No.	
Date	. ()
Miller - Rabin (n)	
Miller-Rabin (n) Se né par e n; 2 devolva "compos/o"	0
Sorteie X ∈ {1,, n-1} aleatoriamente com prob. uniforme	
devolia "composto"	
Encontre se t, so moior possível	
(fermat) a $x = f \le mod n$ devolva "composto" £ncontre $s = t$, $s = o = n = i = poss \(i = t \) t = g = n - 1 = 2^{s} \cdot (t) = s t \in x = mpax$	
par 1 pa	
Calcula x^t , x^{2t} , x^{4t} ,, $x^{2^{5}t} = x^{n-1}$	A CONTRACTOR OF THE PARTY OF TH
para i de 0 a 5-1 verifique se χ^{2it} é uma vaix falsa $\chi^{2it} \neq \pm 1$ $\chi^{2it} = 1$	delo
$\left(\begin{array}{c} \\ \\ \\ \end{array}\right)\chi^{2t} \neq \pm 1$	
$\chi^{2^{i}t} = 1$	·
devolva "provavelment primo"	
	0
n composto émpar	
x é liar	
co algoritmo retorna prov. primo com este x	
# liars $\sqrt{\frac{n-1}{2}}$	
$\lambda = conj de liars$	
$a = g \pmod{bc}$ $a \neq g \pmod{c}$ $a = g \pmod{c}$ $a \neq g \pmod{bc}$	
(A)	
$\mathbb{Z}_n = \{ x \in \{1, \dots, n-1\} : nndc(x, n) = 1 \}$	
(Z_n^*, \cdot) é um grupo \cdot $\forall a,b \in Z_n^*$ $a.b \in Z_n^*$	
o Halbe Zn abe Zn	
$. \forall a_1b_1c : a(b,c) = (a,b).c$	
o acom da o non 7. y a.a = 1 = a.a	0

	No.
	Date .
0	B = Zn é subgrupo se (B,.) é grupo
0	B é subgrupo proprie se B+ IIta
0	A CONTROL OF THE PROPERTY OF T
0.	· Lagrange: 181 = 12/11
	b no intero
	Ideia: B subgrupo de An proprio
	LEB
	121 < 181 < n-1/2
	$ \exists \mathcal{B} = \{ b \in \mathcal{Z}n^* : b^{m-1} \equiv \mathcal{L} (mod n) \} $
0	é sub grupo é proprio : $n \in \mathbb{Z}_n^* = x^{n-1} \neq 1 \pmod{n}$
	e proprio. RENN & A FILMENT
	De né de Carmichael
	fato: De pé primo, p2+n
0.	
	Teorema do resto chines: (TRC)
	Teorema do resto chines: (TRC) Sistema $X = a_1$ (mod n_1) mdc $(n_i, n_j) = 1$ $X = a_2$ (mod n_2) $i \neq j$ $i \neq j$
	$ \begin{array}{cccc} X = U2 & (\gamma V/\alpha U n_{\alpha}) & \lambda \neq j \\ \vdots & \vdots & \ddots & \ddots \end{array} $
0	$X \equiv Q_K \pmod{n_K}$
()·	
	I × satisfazendo o sistema
	$\exists \times satisfazendo o sistema$ se $\times 1$, $\times 2$ soluções $\times 1 \equiv \times 2 \pmod{n_1n_K}$
0	
0	Suporka $p^2/n \Rightarrow n = p^2, q \cdot mdc(p,q) = 1$
0	
	$\begin{cases} n \equiv p+1 \pmod{p^k} & \exists n \text{ pelo TRC} \\ n \equiv 1 \pmod{q} & \Rightarrow \end{cases}$
0	(N = 4)
0	
	그리는 그리는 사람들이 들어 있다. 가장 중에는 생각이 되었습니다. 그리는 사람들이 되었습니다. 그리는 생각이 되었습니다.

```
(p+1)^p = \sum_{i=1}^n {n \choose i} p^i \equiv 1 \pmod{p^2} if (mdc(x_in)=1)
F \times {n-1} \equiv (p+1)^{n-1} \not\equiv 1 \mod (p^k)
\stackrel{\text{(p)}}{\Rightarrow} \times {n-1} \not\equiv 1 \mod n
((p+1)^p) \equiv 1 \mod (p^2)
  (p+1)^n \equiv 1 \pmod{p^2}
             mdc(p+1,p^2) = 1
    (p+1)^{n-1} \equiv (p+1)^{-1} \pmod{p^2}
        j = max { i e 20, ..., 5-1} | 7 v e 2n*,
   (n-1)^{2^{\circ}t} = 1 \pmod{n}
B = \{ x \in \mathbb{Z}_n^* \mid x^{a^t t} \equiv \pm 1 \pmod{n} \}
    B é proprio
       W = V (mod ns)
                1 (mool n2)
                         RC M J W
```

	No.		
The second secon	Onlo	* **** Augusto wilese	F
$w^{2/t} = v^{2/t} \pmod{n_t}$	the continuent of the continue		
$w^{e^{ik}} \equiv 1 \pmod{ne}$			og nagsféldiða om sam sem e
$-\sqrt{a^{j}t}$			
sec: Vale = - 4 (mod n)			
- W&B			
$w \in \mathbb{Z}_n$ (facil)			
Decompose wait = 1 (mod n)			
=-1(mod u) (-> (-)			
2/4			N. J. Street of the property
- I rruce rid (-) (-)	Para salahari menanggalan di salahari di s	and fig. St. of the late and product the agriculture of	
2 /2 (a) 10 /4		the later and the second second	The Mills and Mills county and the
6			-
	COURT ET AND STORES BUILDING AND TO SECURE		***************************************
5	13 =	. 2	
$ \begin{array}{cccccccccccccccccccccccccccccccccccc$	5	7	- all \$4.00 to 10.00 and 10.00
AAA(c,d)	Providence Schools of the confliction of the Schools of the confliction of the conflictio		and having the later common to the
			manufacture of the second state and the
	And the second of the second	Consider were resident and the second	and participation of the terms
			to a grand space of the state of
	Harmon Mandamentor parte land, was to the state of the st	TARRETON LETS THE MISSES OF BEING	
	of National and American Services	and the state of t	
	marriages and an organization of some	manufactured recognition of	en en
	$\omega^{2/k} \equiv -1 \mod n$ $\equiv 1 \mod n \qquad (-> \leftarrow)$ $0 \qquad \qquad$	$ \begin{array}{cccccccccccccccccccccccccccccccccccc$	$w^{a'k} = V^{a'k} (mod n_{a})$ $w^{a'k} = I (mod n_{a})$ $= I (mod n_{a})$ $= I (mod n_{a})$ $= I mod n_{a}$ $= I mod n_{a$