JFRS- Universidade Federal do Rio de Saneiro	A What he was a Sad
lio de Saneiro, 30 de Maio de 2017	
	(102 box 501 I 18
AULA PASSADA:	- Con port son 178
(5.7)	
TESTE DE LUCAS :	300kg a 80k
Seja n um Inteiro positivo (impar).	Então, né primo se e somente se
existe 2565 n.1, tal que:	•
La La Cara de La Cara	28 3 3 5 9 1 7
id bom) 1 = 1 (mod n) =	(2) 6 (n-1)/1 ± 1 (mod n) para todo
fator primo p de n-1.	X= d
- AGORA:	Sold to and A sold
	Sent the state of
TESTE DE LUCAS MELHORADO:	A SULL BOAL F E S E HAVE
	1.0
Seja n um inteiro positivo (impar). Enti	ao, n é primo se e somente se,
para cada fator primo Pi de n-1, existe u	
r r	Gent Land & 5 sot
(1) b; 1 = 1 (mod n)	(me won) to a me
(2) 6; (n-1) /F = 1 (mod n)	Jon 2 101
ho to be a	
Exemplo: n= 103 (Lucas: 6=5)	Sycal con a
	*
b=2, n-1= 102 = 2.3.17	the state and state on the state of
2 = 4 (mad 103) / 2 102/47 = 26	= 64 (mod to 3) V (set 1 - 4 (1)
	(a boat 1 \$ 96.01, d (s)
2 = 2 = 46 (mod 103) V	
	tilibra

3 = 1 (mod 403) 351 = 102 (mod 103) 103 é primo. Exemplo 2: n= 109 (LUCAS: 6=6) n-1=108 = 22.33 2 to 3 = 1 (mo d 104) V 2 10812 = 2 54 = 108 (mod 109) V 2 103/3 = 2 = 1 (mod 109) x 3 = 4 (mod 109) 336 = 03 (mod 409) 109 é primo. - DEMONSTRAÇÃO: Seja Pi um fotor primo de n-1. Seja bi, tal que: (1) b; n-1 = 1 (mod m) (2) bi (m-1)/P # 1 (mod m)

Por (1) e polo Lema-chave a ordem de bi (vamo	os chamá-la de Si) divide
n-1> n-1 = S; · t . d no obered when up able	La Se e Renter o
metro protects by policy made a mobile of epingul de	ol 7 x-1
Por (2) e pela lema chave, si não divide (n.1)/Pi. Va	mos escrever a fotoração de
(n-1)	16 12 cd
Ly a dulin 2" a	
n-1= P1 21 P22, P22 P22	2 60.06
10 to should	12 dona6 2 1
St divide n-1	mit above in
L> Si tem os mesmos fatures primos de n-1	
he she makes a substance of	blow a arrival
Si = Pitiple Piti Pite onde fi = R; para to	10 15 j 5 K
	last state from
No caso particular do fator Po que estamos analisando.	
Pi & Pi	(of shows 2)
	come of samuely of
Por outro Judo,	core tag
(0-1) - P1 2 P2 Pi 21-1 Px 2K	the man con the file of the state of the sta
Pi	(1)
	1-3-1-0
Si não divide (n-1)/Pi	77/20
L> P; > P; - A	·
$\ell_1 \leq \ell_1$	
$\Rightarrow f_{\lambda} = Q_{i}$	
$P_i > Q_i - \Lambda$	ACTIVITY OF THE STATE OF THE ST
La suppose parist a son serial	The common call supported
Logo, 5; é a orden de bil	1 5
Logo, the distriction of	the state of the s
, AKA	tilibra

Si é a ordem de li Ly Si e a ordem do subgrupo cíclico genido por bi L's Polo teorema de Lagrange, a ordon de um subgropo divide a orden do grupo. L> Si divide of ent Esse raciocinio é ralido para todos os patores do n-1. diride Fin P2 02 divide pen) divide Pin) n-1 divide pen) Ly POTONCIAS DE PRIMOS n-15 0 cm DISTINTOS RESULTADO GERAL: PCA) & N-4 n-1 = 6 cm den) = n - 1 \$ cm + n-1 n & primo. Vamos estudora agora mais dois algoritmos de fatoração, especitivos prima a Patoração de números de Mersenne e Fermat, respectivamento. 1) Método de Fermat para a fatoração dos números de Mersanno Man1=2" -1 , n>1

