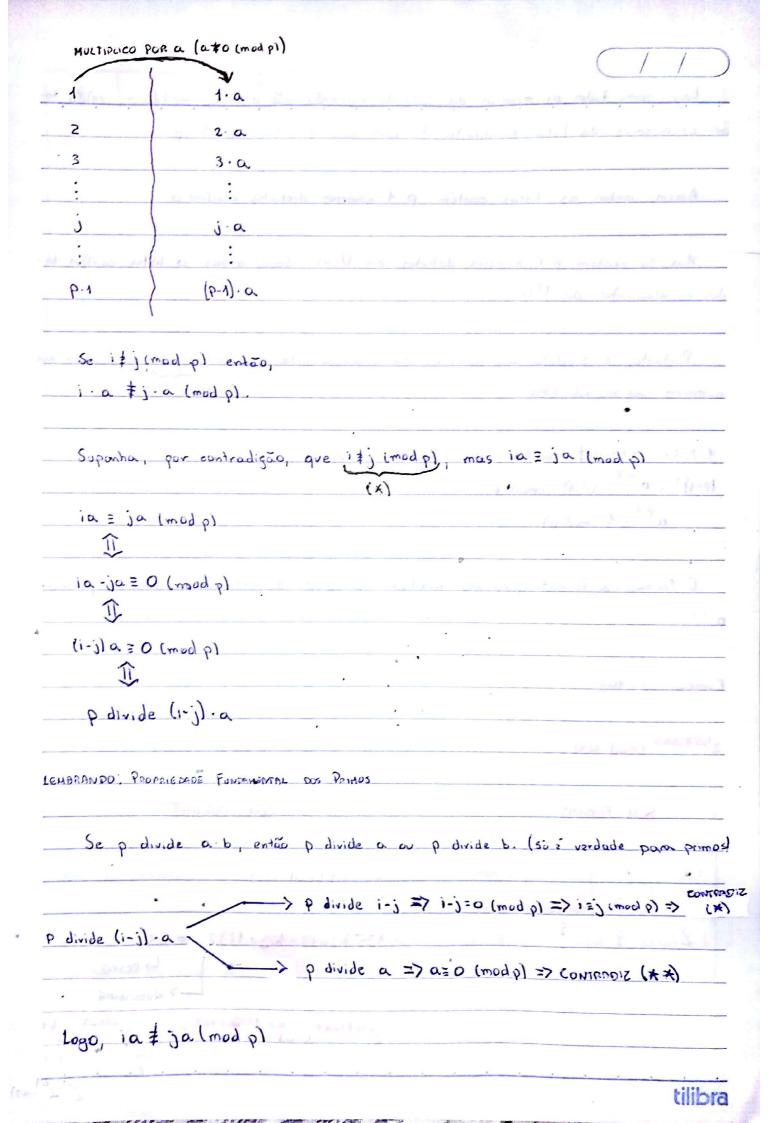
			e New Allens	C ARL	- 1000000
QUAGGES LINEARES					
and de la part of any late wat					er med
Bx = Z  MULTIPLIED OS POÍS					and broth destroy
LADOS PELO INVERSO					1.0
HUCTIPLICATIVO DE 3					
	1 5				
$\left(\frac{1}{3}\right)\cdot 3\iota = \left(\frac{1}{3}\right)\cdot 2$					0.54512
2					
x= 2/3		4.8	Separ L	G	18
CONGRUÊNCIAS LINEARES		- 0.62	L. L. F. D. L.		3 - of 2
3x = 2 (mod 7)	,K	Q	$\propto$	8	7
MULTIPLICO OS DOIS	3	-	1	0	
lados pelo inverso	7	~	0	1	u s profiles contact
HUGIPLIENTIVO DE 3.	3	0	1	0	
	11	2	-2	1	Vorest
5.3x = 2.5 (mod 7)	\ 0	3	) —	1 - 1	
			1	125-	<u> </u>
X = 3 (mod 7)	-2:5(	mod 7) -	> Invers	0	4 1 7 2 1
ax = b (mod n)				Oleme 1	S
we go thing it!			(in bom)	Ste) 8	Ment disco Peul
Se a tem inverso multiplicat	ivo médulo n	0	vue a -		na dos
ugão X = at b (mod n)		Cont	Sivencia	TEM U	ma unica
0910					

