THE THE TENERAL OF THE PE JUNETIN	UFRS - Universidade	Federal	do	Rio .	le Sameiro
-----------------------------------	---------------------	---------	----	-------	------------

Aio de Janeiro, 02 de Maio de 2017

(X = 1 (mod 13)	Ŗ	Q	×	Y	
(X = 4 (mod 15)	13	_	1	c	
(x = 8 (mod 19)	15	_	0	4(00)	f bore was a m
	43	0	1	O	
X = 1 + 13 K	2	1	51	1	1
1+131 = 4 (mod 15)	4	6	7	-6	1 12 pm
13K = 3 (mod 15)	0	2	_	-	

7.13K = 7.3 (mod 15)

K = 21 (mod 15)

K = 6 (mod15)

K= 6 + 12 l

X = 4143 K

X= 1+13(6+152)

RE 1 +78+ 495 &

2=79+1952

x=79 (mod 195)

X = 79 (mod 195)

(Pt Gom) 8 =x

-> x=79+195R

79+1952 = 8 (mod 19)

3+52=8 (mod 10)

52 = 5 (mod 19)

REA (mod 19)

2= 1+ 19 m

tilibra

X= 79+195 R X= 19 + 195 (1+19 m) X= 79+ 195+3705 m X= 274 + 3705 m X = 274 (mod 3705) Esse método de resolução de sistemas de congruências é conhecido como Algoritmo Chinas do Aesto - TEOREMA CHINGS DO RESTO Séjam m c n inteiros positivos tais que MDC(m,n)=1. Então, o sistema: sempre tem uma única solução módulo mn. - EXISTÊNCIA (PROVA CONSTRUTIVA) x=a (mod m) x = at mx 1201 bom) pt : x + x = b (mod n) atmk = b (modn) m K = (b-a) (mod n) Preciso calcular o inverso de m módulo n. Como MDC (m,n)=1, esse inverso existe e pode ser obtido com o algoritmo evolidiano estendido. Seja m'

este inverso, m'é o inverso de m modulo n.

tilibra

P chia U
•
entre m en
AL y
,
(mbord n2x)
(n ben) d Ix)
is I am allow
(x) frambon) sxf,x
(m bon) DIV
(whom) de px
(m bum) o =,X
love me (n bon) die
(abor) O = x - x
VI.
X - X shirt m
1-1- ml d = x
Conseque Colored as a
Calal Os x a
10
1× 1× 060000
3 F. 40.000
om S CX 11 SC C
2000

tilibra

1				7 to see the second
	-	-		100 1 5 105 410
				12 1-13 -111
o mh.				the rest of the second
				In my
			1+1	W- 1- 1- 1- 1
		1	1	hum stimm
R	a	X	Y	bom 1 S S m
3	_	4	0	244455m
7	_	0	1	
3	0	4	6	P _ 2
4	2	-2	1	- 1 = 1 1 1 4 10 -
0	3	-	FA	E= 4 [] 1 P _
			٧	1593-1994
	6		. /	
				The selection a
			U.E.	Lt. Le una yindaya
7-R=3 (mod 11)				
λ:	= 4714	M		
Nust D	(24)	Luci		<u> </u>
x= 7.	+212 =			The state of the
= 71	121(4)	11m)		
= 7+84+231m				
= 91	1+234 ~	1		
				FF T
PEK	1 (mod	231		
	Market of the second of the se	•		F ₂ () = 0
ra seli				
	R 3 1 3 1 0 7+24 7+10 110= 7-2 2 2 2 3 1 1 0	R Q 3 - 7 - 3 0 1 2 0 3 7+24	R Q X 3 - 1 7 - 0 3 0 1 1 2 -2 0 3 - 2 0 3 - 2 102-1 (mod 11) 7-2=3 (mod 11) 2=4 (mod 11) 2=4 (mod 11) 2=4+11 m x=7+212= =7+21(4+11m)	R Q X Y 3 - 1 0 7 - 0 1 3 0 1 6 1 2 -2 1 0 3 100 3 1100 3

