UFRS - Universidade Federal do Rio de Sanziro	1.03.03 (14)	(1 (1 - (1)) - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1
Rio de Saneiro, 27 de Abril de 2017	1	
- NUHBRO DE CARMICHAEL => (2)	m 3 a 3 h Calindon	9 0 - 9 16 19
(2) = p² não divide n	- 15 CL 2 (1 19	William a possible
Suponha que n é um número de Carmiehae	l. Gatão, é composto	(atom) a sia
a" = a (mod n)	armin de larre	Logo o a um
Para todo 25 a 5 n-1 em particular, se	p é um fator pri	mo de n. então
2 = p = n-1. Logo, p" = p (mod n)		
الم (×)	(1) 5- Ban	Las I to also id
Isto é, n divide p'n- P	(5) 5- 1300	- Numero Conner
Suponha, por contradição, que p² divid	len.	
Então	1 (4) ==	- Miner L Company
$ \begin{array}{c} p^{2} \text{ divide } p \\ p \text{ divide } p^{n} - p \end{array} $ $ \begin{array}{c} p^{2} \text{ divide } p^{n} - p \\ p^{2} \text{ divide } p^{n} - p \end{array} $		
$p(p^{n-1}-1) = p^{n-1} \cdot t$ $p^{n-1}-1 = pt$		
pn-1 - pt = 1		
$p(p^{n-2}-t)=1$		
p divide 1		
tilibra		

) + (* *) -> CONTRADIÇÃO	d stock of and
Logo, p² não divide n. + "a shrib n	10 11 0 show (16 m (16)
ESTE DE HILLER (OU MILLER. RABIN)	(a) A - E - A (a)
-> Ideia semelhante à do teste baseado no teore	ma de Fermat
-> Permite determinar que alguns números são e	compustos sem fatorá-los.
-> Consegue distinguir mais números compostos	do que o Teste antenior.
Suponha que n é primo. Seja 2 ≤ a ≤ n·1.	Então, pelo teorema de Fernat,
an-1 = 1 (mod n) 1 = 1	s . t
Q 21 (mod c)	9 6 5000
a = 1 (mod a)	ф радав , г
₩	4
₩	(a (
n divide an-4-4. Suponha que n é impar e n>3. O expounte	n-1 na politicia and é major
n divide a ⁿ⁻¹ -4. Siponha que n é impar e n >3. O exposite qual a 2 e par -> n-1 é um número inteiro.	n-1 na politique and é maior
n divide a ⁿ⁻¹ -4. Suponha que n é impar e n >3. O expounte yal a 2 e par -> n-1 é um número inteiro.	n-1 na politique and é maior
n divide $a^{n-1} - 4$. Suponha que n é impar e n > 3. O expounte val a 2 e par -> $\frac{n\cdot 1}{2}$ é um número inteiro. $a^{n-1} = \left(\frac{n\cdot 1}{a^2}\right)^2 - 4^2 = \left(\frac{n\cdot 1}{a^2} + 4\right) \left(\frac{n\cdot 1}{a^{-2}} - 1\right)$	n-1 na polòncia ant é maior
Signa Re $n-1$ - 1.	n-1 na polòncia ant é maior
Siponha que n'é impar e n'3. O exposite Juli a 2 e par -> $\frac{n\cdot 1}{2}$ é um número inteiro. $a^{n\cdot 1} = \left(\frac{n\cdot 1}{a^2}\right)^2 - 1^2 = \left(\frac{n\cdot 1}{a^2} + 1\right) \left(\frac{n\cdot 1}{a^2} - 1\right)$ Seja $R = \frac{n\cdot 1}{2}$ $a^{n\cdot 1} = \left(a^{K} + 1\right) \left(a^{K} - 1\right)$	n-1 na polòncia and i é maior de la solution de la
5. Suponha que n'é impar e n'3. O expounte pual a 2 e par -> $\frac{n\cdot 1}{2}$ é um número inteiro. $a^{n\cdot 1} = \left(\frac{n\cdot 1}{a^2}\right)^2 - 1^2 = \left(\frac{n\cdot 1}{a^2} + 1\right) \left(\frac{n\cdot 1}{a^2} - 1\right)$	n-1 na polòncia anil é maiore

ou p divide b (x) -> n divide a*+1 ov n divide a*-1 a = -1 (mod n) = 1 (mod n) - VAMOS REFINAR UN POUCO 855 A IDELA : n-1 é par. Então, posso escrever n-1 = 2. a onde q à impar e t >1 a = 1 (mod n) 22.4 = 1 (mod n) n divide azt. q -1 02 · 9 - 1 = (22 · 1.4) 2 - 12 = (22 · 1.9 + 1) (26 · 1.9 - 1) n divide azerta + 1 FORMATO IGUAL AD DA n divide a26-1.9 - 1. 22-1.9=-1 (mod n) ou 02-1.9= 1 (mod n) 0 2000550

Se t-1 = 0,	(report 1- = p. 100	(= A+ A+ 1 B 26018 17)
		Vo
az 6-1. 9 = 1 (mod n)	Labord L & P SO	S= N-P 1/2 shrikanis
WATER A CHARLES	Det Dies SM 4-1	
a = 1 (mod n)		9.5
		uest-
Se 6-1 21,		
		(n bum) 1-3 P. 120
$a^{2^{i-1} \cdot q} - 1 = (a^{2^{i-2} \cdot q})^2$	- 12 = (a26.24+1) (a26.2.4	-1
	y	aborder
n divide	, a ^{2 + 1}	- Charles a second constraint
	oU	ρ ** 8 = 1 · γ
n divide	a2t-2,9-1	
		all to I
a2 -1 (mod n)		
อง		7 6 60
a26-2 - 9 = 1 (mod n),		1 324 (20
	depetir o processo de novo	
		country is at 10)
Seja jo menor interro	não-negativo talque:	
	wanting & = " to	P'O P'SO P'SO PA
a2) : 9 = 1 (mod n)		
	untas, um	Physics server was 150
5e j= 0,		
		ly bem 1 + 1 D
a9 = 1 (mod n)		00
the p stanger & Com	aring a last short analogue	Alama das antimores da
Sc.j.>0.		
5	+ " " o o (a bom) +	to be promised for the
$a^{2^{3}-9}-1=(a^{2^{3-4}-9})^{2}$	- 12 = (02)-1.9 +1) (02).1.4	-1) 20 volos de 100

