ARITMETICA MODULAR	-purison portami mo mi ajae i progrega	
AUG MODIM D	neorema: seja m um interea positivo:	
{0,m-1}	temos que: (100m) b + d = 0 + 0 (1)	
9 3 - 0000 20 to ms :0	(1) a+b= (a moo m) + (bmoom) (moom	
6 CIO- XMOD m = 0	(moom) (moom) (moom) (moom)	
DIET-DEX-MUD	คลูห์ดูดดูนิยะ ขอ ดอกปุ่มปลิทศาล	
Los exemplo so relogio: 1827 eou	exemplo: calcule o 18570 De (2020 + 2011)	
2) 12 0 no relogion porque modera	por 7.	
12 moo 12 = 0 1 em 00 0 "Universo"	50maão: 2020+2021= (2020 mod 7)+	
mobile val de o cité 11.	(FOOM) (FOOM 1505)	
H= 5 (moors) -> congruência	JUP SOMED S (FOUM) P = OSOS ←	
QUA : 3 C TEC = 2 6 D VEC	a=b (moo) -> a+k = b+k (moo). (1)	
oefinição: sejom a e m intereos	EULO: 5050= A (WOOD) -> 5051= 2 (WOD)	
positivos. Núes denotomos a mod m	E 2070 + 2071 = 4+5 (moo =) 0 100p	
como o resto quando a é dividido parm.	2 = 07037 03 (400m) P = 1505 + 0505	
• 15 mod 12 = 3 mod 12 = 3 mod .	SEXTO: DIQ 5	
votocco pe congivência:	exemple: cornie o lesto (1050 + 1051 + 105)	
-> or usuace die d=p (woom) aberos	Por 7. E SERIC ? DESC . F SOR	
SE a mod mos mod mos E É Fácil	solució: sobemos (pow ex um) que:	
ver que m pivide a-6. Ou seja:	10 20 01 20 1 = 150 + 0505	
15 = 3 (moo 12) m or -	E pero propiedade O pademos Fazer:	
00: 4=2 (m005) (F 90m) & EXC	SENDO 7070 = 4(mod +) ->	
0 3 OC D, MYD 3 UP SSV 000T +	\$0000000 (coom) F = 5000	
20570. Wimero menor	HOS , 7 MOD 7 = 0 , entrão Ficeríamos com:	
das o woonso	9(moo7) (++7(moo7) = (d+0)	
Teorema: a congluência tem as	2 + 3000 WADE @ 0 (1)	
oeguintes propriencoes:	exemplo: carche o response soro sori	
i) se a=b(moom), emão b=a(moom)	(F dom)	
i) SE DZb (MOOM) E bZ C (MOOM) (EMOO	(F dom/1305 (F dom) 05 05 = 15 05 . 0505	
Q = C (mom) (FOUN) & = Of	2020. 2021 = 4.5 (mop 7)	
4 m 1 (a - b) 2-> : OAros	20 20.2021 = 20 (mon 7) = (Tilibra)	
a=b (mob m)	(MIDIC)	

se 0= b (moom) e c= d (moom):	o d = p (woom)
i) a+c = b+d (moo m) au =>mot	c'c > uew sembre;
(ii) OC = bd (moom) on 0) = d+0	em alguns cosus a pivisou à
(mappe) (maxmd) (maxma) EdD (ii	clara: Sabliter = 6/2 = 3 mod
algumas apricações:	que é quarta-Feira.
· PUNCTOES HASHING: h(K) = K (MOD n)	was ter/qua = 2/3 . & não tha
· números pseuporamdômicos	balliamos com pios fracionax
· criprogratia:	. como colcilarz o = si aom sl
cipia de deswcamento	por tentativa: 10 0 00 100 stoom
· · · · · · · · ·	TER/QUA = X -> X QUA = TER
(1) (00m) x+d = x+p <- (00m) d=p	QUA = 3 & TER = 2.
ence con 23000000 s colomoxs	3.3 = 19 (mora) = 20 . Ocomiso
@ qual o resultado de quinta + sexta?	X2 QUANTA FEIROU POIS:
Quima 1004 (5000 4+5=91 0101	. S 3 X , (Foom) d = x.p orm.
SEXTO: DIG 5	· Generalizon por a saución: el
9 moo 7 = 2 -> Terga Fereas . argmors	→ q.i=1 (moon) rié von
Quimo · Sexta ?	inverso be a (moon). (0).
(4,5) moo 7 -> 20 moo 7 = 56b.00	no ontmérica usual room o 30
(3) (56bado) 1-1(faom) 0 = 1505 + 0505	0x = 6 -> x = 6.1/an aup 10
(c)2 mon 20> 36 mon 2 5 5 6 g / 50	-> na modulary & = 31
REUDO SOID E OFFICE	3x = 2(mop 7) (2 gam) Salt 100
Prodrigocoes: (FORM) F E 6303	quem é 3.1 = (1) (mod 7) ? = 3
1) Communicates, o = Facint, 2011	0 inuliso de 3 (mod 7) é ⑤.
moom (0+0) = moom (d+0)	PODEMOS FORET!
ii) associativi dade	1 (3.3) x = 2.3 (moo 7) 0 :000
((a+b)+c) moom = (a+(b+c)) moom	X = 2.3 (Edom) & strings
i) Elemento neutro (f dom)	1) SE OF EMODOR (FORM OF EX (MODEN)
. 100 90m 0:10 (Facatosos = 1303 -0305	Som Mas sabemas: 3 (moom) de 0 32 la
· DO - SUPERTO MUNICIPALE DO .	00 = 3 (mon 7) (conomi J = 0
tilibra @= (Foam) at = 1505.05 as	EUTÃO: X=3 d-0/1 m >

