			1 1
UFRS- Universidade Federal	do Rio de Sareiro		= 437
Bio de Saneiro, 11 de			120
	3		327-1
TEOREMA DA DIVISÃO			d 2 7- 1 20
DA DIVISÃO			100 des
0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1		a nor only to war	1 0
		existem doir inteiros	
mados de quoiente e re	esto da divisão inteira	de a porbl tais que	
0=pd+L			0:6:0
05766			0 - 0
034.50			
		C100700 7- 010	
Além disso os inter	vos q er que satis	fazem estas duas con	ndições são
Únicos.			110-010
Existência -> basta	exitimos uma maneiro	a qualquer de calcular	ester valore
Exemplo: Algoritmo "bobo"			
. 0			0 = 7-7
UNICIOADE -> PADVA	POR CONTRADICAD Sugar	ha pr contradição, que es	
e r ≠ r' tais que'	son son and a corpora	not be consequed die of	usiem, 4+4
		75- 5:	2 - 6:2
a=bqtr	(a=bg'+v'		
05 ~ < 6	06766		
	(=(, , )	20101 64 7 60	
	4		
0=69+		experience a second	a pl
(-) a= b q + 1		out adopted to so	36 303 115 3
	ilea on let or one	to come one steve	50 d 26 dg
p(q-q')=r-r	E) 40%		
onlines south bourson	a continua conta	cab do a major i	- her 130
Soponha sem perda	de generalidade, que	2 7'27	Js a swiss
at		r> 2 20	d
		-	
	· · · · · · · · · · · · · · · · · · ·		
			tilibra

F ( ) 6.47 6-866 05 r'-r 4 b 0 5 6 (0-4) 66 40 James 1000 100 B 0:9-9'44 9-9,20 9=9 9=9' + 9 \$9' -> contamongou b (q-q')=r'-r 6,-1 = O rer r=r' + r +r' -> Commonio lago, qe r são únicos. Squim a e b dois interes, com b to, dicemos que b divide a ou b édirisor de a ou b é fator de a ou a é divisível por b ou a é multiplo de b ac existe um número inteiro x tal que a = b.x.

entre a el é o major inteiro d'al que dédivisor de a etambém de b.

- ALGORITMO "INGÉNIO" PARA O CÁLCU-O PO HOC:

Dados a e b, calculo a lista detodos os divisores de a, calculo a lista de todos os divisores de b e busco o maior inteiro que aparece nas duas listas. Los é extremamente lento.

- ALGORITHO MAIS CFICIENTS: ALGORITHO EVELIDIANO

-EMEMPLO : MOC ENTRE 1234 & 54 MOC (4234, 54) = 2

	22	, <b>1</b> , ,	5	.4	3	and the same
1294	54	n 46	× 8	<b>73</b> 6	70-	HDC .
-	46	8	6	z	0,,	an areal m

- Dividir 1234 por 54 -> q= 22 - HOU GENÉRICO MUNTE:

a= bq+r+ 0 = r+ 6

- Dividir 54 par 46 -> q= 1 b= +192 tre 05 12 < 14

r=8 r= r2 q3+ r3 0 5 r3 6 r2

- Dindir 46 por 8 -7 9= 6 9= 511 9112 + 1312 0 < 1312 < 1311

 $r_{n-2} = r_{n-1} \cdot q_n + r_n$   $= D_{\text{ividir}} \cdot 8 \cdot p_0 \cdot 6 \Rightarrow q = 1$ 

r = 6

Y= Z L> técnino

- Dividir 6 por 2 -> 9=3 - 0 MDC & o Oltimo resto diferente de O.

