APOSTILA CRIPTOGRAFIA RSA

Sumário

1 Teoria dos Números **1**

1.1 Divisibilidade 1

1.2 Divisão Euclidiana 2

1.3 Máximo Divisor Comum (mdc) e Algoritmo de Euclides 3

1.4 Equações Diofantinas 6

1.5 Números Primos 10

2 Aritmética Modular **15**

2.1 Congruências 15

2.2 Teorema de Euler e Pequeno Teorema de Fermat 18

2.3 Congruências Lineares 20

2.4 Sistema de Congruências e o Teorema Chinês dos Restos 25

3 Criptografia **31**

3.1 Cifras de Transposição e Substituição 31

3.2 Criptografia nos séculos XIX e XX 35

3.3 Criptografia no pós-guerra: Diffie-Hellman e RSA 37

4 Criptografia RSA **41**

4.1 Pré-Codificação 41

4.2 Codificação 42

4.3 Decodificação 43

4.4 Funcionamento 45

4.5 Segurança 47

Resolução dos Exercícios **51**

Resoluções – Capítulo 1 51

Resoluções – Capítulo 2 58

Resoluções – Capítulo 4 68

Capítulo 1

Teoria dos Números

1.1 Divisibilidade

Você certamente viu no 6º ano o conceito de divisibilidade. Termos como "Múltiplo", "Divisor", "Divisível", entre outros. Certamente vocês viram também os critérios de divisibilidade (por 2, 3, 5, 6, 10, etc). Vamos trazer uma definição mais "formal" para esse conceito.

Se eu tenho dois números inteiros a e b, com $a \neq 0$, nós dizemos que a divide b, notação $a \mid b$ quando existe um outro número inteiro c de modo que $b = a \cdot c$.

Essa definição é bem equivalente a: "O número b é *divisível* pelo número a" ou até mesmo "a é *divisor* de b".

Re-escrevendo essa definição, nós temos: Um número inteiro a ($a \neq 0$) divide outro número inteiro b quando o resto da divisão (euclidiana) de b por a for igual a zero.

O caso negativo dessa definição é: Um número inteiro a ($a \neq 0$) **não** divide outro número inteiro b (notação: $a \nmid b$) quando o resto da divisão (euclidiana) de b por a for **diferente** de zero.

Exemplo 1. a) $3 \mid 27$ pois $27 = 3 \cdot 9$

b) $4 \mid 48$ pois $48 = 4 \cdot 12$

c) $6 \nmid 64$ pois não existe inteiro c tal que $64 = 6 \cdot c$

Alguns casos particulares (com $a \in \mathbb{Z}$):

- $1 \mid a$, pois $a = 1 \cdot a$.
- $a \mid 0$, pois $0 = a \cdot 0$.
- $a \mid a$ pois $a = a \cdot 1$.

1.1.1 Exercícios

1) Responda, **justificando**, quais afirmações são verdadeiras ou falsas:

a) $9 \mid 495$
b) $7 \mid 1260$
c) $8 \mid 349$
d) $12 \nmid 378$
e) $14 \mid 182$
f) $3 \nmid 46809$

2) Dona Augusta quer colocar 255 balas em saquinhos, todos com a mesma quantidade de balas, mas de modo que não sobre nenhuma. Que quantidade de balas ela pode colocar em cada saquinho: 8 balas, 12 balas ou 15 balas? **Verificar cada caso.**

1.2 Divisão Euclidiana

Quando queremos dividir dois números inteiros a e b, com $0 < b < a$, a partir dessa divisão são gerados um *quociente* (q) e um *resto* (r), de modo que a relação entre eles é dada da seguinte forma:

$$\underbrace{a}_{\text{Dividendo}} = \underbrace{b}_{\text{Divisor}} \cdot \overbrace{q}^{\text{Quociente}} + \underbrace{r}_{\text{Resto}}, \text{ com } 0 \leq r < b \tag{1.2.1}$$

A partir dessa igualdade, podemos resolver muitos problemas envolvendo divisões:

Exemplo 2. Encontre o número natural que ao ser dividido por 7 resulta um quociente 4 e resto maior possível.