CONCINSCES:	calculando conecuências:	
i) wem sempre a conguência	3) quanto estamos buscanto o va-	
ax = b (mwo m) Tem sowcoo!!!	LOV DE X em OX = b (moo m), pre-	
ii) WEM SEMPRE PODEMOS DIVIDIR :0	cisamos calcular o inverso de a	
iii) x = V (mon m), apenas	(moom). Como? Pa que?	
SE moc (C, m)=1, ist0 É:	-> sedo à um inteiro de modo que	
que sesam primos entre si!!	$\bar{a} \cdot a = 1 \pmod{m}$	
6 (mco 4)	oi remos que à é o inverso de almod	
* Lema: se 0, b e c sou inteleus	Como encontror 0 ? a como E = 1	
c- d 9 a sup amros so eovinted	· como mpe (a,m)=1 =>	
são primos emizesi e o 1 bc	1. 0 +T. m = 1 (T. bezout)	
emao alc.	Emoo: AQ+T.M = 1 (moo m)	
Seminary on I:	VO EI (WOD M) = C SESSIO I SOMET	
teorema: seja m um intereo posi-	l, o coericionte de a na combi-	
TIVU E SEJOM Q C B E C INTERIOS:	nacco linear & o Inverso de almod	
se aceba (moom) ecem	Ly conjoint dos influents winners	
gão primos entre si emão a = b	A examplo; calcule o inverso of : Jup	
(moo m).	MISSON 3 MODE OF SOM E	
OU SEDQ:	$Q=3$, $\bar{Q}=\bar{Z}$	
Q.C = b.C (moom)	0.3 = 4 mon +2, 4,6-, F = E	
C C C C C	Como sabomos que moc (3,7)=1:	
$a = b \pmod{m}$	1 = 1.3 + 4.7 PROTH-13 = E	
apenas se c e m são primos	aplicando o alguntimo de Euclides itemos	
entre si (moc(c,m)=1).	1 = -2, Dentro 00 moo 7 (0 a 6), TEMO	
* o mesmo no exemplo;	que 0 = 5 , ou 0 = -2 (moo 7) = -200	
$x \cdot Q = b \pmod{m}$	Email Pala saucionarmos OX = 6 [moom):	
$\langle x q = b \pmod{m}$	-> enconredmos annumo = E+ S+ L+ 0	
a a a	s come i (m dom) L = p. B om oo ~	
apenas se moclaim) = 1	-> x 0 : Q = b . 0 (moom) 0 . 0 . 0 . 0	
	-> emrao: X = b a l moom)	
	18. 8 12. 0 } w {8. 8. 7.0} (tilibra)	

CIASSES DE CONGRUENCIA	\$100 a.k.s 1000 esiña (12 a.c.)
20 ecolor, m cour dereviru al	Diombiuphas a signific mount
wimeros popern ser reducioos a	11 dapude mer (meun) de re
000000 001001-100 000000 000000	O: 270/400 COMPAGE 939 (192 M.S.)
Por exemply: map y mas (marris)	ennygp ; (m davn) Y = X (
quais os respos possíveis? 0,11,2,3.	: \$ One; , 1 = (mr, 2) 3e
· isoo sigmirica que:	file same comive morse sup
I = O (mop 4) ou o a special o	publication of the second
LE 1 (mop 4) OU or moons amou	Service of p. 6 c. of p. out.
iz 2 (mon 4) mod om omod .	end 9 to Eup Amina 90 BOVILLED
i= 3 (mob 4). 17 7 7 + D.A.	100 10 9 is same coming ou
CM GONT & ETHOR M)	- 210 om
TOMOS 4 CLOSSES DE CONQUÊNCIO	8 8 7 6 6 Car and 6
Odmoo on a sq amoioreson o el	DECEMBER OF STATE OF
D=12 = 8-124,0 ; 4 - 811. } con	ROWLES COM O C & C MARINOS
Ly conjunto pos infinitos números	000000 (madam) 00 50000
que ao serem ofividios por 4,000	den domo, le agris company de
RESTO O. Analogamente:	(m som
166, 1000 1 4 10 00 13:0 108:0	DCSCV
3 = {7, -3, 1,559000 } € € . D	(moom) 5 d = 5 D
2 = { 6 , - 2 , 2, 6 , 10} 00 mos	3 3
3 = {5,-4,3,4,11,-3&2 = 6	(mapm) d = D
ablication a algorithme as suchass frames	apendo se e em soc primos
00 mi moros que estão na mesmo A	(1= (m,0) oam) ie 39 mo
Close são conquentes pontro do mody.	: o igitraka air omesin o i
esses conjuntos são dissumos e a união	x.a. = b (moom) d = b.x.
0+1+2+3 = conjunto ros inteiros(2)	(makin) d = b x
E podemos diver que: / L = p o omo	0 0
= Q = Q = 300000 00 2n= 34	panoe se moc(o,m) + 1 e son
e o conjunto dos chases de c. do mod 4:	#0 2 3 (m00 a)
(tilibra) {0,7,2,33 0 44,5,6,73	quality 2.2 &