Universidade Federal de São Carlos – Departamento de Computação
Matemática Discreta – Profa. Helena Caseli

Sétima Lista de Exercícios – Teoria dos Números

1) Para os pares de inteiros a e b a seguir, determine q e r tais que $a = qb + r$ e $0 \leq r < b$.
   a) $a = 100$, $b = 3$.
      100=3*33 + 1
      q=33
      r=1
   b) $a = -100$, $b = 3$.
      -100= -34*3 + 2
      q = -34
      r = 2
   c) $a = 99$, $b = 3$.
      99 = 33*3
      q = 33
      r = 0
   d) $a = -99$, $b = 3$.
      -99 = -33*3
      q = -33
      r = 0
   e) $a = 0$, $b = 3$.
      q = 0
      r = 0

2) Para cada par de inteiros a e b do exercício anterior, calcule a div b e a mod b.

a) $a = 100$, $b = 3$.
   100 Div 3 = 33
   100 Mod 3 = 1
b) $a = -100$, $b = 3$.
   -100 Div 3 = -34
   -100 Mod 3 = 2
c) $a = 99$, $b = 3$.
   99 Div 3 = 33
   99 Mod 3 = 0
d) $a = -99$, $b = 3$.
   -99 Div 3 = -33
   -99 Mod 3 = 0
e) $a = 0$, $b = 3$.
   0 Div 3 = 0
   0 Mod 3 = 0

3) Calcule usando o Algoritmo de Euclides:
   a) mdc(20,25).
      20 mod 25 = 20 => mdc(20,25)= mdc(25,20)
      25 mod 20 = 5 => mdc(25,20)= mdc(20,5)
      20 mod 5 = 0 => mdc(20,5)= 5

      PASSO A PASSO DO ALGORITMO DE EUCLIDES:
      Iniciamos com a = 20 e b = 25
      Calculamos c = 20 mod 25 = 20

Como 20 é diferente de 0, devemos calcular mdc(25, 20)

Reiniciamos o processo com a = 25 e b = 20
Calculamos c = 25 mod 20 = 5
Como 5 é diferente de 0, devemos calcular mdc(20, 5)

Reiniciamos o processo com a = 20 e b = 5
Calculamos c = 20 mod 5 = 0
Como obtemos c=0, obtemos a resposta mdc(20,5) = 5 e, portanto, mdc(20, 5) = mdc(25, 20) = 5.

b) mdc(123, 23).
123 mod 23 = 8 => mdc(123,23)= mdc(23,8)
23 mod 8 = 7 => mdc(23,8)= mdc(8,7)
8 mod 7 = 1 => mdc(8,7)= mdc(7,1)
7 mod 1 = 0 => mdc(7,1)= 1

PASSO A PASSO DO ALGORITMO DE EUCLIDES:
Iniciamos com a = 123 e b = 23
Calculamos c = 123 mod 23 = 8
Como 8 é diferente de 0, devemos calcular mdc(23, 8)

Reiniciamos o processo com a = 23 e b = 8
Calculamos c = 23 mod 8 = 7
Como 7 é diferente de 0, devemos calcular mdc(8, 7)

Reiniciamos o processo com a = 8 e b = 7
Calculamos c = 8 mod 7 = 1
Como 1 é diferente de 0, devemos calcular mdc(7, 1)

Reiniciamos o processo com a = 7 e b = 1
Calculamos c = 7 mod 1 = 0
Como obtemos c=0, obtemos a resposta mdc(7,1) = 1 e, portanto, mdc(7, 1) = mdc(8, 7) = mdc(23, 8) = 1.

c) mdc(89, 98).
89 mod 98 = 89 => mdc(89,98)= mdc(98,89)
98 mod 89 = 9 => mdc(98,89)= mdc(89,9)
89 mod 9 = 8 => mdc(89,9)= mdc(9,8)
9 mod 8 = 1 => mdc(9,8)= mdc(8,1)
8 mod 1 = 0 => mdc(8,1)= 1

d) mdc(54321, 50).
54321 mod 50 = 21 => mdc(54321,50)= mdc(50,21)
50 mod 21 = 8 => mdc(50,21)= mdc(21,8)
21 mod 8 = 5 => mdc(21,8)= mdc(8,5)
8 mod 5 = 3 => mdc(8,5)= mdc(5,3)
5 mod 3 = 2 => mdc(5,3)= mdc(3,2)
3 mod 2 = 1 => mdc(3,2)= mdc(2,1)
2 mod 1 = 0 => mdc(2,1)= 1

e) mdc(1739,29341).

