	10
- AULA PASADA	
TESTE BASEADO NO TEOREMA DE FERHAT	/ 0
Quero testar se n é primo	ou composto.
Selectiono uma base 1 < a <	n.,
testemunha de que n é composto.	certeza é composto. Neste caso, a é uma
Se and = 1 (mod n), o res	ultado do testo é inconclusivo.
n pude ser primo ou n pseudoprimo para a base a)	pode ser composto (neste caso, né um
Se testarmos com várias bases probabilidade de ser primo aumenta.	e o resultado dor sumpre inconclusivo, a
Eseeu testar com todas as bases?	(Inviavel na prática)
	ultado vai ser inconclusiro para todas.
	Seja então pum fator de n (16fen)
$D = f \cdot D$	(*)
A	
Vamos realizar a teste esculhendo	f como base:
131 mm	

pn. 1 = 1 (mod n)	continue and the will be to a surface for fully
	The second secon
Suponha que part = 1 (mod a) então por	ut -t é multiplo de n. Em outras pala
Suponha que f ⁿ⁻¹ = 1 (mod n) então f ⁿ n divide p ⁿ⁻¹ - 1.	areal so (a book) & the
f divide p ⁿ⁻¹ - 1 f divide p ⁿ⁻¹ - 1	a s) 29% our lat or and what was
of divide fort - 1	
f divide part - 1)	De color savelas cales al
Frederings is (1-hos) pri-1= p. tom las de sus	al one is steel estangenes to a sea sont
	10 06 rates on rost ser
Pn-1 -1 = f. E	The state of the s
Prot - P. E = 10 was made a many light and	i stat a gramina isden uria m. A
p(pn-2 - f) = 1	und a summer today on a A
. ↓ !	
P divide + alasta and at amount many	a material whiching an elementer!
1	
> P= 1 } (N)	and an election where or real
Amenica Alexander a state a more more and	of a southern of suit was any cot forus
(x)+(xx) => CONTRADIÇÃO	in boots man) she come and is your
Portanto,	and the world my and wife to make the
	Good Anna A Margagaile and Mary 200
f " = 1 (mod n)	
	Contact to " a
(quando n é composto e 14pan	fator den)
1 danne	1 = (au) ight malet a set me
Pelo teste, p será uma testemenha	
	dense a continue of the
Logo, se n è composto, o teste não	pode produzir resultado incopelos.vo
	(women) It to Betal
ALT INCOME	
	tilibra

In pelizmente, existem números, conhecidos como, Números de Cormichael, que rap números com postos, mas que and = + (mod n) -> (TESTE INCONCLUSIVO) pura toda base a tal que MDC (a,n) = 1. Em outras palarras, para estes números, oncontrar uma base que nos permita ter certeza que n é composto (isto é, uma base b tal que bnit \$1 (modn) à equivalente a encontrar um fator de n. Assim, para estes números, o teste é tão difícil quanto a fatoração quanto a fato. ração direta do número. Infelizmente ao quadrado, existem infinitos Números de Carmichael. Assim, na prática, o teste ma permite determinar com certeza que alguns números são compostos, mas não que um número é primo. Alám disso, o leste é initil para números como os Múmeros de Carmichael. opservação: Para ser um número de Cormichael, o número deve ser composto. Números primos tombém sidizfazem a condição and = 1 (mad n) para todo a tal que MDC (a, n) = 1, mas não são números de Carmichael. 561 é o menor número de Cormichael. 564 = 3.41. 17 (COMPOSTO)

rilibra

definir um número de Carmichael	como um número co	mposto talque a" = a (mod n)
para todo 1 a Cn.	9 7	and the sen apple
201 of Lay Me 201 41.00	change to provide	a way well below a
25 a 5 560	,	
Carp as was	udo cm.) a fore-catalon	1 1 1 36 - 6 19 (1)
a ⁵⁶¹ = (mod 561)		
Wash with a plat on the B		or start our to (s)
a561 = (a2)280 · a = a (mod 3)		
1		(1)
0,664 = (a10) 56 · a = a (mod 11) -	> Mánu	LOS PRIMOS
and at all a fine (s) a (s) a (s)	TO SEE OF SECURITION OF SECURITION	9 ob loser out in all
2561 = (a16)35 · a = a (mod 17)		0.5
31	(an atar a	Jan 1 7 3 6 5 5 - 1/42
,	\$2.200.50	ALL STATES
\$64		\$ - 5 - 8
sul = a (mod 3)	2)) 564	1 1125 (2)
CEAL	3 divide aset - a	MDC (3, A1) = 4
2561 = a (mod 11)	H divide asot - a	> MDC (3, 47):1
	47 divide assi -a	HOC (41,47) = 1
2561 = a (mod 17)		
		turney sib warment will
EMA DA SEGUNDA SEMANA DE AVIA: S	· MDC (a, b) = 1,	a divide c e b divide c
ntão ab divide c.		(19 bon) 1 = 1 0
O MDC entre dois primos disti	intos é gempre 1.	- P - P rug or about
	•	
PNCLUSÃO: O produto 3-11-H=561 divi	de 2564 - 2 1 ma	n.p (11) = n
O Production of the Otto		
a 561 = a (mod 501)		LEV III - 18
a = a [mad 301]		IF GALLERY AND
_		
sed i como de Cormichael.		

TEOREMA DE KORSELT	Landson) als on the	
Seja n>2 um inteiro composto. n é, para todo pator primo p de n, as seguintes	um número de Carmichael	50 0 50 m
e, para todo pator primo poe n las seguines	- zonargues - sans perio	005505
(1) p-1 divide n-1 (n deixa vesto + na divi	500 per p-4)	
	(400 (400)	E 1 A
(2) p2 não divide n. (p só aparece um	na vez na fatoração de	1) L
•	(8/10/03/03/0	
$\uparrow\uparrow$		ř
- Marie Pancel	- (1) 1 . 1 o T n -	** (81) = F5
Siponha que, para todo fator primo p de n	1 as condições (4) e (2)	são satisfeit
	(=1 hom) 0 = 0	(2) = 10
Seja 2 4 a 5 n-1, pela condição (2),		ř
n= P4-P2, P3, , Px	16	Long o
(P, 2P, 2P, 2, 2Px)		
11 day 64 6 12 (3 49) A	- h	1 de 1 de
You calcular a modulo Pi, para todo	1213 K	
	(1)	-nl - = 1
Pelo Feorema de Fermat,		
a short to a selection of fundamental	il i pius sa . pius so	44000 000
$\alpha^{P_{\lambda}-1} \equiv 1 \pmod{P_{\lambda}}$	3 34	d do 070
Divido o por Pi-1:	dologent of	oon o
n=(p:-1). q+r	6-6 6-8-14 M & of de-	o tolens
Pela condigão (4): r=1,	((, b, n))	- 122 0
		Į.
	attends one of comme	

tilibra

Cn = (Pi-1) -9H = { 2.4 }"	10 70 1 121
(a)	·a =a (mod Pi)
4	
Pi divide an- a para toda	o Aliek
, ,	
Logo, o produto P. Pz P	x = n divide an = a (mod n)
11	
an = a (mod n), par	ra todo 26 asn-1
Logo, n é un nûmer	de Cormichael.
301	
TALTA MOSTRAR:	
1031630	
- Número DE CANHICHAEL	-> (A)
- Número pe CARMCHAEL -	·> (2)
	-> MAIS THADE (PRECISA DE UM RESULTADO CHAMADO "TEOREMA DA
	RAIZ PRIMITIVA", QUE É DADO NO SERGO FINAL DO CURSO)

tilibra