UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO – UFRPE
Matemática Discreta – Bacharelado em Sistemas de Informação
RESOLUÇÃO - 5ª Lista de Exercícios

Teoria dos Números

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

a) a=100 b=3 | b) a= -100; b=3 | c) a=99, b=3 | d) a=-99; b=3 | e) a=0; b=3

a)	b)	c)	d)	e)
-100 |3	**100 |3**	**99 |3**	**-99 |3**	**0 |3**
(1) 33	**(2) -34**	**(0) 33**	**(0) -33**	**(0) 0**
q = 33	**q = -34**	**q = 33**	**q = -33**	**q = 0**
r = 1	**r = 2**	**r = 0**	**r = 0**	**r = 0**

2. Calcule:

a)mdc(123,-123) = **123**

	1
123	**123**
0	

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

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

c)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) 123x + (-123)y = 123
123x – 123y = 123
x = y = 1

b) -89x + (-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))= 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

c) 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 1000 algarismos cada, em um computador que pode efetuar 1 bilhão de divisões por segundos. Qual é o tempo aproximado para calcular o mdc pelo método das divisões?

Para um número possuir 1000 algarismos ele deve ser da ordem 10^{1000}. Suponha b =~ 10^{1000}. Pelo método das divisões, será necessário testar se x|a e x|b, para x variando de 1 até b. Logo teremos $2x10^{1000}$ divisões. Como o computador efetua 10^9 div/s temos:

10^9 div --------- 1 seg
$2x10^{1000}$ --------- x seg

$$x = \frac{2x10^{1000}}{10^9} = 2x10^{991}\ s.$$

Portanto teremos aproximadamente $3x10^{980}$ milênios

Monitor: Cleiton Pedrosa (cleiton7@msn.com)

UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO – UFRPE
Matemática Discreta – Bacharelado em Sistemas de Informação
RESOLUÇÃO - 5ª Lista de Exercícios

5. Suponhamos que a e b sejam “primos entre si” e que a|c e b|c. Prove que (a.b)|c.

Sendo a e b primos entre si, temos mdc(a,b) = 1, ou seja ax + by = 1
Temos também que:
a|c → c = ak1, k1 inteiro (1)
b|c → c = bk2, k2 inteiro (2)
Queremos provar que:
ab|c → c = abk, com k inteiro

Em ax + by = 1 (xC)

acx + bcy = c. Substituindo (1) no 1º termo e (2) no 2º termo da soma, temos:
a(bk2)x + b(ak1)y = c, fazendo k2x = k3 e k1y = k4, já que x e y são também inteiros
abk3 + abk4 = c
ab(k3 + k4) = c, fazendo k3 + k4 = k
abk = c

Portanto ab|c.

6. Sejam a, b e n inteiros com n>0 e ab $\equiv$ 1 (mod n). Prove que a e b são relativamente primos com n.

Temos que n| ab – 1, ou seja, ab -1 = nk

ab - nk = 1 , com k inteiro
ab + n(-k) = 1

Como se dois números a e b são primos entre si, temos que ax +by = 1 com x e y inteiros, temos:
Fazendo x = b e y = -k:
ax + ny = 1, logo a e n são primos entre si.
Da mesma forma, fazendo x = a e y = - k:
bx + ny = 1, logo b e n são primos entre si.

Portanto a e b são relativamente primos com n.

7. Considere duas taças para medida. Uma tem capacidade de 8 onças e a outra tem capacidade de 13 onças. Se a pessoa quiser medir 5 onças, deve encher a taça de 13 e usa-la para encher a taça de 8, ficando com 5 onças na taça maior.
a) mostre como usar essas taças para medir exatamente 1 onça.