LEMPRANOUS Son & compasso, Ment & contamonto composto. Son o primo, Ment Pude ser prime ou compusto. Coja evilão Mepl com p primo. Esponha que q a um fator primo de Mipla 2 Pad L> q divide 20-1 11 2 -1 = 0 (mal 9) 20 = 1 (mod 9) Como 2º 1 (mad q1, pelo lema chave, a ordem de 2 divide p. Orden de 2 é 1 ou p. 2' \$ 1 (mod 9) A ordem de Z é p. Polo paqueno teorina de Format, 29-1 2 1 [mod q) Polo lema chine,

A ordem de Z, que é p, divide q-1. 9-1 = p.t Se assumirmas p=3, p é impar. Mcp = 2 P-1 também é impar L> Todo fator de Mcp1 também é impor L> q élimpur t é par L> 4=2.4 9=1+2rp Logo, se q é un fator primo de Mcpi, entaño q tem o formato 9=1+2rp Suponha que q é o menor fator primo de Mcpi 9= VMCP) = VZP-1 < VZP 1+2rp < V2P 2rp 2 12p -1

								/ /	
B	sco o fat	or a r	o formato	ie d Caree	Cat S	mer solo?	1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1	Wilsh 15	i.
		. •				A FE			
	9=4+	2rp.							
				. (m. 7 36 am	no mil	01 01 3 0	S. A).	1.2.2	
C	m r no	in deere	١_					,	
	IM	J 111 - C1 14			10	(mm) 0 =	(A) 9	offer 3	
	1584	JE - 1				4			
		Zρ			10	buml O3 3	22 K		
	1 ,		<i></i>	(M 7		4			
	mo_testar	c se q	e fator	de Mip) ?	1.1	wm) 1-5	7 5 C		
		- P			101	NEW J. L.			
les	sto se	2' = 1	(mod a)				1 1	/ 4	
				_ 1 1	obinti	1 00. 200	at unb	Loweld .	
EXENDO:	Man =	24-42	2044					(-4)2	
	,		<u></u>			hoom) F 3			
Υ				22	= 44,	7		1 5.35	
	2	. 44	2			100	um) k	2	
			1	•					
5	9 h 200	10 21	1545	125 spart 5	ale m	sebro a	mids.	umal 0/27	
			L>	r=1 ov r=2			N+X	2 + mos	35
req								eult	
•	- 412	. 1 . 11 =	422 = 23						
9=1+2 c	P = 412	-	1120 - 23			/	1 / 4 \$	2 E A	
44		6 614	.			1 2 13 14/15			
2" = 1	(mod 23	7: 21W			(- Z	()	e1 7	
		E	IMPAR		main u	o stars		in airtail	
R	B			Logo, 23	e fot	lor de Mi			
1	1	11	51M		-	Frag	divil.	4 55 000	n A
2	4	500 3	SIM	3 C de mater	A)				
8	16	2	hão			ote 2k	4 No	alem de 2	io A
8	3	1	514						
4	9	0	LOON	man) 1 = 1-1	5 .	La Person	L Mary	1-1-069	

