UNIVERSIDADE FEDERAL DE VIÇOSA

DEPARTAMENTO DE INFORMÁTICA

(DPI)

LISTA DE EXERCÍCIOS 3

RESPOSTAS

Rafael Zardo Crevelari – ES105468

Uma imagem contendo Logotipo

Descrição gerada automaticamenteDisciplina: Matemática Discreta

Professor: André Gustavo Dos Santos

21 de julho 2022

**RESPOSTAS:**

**Exercício 1:**

**Letra A)** Para obter quociente e o resto de 44 dividido por 8, basta realizar os seguintes cálculos, temos que 44 = 8 \* 5 + 4, com isso podemos perceber pelo algoritmo de divisão que o quociente é 5, que é igual a 44 **div** 8. Além disso, temos que o resto é 4, que é igual 44 **mod** 8.

Padrão do plano de fundo

Descrição gerada automaticamente com confiança baixa

**Letra B)** Para obter quociente e o resto de 0 dividido por 9, basta realizar os seguintes cálculos, temos que 0 = 19 \* 0, com isso podemos perceber pelo algoritmo de divisão que o quociente é 0, que é igual a 0 **div** 19. Além disso, temos que o resto é 0, que é igual 0 **mod** 19.

**Letra C)** Para obter quociente e o resto de -123 dividido por 19, basta realizar os seguintes cálculos, temos que -123 = 19 \* (-6) + 9, com isso podemos perceber pelo algoritmo de divisão que o quociente é -6, que é igual a -123 **div** 19. Além disso, temos que o resto é 9, que é igual -123 **mod** 19.

Padrão do plano de fundo

Descrição gerada automaticamente com confiança baixa

**Letra D)** Para obter quociente e o resto de -1 dividido por 4, deve-se perceber antes de realizar os cálculos, que 4 não divide -1, uma vez que, pela definição de divisão, não há um inteiro C tal que -1 = 4 \* C, ou seja,

-1 / 4 não é um número inteiro.

**Exercício 2:**

**Letra A)** Para obter quantas horas marca um relógio 80 horas depois de marcar 10 horas, basta usar o conceito de aritmética modular, ou seja, 80 **mod** 24 = 8, além disso podemos saber quantas voltas completas o relógio fez através do seguinte cálculo, 80 **div** 24 = 3. Logo, temos que o relógio deu 3 voltas completas e sobrou 8 horas para percorrer no relógio. Sabendo que o relógio já estava marcando 10 horas, basta somar do que faltou percorrer das 80 horas, logo, temos que o relógio marcara 10 + 8 = 18 horas, 80 horas depois de marcar 10 horas.

Padrão do plano de fundo

Descrição gerada automaticamente com confiança baixa

**Letra B)** Para obter quantas horas marca um relógio 100 horas depois de marcar 8 horas, basta usar o conceito de aritmética modular, ou seja, 100 **mod** 24 = 4, além disso podemos saber quantas voltas completas o relógio fez através do seguinte cálculo, 100 **div** 24 = 4. Logo, temos que o relógio deu 4 voltas completas e sobrou 4 horas para percorrer no relógio. Sabendo que o relógio já estava marcando 8 horas, basta somar do que faltou percorrer das 100 horas, logo, temos que o relógio marcara 8 + 4 = 12 horas, 100 horas depois de marcar 8 horas.

Padrão do plano de fundo

Descrição gerada automaticamente com confiança baixa

**Exercício 3:**

Antes de iniciar o exercício devemos encontrar o valor de A e B, para encontrar o valor de A e B devemos realizar os seguintes cálculos:

A ≡ 11 (mod 19)

A = 11

B ≡ 9 (mod 19)

B = 9

**Letra A)** Para encontrar o valor de C devemos realizar os seguintes cálculos:

C ≡ 13 \* [11 (mod 19)] (mod 19)

C ≡ 13 \* 11 (mod 19)

C ≡ 143 (mod 19)

C = 10

Além disso, podemos provar a congruência da seguinte forma: 143 - 10 = 133, que é um número divisível por 19.

