Aio de Sanciro, 18 de Maio de 2017

- SUBGRUPOS CÍCLICOS

$$U(20) = \{ \overline{1}, \overline{3}, \overline{4}, \overline{9}, \overline{11}, \overline{13}, \overline{14}, \overline{19} \}$$

$$\emptyset$$
 (20) =  $\emptyset$ (22.5) =  $\emptyset$ (22).  $\emptyset$ (5) =  $2 \cdot (2-1) \cdot (5-1) = 2 \cdot 4=8$ 

i <sup>a</sup> :1	ā1 = ā	71 = 7	q 1 : q	11 = 11
41 = {4}	32 = 9	72 = 49 = 9	92=81=1	112 = 121 = 7
	3 = 7	$4^3 = 63 = 3$	Hq = { 7, 9}	HM = {1, 11}
	34 = 1	74 = 27 = 1	$\downarrow$	
	H3 = {1 3 7 4}	H== {1,3,7,9}	36, 4 6 1	
		H4 = H3	1	

13 = 13	17' = 17	19 = 19
132 = 169 = 9	11 = 294 = 9	192 = 361 = 1
133 = 117 = 17	173 = 153 = 13	H19= { 1, 19} - 120 - 120 - 100
134 = 221 = 1	174 = 221 = 1	,
	H17 = { T , 9, 13, 17}	1 5 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1
	H47 = H43	de la directo to

- TEOREMA DE GULER

Sejam a en inteiros positivos tais que n > 2 e HDC(a,n) = 1. Então,

aden) = 1 (mod n)