-> HOC (a, w) = r n-1

VAMOS MUSTROR QUE O ALBORITMO SCHORE TERHING : P>41 245 243 5 5 7 5 0 Todos os restos são interros. Existe uma quantidade Pinita de interros entre b e O. Logo, em algum momento, algum dos restos da sequência será igual a O. e o algoritmo terminára. - VANOS MOSTRAR QUE O ALGORITMO PRODUZ O RESULTADO CORRETO, 1510 É, QUE O ÚL-TIMO RESTO DIFERENTE DE ZERO É REALMENTE O MOC ENTRE A E B: Para isso precisamos de um lema auxiliar. Leng: sejam or, le, g e S inteiros positivos tais que a= byts. Então, HOC (a, b) = MDC (b,s) Seja di= HDC (a,b) e do= MDC (b,s). Quero mostrar que di=do. > 0=01.K dy = HDC (a,b) > b= b, l a= bg ts 0, K = d, l + 5 14K-01lg=S a, (x-lg)=5 d. DIVIOG 5 > di é divisor comum de bes. of divide 5

tilibra

Como de á o máximo divisor comum de bes, então desde  de thoc(s, s)  De de m  De bes en m  De bes en máximo divisor comum de a e b  de divide a de de máximo divisor comum de a e b  Como de é o máximo divisor comum de a eb, então de de  de divide la  De pode nos dar mais o algoritmo exclutiano, ala pode nos dar mais de  De vións alám do MOC.  Les Alboritmo Cocentras de Staveno (pronoco no knota)  Dudos dois interos partiros a e b, quere calcular dois interos (mão necessamente positivos) a e P tais que:  ace a + P b = d.  Aleccumo Senço Proundo Generocamente (per una phonum)		120		
b=d2·m  b=d2·m  b=d2·m  A=byts  a=d2·my td2·n=d2·(mytn)  d2· anvior A  common d2· a common de a common		(**)		
b=d2·m  b=d2·m  b=d2·m  A=byts  a=d2·my td2·n=d2·(mytn)  d2· anvior A  common d2· a common de a common	Como de é o mas	imo divisor comum d	e bes então	01 5 95 THE
de HDC(b,s)  S=de n  S=de n  A=bg+s  a=de mg+de n = de (mg+m)  de nome A  de divide a  de divide b  Como de é o máximo divisor comum de a e b  de divide b  Como de é o máximo divisor comum de a e b  de de de de nome de nome de a e b  de de de de nome de			• • • • • • • • • • • • • • • • • • •	
S=d2·n  a=bg+s  a=d2·mg+d2·n=d2·(mg+n)  d2·bivide a  d2·divide b  Como d4·é o máximo divisor comum de a eb  d4·2 divide b  Como d4·é o máximo divisor comum de a eb, enlão d2·éd4  d1·2 d2  d2·2 d4  d4·2 d2  d2·2 d4  Befinando um pouco mais o algoritmo euclidiano, ale pode nos dar mais de us utáis alám do MDC.  L> Aleanitmo cucationemo Esteurino (proreso no neuvin)  Budos dois inteiros positivos a e b, quero calcular dois inteiros (mão miceso amente positivos) a e P tais que?  amente positivos) a e P tais que?		b = d2 · m	372 207 3	E 4 1 E 2
a=bgts  a=d2mg+d2n=d2 (mgtm)  d2 nwive A  como d1 é o maximo divisor comum de a e b  d1 divide b  como d1 é o maximo divisor comum de a e b  d2 divide b  como d1 é o maximo divisor comum de a e b, então d2 \( \delta \) \( \del	d2 = HDC(0,0)		*	:
a=bgts  a=d2mg+d2n=d2 (mgtm)  d2 nwive A  como d1 é o maximo divisor comum de a e b  d1 divide b  como d1 é o maximo divisor comum de a e b  d2 divide b  como d1 é o maximo divisor comum de a e b, então d2 \( \delta \) \( \del		S=d2·n	17 3 03 0	7+ 19
a=bg+s  a=d2mg+d2n=d2(mg+n)  d2 DNIDE A  d2 divide a  d2 divide b  Como d4 é o maximo divisor comum de a eb, então d2 d4  d1 > d2  d2 > d1  d2 > d1  Definando um pouzo mais o algoritmo euclidiamo, ale pade nos dar mais de a utáis alám do MDC.  L> ALECATIMO CUCLIDIAMO ESTENDIDO (PROPOSO POR KRUTH)  Dados dois inteiros positivos: a e b, quero calcular dois inteiros (mão miceso amente positivos) ~ e & tais que:  como d4 é o MDC (a,b)	la la			
a=d2 mg +d2 n = d2 (mg+n)  d2 price A  d2 divide a d3 divide b  Como d4 é o maximo divisor comum de a eb, então d2 d4  d4 divide b  Accominanto um pouco mais o algoritmo euclidiamo, ale pade nos dar mais de su vitárs além do MDC.  L> Alecanmo cucaranmo esteurino (recroso roc knuth)  Budos dois inteiros positivos a e b, quero calcular dois inteiros (mão recesso amente positivos) a e P tais que:  ax-a + P b = d.		,		