**Letra B)** Para encontrar o valor de C devemos realizar os seguintes cálculos:

C ≡ [ 9 (mod 19) - 11 (mod 19)] (mod 19)

C ≡ (9 - 11) (mod 19)

C ≡ -2 (mod 19)

C = -2

Com precisamos achar um C no intervalo 0 ≤ C < 19, precisamos encontrar o próximo número congruente, é igual a 17. Com isso, C = 17.

Além disso, podemos provar a congruência da seguinte forma: -2 - 17 = -19, que é um número divisível por 19.

**Letra C)** Para encontrar o valor de C devemos realizar os seguintes cálculos:

C ≡ 2 \* 11 + 3 \* 9 (mod 19)

C ≡ 22 + 27 (mod 19)

C ≡ 49 (mod 19)

C = 11

Além disso, podemos provar a congruência da seguinte forma: 49 - 11 = 38, que é um número divisível por 19.

**Letra D)** Para encontrar o valor de C devemos realizar os seguintes cálculos:

C ≡ 121 - 81 (mod 19)

C ≡ 40 (mod 19)

C = 2

Além disso, podemos provar a congruência da seguinte forma: 40 - 2 = 38, que é um número divisível por 19.

**Exercício 4:**

**Letra A)** Encontrando MDC (36,120) da forma solicitada:

36 = 1, 2, 3, 4, 6, **12**, 18, 36

120 = 1, 2, 3, 4, 5, 6, 8, 10, **12**, 15, 20, 24 ... (os próximos não importam, pois não existem divisores de 36 maiores que 36)

**Letra B)** Encontrando MDC (36,120) da forma solicitada:

120 = 23 \* 31 \* 51

36 = 22 \* 31 \* 50

MDC = 22 \* 31 \* 50

MDC = 4 \* 3 = 12

**Letra C)** Encontrando MDC (36,120) da forma solicitada:

1) Pelo algoritmo da divisão, 120 = 36 \* 3 + 12

2) Qualquer divisor de 120 e 36 é divisor de 120 - 36 \* 3 = 12

3) E qualquer divisor de 36 e 12 é divisor de 36 \* 3 + 12 = 120

4) Então MDC (36,120) é o mesmo que MDC (36,12)

5) Pelo algoritmo da divisão 36 = 12 \* 3

6) Como 12 | 36, MDC (36,12) = 12; Assim MDC (120,36) = MDC (36,12) = 12.

**Exercício 5:**

**Letra A)** Utilizando o algoritmo de Euclides para encontrar MDC (21,44), temos:

44 = 21 \* 2 + 2

21 = 2 \* 10 + 1

2 = 1 \* 2

MDC (21,44) = 1

Para encontrar a combinação linear precisamos encontrar o algoritmo de Euclides estendido:

1 = 21 - 2 \* 10

2 = 44 - 21 \* 2

1 = 21 - ( -21 \* 2 + 44) \* 10

1 = 21 - (-21 \* 20 + 44 \* 10)

1 = 21 + 21 \* 20 + 44 \* (-10)

1 = 21 \* 21 + 44 \* (-10)

**Letra B)** Utilizando o algoritmo de Euclides para encontrar MDC (33,44), temos:

44 = 33 \* 1 + 11

33 = 11 \* 3

MDC (33,44) = 11

Para encontrar a combinação linear precisamos encontrar o algoritmo de Euclides estendido:

11 = 44 + 33 \* (-1)

**Letra C)** Utilizando o algoritmo de Euclides para encontrar MDC (35,78), temos:

78 = 35 \* 2 + 8

35 = 8 \* 4 + 3

8 = 3 \* 2 + 2

3 = 2 \* 1 + 1

2 = 2 \* 1

MDC (35,78) = 1

Para encontrar a combinação linear precisamos encontrar o algoritmo de Euclides estendido:

1 = 3 - 2 \* 1

2 = 8 - 3 \* 2

3 = 35 - 8 \* 4

8 = 78 - 35 \* 2

1 = 3 - (8 - 3 \* 2) \* 1

1 = 3 + 3 \* 2 - 8

1 = 3 \* 3 - 8

1 = 3 \* (35 - 8 \* 4) - 8

1 = 3 \* 35 - 8 \* 12 - 8

1 = 3 \* 35 - 8 \* 13

1 = 3 \* 35 - (78 - 35 \* 2) \* 13

1 = 3 \* 35 - 78 \* 13 + 35 \* 26

1 = 35 \* 29 + 78 \* (-13)

**Exercício 6:**

**Letra A)** Para encontrar o inverso precisamos desenvolver o algoritmo de Euclides estendido. Assim, temos:

2 (mod 17)

17 = 2 \* 8 + 1

2 = 1 \* 2

1 = 17 + 2 \* (-8)

Para encontrar o inverso, devemos calcular -8 mod 17 = 9. Logo o inverso é 9, e qualquer número congruente a -8 mod 17.

**Letra B)** Para encontrar o inverso precisamos desenvolver o algoritmo de Euclides estendido. Assim, temos:

89 (mod 144)

144 = 89 \* 1 + 55

89 = 55 \* 1 + 34

55 = 34 \* 1 + 21

34 = 21 \* 1 + 13

21 = 13 \* 1 + 8

13 = 8 \* 1 + 5

8 = 5 \* 1 + 3

5 = 3 \* 1 + 2

3 = 2 \* 1 + 1

2 = 1 \* 2

1 = 3 - 2 \* 1

2 = 5 - 3

3 = 8 - 5

5 = 13 - 8

8 = 21 - 13

13 = 34 - 21

21 = 55 - 34

34 = 89 - 55

55 = 144 - 89

1 = 3 - (5 - 3)

1 = 3 \* 2 - 5

1 = 2 \* (8 - 5) - 5

1 = 2 \* 8 - 3 \* 5

1 = 2 \* 8 - 3 \* (13 - 8)

1 = 2 \* 8 - 3 \* 13 + 3 \* 8

1 = 5 \* (21 - 13) - 3 \* 13

1 = 5 \* 21 - 5 \* 13 - 3 \* 13

1 = 5 \* 21 - 8 \* (34 - 21)

1 = 5 \* 21 - 8 \* 34 + 8 \* 21

1 = 13 \* (55 - 34) - 8 \* 34

1 = 13 \* 55 - 13 \* 34 - 8 \* 34

1 = 13 \* 55 - 21 \* (89 - 55)

1 = 13 \* 55 - 21 \* 89 + 21 \* 55

1 = 34 \* (144 - 89) - 21 \* 89

1 = 34 \* 144 - 34 \* 89 - 21 \* 89

1 = 34 \* 144 + 89 \* (-55)

Para encontrar o inverso, devemos calcular -55 mod 144 = 89. Logo o inverso é 89, e qualquer numero congruente a -55 mod 144.

**Exercício 7:**

**Letra A)** Devemos realizar os seguintes cálculos para encontrar a congruência:

2x ≡ 5 (mod 17)

9 \* 2x ≡ 9 \* 5 (mod 17)

18x ≡ 45 (mod 17)

x ≡ 11 (mod 17)

11 e qualquer valor congruente a 11 modulo 17 é a solução.

**Letra B)** Devemos realizar os seguintes cálculos para encontrar a congruência:

89x ≡ 4 (mod 144)

89 \* 89x ≡ 4 \* 89 (mod 144)

7921x ≡ 356 (mod 144)

x ≡ 68 (mod 144)

68 e qualquer valor congruente a 68 modulo 144 é a solução.