- PEQUENO TEOREHA DE FERMAT;  Seja p um número primo. Seja a um inteiro tal que a +0 (mod p) (1) p rão divide a) então,  (***)  a <sup>P-1</sup> = 1 (mod p)	Seja p um número primo. Seja a um interio tal que a #0 (mod p) (15to o divide a) então,  ap-1 = 1 (mod p)  avação: Não podemos aplicar o teorema de Fermut se o módulo for um número osto!  sulvos vensão po Teorema:  Seja p um número primo. Então,  ap = a (mod p)  tonstração.  Vamos considerar os elementos do conjunto  (n) = Z p - {ō}  = {1, z, 3,, p-1}	pode não tor nenhuma solve	ing on bags yet novi	as solveres.	2.73
Seja p um número primo. Seja a um inteiro tal que a #0 (mod p) (1 p não divide a) então,  ap-1 = 1 (mod p)  Dosservação: Não podemos aplicar o tecremo de Fermat se o módilo for um núm composto!  - Séculvos versão 20 Teorems:  Seja p um número primo. Então,  ap= a (mod p)  - Demonstração:  Vamus considerar os elementos do conjunto  U (p) = Z p - {ō}  = {1, 2, 3,, P-1}	Seja p um número primo. Seja a um inteiro tal que a #0 (mod p) (15to o divide a) então,  ap-1 = 1 (mod p)  avação: Não podemos aplicar o teorema de Fermut se o módulo for um número osto!  sulvos vensão po Teorema:  Seja p um número primo Então,  ap = a (mod p)  tonstração.  Vamos considerar os elementos do conjunto  (n) = Z p - {ō}  = {1, z, z,, p-1}			tial shill shore and	16.1
p não divide a) então,  ap-1 = 4 (mod p)  Descrinção: Não podemos aplicar o teorema de Fermat se o módilo for um núm composto!  - SEGUNDA VERSÃO DO TEOREMA:  Seja p um número primo. Então,  ap = a (mod p)  - DEMONSTRAÇÃO.  Vomus considerar os elementos do conjunto  U (p) = Z p - {ō}  = {1, 2, 3,, p-1}	so divide a) então, $ a^{p-1} \equiv 1 \pmod{p} $ evação: Não podemos aphiar o tecremo de Fermat so o módulo for um número osto!  Sulva Versão Do Tearéma:  Seja p um número prima. Então, $a^p \equiv a \pmod{p}$ tonstanção:  Vamos considerar os elementos do conjunto $ a^p \equiv Z_p - \{\vec{o}\} $ $ \equiv \{\vec{1}, \vec{2}, \vec{3},, \vec{p-1}\} $	- PEQUEND TEOREHA DE FERMAT	;		
p rão divide a) então,  ap-1 = 4 (mod p)  OBSERVAÇÃO: Não podemos aplicar o tecremo de Fermat se o módilo for um núm composto!  - SEGUNDA VERSÃO DO TEOREMA:  Seja p um número primo. Então,  ap= a (mod p)  - DEHONSTRAÇÃO:  Vomus considerar os elementos do conjunto  U (p) = Z p - {ō}  = {1, 2, 3,, p-1}	so divide a) então, $ a^{p-1} \equiv 1 \pmod{p} $ evação: Não podemos aphiar o tecremo de Fermat so o módulo for um número osto!  Sulva Versão Do Tearéma:  Seja p um número prima. Então, $a^p \equiv a \pmod{p}$ tonstanção:  Vamos considerar os elementos do conjunto $ a^p \equiv Z_p - \{\vec{o}\} $ $ \equiv \{\vec{1}, \vec{2}, \vec{3},, \vec{p-1}\} $	Seja p um nûnaero p	rimo. Seja a um inte	piro tal que la to (mod b), (	isto
DOSERVAÇÃO: Não podemos aplicar o teoremo de Fermat se o módulo for um núm composto!  - SEGUNDA VERSÃO DO TEORÉMA:  - Seja p um número primo. Então,  - DEMONSTRAÇÃO:  Vamos considerar os elementos do conjunto  U (n) = Z p - {ō}  - {ī, z, z,, p-4}	EVAÇÃO: Não podemos aplicar o teoremo de Fermat se o módulo por um número posto!  Supon versão Do Teorema:  Seja p um número primo. Então,  a? = a (mod p)  tonistração:  Vamos considerar os elementos do conjunto  col = Zp - {ō}  = {1, 2, 3,, P-1}		- 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1		
DBSERVAÇÃO: Não pudemos aplicar o teoremo de Fermat se o módilo for um núm composto!  - SEGUNDA VERSÃO DO TEOREMA:  Seja p um número primo. Então,  a P = a (mod p)  - DEMONSTRAÇÃO:  Vamos considerar os elementos do conjunto  U col = Z p - {ō}  = {1, z, 3,, p-4}	evação: Não podemos aplicar o teoremo de Fermat se o módulo for um número osto!  Sunoa versão Do Teorema:  Seja p um número primo. Então, $a^p \equiv a \pmod{p}$ tonistração:  Vamus considerar os elementos do conjunto $a^p \equiv \{\overline{1}, \overline{2}, \overline{3}, \dots, \overline{p-1}\}$	a P-1 = 1 (mod p)			