1739 mod 29341 = 1739 => mdc(1739,29341)= mdc(29341,1739)
29341 mod 1739 = 1517 => mdc(29341,1739)= mdc(1739,1517)
1739 mod 1517 = 222 => mdc(1739,1517)= mdc(1517,222)
1517 mod 222 = 185 => mdc(1517,222)= mdc(222,185)
222 mod 185 = 37 => mdc(222,185)= mdc(185,37)
185 mod 37 = 0 => mdc(185,37)= 37

4) Para cada par de inteiros a, b do exercício anterior, determine os inteiros x e y tais que $ax + by = \text{mdc}(a, b)$.

a) mdc(20,25)=5.
20 mod 25 = 20 e 20 div 25 = 0
25 mod 20 = 5 e 25 div 20 = 1
20 mod 5 = 0 e 20 div 5 = 4

Escrevendo na forma a = qb + r
20 = 0*25 + 20
25 = 1*20 + 5
20 = 4*5 + 0

Isolando r
20 = 20 - 0*25
5 = 25 - 1*20
0 = 20 - 4*5

Utilizando a segunda equação que corresponde ao 5 (mdc entre 20 e 25)
5 = 25 - 1*20

Substituindo o 20
5 = 25 - 1*(20 - 25*0)
5 = 25 -20 + 25*0

Substituindo o 0
5 = 25 -20 + 25*0
5 = 25 -20 + 25*(20 – 4*5)
5 = 25 -20 + 25*(20 – 20)
5 = 25 -20 + 25*0
5 = 25 -20

Logo, x=-1 e y=1

b) mdc(123, 23)=1
123 mod 23 = 8 e 123 div 23 = 5
23 mod 8 = 7 e 23 div 8 = 2
8 mod 7 = 1 e 8 div 7 = 1
7 mod 1 = 0 e 7 div 1 = 7

Escrevendo na forma a = qb + r
123 = 5*23 + 8
23 = 2*8 + 7
8 = 1*7 + 1
7 = 7*1 + 0

Isolando r
8 = 123 - 5*23
7 = 23 - 2*8
1 = 8 - 1*7
0 = 7 - 7*1

Usando a equação 3:
1 = 8 - 1*7

Substituindo o 7
1 = 8 - 1*7
1 = 8 - 1*(23 - 2*8)
1 = 8 + 2*8 -1*23
1 = 3*8 -1*23

Substituindo o 8
1 = 3*8 -1*23
1 = 3*(123 - 5*23) -1*23
1 = 123*3 -15*23 -1*23
1 = 123*3 -16*23

Logo, x=3 e y=-16

c) mdc(89, 98)=1
89 mod 98 = 89 e 89 div 98 = 0
98 mod 89 = 9 e 98 div 89 = 1
89 mod 9 = 8 e 89 div 9 = 9
9 mod 8 = 1 e 9 div 8 = 1
8 mod 1 = 0 e 8 div 1 = 8

Escrevendo na forma a = qb + r
89 = 0*98 + 89
98 = 1*89 + 9
89 = 9*9 + 8
9 = 1*8 + 1
8 = 8*1 + 0

Isolando r
89 = 89 - 0*98
9 = 98 - 1*89
8 = 89 - 9*9
1 = 9 - 1*8
0 = 8 - 8*1

Utilizando a equação 4
1 = 9 - 1*8

Substituindo o 8
1 = 9 - 1*8
1 = 9 - 1*(89 - 9*9)
1 = 9 -1*89 + 9*9   (deveria ter feito: 1 = -1*89 + 10*9)

Substituindo o 9
1 = 9 -1*89 + 9*9
1 = 9 -1*89 + 9*(98 - 1*89)
1 = 9 -1*89 + 9*98 - 9*89
1 = 9 -10*89 +9*98

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

Substituindo novamente o 9 (essa parte não seria necessária)
1 = 9 -10*89 +9*98
1 = (98 - 1*89) -10*89 +9*98
1 = 98 - 1*89 -10*89 +9*98
1 = -11*89 + 10*98