primo, (n) = n-1

Scja K a ordem de Um).  Scja K a ordem de ā.  a <sup>K</sup> = 1 (moda)  ā é o gerador de um subgrupo ciclico de ordem K de Um).  Polo teoremo de Lagrange, a ordem de qualquer subgrupo deve dividir a rivem do grupo.  X divide d'on)  A divide d'on)  Scia K e = (a <sup>C</sup> ) = 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1	se inc (a,n) 2 1	então a e U		*1c	S sa oleft	16 10 ,0	Part Sand
Seja K a ordern de a.  a <sup>K</sup> = 1 (modn)  ā é o gerador de um subgrupo ciclico de ordern K de Ucn).  Polo teorema de hagrange, a ordern de qualquer subgrupo deve dividir a rdern do grupo.  K divide d'an)  Ø(n)= K t  a <sup>6(n)</sup> = a <sup>K t</sup> = (a <sup>K)</sup> = q <sup>t</sup> = q émod h).  MAN - CHIVE: Seja (6, X) um grupo e a E G. Entaïo, a = 2 se e somente se a e a divide t.  Vamos dividir t por K:  t= Kqtr  02 r 4 K	d'int é a orde	em de U(n).				41.754	
at = 1 (mod n)  ā é o gerador de um subgrupo ciclico de ordem K de Ucn).  Pelo teorema de hagrange, a ordem de qualquer subgrupo deve dividir a rdem do grupo  K divide d'en)  O(m)= x·t  O(m)= x·t  Alini = ak·t = (ax) = = 1 timod n).  EMA-CHNVE: Seja (6, x) um grupo e a = 5. Entas, at = a se e somente se a e a divide t.  U) Seja x a ordem de a.  Ax = 2  Vanus dividir t por x:  t= Katr Otrok						703.057	ACCEPTAGE
E é o gerador de um subgrupo cicliero de ordem K de Ucn).  Polo teorema de Lagrange, a ordem de qualquer subgrupo deve dividir a ndem do grupo.  K divide d'un)  O(n)= K. t  adini = a K. t = (ax) = 4 = 4 tmod ti).  EMA-CHAVE: Seja (6, x) um grupo e a e G. Entañ, a = 2 se e somente se a e a divide t.  U) Seja x a ordem de a.  Vamos dividir t por x:  t = Katr OLTCK	Seja K a onle	em de ā.		P) (1)	1,11 P	T. 8. T.	· (as) ()
E é o gerador de um subgrupo cicliero de ordem K de Ucn).  Polo teorema de Lagrange, a ordem de qualquer subgrupo deve dividir a ndem do grupo.  K divide d'en)  O(n)= K. E  Q(n)= K. E  Q(n)= (A) = 4 = 4 (mod h).  EMA-CHNVE: Seja (6, *) um grupo e a e G. Entañ, a = 2 se e somente se a e a divide t.  U) Seja K a ordem de a.  Vamos dividir t por K:  L= Katr OLTCK	ak = 1 (mo	ارمه					- 19
Polo teorema de Lagrange, a ordem de qualquer subgrupo deve dividir a rdem do grupo.  K divide Ocn  K divide Ocn  (a) = x t  (a) = 1 = 1 t mod 1).  (m) = chove: Seja (6, x) um grupo e a e G. Enlag, a = 2 se esomente se a e e a divide t.  U) Seja x a ordem de a.  A = 2  Vamos dividir t por x:  t = Kgtr 0 t r 4 x	8	MA 6 = (4-5)	(K C)	g = (d)	(25) 9 -	(5 2)	= (Q1 N
Polo teorema de Lagrange, a ordem de qualquer subgrupo deve dividir a ndem do grupo.  X divide d'en  (m) = x t  (m) = x t = (ax) t = 1 t = 1 t mod t).  EMA-CHOVE: Seja (6, *) um grupo e a e G. Enlag, a = 2 se e somente se a e e a divide t.  U) Seja x a ordem de a.  Vamos dividir t por x:  t = Katr  0 < r < K	ā é o gerador	de um subgr	igo cícli	co de or	dem K d	U cm).	F-
rdem do grupo.  X divide $\psi$ cm $\psi(n) = x \cdot t$ $\psi$	FF = 11	p : P		F			(-)
Administration of the state of	Pelo teorema	de Lagrange,	a orden	de quali	over subg	upo deve	dividir a
X divide $\phi$ cm $\phi(n) = x \cdot t$ $\phi($		{p, F}= = H	ž:	1-14		T :	
din = x.t = (ax)t = 1t = 1 t mod n).  MA - CHOVE: Soja (6, x) um grupo e a e G. Entañ, at = 2 se e somente se a e e a divide t.  U) Seja x a ordem de a.  Vamos dividir t por x:  t = Katr Otr Lx	3.040	1	Ť -	F5 = "T		7 = 18	
dint = x.t.  adint = ax.t = (ax)t = 1t = 1 t mod n).  EMA-CHIVE: Seja (6, x) um grupo e a e G. Entas, at = 2 se e somente se a e  e a divide t.  V) Seja x a prodem de a.  Varnos dividir t por x:  t = Katr Otrtx		x divide \$	cm	13 = 14	EF F	11-14	
$a^{(kn)} = a^{k \cdot \ell} = (a^k)^{\ell} = 4^{\ell} = 4 \pmod{n}$ . $(Mn - CHNVE)$ : Seja $(G, *)$ um grupo e $a \in G$ . Entaŭ, $a^{\ell} = a$ se esomente se $a$ e a divide $t$ . $(Mn - CHNVE)$ : Seja $(G, *)$ um grupo e $a \in G$ . Entaŭ, $a^{\ell} = a$ se esomente se $a$ e $a$ divide $a$ . $(G, *)$ um grupo e $a \in G$ . Entaŭ, $a^{\ell} = a$ se esomente se $a$ e $a$ divide $a$ . $(G, *)$ um grupo e $a \in G$ . Entaŭ, $a^{\ell} = a$ se esomente se $a$ e $a$ divide $a$ . $(G, *)$ um grupo e $a \in G$ . Entaŭ, $a^{\ell} = a$ se esomente se $a$ e $a$ divide $a$ . $(G, *)$ un grupo e $a \in G$ . Entaŭ, $a^{\ell} = a$ se esomente se $a$ e $a$ divide $a$ esomente se		1.		14 = 14			
adin) = ak. e = (ak) = q = 1 tmod h).  EMA-CHIVE: Soja (G,*) um grupo e a e G. Entaŭ, at = a se e somente so a e e a divide t.  U) Soja x a ardem de a.  Vamos dividir t por x:  t= Kqtr 0 < r < K	·	Oin's Kit	1 51		FI - II		1721
EMA-CHAVE: Seja (6,*) um grupo e a e G. Entaïo, at = a se e somente se a e a divide t.  U) Seja K a ordem de a.  ax = a  Vamos dividir t por x:  t = Kgtr 0 & r < K		Tabut :	5 5	P	CHES : TH		Pat s 1
EMA-CHOVE: Seja (6,*) um grupo e a e G. Entaïo, at = a se e somente se a e e a divide t.  U) Seja K a ordem de a.  a* = Q  Vamos dividir t por K:  t = Kqtr 0 & r < K	den) = K.E = [	nx) = 1 = 1 in	nod h).	Ēħ.	Fa : 91	V	: 111 - 1/
EMA-CHOVE: Seja (6,*) um grupo e a E G. Entañ, at = a se e somente se a e a divide t.  b) Seja x a ordem de a.  ax = 2  Vamos dividir £ por x:  £= Kgtr O£r 4 K	α - ω - ι				No. of Park	E	2755 6 19
Vamos dividir & por K:  t = Kgtr	cus custo' Sa's (	6 4) um avued	ه م د و	Então.	a = 2 5	e somente	se a o
Vamos dividir & por k:  £= Kqtr = 0 & r < K		0, 11 3111 31043			HAREHAM		
Vamos dividir & por x:  t=Kqtr O&r < K	e a divide c.						
Vamos dividir & por k:  E=Kq+r= 0&r < K	b) Seja K a pro	dem de a.				3	a an mast
Vamos dividir & por x:  E=Kqtr = OErck	0 × 0	79K s 150	man de al	, marked	o vozvalov	0.3.4	- 442
t=Kqtr, otrkk					1		and the second s
par in land	Vamos dividir	€ por x:		la	bear) ti	(mb)	
And the same of th		OFLEK	h ii.	-6-2			. Maria de la composition della composition dell
#DL# 17 W	t=Kgtr						