- SEGUNDA VERSÃO DO TEORÉMA:  Seja p um número primo. Então, $a^{p} = \alpha \pmod{p}$ - DEHONSTRAÇÃO:  Vamos considerar os elementos do conjunto  U (p) = $\mathbb{Z}_{p} - \{\bar{0}\}$ $= \{\bar{1}, \bar{2}, \bar{3},, \bar{p}-A\}$	SUNDA VERSÃO DO TEORÉMA:  Seja p um número primo. Então, $a^{p} \equiv \alpha \pmod{p}$ HONSTRAÇÃO:  Vamos considerar os elementos do conjunto $(n) = \mathbb{Z}_{p} - \{\bar{o}\}$ $= \{\bar{1}, \bar{z}, \bar{3},, \bar{p-4}\}$		olicar o teoremo de Ferm		
Seja p um número primo. Então, $a^{p} = a \pmod{p}$ - Demonstração. $V_{amos} = considerar os elementos do conjunto$ $U(p) = \mathbb{Z}_{p} - \{\bar{o}\}$ $= \{\bar{1}, \bar{z}, \bar{3}, \dots, \bar{p-1}\}$	Seja p um número primo. Então, $a^p \equiv \alpha \pmod{p}$ Honstenção:  Vamos considerar os elementos do conjunto $a^p \equiv Z - \{\bar{o}\}$ $a^p \equiv Z - \{\bar{o}\}$ $a^p \equiv Z - \{\bar{o}\}$	composto.;			
$Q^{P} = \alpha \pmod{p}$ - DEMONSTRAGEO.  Vamus considerar os elementos do conjunto $U(p) = \mathbb{Z}_{p} - \{\overline{0}\}$ $= \{\overline{1}, \overline{2}, \overline{3}, \dots, \overline{p-1}\}$	$a^{P} \equiv \alpha \pmod{p}$ Nonstrangão.  Vamos considerar os elementos do conjunto $a^{P} \equiv \alpha \pmod{p}$ $a^{P} \equiv \alpha \pmod{p}$ $a^{P} \equiv \alpha \pmod{p}$ $a^{P} \equiv \alpha \pmod{p}$	- SEGUNDA VERSÃO DO TEORES	ላች:	5	
- DEMONSTRAÇÃO:  Vamos considerar os elementos do conjunto $U(p) = \mathbb{Z} p - \{\bar{0}\}$ $= \{\bar{1}, \bar{2}, \bar{3}, \dots, \bar{p-1}\}$	Vomos considerar os elementos do conjunto $cp1 = \mathbb{Z} p - \{\bar{0}\}$ $= \{\bar{1}, \bar{2}, \bar{3}, \dots, \bar{p-1}\}$	Seja p um número p	primo. Então,		
Vamos considerar os elementos do conjunto $U(p) = \mathbb{Z} p - \{\vec{0}\}$ $= \{\vec{1}, \vec{2}, \vec{3}, \dots, \vec{p-1}\}$	Vamos considerar os elementos do conjunto $ cp1 = \mathbb{Z}_p - \{\vec{o}\} $ $ = \{\vec{1}, \vec{2}, \vec{3}, \dots, \vec{p-1}\} $	ap = a (mod p)	(° 7'		- , b
Vamos considerar os elementos do conjunto $U(p) = \mathbb{Z} p - \{\vec{0}\}$ $= \{\vec{1}, \vec{2}, \vec{3}, \dots, \vec{p-1}\}$	Vamos considerar os elementos do conjunto $ cp1 = \mathbb{Z}_p - \{\vec{o}\} $ $ = \{\vec{1}, \vec{2}, \vec{3}, \dots, \vec{p-1}\} $	0 1	2	<u> </u>	
$U(p) = \mathbb{Z}_{p} - \{\vec{o}\}$ $= \{\vec{1}, \vec{2}, \vec{3}, \dots, \vec{p-4}\}$	$cp1 = \mathbb{Z}_{p} - \{\vec{o}\}$ $= \{\vec{1}, \vec{2}, \vec{3}, \dots, \vec{P}-1\}$	- DEMONSTRAÇÃO .	-	32.00	
$U(p) = \mathbb{Z}_{p} - \{\vec{o}\}$ $= \{\vec{1}, \vec{2}, \vec{3}, \dots, \vec{p-4}\}$	$cp1 = \mathbb{Z}_{p} - \{\vec{o}\}$ $= \{\vec{1}, \vec{2}, \vec{3}, \dots, \vec{P}-1\}$			Est properties	_
$= \left\{ \overline{1}, \overline{2}, \overline{3}, \dots, \overline{p-4} \right\}$	$= \left\{ \overline{1}, \overline{2}, \overline{3}, \dots, \overline{P-\Lambda} \right\}$	Vamos considerar os eleme	ofrijnos do conjunto		ı
$= \left\{ \overline{1}, \overline{2}, \overline{3}, \dots, \overline{p-1} \right\}$	$= \left\{ \overline{1}, \overline{2}, \overline{3}, \dots, \overline{P-\Lambda} \right\}$			(rua) : 3 = x	i è
$= \left\{ \overline{1}, \overline{2}, \overline{3}, \dots, \overline{p-1} \right\}$	$= \left\{ \overline{1}, \overline{2}, \overline{3}, \dots, \overline{P-\Lambda} \right\}$	U(p) = Zp - {o}			
			- (+		, k
In board of a continue of a college with internal more material and a college of the college of	In bond of the analysis of the				
The same and applications of a citizen with internal man and a significant of the same and a sig				(a k - 1 d -	
The same and also server a college and later a man and a significant and a significa					
The same was also server a college of the fact of the same of a six	(a Land d'as a x				
	(a ball d'alexante de la companya de	A state and make a series	the a solution was	Constitution of the second	
	The same and the s			folioned disex	
	And a second sec				

