\phi(n)} \equiv a^{k \cdot t} \equiv (a^k)^t \equiv 1^t \equiv 1 \pmod{n}.$$

LEMA-CHAVE: Seja $(G,*)$ um grupo e $a \in G$. Então, $a^t = e$ se e somente se a ordem de a divide t.

($\Downarrow$) Seja k a ordem de a.

$$a^k = e$$

Vamos dividir t por k:

$$t = kq + r \qquad 0 \leq r < k$$

$$e = a^t = a^{kq+r} = \underbrace{(a^k)^q}_{e} * a^r = a^r$$

$a^r = e$

Como k é a ordem de a, k é o menor inteiro positivo tal que $a^k = e$.

$$\left.\begin{array}{l} a^r = e \\ r < k \end{array}\right\} \quad r = 0$$

$$\Downarrow$$

k divide t

($\Uparrow$) Suponha que k divide t.

$t = k t'$

$$a^t = a^{kt'} = \underbrace{(a^k)}_{=\,e}{}^{t'} = e^{t'} = e.$$

-TEOREMA DE LAGRANGE:

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

NOTAÇÃO: $|G|$ = ordem de $(G, *)$

$|H|$ = ordem de $(H, *)$

-DEMONSTRAÇÃO:

No caso em que $|H| = |G|$, o teorema é verdadeiro. Suponha então que $|H| < |G|$. Então, existe pelo menos um elemento g_1 no conjunto $G - H$.

Vamos denotar os elementos de H como:

/ /

$H = \{h_1, h_2, h_3, \dots, h_t\}$
$(t = |H|)$

Vamos construir o conjunto $g_1 H$ como:

$$g_1 H = \{g_1 * h_1, g_1 * h_2, g_1 * h_3, \dots, g_1 * h_t\}$$

Se $i \neq j$, então:

$$g_1 * h_i \neq g_1 * h_j. \rightarrow *$$

Suponha, por construção, que $i \neq j$ e $g_1 * h_i = g_1 * h_j$.

Operando os dois lados com o inverso de g_1 (g_1^{-1}), obtenho:

$$\underbrace{g_1^{-1} * g_1}_{e} * h_i = \underbrace{g_1^{-1} * g_1}_{e} * h_j$$

$$e * h_i = e * h_j$$

$$h_i = h_j \rightarrow **$$

$(*) + (**) \Rightarrow$ CONTRADIÇÃO

Logo, todos os elementos de $g_1 H$ são distintos entre si. Então,

$$|g_1 H| = |H|$$

Vamos considerar

$$H \cup g_1 H$$

Se $H \cup g_1 H = G$, eu paro a construção.

Se não, existe pelo menos um elemento $g_2 \in G - (H \cup g_1 H)$. Construo,

$$g_2 H = \{g_2 * h_1, g_2 * h_2, g_2 * h_3, g_2 * h_4\}.$$

$$|g_2 H| = |H|$$

Considero,

$$H \cup g_1 H \cup g_2 H$$

Se $H \cup g_1 H \cup g_2 H = G$, eu paro a construção.

Se não existe $g_3 \in G - (H \cup g_1 H \cup g_2 H)$

Construo $g_3 H \ldots$

Continuo este processo até obter

$$G = H \cup g_1 H \cup g_2 H \cup g_3 H \cup \ldots \cup g_s H.$$

$$|G| = |H \cup g_1 H \cup g_2 H \cup g_3 H \cup \ldots \cup g_s H|$$

[Se os conjuntos $H, g_1 H, g_2 H, \ldots, g_s H$ forem disjuntos entre si] obtenho.

$$|G| = |H \cup g_1 H \cup \ldots \cup g_s H| = |H| + \underbrace{|g_1 H|}_{|H|} + \ldots + \underbrace{|g_s H|}_{|H|} = (s+1)|H|$$

$|G| = (s+1)|H| \Rightarrow |H|$ divide $|G|$, que é o que eu queria demonstrar.