de divide a de é divisor comum de a e b  Como de é o máximo divisor comum de a e b, então de é de  de divide b  Como de é o máximo divisor comum de a e b, então de é de  de de de de de de de máximo divisor comum de a e b, então de é de  de de de de de de de de divisor comum de a e b, então de é de  De de de de de de de de de de de de de de	•			
Oz divide a de é divisor commo de a e b  Como de é o máximo divisor commo de a eb, então de éde  de divide b  de divide b  de de o máximo divisor commo de a eb, então de éde  de de de de o máximo divisor commo de a eb, então de éde  de de de de de o máximo divisor commo de a eb, então de éde  de de de o máximo divisor commo de a eb, então de éde  de de o MOC (a,b)  de de o MOC (a,b)	9	all the same of th	045 450	7 4 P 4
de divide b  Como de é o máximo divisor comum de a eb, então de éd.  de divide b  Como de é o máximo divisor comum de a eb, então de éd.  de d				
Ecomo de é o máximo divisor como de a eb, então de	de divide a d			
Ecomo de é a máximo divisor comum de a eb, então de é de de de a eb, então de é de solar mais de de es estás além do MDC.  Ly Alboratmo cucerosmo estevarios (recosso ros xxvita)  Budos dois inteiros positivos: a e b, quero calcular dois inteiros (não necesso amente positivos) a e P tais que:  anente positivos) a e P tais que:		2 8 014150x com/m		
Ecomo de é o máximo divisor comum de a eb, então de é de de de o máximo divisor comum de a eb, então de é de so máximo divisor comum de a eb, então de é o MOC (a, b)  Ecomo de é o máximo divisor comum de a eb, então de pode nos dar mais de de so de so máximo evalutados de pode nos dar mais de de so de pode nos dar mais de pode nos de mais de la pode nos de pode nos dar mais de la pode nos de pode nos dar mais de la pode nos de pode nos dar mais de la pode nos de la pode nos dar mais de la pode nos de la pode nos dar mais de la pode nos de la pode nos dar mais dar mai	d <sub>2</sub> provide is	100,1000,00	7 34 7 7+1	(To 14 ) 12 0 7 40
Befinando um pouco mais o algoritmo euclidiamo, ale pode nos dar mais do sutéis além do MDC.  L> ALGORITMO CUCLIDIANO ESTENDIDO (PROPOSO POR KNUTH)  Dudos dois inteiros positivos a e b, quero calcular dois inteiros (não necessamente positivos) « e p tais que:			0	1 X - X - X
Dudos dois inteiros positivos a e b, quero calcular dois inteiros (não necessamente positivos) a e p tais que:  amente positivos) a e p tais que:  aca + P.b = d.	Bermando um pouco	mais o algoritmo euclic		. 9
Ly Alboritho Cucardiano Estendino (Proposo por Knuth)  Dados dois inteiros positivos a e b, quero calcular dois inteiros (não necessimente positivos) a e p tais que:  anente positivos) a e p tais que:  ale d é o MOC (a,b)			1 -10 Page	au mas de
Dudos dois inteiros positivos: a e b, quero calcular dois inteiros (não necessamente positivos) $\alpha$ e $\beta$ tais que: $\alpha \cdot \alpha + \beta \cdot b = d$ ,  ode $d \in a$ MDC $(a,b)$			Dien and water	- d . K + D+ . x /s
Amente positivos) $\alpha \in \beta$ tais que! $\alpha \cdot \alpha + \beta \cdot b = d$ ,  ode $d \in o MDC(a,b)$				
$a \cdot a + 7 \cdot b = d$ , $a \cdot a + 7 \cdot b = d$ , $a \cdot a + 7 \cdot b = d$ , $a \cdot a + 7 \cdot b = d$ , $a \cdot a + 7 \cdot b = d$ ,			I D. MICHALL QUIZ	interest indo peces
$a \cdot a + 7 \cdot b = d$ , $a \cdot a + 7 \cdot b = d$ , $a \cdot a + 7 \cdot b = d$ , $a \cdot a + 7 \cdot b = d$ ,	Marine Bostillo		/W3 Were ) 240	
de dé o MDC (a, b)	0x-a + 8.6			0.300 19 1000
ALGORIMO SENDO PROVADO GENERICAMENTE (POS XIMO DÁGINA)  Tilibr				
tilipa	Alcontra Sérios Por	IAND FAMEDICAMENTE (D.	26 - 10 - 1	
rilibr	WEGGEN HO GONDO AKON	HOO BONCKICHLENIE (AC	(NAINU NOONA)	
rilibr				
rilibr				