/_ /)		And the last of th		•		1	
91+ 231 m = 2 (mod 19)		R	Q	WAXON!	×	* July	<u> </u>
15+ 3m = z (mod 19)		3	-	1	0		
3m = -43 (mod 44)		19	Lance and	0	1		
Bm = 6 (mod 19)		3	0	1	0		
13-3 m = 6.13 (mod 14)		4	6	-6	1	1	
m = 78 (mod 19)		0	3	_			
m = 2 (mod 19)					(2)	1 - v	
m=2+19 n							
					() (jes.)	AIN	
x= 91 +231 m=				()	ap (100)	5 1	
= 94 + 231 (2+19 n) =							
= 44+462+4389n=					To be	JASKÉ	
= 553 + 4389 n						FIFT	
ALGORITMO CHINDS DO RESTO PAC		Porducia				n : NEW - E N & 1 E n & - E n & e	
ALGORITMO CHINES DO RESSO PAC 26754 (modulo 1455)	A CÁLCULO OF	ortgine/v		1(4.1		8 K E E E E E E E E E E E E E E E E E E	
ALGORITMO CHINSS DO RESSO PAC 26754 (modulo 1155) Não posso fazer 2 = 1 (A CÁLCULO OF	ortgine/v		1(4.1		8 K E E E E E E E E E E E E E E E E E E	0
ALGORITMO CHINES DO RESSO PAC 26754 (modulo 1455)	A CÁLCULO OF	Putilancia) teore		1(4.1		8 K E E E E E E E E E E E E E E E E E E	0
ALGORITMO CHINBS DO RESSO PAC 26754 (modulo 1155) Não posso fazer 2 154 = 1 (η Εάι ευιο οξ ς mod 1155).	Puténcia) teore		1(4.1	số é v	8 K E E E E E E E E E E E E E E E E E E	
ALGORITMO CHINES DO RESSO PAC 26754 (modulo 1155) Não posso fazer 2 1154 = 1 (mod 1155).	Putilancia Deleve		1(4.1	số é v	áliolo se	
ALGORITMO CHINES DO RESSO PAC 26754 (modulo 1155) Não posso fazer 2 ¹¹⁵⁴ = 1 (Undo for primo.! Correço fatorando:	mod 1155).	Detension		1(4.1	56 é v	álido se	×
ALGORITMO CHINBS DO RESSO PAC 26754 (modulo 1155) Não posso fazer 2 154 = 1 (mod 1155).	Detension		1(4.1	56 é v	áliolo se	×
ALGORITMO CHINÈS DO RESSO PAC 26754 (modulo 1155) Não posso fazer 2 154 = 1 (Vulo for primo.! Correso fatorando:	mod 1155).	De leore		1(4.1	56 é v	alido se	×
ALGORITMO CHINES DO RESSO PAC 26754 (modulo 1455) Não posso fazer 21154 = 1 (Vilo for primo.! Corrego fatorando:	mod 1155).	De leore		1(4.1	56 é v	alido se	×
ALGORITMO CHINES DO RESSO PAC 26754 (modulo 1455) Não posso fazer 2 1154 = 1 (Volo for primo.! Corrego fatorando: 1155 = 3.5.7.11 Vou calcular:	mod 1155).) teore		1(4.1	56 é v	alido se	*
ALGORITMO CHINÈS DO RESSO PAC 26754 (modulo 1155) Não posso fazer 2 154 = 1 (Vulo for primo.! Correso fatorando:	mod 1155).) teore		1(4.1	56 é v	alido se	X.

E gludom	µF €N BX
2 \$ 0 (mod 3)	(7 pm) 1 8 + 8 + 8 +
$2^2 \equiv 1 \pmod{3}$	(bont to set
$2^{6754} \equiv (2^2)^{33+7} \equiv 4 \pmod{3}$	/2 hom) 1 5 x
1 ₁₁	Q 2 4 Y = 34
- Mô DUZO 5	= 113 x =
	(27++18475
2 \$0 (mod s)	= 171+841=
2 = 1 (mods)	= 1 - 1 - 2 - 2 - 1 - 1 - 1 - 1 - 1 - 1 -
26754 = (24) 1688 · 22 = 4 (mod 5)	
11	(+pom) == 2711A
	(Phanle-17
- HÓDULO 7	(1 bun 1 2 - = 2 1 miles)
2 to (mod 7)	(Y 62 1 7 = 6
26 = 1 (mod 7)	
26454 = (28) 1125 · 24 = 16 = 2 (mod 7)	m = +2=1
1)	= 9=8+1-=)
- Hôpuzo 14 .	= /m=+ 121410 -
2 0 (mod 11)	2/_300 + 71 + 42
2" = 1 (mod 11)	7 CIA+ F
26754 = (210) 075 = 16 = 5 (modan)	
2 -2 2 = 10 - 3 (mooth)	(ALICA) 7 = 10 7011 P
1	1 EL DA TO CO TO COLLE
(x=1(moda)	(II bom) 8 = mod 1)
	(1+ hum + - mo
X = 4 (mod 5)	
$X \equiv 2 \pmod{7}$	(1) Luni Timy
(X = 5 (mod 11)	
CONTINUE PRIMOS DISTINTOS	· · · · · · · · · · · · · · · · · · ·
	tilibro