- H= { h, h, h, he}		
(¿= \HI)		
	a st astan	0 - V
V		
Vamos construir o conjunto 9,4 como		2 : 7
8+ H= { 8+ + h, 8+ + hz   8+ + hz     8/1 *	he?	) ————————————————————————————————————
Se i + j, então:	A 36. 16	Ď.
91 × hi + 91 × hj.	4 short & m	H udarge? (: )
Suponha, por construção, que itj e	8, * hi = 81 2 h;	(+ X + )
Operando es dois lados com o invers	o de 81 (g. 1), oblenho:	) - <sup>3</sup> a = <sup>*</sup> a
8, 1 x 8, x h; = 9, 1 x 8, x h;		
<b>Q</b> Q	- Auna	1861-80 × 169-4181 =
2 * h; = 2 x h;	AD a whon I very one	
	(+, 5) no mod	Secondary (* t
h; = h; -> **	(by ) sp maly a	<i>I</i> : 1
(+)+(+x) => CONTRADIGED	(a) ab may a	
Logo, todos os elementos de gytl são	distintar entre si. Ent.	io, capationeio
- 18, H = H with the	t a 1H = 101 mp a	9 500 011
14-2 others in the opposition	is my wan olig stims	10 1 1 1 1 1 E
Vamos considerar	ste allegate co sut	
HV 81H		