 $a = ba, +r_1$   $b = r_1a_1 + r_2$   $c = r_2a_3 + r_3$   $c = r_2a_3 + r_3$   $c = r_3a_1 + r_3a_1$   $c = r_3a_1 + r$ 

(A)  $(x_1 \cdot a + y_1 \cdot b = x_1$   $(x_2 \cdot a + y_1 \cdot b = x_2$   $x_3 \cdot a + y_2 \cdot b = x_3$   $x_3 \cdot a + y_3 \cdot b = x_3$   $x_{3,1} \cdot a + y_{3,1} \cdot b = x_{3,1}$ 

x; a+ y, b= (x; a+ y; + b) . 9; + (x; a+ y; t b)

x at y b - x in a 9 jtz - Y jnb 9 jrz = x jrz at y jrz b

(x3-x3+ . 9,12) a+(y3-43+ . 9,12) b= x312 x + x312 b

 $(x) \times_{-1} \cdot \alpha + Y_{-1}b = \alpha \implies x_{-1} = 1 / Y_{-1} = 0$  $(x) \times_{0} \cdot \alpha + Y_{0}b = b \implies x_{0} = 0 / Y_{0} = 1$ 

EVEMPLO NUMÉRICO: MOC (1284, 54) -> PRÓXIMO PÉGINA

1234 54 46	4,00,010	ie o	l ov X		P OU Y	wall 6	31 6	man) 3	h ask
54 46	-		1						
416	1 50	1	1		0				
			0	601	march 1 our	GLISH.	or our	MARK AD	Nan-
Q	22		4		-22				
8	4 41	gutav	-1		23		P = (53	suct,	DOM
6	5		6		-13	1			·
2	4	6	a 71		× 60 160	arws -		01807	
0	3	Ç	) _		۸ ـ	e-1	J	*+3*	
					0	0	ກຸກນັ້ນ 5	ai o Ma	J e.
		Bo- : 1	20-0	ħ	-0:0-1		a e		
					10-1a1 =			8.8	
	5	14250	· 6- 79-	E	8-1-2-6-1-3	2		8	
					= 6 12-1-	13		9	
	l Cogo	718	1-72)	21:	(A-) 1-E	ž.		2	
					_	8		3	
nstda wag	what is made	czysde	J	5 s	0 vo/.v	ab.bad	25	ad 1545	O me
					IGM : 6.				
ide south and I									
100 6952	<del></del>								
	(white )	off Class	0.150	-	t = (a) D	3 4	150	9691 6	io and
				<u>Opedan</u>	Aug.		Tin II	56 7,000	Lyx
- Pg 9					(4			0 L . W	1
54						-40	67	= × 9	