X=113x 113x= 41 (mod 5) X= 1 (mod 5) K= 1 (mod 5) K= 1+52 X=1+3X= = -1+3(1+52) = 1+3+152= = 4+152 4+152 = 2 (mod 7) 4+1 = 2 (mod 7) 2= 5 (mod 7) 2= 5 (mod 7) 2= 5 (mod 7) 2= 5 (5 + 7 m) = -1				r
$3x = 4 \pmod{5}$ $x = 1 \pmod{5}$ $x = 1 + 3x = 2 \pmod{7}$ $2x = 1 + 3x = 2 \pmod{7}$ $2x = 1 + 3 + 15x = 2 \pmod{7}$ $2x = 1 + 3 + 15x = 2 \pmod{7}$ $2x = 1 + 3 + 15x = 2 \pmod{7}$ $2x = 1 + 3 + 15x = 2 \pmod{7}$ $2x = 1 + 15x = 2 \pmod{7}$ $2x$	X= 1+3 K			
$3x = 4 \pmod{5}$ $x = 1 \pmod{5}$ $x = 1 + 3x = 2 \pmod{7}$ $2x = 1 + 3x = 2 \pmod{7}$ $2x = 1 + 3 + 15x = 2 \pmod{7}$ $2x = 1 + 3 + 15x = 2 \pmod{7}$ $2x = 1 + 3 + 15x = 2 \pmod{7}$ $2x = 1 + 3 + 15x = 2 \pmod{7}$ $2x = 1 + 15x = 2 \pmod{7}$ $2x$				(Lhorn of s
K = 1 + 51 $K = 1 + 51$ $X = 1 + 31$ $X = 1 + 3 + 152 = 2 + 4 + 152$ $= 2 + 4 + 152$ $4 + 152 = 2 + 4 + 152$ $4 + 152 = 2 + 4 + 152$ $4 + 152 = 4 + 152 = 2 + 152 = 2 + 152 = 2 + 152$				11111111 1 1 1 5
			1. 1	1 016
x = 1+3x = $= 1+3(1+5x)$ $= 1+3+15x =$ $= 4+15x =$ $= 4+15x =$ $= 4+15x =$ $= 4+15x =$ $= 1+3x =$	K = 1 (mod 5)			
$x = 1+3x =$ $= 1+3(1+5x)$ $= 1+3+15x =$ $= 4+15x =$ $= 4+15x =$ $= 4+15x =$ $= 4+15x =$ $= 2 \pmod{7}$ $4+1 \le 2 \pmod{7}$ $4+1 \le 2 \pmod{7}$ $2= 2 \pmod{7}$ $2= 2 \pmod{7}$ $2= 3 \pmod{7}$ $2= 3 \pmod{7}$ $2= 3 \pmod{7}$ $2= 3 \pmod{7}$ $3 \ge 3 \ge 7$ $3 \ge 7$ $4 \ge 7$	K= 1+52			
=1+3+15l= $=4+15l=$ $=4+15l=$ $=4+15l=$ $=4+15l=$ $=1+15l=$ $=1$	X = 4+3× =			7 u.m. M =
$= 4+15$ \(\frac{1}{2} \) 44+15 \(\left\) = 2 \(\left(\text{mod } \frac{1}{2} \) $= 2 + 15$ \(\left(\text{mod } \frac{1}{2} \) $= 2 + 16$ \(\text{mod } \frac{1}{2} \) $= 2 + 16$ \(\text{mod } \frac{1}{2} \) $= 2 + 16$ \(\text{mod } \frac{1}{2} \) $= 2 + 16$ \(\text{mod } \frac{1}{2} \) $= 2 + 16$ \(\text{mod } \frac{1}{2} \) $= 2 + 6$ \(\text{mod } mod				
$\begin{array}{cccccccccccccccccccccccccccccccccccc$				
4+15 $Q \equiv 2 \pmod{7}$ 4+1 $Q \equiv 2 \pmod{7}$ $Q = -2 \pmod{7}$ $Q \equiv 5 \pmod{7}$ $Q \equiv 5 \pmod{7}$ $Q \equiv 5 \pmod{7}$ $Q \equiv 4 \pmod{7}$ $Q \equiv $				I Land He
$4+1=2 \pmod{1}$ $2=-2 \pmod{1}$ $2=5 \pmod{4}$ $3=5 \pmod{4}$ $3=5$	-4+15 X			E = 1 (E) = - 14.
$4+1=2 \pmod{1}$ $2=-2 \pmod{1}$ $2=5 \pmod{4}$ $3=5 \pmod{4}$ $3=5$	4+15 & = 2 (mod7)) () }