Resolução. Sabemos que $b = 7$, $q = 4$, o resto é o maior possível e queremos encontrar a. Da igualdade 1.2.1, nós sabemos que o resto deve ser menor que 7, então o maior resto possível é $r = 6$. Com essas informações, podemos calcular o que queremos:

$$a = 7 \cdot 4 + 6 = 28 + 6 = 34$$

Ou seja, 34 é o número encontrado.

Exemplo 3. Na divisão de dois números inteiros, o quociente é 16 e o resto é o maior possível. Se a soma do dividendo e do divisor é 125, determine o resto.

Resolução. Do enunciado, sabemos que $q = 16$, que r é o maior possível, ou seja, $r = b - 1$ e que $a + b = 125$. Descobrindo o valor de b, nós podemos encontrar o resto dessa divisão. Vamos substituir os valores conhecidos na igualdade 1.2.1:

$$a = 16b + b - 1 \Rightarrow a = 17b - 1$$

Somando-se b em ambos os lados:

$$a + b = 17b - 1 + b \Rightarrow 125 = 18b - 1$$

Resolvendo essa equação:

$$125 = 18b - 1 \Rightarrow 18b = 126 \Rightarrow b = \frac{126}{18} \Rightarrow b = 7$$

Ou seja, $b = 7$. Como queremos achar o resto, e que já sabemos que $r = b - 1$, então $r = 7 - 1 = 6$. Portanto, o resto dessa divisão é igual a 6.

1.2.1 Exercícios

3) Encontre o número natural que ao ser dividido por 12 resulta um quociente 8 e resto maior possível.

4) Na divisão de dois números inteiros, o quociente é 23 e o resto é o maior possível. Se a diferença do dividendo e do divisor é 206, determine o resto.

5) Em uma divisão, o dividendo é 463 e o quociente é igual a 15. Sabendo que o resto dessa divisão é o maior possível, qual é o valor do divisor?

6) Calcule o resto da divisão de 26877 por 9 sem efetuar divisões.

7) Se o resto da divisão do número inteiro positivo b por 7 é igual a 5, então o resto da divisão do número $b^2 + b + 11$ por 7 é igual a quanto?

1.3 Máximo Divisor Comum (*mdc*) e Algoritmo de Euclides

Se temos dois números inteiros a e b, o máximo divisor comum (mdc) entre eles é um número d que *divide* ambos esses números e, além disso, é o maior número que divide eles. Usando a notação de divisão, essa definição fica da forma:

i) $d \geq 0$

ii) $d \mid a$ e $d \mid b$

iii) Se $d' \mid a$ e $d' \mid b$ então $d' \mid d$

Denotaremos o mdc entre dois números inteiros a e b por $mdc(a, b)$.

Alguns casos particulares do mdc. Dados $a, b \in \mathbb{Z}$, com $a \neq 0$. Então temos que

i) $mdc(0, a) = |a|$ (módulo de a)

ii) $mdc(1, a) = 1$

iii) $mdc(a, a) = a$

iv) $a \mid b \Rightarrow mdc(a, b) = a$

Além disso, dois números inteiros a e b são considerados **co-primos**, ou **primos entre si** se $mdc(a, b) = 1$.

Exemplo 4. Calcule $mdc(100, 28)$

Resolução. Utilizando o procedimento normalmente usado no ensino fundamental:

100,28	2
50,14	2
25,7	5
5,7	5
1,7	7
1,1	$2 \cdot 2 = 4$

Com isso, $mdc(100, 28) = 4$

Esse método é útil quando queremos calcular o mdc de números relativamente pequenos, mas se quisermos, por exemplo, calcular $mdc(2028, 120)$, o procedimento acima seria bem longo e tedioso. Em relação a isso, existe um algoritmo voltado a obtenção do mdc de números grandes, chamado de **Algoritmo de Euclides**.