 $n \text{ divide } a^{2^{j+1} \cdot q} - A \implies a^{2^{j+1} \cdot q} \equiv 1 \pmod{n}$ LY ESSE CASO NÃO PODE ACONTÉCER ·9 = -1 (mod n) Lembrando, n-4 = zt . q Então. 0835 E 05)-156-1 Calculo as potâncias => t politicias Pelo que vimos, se n é primo, então a9 = 1 (modn) Alguma das potências da sequência (pode ser a primeira) é congruente a No sentido inverso, se a \$4 (mod n) e a2" 9 \$ 1 (mod n), para todo o≤u≤t, então v com certeza é composto.

	- 120	
1	1	1
)
/	,	

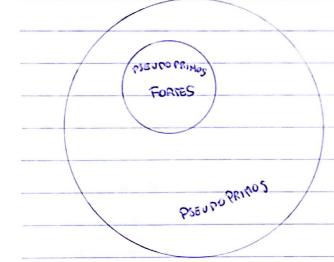
Esse é o Tesse de MILLER - RABIN.

Assim como o teste anterior, este teste produe como resultados composto ou inconclu-

Um número composto que retorna resultado incon clusivo no teste de Hiller-Rabin com a base a é chamado de pseudoprimo forte para a base a.

Existem menos pseudoprimos portes do que pseudoprimos para a base a.

Todo pseudoprimo forte para a base a á um pseudoprimo para a base a. Mas o inverso não é verdadeiro.

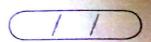


		1 1			1
EXEMPLO 1: n=344 (PSEUDO	PRIMU PARA A BASE 2)	R	A	E	EIMPAN
939 2 4		1	2	8.5	51H
n-1=340 = 22 · 859	235 = 82 \$ tall mod 341)	2	4	42	りが
2 (8%) \$ 1 (may re-		2	16	21	514
t=2	2 = 32 = 1 (mad 341) (2	32	256	10	Não
9 = 85	↓	32	64	5	Sin
a= 2 76-4	COHPOSTO	2	4	2	พร้อ
9 21.9	OW	2	16	1	5:M
(a) ²	aged along and aged in the	32	526	0	พรือ

SEMPLO 2 n=564 (CARMICHAEL)		T many he	- 30 11	7	,
	2	A	E	IMPOR	
n-45 560 = 24 · 35	1	2	35	SIM	
	2	4	47	SIM	
t=4	8	16	8	พลัง	
9=35	8	256	ч	Não	
	8	460	2	Não	
Q= 2	8	103	1	SIM	
a Service of the Control of the Cont	263	511	0	200	3
235 = 263 \$ 14 (mod 564)	•				
22.95 = 263 = 166 \$ + 1 (mad 561)				1. 4 1	aT.
21 35 = 16 = 67 = 14 (mod 564)			and the same	100	Octor.
223 -35 = 672 = 1 \$ -1 (mod 561)					
J					
EOHPOSTO					
Bonvosio			Co. miles		
			- Carrier		
xerco 3. n=25	AMP of the second secon				
a= 1		Conse			
			Y		
n-4224 = 2 ⁵ .3					
€=3	(AFÉID	1 016
9=3				~	
5 - F F E	Comment 1 : 5	- 4	19.0	· · · · · · · · · · · · · · · · · · ·	m-5 - 1
73 = 18 \$ 1 (mod 25)					
$7^{2.3} = 18^2 = 24 = -1 \pmod{25}$	(newality set	17			5 = 2
722.3 = PRODUCMA	V				28 -
CMA V	076037803			1-38.	F 21
	The second secon				

L) 25 É PSEUDO PRIMO FORTE PARA A BASE 7

INCONCLUSIVO



OBSERVAÇÕES.
(701 hom) PF = X
1) Não existe o equivalente dos números de Carmichael pro toste de Hiller.
c) Ao testar com uma base selecionada aleatoriamente no intervalo 2 ≤ a ≤ n-1 e o
resultado der Inconclusivo, a chance de n ser primo é = 3 e de ser composto é
$\Delta e \approx \frac{1}{4}$.
Logo, testando com K bases distintas escolhidas abatoriamente, se os testes derem
inconclusivo com todas as bases, a chance de ser composto é de $\approx \frac{1}{4^{2}}$
Com 10 bases é menor que 1 em 1 bilhão.
- RESCRUÇÃO DE SISTEMAS DE CONSERVÂNCIAS.
/ X = 1 (mod +3)
1 x = 4 (mod 15)
$x \equiv 4 \pmod{43}$ $x \equiv 4 \pmod{43}$ $x \equiv 8 \pmod{43}$
> x=1 (mod 13)
x-1=13 K
X= 1+13K
1413 K = 41 (mod 15)
13x ≥ 3 (mod 15)
L> CALCULAR O INVERSO DE 13
7-13K= 7-3 (mod 15)
K = 6 + 15 8
x = 1+13 (6+152) = 1 + 78 +195 2 = 79+195 2
$x = 79 \pmod{195}$

x= 19 (mod 195) (mad 19) tilibra