$ \begin{aligned} 2 &= -2 \pmod{4} \\ 2 &= 5 \pmod{4} \\ \end{aligned} $ $ \begin{aligned} 2 &= 5 &\neq 7 \\ 2 &= 4 + 15 \neq 105 \\ 2 &= 4 + 105 \\ 2 &= 4 + 105 \\ 3 &= 5 \pmod{41} \\ 2 &= 6 \\ 6 &= 3 \pmod{41} \\ 2 &= 6 \\ 6 &= 2 &= 3 \\ 6 &= 4 &= 4 \\ 6 $				
$ \begin{array}{llllllllllllllllllllllllllllllllllll$				4 300,41-
$ \begin{array}{llllllllllllllllllllllllllllllllllll$				(16 grate
x = 4145 = = 4145 ($547m$) = = 4145 ($647m$) = = 4145 ($647m$) = 414 ($647m$) = 41				(that the
$ \begin{array}{cccccccccccccccccccccccccccccccccccc$	l=5+7m	(to bear	10 2 2 (= F((3) - Fees
$ \begin{array}{cccccccccccccccccccccccccccccccccccc$				1
$ \begin{array}{cccccccccccccccccccccccccccccccccccc$	X=415Q=			
$ \begin{array}{c ccccccccccccccccccccccccccccccccccc$	= 9+ 15 (5+7m) =			the gasalis
$ \begin{array}{c ccccccccccccccccccccccccccccccccccc$	= 4+ 75 + 105m)=			1116.01.515
79+105 m = 5 (mod 11) 2+6m=5 (mod 11) 6 - 1 6 m=3 (mod 11) 11 - 0 1 2-6m=2-3 6 0 1 0 m=5 (mod 11) 1 1 2 -1 m=5+11 n				(04/00)-6=0,
$ \begin{array}{cccccccccccccccccccccccccccccccccccc$		(ALL ON)	7 = 4	E HE ME GE HOUSE
$2 + 6m = 5 \pmod{11}$ $6m = 3 \pmod{11}$ $11 - 0 1$ $2 \cdot 6m = 2 \cdot 3$ $6 0 1 0$ $m = 6 \pmod{11}$ $5 1 - 1 1$ $1 2 - 1$ $m = 6 + 11 $ $0 5 - 1$	79+105 m = 5 (mod 14)	, Q	(a)	× } Y
$6m = 3 \pmod{11}$ $2 \cdot 6m = 2 \cdot 3$ $6 0 1 0$ $m = 6 \pmod{14}$ $5 1 -1 1$ $1 1 2 -1$ $m = 5 + 11 0 5 -1 -1$		6	_	1 0
$2.6m = 2.3$ $m = 5 \pmod{44}$ $5 \qquad 1$ $1 \qquad 2 \qquad -1$ $m = 5 + 41$ $0 \qquad 5 \qquad -1$		11	-	0 (61840) 10
$m = 6 \pmod{14}$ $5 \qquad 1 \qquad -1 \qquad 1$ $1 \qquad 1 \qquad 2 \qquad -1$ $m = 5 + 11 \qquad 0 \qquad 5 \qquad -1 \qquad -1$	And the second s	6	0	1 1 60 - 3
m = 5 + 41	The Control of the Co	2	1	-4 (F/164) Page
m=5+11n	111	1	1	2 (0) (0-1)
m = 64 M/V	- r d 41 a	0		10-11-
	tilibra			

7= 79+105 m =	
= 79+405 (6+110) =	
= 79+ 630 + 1155n	
= 709 + 1155 n	
X= 709 (mod 1155)	
26754 = 709 (mod 1155)	
concusão: Quando o módulo é composto, mas é o produto de puiso usar o alguritmo chinés do resto em conjunto com o Teor cilitar o cálculo de potências.	
- MATÉRIA DA PZ:	
CAPÍTULO 5 - COLLIER (EXCETO "PRINCIPIO DA INQUEÃO") CAPÍTULO 3 - COLLIER CAPITULO 3 - COLLIER PRATES EQUIVALENTES DOS CAPITULOS 2 E 3 DO MENASC	NÆ
	tilibra