Falta apenas mostrar que estes conjuntos são realmente disjuntos entre si.

Para uniformizar a notação, vamos denotar $g_0 = e$ e escrever H como g_0H.

Suponha, por contradição, que existe um elemento que pertence a g_iH e g_jH, com $j > i$.

Se o elemento pertence a g_iH, ele pode ser escrito como $g_i * h_m$. Se o elemento pertence a g_jH, ele pode ser escrito como $g_j * h_n$.

$$g_i * h_m = g_j * h_n$$

$$g_i * h_m * h_n^{-1} = g_j * \underbrace{h_n * h_n^{-1}}_{e} = g_j$$

$$g_j = g_i * \underbrace{h_m * h_n^{-1}}$$

$$h_n \in H \Rightarrow h_n^{-1} \in H$$

$$\left.\begin{array}{l} h_m \in H \\ + \\ h_n^{-1} \in H \end{array}\right\} h_m * h_n^{-1} \in H$$

$$\Downarrow$$

$$h_m * h_n^{-1} = h_e$$

$$g_j = g_i * h_e$$

$$\Downarrow$$

$$g_j \in g_iH$$

Mas, como $j > i$, g_j, pela construção, deveria ser um elemento fora de

$$H \cup g_1H \cup g_2H \cup \dots \cup g_iH \cup \dots \cup g_{j-1}H$$

Contradição.

tilibra

PROPOSIÇÃO: Seja $(G, *)$ um grupo finito de ordem t e $a \in G$. Então, a ordem de a divide t. Seja K a ordem de a. a gera um subgrupo de $(G, *)$ de ordem K. Pelo teorema de Lagrange, a ordem do subgrupo deve dividir a ordem do grupo, logo K divide t.

PROPOSIÇÃO: Seja $(G, *)$ um grupo finito de ordem t e $a \in G$. Então, $a^t = e$ em $(G, *)$. Seja K a ordem de a. Vimos na proposição anterior que K divide t. Logo, pelo LEMA-CHAVE, como a ordem de a divide o expoente t, então $a^t = e$.

TEOREMA: Seja $(G, *)$ um grupo finito cíclico de ordem t e g um gerador do grupo então, g^m também é um gerador do grupo se e somente se $MDC(m, t) = 1$.

$(\uparrow)$ Suponha que $MDC(m, t) = 1$. Seja K a ordem de g^m. Quero mostrar que $K = t$.

$$(g^m)^K = e$$

$$g^{mK} = e$$

Como g é gerador, a ordem de g é t.

Pelo lema-chave, como $g^{mK} = e$, então a ordem de g divide o expoente mK, t divide mK.

$$\left.\begin{array}{l} t \text{ divide } mK \\ \\ MDC(m, t) = 1 \end{array}\right\} t \text{ divide } K \rightarrow *$$

K é ordem de g^m. t é ordem do grupo. Pela preposição anterior, K divide $t \rightarrow **$

/ /

$(*) + (**) \Rightarrow k = t.$

($\Downarrow$) Suponha que $d = MDC(m,t)$ e $d > 1$.

$m = d \cdot m'$

$t = d \cdot t'$

Seja k a ordem de g^m

$(g^m)^k = e.$

$g^{mk} = e.$

$g^t = e.$

t é ordem de g. Como $g^{mk} = e$, pelo lema-chave, t divide mk.

$g^m = g^{d \cdot m'}$

$(g^m)^{t'} = (g^{d \cdot m'})^{t'} = g^{dm't'} = g^{dt'm'} = g^{tm'} = (\underbrace{g^t}_{e})^{m'} = e^{m'} = e$

$(g^m)^{t'} = e.$

Pelo lema-chave, a ordem de g^m (k) divide t'.

k divide t'.

Mas, como $d > 1$, $t' < t$, logo, $k < t$ e g^m não é gerador.