Matemática Discreta – Bacharelado em Sistemas de Informação
RESOLUÇÃO - 4ª Lista de Exercícios – parte 2

Nome _____ Nota _____

RESOLUÇÃO - Teoria dos Números

1) Determine os inteiros q e r tais que **a = b. q+r** e **0 ≤ r < b**, sendo:

a) a = 200, b = 6

200| 6
(2)33

r = 2
q = 33

b) a = 200, b = 6

-200| 6
(4)-34

r = 4
q = -34

c) a = 44, b = 2

44|2
(0)22

r = 0
q = 22

d) a = -44, b = 2

-44|2
(0)-22

r = 0
q = -22

e) a = 0, b = 2

0| 2
(0) 0

r = 0
q = 0

2) Calcule o máximo divisor comum:

a) mdc(45,-45) = **45**

	1
45	**45**
0	

b) mdc(-89,-98) = **1**

	1	9	1	8
98	89	9	8	**1**
9	8	1	0	

c)mdc(324 e 252) = **36**

	1	3	2
324	252	72	**36**
72	36	0	

d)mdc(1739,29341) = **37**

	16	1	6	1	5
29341	1739	1571	222	185	**37**
1517	222	185	37	0	

3) Para cada item do exercício anterior, calcule x e y tais que ax+by=mdc(a,b)

a) 45x +(-45)y = 45
45x -45y = 45
x = 1; y=0

b) (-89)x + (-98)y = 1
DECOMPOSIÇÃO DOS RESTOS

1 = 9 – 1(8)
8 = 89 – 9(9)
9 = 98 –1(89)

SUBSTITUINDO

1 = 9 – 1(8)
= 9 – 1(89 – 9(9))

c) 324x+ 252y = 36
DECOMPOSIÇÃO DOS RESTOS
36 = 252 – 3(72)
72 = 324 – 1(252)

SUBSTITUINDO
36 = 252 – 3(72)
= 252 – 3(324 – 1(252))
= 252 – 3. (324) + 3.(252)
= 4.252 – 3.324

Logo x= 4 e y = -3

= 9 – 89 +9(9)
= -89 + 10(9)
= -89 + 10(98 –1(89)) =
= -89 + 10(98) – 10(89) =
= -11(89) + 10(98)

obs.: inverter os sinais para mdc(-89,-98)

= 11(-89)-10(-98)
= -89(11) -98(-10) = 1

Logo: x = 11 e y = -10

d) 29341x + 1739y = 37

DECOMPOSIÇÃO DOS RESTOS

37 = 222 – 1(185)
185 = 1571 – 6(222)
222 = 1739 – 1(1571)
1571 = 29341 – 16(1739)

SUBSTITUINDO

37 = 222 – 1(185)
= 222 – (1571 – 6(222)) =
= -1571 + 7(222) =
= -1571 + 7(1739 – 1571) =
= 7(1739) – 8(1571) =
= 7(1739) – 8(29341 – 16(1739)) =
=29341(-8) + 1739(135)

Logo: x = - 8 e y = 135

4) Suponha que queiramos calcular o mdc de dois números de 10000 algarismos cada, em um computador que pode efetuar um bilhão de divisões por segundos. Qual é o tempo aproximado para calcular o mdc pelo método das divisões?

Para um número possuir 10000 algarismos ele deve ser da ordem 10^{10000}. Suponha b $\cong 10^{10000}$. Pelo método das divisões, será necessário testar se x|a e x|b, para x variando de 1 até b. Logo teremos $2x10^{10000}$ divisões. Como o computador efetua 10^9div/s temos:

10^9 div --------- 1 seg
$2x10^{10000}$ --------- x seg
$x = 2.10^{99991}$seg

5) Suponhamos a, n ∈ Z com n > 0. Suponhamos também que existe um inteiro b tal que ab ≡ 1 (mod n). Prove que a e b são relativamente primos com n.

Por hipótese temos que ab ≡ 1 (mod n), ou seja, n|(ab-1). Assim **ab - 1=n.k, k ∈ Z. Reescrevendo temos: ab -n.k=1**

Queremos provar que a e b são relativamente primos, ou seja, existem inteiros x e y, tal que
ax + n.y = 1 (I) e **bx + n.y = 1 (II)**

Como ab -n.k=1, podemos concluir (I) atribuindo x=b e y=-k e concluir (II) fazendo x=a e y=-k.
Portanto, existem inteiros x e y, tais que ax+ny=1 e bx+ny=1. Assim a e b são relativamente primos com n.