Logo, x=-11 e y=10

d) mdc(54321, 50)=1
54321 mod 50 = 21 e 54321 div 50 = 1086
50 mod 21 = 8 e 50 div 21 = 2
21 mod 8 = 5 e 21 div 8 = 2
8 mod 5 = 3 e 8 div 5 = 1
5 mod 3 = 2 e 5 div 3 = 1
3 mod 2 = 1 e 3 div 2 = 1
2 mod 1 = 0 e 2 div 1 = 2

Escrevendo na forma a = qb + r
54321 = 1086*50 + 21
50 = 2*21 + 8
21 = 2*8 + 5
8 = 1*5 + 3
5 = 1*3 + 2
3 = 1*2 + 1
2 = 2*1 + 0

Isolando o r
21 = 54321 - 1086*50
8 = 50 - 2*21
5 = 21 - 2*8
3 = 8 - 1*5
2 = 5 - 1*3
1 = 3 - 1*2
0 = 2 - 2*1

Utilizando a equação 6
1 = 3 - 1*2

Substituindo o 2
1 = 3 - 1*2
1 = 3 - 1*(5 - 1*3)
1 = 3 -1*5 + 1*3
1 = -1*5 + 2*3

Substituindo o 3

1 = -1*5 + 2*3
1 = -1*5 + 2*(8 - 1*5)
1 = -1*5 + 2*8 - 2*5
1 = -3*5 + 2*8

Substituindo o 8
1 = -3*5 + 2*8
1 = -3*5 + 2*(50 - 2*21)
1 = -3*5 + 2*50 -4*21

Substituindo o 5
1 = -3*5 + 2*50 -4*21
1 = -3*(21 - 2*8) + 2*50 -4*21
1 = -3*21 +6*8 + 2*50 -4*21
1 = -7*21 +6*8 + 2*50

Substituindo o 8
1 = -7*21 +6*8 + 2*50
1 = -7*21 +6*(50 - 2*21) + 2*50
1 = -7*21 +6*50 - 12*21 + 2*50
1 = -19*21 +8*50

Substituindo o 21
1 = -19*21 +8*50
1 = -19*(54321 - 1086*50) +8*50
1 = -19*54321 + 20634*50 +8*50
1 = -19*54321 + 20642*50

Logo, x=-19 e y=20642

e) mdc(1739,29341)=37
1739 mod 29341 = 1739 e 1739 div 29341 = 0
29341 mod 1739 = 1517 e 29341 div 1739 = 16
1739 mod 1517 = 222 e 1739 div 1517 = 1
1517 mod 222 = 185 e 1517 div 222 = 6
222 mod 185 = 37 e 222 div 185 = 1
185 mod 37 = 0 e 185 div 37 = 5

Escrevendo na forma a = qb + r
1739 = 0*29341 + 1739
29341 = 16*1739 + 1517
1739 = 1*1517 + 222
1517 = 6*222 + 185
222 = 1*185 + 37
185 = 5*37 + 0

Isolando o r
1739 = 1739 - 0*29341
1517 = 29341 - 16*1739
222 = 1739 - 1*1517
185 = 1517 - 6*222
37 = 222 - 1*185

0 = 185 - 5*37

Utilizando a equação 5:
37 = 222 - 1*185

Substituindo o 185
37 = 222 - 1*185
37 = 222 - 1*(1517 - 6*222)
37 = 222 - 1*1517 + 6*222
37 = - 1*1517 + 7*222

Substituindo o 222
37 = - 1*1517 + 7*222
37 = - 1*1517 + 7*(1739 - 1*1517)
37 = - 1*1517 + 7*1739 - 7*1517
37 = 7*1739 - 8*1517

Substituindo o 1517
37 = 7*1739 - 8*1517
37 = 7*1739 - 8*(29341 - 16*1739)
37 = 7*1739 - 8*29341 + 128*1739
37 = - 8*29341 + 135*1739

Logo, x=-8 e y=135

5) Escreva as fatorações em primos dos números a seguir:
a) 201 = 3 * 67
b) 1001 = 7 * 11 * 13
c) 201000 = $2^3 * 3 * 5^3 * 67$