tilibra



		)							
Logo,	como 3	lodos os	mimoros da	lista	da esqueda são distintos modo	lop, então to-			
% 05 no	meros	da lista	da direlta	. tam	bém são distintos módulo p				
Asim	, ambo	as as li	stas contév	n P-	1 números distintos módulo p.				
		tem p-1		sofnites	em Ucpi. Logo, ambas as li	stus contém to-			
Porta	nto, o	otuborg	dos númer	ros no	a primeira lista vai ser igual	, ao produto dos			
		gunda lista			Μόρυισ	P			
4.2.3.	•(p	1) = 1·a·	Z·a·3·a·	· (r-4)·	a (mud p)	arthur de			
			(q bon		111				
,	P-4 = 1	(q bom)	1.		17.60.51	8. 7. 5. Al.			
U Tes	rema b	e termat	pode nos	avžilia	r no cálculo de potências módo	£			
ettle.	0:103					No.			
,10,11	,				p 10 1	669			
12542683	(mad	403)							
						1 1/2 11/2 11/2 1			
	SEN FE	PRHAT			COM FERMAT				
	00,,				I a la l				
18	A	16	É IMPAR ?		2102 = 1 (mad 403)				
man A C	2	125 PC83	514	12					
2	4				12572683=102 . 123 261 + 64	(1-1) show 8 9			
4	1	2100	ghom Si	10 CE	0 360 b 9 C	resto			
		,				10CIENTÉ			
					242572693 = 2102.123261764 = (2	123254 64 102) · Z			
					2 = 2 de han 1 = (2	102			
	i de la companya de					111 111 111 111 1			