6) Sejam a e b relativamente primos, e que a|b e b|c. Prove que ab|c.
Sendo a e b primos entre si, temos que ax + by = 1
Temos também que:
a|b → b = ak$_1$, k$_1$ inteiro (1)
b|c → c = bk$_2$, k$_2$ inteiro (2)
De (1) e (2) concluímos que a|c, pois c=ak$_1$k$_2$ (3)
Queremos provar que:
ab|c → c = ab.k, com k inteiro

Multiplicando a equação (ax + by = 1) por c teremos:
acx + bcy = c.
Substituindo (2) no 1º termo e (3) no 2º termo da soma, temos:
a(bk$_2$)x + b(ak$_1$k$_2$)y = c. Assim,
ab(k$_2$x+ k$_1$k$_2$y) = c. Como k$_2$, x, k$_1$ e y são inteiros, tem-se que k= k$_2$x+ k$_1$k$_2$y também é um inteiros. Logo.
abk = c

Portanto ab|c.

7) Prove que inteiros consecutivos devem ser relativamente primos.
Sendo n e n- 1, inteiros consecutivos. Queremos provar que nx + (n-1)y = 1. Se x = 1 e y = - 1, teremos: n(1) + (n-1)(-1) = 1, logo existe dois números inteiros x e y que satisfazem nx+(n-1)y=1. Portanto dois inteiros consecutivos são relativamente primos.

8) Considere dois recipientes para medição. Um tem capacidade de 6 ml e o outro tem capacidade de 11ml. Se a pessoa quiser medir 5 ml, deve encher o recipiente de 11 e usá-lo para encher o de 6, ficando com 5ml no recipiente maior
.
a) mostre como usar essas taças para medir exatamente 1 onça.
11x – 6y = 1
11x +6(-y) = 1
mdc(11,6) = 1

	1	1	5
11	6	5	1
5	1	0	

DECOMPOSIÇÃO DOS RESTOS

1 = 6 – 1(5)
5 = 11 – 1(6)
SUBSTITUINDO

1 = 6 – 1(11 – 6)
1 = (6) – 11 + (6)
1 = 2.(6) -1.(11)

Portanto temos que encher 2 vezes o recipiente de 6ml e retirar 1 vez o de 11ml.

b) Generalize esse problema supondo que os recipientes tenham medidas a e b ml, sendo a e b inteiros positivos. Estabeleça condições necessárias para a e b de forma que seja possível medir exatamente 1 onça.

ax + by = 1 **mdc(a,b) = 1**
a e b inteiros positivos

9) Em Z_{10}, calcule (as operações são modulares):
a) 7+3= **(7+3) mod 10 = 0**
b)12+4 = **Operação inválida já que 12 não pertence ao Z_{10}**
c) 3*3 = **(3*3) mod 10 = 1**
d) 7 * 1 = **(7*1) mod 10 = 7**
e) 6 – 9 = **(6-9) mod 10 = 7**
f) 5/9 = **$5x9^{-1}$**

calculando 9^{-1} :

mdc (9,10)

	1	9
10	9	1
1	0	

1 = 10 – 1(9)
1 = 10 + 9(-1)
Acontece que -1 não faz parte de Z_{10} , logo:
-1 mod 10 = 9
Logo 9^{-1} = 9

5/9 = $5x9^{-1}$ = (5x9) mod(10) = 5

g)8/7 = **$8x7^{-1}$**

calculando 7^{-1} :

	1	2	3
10	7	3	1
3	1	0	

Como mdc(10,7) = 1 existe x e y tal que 10x +7y = 1 e y será o inverso de 7:

DECOMPOSIÇÃO DOS RESTOS
1 = 7 – 2(3)
3 = 10 – 1(7)

Logo 7^{-1} = 3

SUBSTITUINDO
1 = 7 – 2(3)
= 7 - 2(10 – 7)
= 7 – 2(10) + 2(7)
= 3(7) – 2(10)

8/7= $8x7^{-1}$ = (8x3) mod(10) = 4

10) Resolva as equações em relação a X no Z_n indicado:

a) $5 \otimes X = 48$ em Z_{112}
$5 *x = 48$ (multiplicando ambos os lados pelo (5^{-1}))