**Exercício 8:**

Para encontrar todas as soluções do sistema em questão utilizando o teorema chines, temos os seguintes cálculos:

m = 3 \* 4 \* 5 = 60

m1 = 60 / 3 = 20

m2 = 60 / 4 = 15

m3 = 90 / 5 = 12

**Inverso de m1:**

20 (mod 3)

20 = 3 \* 6 + 2

3 = 2 \* 1 + 1

2 = 1 \* 2

1 = 3 - 2

2 = 20 - 3 \* 6

1 = 3 - (20 - 3 \* 6)

1 = 3 - 20 + 3 \* 6

1 = 3 \* 7 + 20 \* (-1)

Inverso de m1 = -1 mod 3 = 2

**Inverso de m2:**

15 (mod 4)

15 = 4 \* 3 + 3

4 = 3 \* 1 + 1

3 = 1 \* 3

1 = 4 - 3

3 = 15 - 4 \* 3

1 = 4 - (15 - 4 \* 3)

1 = 4 + 4 \* 3 - 15

1 = 4 \* 4 + 15 \* (-1)

Inverso de m2 = -1 mod 4 = 3

**Inverso de m3:**

12 (mod 5)

12 = 5 \* 2 + 2

5 = 2 \* 2 + 1

2 = 2 \* 1

1 = 5 - 2 \* 2

2 = 12 - 5 \* 2

1 = 5 - 2 \* (12 - 5 \* 2)

1 = 5 - 2 \* 12 + 5 \* 4

1 = 5 \* 5 + 12 \* (-2)

Inverso de m3 = -2 mod 5 = 3

Assim, com isso:

X = 2 \* 20 \* 2 + 1 \* 15 \* 3 + 3 \* 12 \* 3

X = 80 + 45 + 108

X = 233

233 é congruente a 55 (mod 60)

**Exercício 9:**

**Letra A)** Utilizando o pequeno teorema de Fermat, temos:

373 (mod 5)

34 ≡ 1 mod 5

(34)k ≡ 1 mod 5

73 = 4 \* 18 + 1

373 = 34 \* 18 + 1

(34)18 \* 3 ≡ 118 \* 3 ≡ 3 mod 5

373 mod 5 = 3

**Letra A)** Utilizando o pequeno teorema de Fermat, temos:

373 (mod 11)

310 ≡ 1 mod 11

(310)k ≡ 1 mod 11

73 = 7 \* 10 + 3

373 = 37 \* 10 + 3

(310)7 \* 33 ≡ 17 \* 27 ≡ 5 mod 11

373 mod 11 = 5

**Exercício 10:**

**Exercício 11:**

Seja (n, e) = (33, 3) a chave publica escolhida por alguém no sistema RSA, para encontrar a chave secreta devemos encontrar um p e q tal que 33 = p \* q, onde p e q são dois primos grandes, com isso devemos encontrar a chave secreta d = inverso de 3 modulo (p - 1) \* (q - 1). Com isso, temos que p = 3 e q = 11 são dois primos grandes, e consequentemente d = inverso de 3 modulo 2 \* 10 = inverso de 3 modulo 20. Agora devemos utilizar o algoritmo de Euclides para encontrar inverso de 3 modulo 20, com isso temos:

20 = 3 \* 6 + 2

3 = 2 \* 1 + 1

2 = 1 \* 2

1 = 3 - 2 \* 1

2 = 20 - 3 \* 6

1 = 3 - (20 - 3 \* 6)

1 = 3 - 20 + 3 \* 6

1 = 3 \* **7** - 20

Logo, d = 7. Desse modo, a chave secreta será 7.

**Exercício 12:**

**Letra A)** Sabendo que escolheram o primo p = 23 e a = 5, temos que cada um enviou a seguinte mensagem para o outro:

1) Alice escolhe um inteiro secreto k1 = 8, e então envia a Bob A = ak1 mod p.

A = 58 mod 23

A = ((25 mod 23)4) = 16 mod 23

A = 16

2) Bob escolhe um inteiro secreto k2 = 5, e então envia a Bob B = ak2 mod p.