6) Calcule o seguinte, no contexto de $\mathbb{Z}_{10}$:
a) $3 \oplus 3$
$3 \oplus 3$ = (3 + 3) mod 10 = 6 mod 10 = 6
b) $6 \oplus 6$
$6 \oplus 6$ = (6 + 6) mod 10 = 12 mod 10 = 2
c) $7 \oplus 3$
$7 \oplus 3$ = (7 + 3) mod 10 = 10 mod 10 = 0
d) $9 \oplus 8$
$9 \oplus 8$ = (9 + 8) mod 10 = 17 mod 10 = 7
e) $9 \oplus 1$
$9 \oplus 1$ = (9 + 1) mod 10 = 10 mod 10 = 0
f) $9 \oplus 9$
$9 \oplus 9$ = (9 + 9) mod 10 = 18 mod 10 = 8
g) $3 \otimes 4$
$3 \otimes 4$ = (3 * 4) mod 10 = 12 mod 10 = 2
h) $9 \otimes 3$
$9 \otimes 3$ = (9 * 3) mod 10 = 27 mod 10 = 7
i) $3 \otimes 3$
$3 \otimes 3$ = (3 * 3) mod 10 = 9 mod 10 = 9
j) $5 \otimes 2$
$5 \otimes 2$ = (5 * 2) mod 10 = 10 mod 10 = 0
k) $6 \otimes 6$

$6 \otimes 6 = (6 * 6) \bmod 10 = 36 \bmod 10 = 6$

l) $5 \theta 8$

$5 \theta 8 = 7$ pois é o valor de x tal que $5 = 8 \oplus x$

m) $8 \theta 5$

$8 \theta 5 = 3$ pois é o valor de x tal que $8 = 5 \oplus x$

n) $8 \oslash 7$

$8 \oslash 7 = 4$ pois é o valor de $8 \otimes 7^{-1}$ e como $7^{-1} = 3$, $8 \otimes 3 = 4$

o) $5 \oslash 9$

$5 \oslash 9 = 5$ pois é o valor de $5 \otimes 9^{-1}$ e como $9^{-1} = 9$, $5 \otimes 9 = 5$

7) Resolva as equações no contexto indicado:

a) $3 \otimes x = 4$ em $\mathbb{Z}_{11}$

Estamos procurando o valor (ou valores) de x tais que (3x) mod 11 = 4, ou seja, 3x deve ser um número inteiro múltiplo de 11 somado com 4, já que

Se a mod b = r então a = q.b + r, q >= 0 e 0 <= r < b.

Logo, como (3x) mod 11 = 4, (3x) = q.11 + 4, para q = 0, 1, 2...

Se q = 0 temos 3x = 11(0) + 4

Assim, 3x = 4 e x = 4/3, tal valor não existe em $\mathbb{Z}_{11}$

Se q = 1 temos 3x = 11(1) + 4 = 15

Assim, 3x = 15 e x = 5

O primeiro valor que estamos procurando é x = 5

Se q = 2 temos 3x = 11(2) + 4

Assim, 3x = 26 e x = 26/3, não está em $\mathbb{Z}_{11}$, portanto não pode ser um dos valores procurados.

Se q = 3 temos 3x = 11(3) + 4

Assim, 3x = 37 e x = 37/3, não está em $\mathbb{Z}_{11}$, portanto não pode ser um dos valores procurados.

A solução para a equação é x = 5.

b) $4 \otimes x = 9$ em $\mathbb{Z}_{11}$

Estamos procurando o valor (ou valores) de x tais que (4x) mod 11 = 9, ou seja, 4x deve ser um número inteiro múltiplo de 11 somado com 9, já que

Se a mod b = r então a = q.b + r, q >= 0 e 0 <= r < b.

Logo, como (4x) mod 11 = 9, (4x) = q.11 + 9, para q = 0, 1, 2...

Se q = 0 temos 4x = 11(0) + 9

Assim, 4x = 9 e x = 9/4, tal valor não existe em $\mathbb{Z}_{11}$

Se q = 1 temos 4x = 11(1) + 9 = 20

Assim, 4x = 20 e x = 5

O primeiro valor que estamos procurando é x = 5

Se q = 2 temos 4x = 11(2) + 9

Assim, 4x = 31 e x = 31/4, não está em $\mathbb{Z}_{11}$, portanto não pode ser um dos valores procurados.

Se q = 3 temos 4x = 11(3) + 9

Assim, 4x = 42 e x = 42/4, não está em $\mathbb{Z}_{11}$, portanto não pode ser um dos valores procurados.

Se q = 4 temos 4x = 11(4) + 9

Assim, 4x = 53 e x = 53/4, não está em $\mathbb{Z}_{11}$, portanto não pode ser um dos valores procurados.