13x – 8y = 1
13x + 8(-y) = 1
Logo o mdc(13,8) = 1

	1	1	1	1	2
13	8	5	3	2	1
5	3	2	1	0	

DECOMPOSIÇÃO DOS RESTOS | **SUBSTITUINDO**

1 = 13 – 1(2)
2 = 5 – 1(3)
3 = 8 – 1(5)
5 = 13 – 1(8)

1 = 3 – 1(5 – 3)
= -5 + 2(3) =
= - 5 + 2(8 – 5) =
= 2(8) -3(5) =
= 2(8) -3(13 – 8) =
= 2(8) – 3(13) + 3(8) =
= 5(8) – 3(13)

Portanto temos que encher 5 vezes a taça de 8 onças e retirar 3 vezes a de 13 onças.

b) Generalize esse problema supondo que as taças tenham medidas a e b onças, sendo a e b inteiros positivos. Estabeleça condições necesssárias 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

8. Em Z_{10}, calcule:

a) 6+6 = **(6+6) mod(10) = 2**

b) 7*1 = **(7x1) mod(10) = 7**

c) 5 – 8 = **(5-8) mod(10) = -3 mod 10 = 7**
- 3 |10
  7 -1

d)8-5 = **(8-5) mod 10 = 3**

e) 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 | **SUBSTITUINDO**

1 = 7 – 2(3)
3 = 10 – 1(7)

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

Logo $7^{-1} = 3$

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

f) 5/9 = $5x9^{-1}$
calculando 9^{-1} :

	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
- 1 |10
(9) -1

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

Logo $9^{-1} = 9$

UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO – UFRPE
Matemática Discreta – Bacharelado em Sistemas de Informação
RESOLUÇÃO - 5ª Lista de Exercícios

9. Resolva as equações em relação a X no Z_n indicado:

a) $3 * X = 4$ em Z_{11}

Como em Z_{11} o $3^{-1} * 3 = 1$, temos que:

$3*x = 4$ (multiplicando ambos os lados pelo (3^{-1}))

$(3^{-1} * 3)*x = (3^{-1} * 4)$

$x = (3^{-1} * 4)$

Devemos calcular 3^{-1} :

Logo:

$x = 4x4 = (4x4) \bmod(11) = 16 \bmod(11) = 5$

x = 5

Mdc(11,3)

	3	1	2
11	3	2	1
2	1	0	

Como o mdc(11,3) = 1 existe x e y tal que 11x+3y=1 sendo y o inverso de 3:

DECOMPOSIÇÃO DOS RESTOS

1 = 3 – 1(2)
2 = 11 – 3(3)

1 = 3 – 1(11 – 3(3)) =
= 3 – 11 + 3(3) =
= -11 + **4**(3)

logo $3^{-1} = 4$

b) $3*X+448 = 73$ em Z_{1003}

3*X+448 = 73 (subtraindo modular em ambos os lados)
3*X+448 – 448 = 73 – 448
3*X = -375

Como -375 não pertence a Z_{1003}, faremos -375 mod 1003 = 628

3*x=628
$x = 3^{-1} * 628$.

Calcular 3^{-1} em $\mathbf{Z_{1003}}$

	334	3
1003	3	1
1	0	

1 = 1003 – 334(3)
3^{-1} = -334 que não pertence a $\mathbf{Z_{1003}}$
-334mod(1003) = 669
x = (669x628)mod(1003)= 878
x = 878

c) 2 * x = 4 em Z10

2 * x=4 (multiplicando pelo inverso inv(2) em ambos lados)
x = 4* ...

mdc = 2, qual seria o inverso? Não há inverso. 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

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

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

d) X*X=14 em Z_{15}

Testar todos os valores de x possíveis em $Z_{15,}$ valores de x de 0 a 14:
Ex.: p/ x = 12, temos (12x12)mod (15) = 144mod(15) = 9 ≠ 14
Testando todos os valores não encontramos nenhum que satisfaça a igualdade, portanto não há solução.

obs.: deve-se efetuar as substituições para todos os valores de x entre 0 e 14.

Há outras formas para resolver d) (equação diofantina), porém não estudamos no curso.