B = 55 mod 23

B = 3125 mod 23

Padrão do plano de fundo

Descrição gerada automaticamente com confiança baixa

B = 20

**Letra B)** Baseado nas mensagens enviadas por Alice e Bob no exercício 12, letra A. Temos que:

1) Com a mensagem recebida por Bob, Alice calculará a chave secreta d1 = Bk1 mod p

d1 = 208 mod 23

d1 = ((400 mod 23)4) = ((81 mod 23)2) = 144 mod 23

d1 = 6

2) Com a mensagem recebida por Alice, Bob calculará a chave secreta d2 = Ak2 mod p

d2 = 165 mod 23

d2 = 1048576 mod 23

Padrão do plano de fundo

Descrição gerada automaticamente com confiança baixa

d2 = 6

Assim, Alice e Bob compartilham a mesma chave secreta d1 = d2 = 6.

**Exercício 13:**

**Letra A)** Mesmo interceptando a mensagem e encontrando os valores p = 23, a = 5, ak1 mod p = 16 e ak2 mod p = 20, para calcular k1, k2e a elevado k1 elevado k2 é necessário utilizar logaritmo discreto, o que torna isso inviável se p e a são suficientemente grandes pois devemos testar cada valor até encontrar o valor correto, assim fica evidente que é mais fácil para eles calcularem a chave secreta que para min.

**Letra B)** Para encontrar a chave secreta, devemos utilizar logaritmo discreto, ou seja, testar valores de k1, k2 até encontrá-los:

1) Encontrando o valor k1, escolhido por Alice, através da fórmula 5k1 mod 23 = 16:

51 mod 23 = 5

52 mod 23 = 2

Padrão do plano de fundo

Descrição gerada automaticamente com confiança baixa

53 mod 23 = 10

Padrão do plano de fundo

Descrição gerada automaticamente com confiança baixa

54 mod 23 = 4

Padrão do plano de fundo

Descrição gerada automaticamente com confiança baixa

55 mod 23 = 20 (demonstração de cálculo no exercício 12, letra A)

56 mod 23 = 8

Padrão do plano de fundo

Descrição gerada automaticamente com confiança baixa57 mod 23 = 17

Padrão do plano de fundo

Descrição gerada automaticamente com confiança baixa

58 mod 23 = **16** (demonstração de cálculo no exercício 12, letra A)

Com isso encontramos o k1 = 8.

2) Encontrando o valor k2, escolhido por Bob, através da fórmula 5k2 mod 23 = 20:

51 mod 23 = 5 (demonstração de cálculo no item 1 desse exercício)

52 mod 23 = 2 (demonstração de cálculo no item 1 desse exercício)

53 mod 23 = 10 (demonstração de cálculo no item 1 desse exercício)

54 mod 23 = 4 (demonstração de cálculo no item 1 desse exercício)

55 mod 23 = **20** (demonstração de cálculo no exercício 12, letra A)

Com isso encontramos o k2 = 20

Tendo os valores k1 e k2, podemos encontrar o valor da chave secreta da seguinte forma:

d = 5k1\*k2 mod 23

d = 540 mod 23 = (52)20 mod 23 = ((25 mod 23)20) mod 23 = ((32 mod 23)4) mod 23 = ((81 mod 23)2) mod 23 = 144 mod 23 = 6.

Assim, conseguimos encontrar a chave secreta d de Bob e Alice, que é d = 6.

**Observação:**

Todos os cálculos foram realizados a mão em um papel, e depois passei as contas mais importantes e resultados de forma organizada em documento de texto. Utilizei o Symbolab (<https://pt.symbolab.com/>), apenas para gerar as imagens de divisão, conforme a de exemplo abaixo, com o fim de deixar minhas respostas mais organizadas:

Padrão do plano de fundo

Descrição gerada automaticamente com confiança baixa