A solução para a equação é x = 5.

c) $3 \otimes x \oplus 8 = 1$ em $\mathbb{Z}_{10}$

Estamos procurando o valor (ou valores) de x tais que (3x + 8) mod 10 = 1, ou seja, 3x + 8 deve ser um número inteiro múltiplo de 10 somado com 1, já que

Se a mod b = r então a = q.b + r, q >= 0 e 0 <= r < b.

Logo, como (3x + 8) mod 10 = 1, 3x + 8 = q.10 + 1 , Logo, 3x = q.10 + 1 -8 = q.10 + -7, para q = 0, 1, 2...

Se q = 0 temos 3x = 10(0) -7

Assim, 3x = -7 e x = -7/3, tal valor não existe em $\mathbb{Z}_{10}$

Se q = 1 temos 3x = 10(1) -7

Assim, 3x = 3 e x = 1

O primeiro valor que estamos procurando é x = 1

Se q = 2 temos 3x = 10(2) -7

Assim, 3x = 13 e x = 13/3, , tal valor não existe em $\mathbb{Z}_{10}$

Se q = 3 temos 3x = 10(3) -7

Assim, 3x = 23 e x = 23/3, , tal valor não existe em $\mathbb{Z}_{10}$

Se q = 4 temos 3x = 10(4) -7

Assim, 3x = 33 e x = 33/3 = 11, tal valor não existe em $\mathbb{Z}_{10}$

A solução para a equação é x = 1.

8) Resolva as equações no contexto indicado (pode haver mais de uma solução, ou nenhuma):

a) $2 \otimes x = 4$ em $\mathbb{Z}_{10}$

Estamos procurando o valor (ou valores) de x tais que (2x) mod 10 = 4, ou seja, 2x deve ser um número inteiro múltiplo de 10 somado com 4, já que

Se a mod b = r então a = q.b + r, q >= 0 e 0 <= r < b.

Logo, como (2x) mod 10 = 4, (2x) = q.10 + 4, para q = 0, 1, 2, ...

Se q = 0 temos 2x = 10(0) + 4 = 4

Assim, 2x = 4 e x = 4/2 = 2

Então, o primeiro valor de x que procuramos é x = 2.

Se q = 1 temos 2x = 10(1) + 4 = 14

Assim, 2x = 14 e x = 14/2 = 7

O segundo valor que estamos procurando é x = 7.

Se q = 2 temos 2x = 10(2) + 4 = 24

Assim, 2x = 24 e x = 24/2 = 12. Mas 12 não está em $\mathbb{Z}_{10}$, portanto não pode ser um dos valores procurados.

As duas soluções para a equação são x = 2 e x = 7.

b) $2 \otimes x = 3$ em $\mathbb{Z}_{10}$

Repetindo o processo anterior, estamos procurando valores de x em $\mathbb{Z}_{10}$ tais que (2x) mod 10 = 3, ou seja, (2x) = q.10 + 3, para q = 0, 1, 2, ...

Se q = 0 temos 2x = 10(0) + 3 = 13

Assim, 2x = 3 e x = 3/2. Mas como 2 não é divisor do 3, tal valor não existe em $\mathbb{Z}_{10}$

O mesmo acontece para qualquer valor de q, logo não há solução para a equação.

c) $9 \otimes x = 4$ em $\mathbb{Z}_{12}$

Estamos procurando o valor (ou valores) de x tais que (9x) mod 12 = 4, ou seja, 9x deve ser um número inteiro múltiplo de 12 somado com 4, já que

Se a mod b = r então a = q.b + r, q >= 0 e 0 <= r < b.

Logo, como 9x mod 12 = 4, 9x = q.12 + 4, para q = 0, 1, 2...

Se q = 0 temos 9x = 12(0) + 4

Assim, 9x = 4 e x = 4/9. Mas como 4 não é divisor do 9, tal valor não existe em $\mathbb{Z}_{12}$

O mesmo acontece para qualquer valor de q, logo não há solução para a equação.

9) Determine quem é $\mathbb{Z}^*$ nos casos abaixo:

a) $\mathbb{Z}_4^*$

R. $\mathbb{Z}_4^* = \{ 1, 3 \}$

b) $\mathbb{Z}_7^*$

R. $\mathbb{Z}_7^* = \{ 1, 2, 3, 4, 5, 6 \}$

c) $\mathbb{Z}_8^*$

R. $\mathbb{Z}_8^* = \{ 1, 3, 5, 7 \}$