R	9	E	E MODE?			1 1/42	
4	٤	64	SIM				
2	4	30	NÃO			11.42	
2	16	15	3111				
38	50	7	SIM				
55	28	3	SIH				
98	63	1	SIM		OFF	<u> </u>	A
47	55	0	NÃO		TR	N.Y	}
		v		2004	2,48	SP.	1
54268	3 = 2 <sup>61</sup>	= 97 (	mod 103)	hila	15	652	)
					Uh.	<b>F</b> 3	,1
Se	gavo cal	icular a	modulo p, com	n p primo:		8.4	Ę.
							7.

Seja n' um número inteiro positivo e a um inteiro tal que 1 < a < n. Se n for primo, pelo Teoremo de Format,

an-1 = 1 (mod n).

Pensando nisso de forma reversa, se ant ± 1 (mod n), então n à compose-

TESTE DE FERMAT:

Dado um inteiro n e um inteiro + < a < n, se a + + (mod n), entaño n é composto. Neste caso, dizernos que a é uma testemunha que n é composto.

Exento: n = 344

Q=3

TESTE: 3340 = 56 \$1 (mod 341)

R	A	Ε	É IMPAR
1	3	340	A)ÃO
4	9	170	NÃO
1	81	85	SIM
81	82	42	NÃO
84	245	21	SM
67	9	10	NÃO
67	84	5	SIM
312	82	2	NÃO
312	245	1	SiM
56	9	0	NÃO

PERGUNTA: E se tivéssemos escolhido a= 2?

2340 = 1 [mod 344]

( - L + 1 / - 1)				
	E IHOUR	ε	A	R
64 NG NG NG	NÃO	340	2	1
	N30	170	41	1
	SIM	85	16	1
188(31) 34 NEW **	N70	412	256	16
	5111	21	64	16
and the second second	NÃO	10	10, 4 + 1	- Albertas
Current and the last and	SIM	5	16	4
Lacyal + 1 "s"	พลัง	2	256	16
a vide	514	1	64	16
	NÃO	. 0	4	1

Sá sabia que 344 era composto, mas obtive 2300 = 4	(med 341). Logg se and 34
(mod n), não posso conclur nada. n pode ser primo ou	
n é composto com carteza e a la l	a é lestemanha de que n é
n a" #1(modn)	sould descript me is 198
$a^{n+1} \equiv 1 \pmod{n}$	
	punt a base 2.
n pode ser primo	
OV	
a pode ser composto	- and and the same
<del></del>	
Dizemos que n é um paudopriv	no para a base a
DEFINIÇÃO: Se n é composto, mas and E1 (modn), entá a base a.  Fixado um a, existem mais primos (verdadeivos) do qua.  Exensicas de 1 ATÉ 109	ve porado primos para a bisse
L> 50 847 584 PRIMOS	only in the describing
L> 5597 PSEUDO PRIMOS PARA A BASE Z	and an adult of I
L> 1272 PSEUDOPRIMOS PARA AS BASES 2 E 3.	
and the continue to an endine a second	
CONCLUSÃO: O Teste de Fermat tem duas respostas possíve	13.
L> COMPOSTO (CENTEZA)	
L> INCONCLUSIVO (PORE SER PAIND ON COMPUSTO)	
	1987年上月
	and the second s
	tilibra