$(5^{-1} * 5) * x = (5^{-1} * 48)$
$x = (5^{-1} * 48)$

Calcular 5^{-1}em Z_{112}

mdc(112,5) =

	22	2	2
112	5	2	1
2	1	0	

Como o mdc(112,5) = 1 existe x e y tal que 112x+5y=1
sendo y o inverso de 5:

DECOMPOSIÇÃO DOS RESTOS
1 = 5 – 2(2)
2 = 112 – 22(5)

SUBSTITUINDO
1 = 5 – 2(112 – 22(5))
1 = 5 – 2.(112) + 44(5)
1 = -2(112)+45*5
Portanto 5^{-1}= 45

X = 48 * 45 = (2160) mod 112 = 32
X = 32

b) $24 \otimes X \ominus 9 = 73$ em Z_{17}
Os números 24 e 73 não estão definidos em Z_{17}. Podemos encontrar os números equivalentes em Z_{17}:
24 mod 17 = 7
73 mod 17 = 5
E resolver a equação $7 \otimes X \ominus 9 = 5$ em Z_{17}

$7 \otimes X \ominus 9 \oplus 9 = 5 \oplus 9$
$7 \otimes x = 14$

Verificar se existe 7^{-1} em Z_{17}. Para isso, calcule o mdc(17,7) e verifique se é igual a 1. Mdc(17,7)=1. Fazendo a substituição dos restos, tem-se que $7^{-1}=5$.
Assim,
$7^{-1} \otimes 7 \otimes x = 7^{-1} \otimes 14$
$x = 7^{-1} \otimes 14 = 5 \otimes 14 =$ 5.14 mod(17) = 70 mod 17 = 2.

Para verificar se o valor está correto, substitua x na equação $24 \otimes x \ominus 9 = 73$ em Z_{17}

c)$2 \otimes x=4$ em Z_{10}

$2 * x = 4$ (multiplicando ambos os lados pelo (2^{-1}))

$(2^{-1} * 2) * x = (2^{-1} * 4)$

$x=(2^{-1} * 4)$

Calcular 2^{-1}em Z_{10}

mdc(10,2) =

	5
10	2
0	

2 não possui inverso, logo não existe x e y tal que 4x+2y=1. Mas, como queremos determinar se existe x que satisfaz a equação, podemos testar todas as possíveis soluções em Z_{10}. (0,1,2,3,4,5,6,7,8,9)

p/ x = 0 temos (2x0)mod (10) = 0 ≠ 4

.

.

.

p/ x = 2, temos (2x2)mod (10) = 4

.

.

.

p/ x = 7, temos (2x7)mod (10) = 4

.

.

.

x = 2 ou x = 7

Esta forma de fazer só se aplica se n for um número pequenos. Por exemplo se estivéssemos em Z_{400} teríamos que testar 400 valores. Inviabiliza a solução!!!!

A melhor forma para resolver é:

Determinar 2*x = 4 em Z10 é o mesmo que: 2 * x ≡4mod(10),

2x ≡4mod(10). Daí, 10 | (2x-4), ou seja, 2x-4 =10k, 2x=10k+4. Com isso, x=5k +2, qualquer k inteiro.
se k=0 então x=2,
se k=1 então x=7;
se k=2 então x=12mod(10)=2
se k=3 então x=17mod (10) =7,
se k=4 então x=22mod10 =2, ...
Para qualquer valor de k, x=2 ou x=7

d) $X \otimes X=14$ em Z_{15}

Testar todos os valores de x possíveis em Z_{15}, valores de x de 0 a 14:

Ex.: para x = 12, temos (12x12)mod (15) = 144mod(15) = 9 que é diferente de 14

Testando todos os valores não encontramos nenhum que satisfaça a igualdade, portanto não há solução.

- **Deve-se efetuar as substituições para todos os valores de x entre 0 e 14.**

e)$X \otimes X=11$ em Z_{13}

Precisamos testar todos os valores possíveis em Z_{13} valores de x de 0 a 12:
$(11x11) \bmod 13 = 121 \bmod 13 = 4 \neq 11$
$(12x12) \bmod 13 = 144 \bmod 13 = 1 \neq 11$. Testando todos os valores não iremos encontrar nenhum que satisfaça a igualdade, portanto não há solução.

f)$X \otimes X-1=0$ em Z_{11}

$X \otimes X=1$ em Z_{11}

Testar todos os valores de x possíveis em Z_{11}, valores de x de 0 a 11:
Ex.: para x = 10, temos $(10x10) \bmod (11) = 100 \bmod (11) = 1$. Logo x = 10.