Se HU mil = G, ou para a construgito. Se naty exists pala manus um elemento ge 6 6 - (11 U gent). Constero, got = { genter gon Ho, gon ho, gon ho} 19241 = 141 Considero, HUgiH UgiH Sc HUg, HUg, H = 6, eu paro a construção. Se não existe 9, 66 - (HUgiHUgiH) Construo 9. H ... Continuo esta processo até outer 6= HU9, HU \$= HU 9= HU ... U 9= H. 161= |10 3,40 g,40 g,40 1.. 0 95H [ Se as conjuntos H, 91H, 82H, ..., 96 H forem disjuntos entre si obtanto. 161= | H U 3, H U ... U 3= H = | H | + | 9+H | + ... + | 9= H | = ( 5+1) | H | ことは、そとは、ととは、中では、日本のとは |c| = (64) |H| => |H| divide |o|, que é o que eu greria demonstrar.

tilibra

Para uniformicar a notação, ramos den	otar go= 2 e escrever 4 como
Suponha, por contradição, que existe u	m elemento que pertonce a giHe!
j>i.	1-1-1H-61
- \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \	
Se o clemento pertenee a gi H, ele po ento pertence a gj H, ele pode ser escrite	como g; xhn,
gixhm = gixhn	1., 1. F. & U.P.
81xhm xhn = 8; xhn xhn =	
ν, Σ	a: H, JUHAUH , 2.
9; = 9; *, h = * b=1,	
(H) LO	nool-ban was ind
hn EH => hn 1 E H	
	. H. S. 141. (-s.)
hm EH	
1 hm *hn-1 = H	
hn'EH	
hm * hn = ha H	EV LAQUHOLF FUN - J
9; = 8i * he	U. CHARUMARUMA UIT.
11/	
9; € 9iH	Hotel Hopel Commercial and I
Mas, como joi, 8j, pela construção,	I de various salation laboration of the
h' (n)	perend ser um elemento fora de
Hしかりし 多.Hし・・・ しかけ	1 10 11

PAOPOSIÇÃO: Seja (G, X) um grupo finito d	e orden to a & G. Entro, a orden de
a divide t. Seja K a ordem de a. e	a gera um subgrupo de (G,*) de ordem
K. Polo teorema de Lagrange, a ordem	to subgrupo deve dividir a ordem do grupo,
logo K divide E.	
	'm b = m
Proposição: Seja (6, x) um grupo finito d	e ordon t e a & G. Então, a = e. em
(6,x). Sija ka orden de a. Vinos na	proposição anterior que re divide t. Logo,
pelo Lena-Criave, como a ordem de a div	ide o expoente t, então a = e.
TEOGEMA: Seja (6, X) um grupo finito eíclico	de ordem & e grumgerador do grupo en-
tão, g <sup>m</sup> também é um gerador do grupo	se e sumente se MDC (m,t)=1.
<u> </u>	A = " a
(1) Suponho que MOC(m, t) = 1. Seja 1	( a ordem de gm. Quero mostrar que
K=t.	Q = <sup>3</sup> @
(gm) = Q de moder and des	A to order by Concept as
g	1. = 10g
Como q é genador, a ovolem de q é	( 136 = ( mo ) = "( mo ) = "( mo )
Pelo lema-chave, como gmx = 1,	então a ordem de g divide o expoen
te mk, & divide mk.	Q = (m <sub>0</sub> )
t divide mx } t divide K -> *	mg someon a mybe and like a
	C. And J. San T.
MDC (m, E)=1	4 1 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2
Ké ordem de gm. té ordem do	grupo. Pela preposição anterior, x di-
ride t -> **	
<b>サ</b> ンし、	Elita
	tilibra

(2) Suponha que de MDC/m, 6) e do1 m = d.m1 Seja ka orden de gm téordem de gr. Como gmx = e, pelo loma-chave, t divide mx. (gm) = (qd.m) = qdmit = qde'm = gem = (ge) = 2 = 2 (gm) = 2. Pelo lema-chare, a orden de gm (K) divide t'. x divide t' Mas, como d>+, t'ct, logo, Kct e gm não é gerador. tilibra