2) Método de Euler para a fatora				
F(K) = 22 +1, K>0		035	4 1 × 13	
	1. 5.3			
Suponha que q é um fatur primo	OE LOW.	alwate		0
Entaro, & ca) = 0 (mod q)				
4		1-7	273	
22 K + 1 = 0 (mod q)		9.5		
11/	Time Make model	3 0 1 2 2	ustual	
22 = -1 (mod q)				
2 2 - 1 (mou q)	Y	14.7-	and the same	J
	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1			
Elevo os dois lados ao quadrado:		- A - 11 gs	= n. 4	
12K)2 12-11	0			
$(2^{2^{K}})^{2} \equiv (-4)^{2} \equiv 1 \pmod{q}$	7.3		11 1	~
			1	7
$2^{2^{k} \cdot 2} \equiv 1 \pmod{q}$		11	S.	
Pelo lema chare, a ordem de 2		1.7		
22 = 1 (mod q) Pelo lema chare, a ordem de 2, com t ≤ K+1.	divide 2x+1, Log	1.7	dem de	
22 = 1 (mod q) Pelo lema chare, a ordem de 2, com t 5 K+1.	divide 2x+1, Log	go, a or	dem de	
$2^{2^{x+1}} \equiv 1 \pmod{q}$ Pelo lema chare, a ordern de 2, com $t \leq x+1$. Mas, $2^{2^x} \equiv 1 \not\equiv 1 \pmod{q}$	divide 2x+1, Log	go, a or	dem de	
22x = 1 (mod q) Pelo lema chare, a ordem de 2, com t ≤ k+1. Mas, 22x = 1 \$ 1 (mod q) Então pelo loma chave, a ordem de	divide 2 ^{K+1} , Log	go, a or	dem de	
Pelo lema chare, a ordern de 2, com t s k+1. Mas, Z ^{2*} = 1 \$= 1 (mod y) Entro pelo lema chare, a ordern de	divide 2x+1; Log	go, a or	dem de	
22x = 1 (mod q) Pelo lema chare, a ordem de 2, com t ≤ k+1. Mas, 22x = 1 \$1 (mod q) Então pelo lema chare, a ordem de ordem de 2 divide 2k+1	divide 2 ^{K+1} ; Log	ALC TA	dem de	
Pelo lema chare, a ordem de 2 com t≤ k+1. Mas, 22x ≤ 1 ≠ 1 (mod q) Entao pelo lema chare, a ordem de a de 2 ordem de 2 divide z*** A orden	divide 2x+1; Log	ALC TA	dem de	
22x = 1 (mod q) Pelo lema chare, a ordem de 2, com t ≤ k+1. Mas, 22x = 1 \$1 (mod q) Então pelo lema chare, a ordem de ordem de 2 divide 2k+1	divide 2 ^{K+1} ; Log	ALC TA	dem de	

Pelo lema charo, a ordem de Z,	que é zx+1, divide q-1, s. + 1 = 0 = s +
9-1 = 2 K11 . +	se midel
1	
q = 1+2 ^{K+1} ·ċ	Total Cast from 1 - 1 - 18
Supunha que q é o menor fator pr	imo de Foxy. Então,
95 VF(K) = 122" +1 = 122" +1	100 = 0104/5- 01 25-10 5- 01
1+2K+1 .+ < 1/2K +1	1. 2 (ero de cor) - 1- 2 38 s
$\frac{1}{2^{K+1}} = \frac{2^{(2^{K})/2}}{2^{K+1}} = \frac{2^{2^{K+1}}}{2^{K+1}}$	= 2 ^{2^{K-1}-K-1} = 0 = 0 = 0 = 0
15t 622K-1-K-1	
Exemplo: F(5) = 225 +4 = 282 +4	
t = 2 = 5-1 -5-1 = 2 = 2 = 2 = 2 = = 2 = = = = = = = =	Ana H
1 € £ € 1024	
t=1 -> q=1+ 26.1= 65	
Testará se	
232 = -4 (mod 65)	

t=2 -> q = 1 + 26 · 2 = 129	and a second of the second of the
	+ 118 c . 1 - β
Testora se	
232 2-4 (mod 129) Não!	3 112 (+1 : P
Edgy (no 3 sh a	my what recover is a posts along?
=10 -> q = 1+26.10 = 1+640 = 64	41 pr ne p > p, ne p : mile ap
232 = -1 (mod 644) 51H!	11 75 x 3 + 1 tx 5+1
Logo, 644 é fator de Fis)	1 2 5 (2) 2 4
	+ 2 t + 2 t + 2 t
	11 3 6 14 35 6 6 1
	5 3-75 F 5-7-1 3 5 2 +
	20 = 1 · 0 9 + 1 · p · + 1 · 3
	,
	(23 6-) 1-2-5
	S- Care