Vamos mostrar esse algoritmo e usá-lo para calcular o mdc acima. Existe um resultado muito importante que relaciona o mdc com a divisão euclidiana, chamada de **Lema de Euclides**:

Sejam a e b inteiros com $b \neq 0$, q e r respectivamente o quociente e o resto da divisão de a por b, isto é, $a = bq + r$, com $0 \leq r < |b|$ Então

$$mdc(a, b) = mdc(b, r), \text{ ou } mdc(a, b) = mdc(b, a - bq)$$

Usando esse lema, o algoritmo consiste em realizar divisões sucessivas até chegarmos uma divisão com resto igual a zero.

O algoritmo detalhado é o seguinte:

Queremos calcular $mdc(a, b)$. Sem perda de generalidade, $b \leq a$. Se tivermos $b = 1, b = a$ ou $b|a$, já vimos que $mdc(a, b) = a$. Então, vamos supor que $b < a$ e que $b \nmid a$. Disso, pela divisão euclidiana, existem $q_1, r_1 \in \mathbb{N}$ tal que:

$$a = bq_1 + r_1, \text{ com } 0 < r_1 < b$$

Disso temos duas situações: Ou $r_1|b$, o que implica em $r_1 = mdc(b, r_1)$, e, pelo Lema de Euclides, $mdc(b, r_1) = mdc(b, a) = mdc(a, b)$ (algoritmo termina). Ou $r_1 \nmid b$, o que nesse caso podemos repetir o passo anterior e fazer a divisão euclidiana de b por r_1:

$$b = r_1q_2 + r_2 \text{ com } 0 < r_2 < r_1$$

Novamente temos duas situações: Ou $r_2|r_1$, o que implica em $r_2 = mdc(r_1, r_2)$, e, pelo Lema de Euclides, $mdc(r_1, r_2) = mdc(r_1, b) = mdc(a, b)$ (algoritmo termina). Ou $r_2 \nmid r_1$, o que nesse caso podemos repetir o passo anterior e fazer a divisão euclidiana de r_1 por r_2:

$$r_1 = r_2 q_3 + r_3 \text{ com } 0 < r_3 < r_2$$

Esse processo deve ser continuado até achar um par r_n, r_{n-1} onde se tenha $r_n|r_{n-1}$. É comprovado que, para algum n, teremos $r_n|r_{n-1}$, implicando em $r_n = mdc(a, b)$.

OBS: Um modo "seguro" de se obter o $mdc(a, b)$, sem deixar nenhum passo faltando é realizar o algoritmo até que o **resto** da divisão euclidiana seja igual a **zero**. Quando isso acontecer, o resto da divisão euclidiana **anterior** será o *mdc*.

Vamos aplicar esse algoritmo ao exemplo anterior:

Exemplo 5. Calcule $mdc(2028, 120)$

Resolução. Vamos fazer as divisões sucessivas:

$$\begin{cases} 2028 = 120 \times 16 + 108 \\ 120 = 108 \times 1 + 12 \\ 108 = 12 \times 9 + 0 \end{cases}$$

Logo, $mdc(2028, 120) = 12$.

Exemplo 6. Calcule $mdc(639, 234)$.

Resolução. Vamos fazer as divisões sucessivas:

$$\begin{cases} 639 = 234 \times 2 + 171 \\ 234 = 171 \times 1 + 63 \\ 171 = 63 \times 2 + 45 \\ 63 = 45 \times 1 + 18 \\ 45 = 18 \times 2 + 9 \\ 18 = 9 \times 2 + 0 \end{cases}$$

Logo, $mdc(639, 234) = 9$.

1.3.1 Exercícios

8) Use o *Algoritmo de Euclides* para calcular o *mdc* de cada par de números a seguir:

   a) $mdc(202, 28)$
   b) $mdc(389, 167)$
   c) $mdc(3387, 637)$
   d) $mdc(874, 551)$
   e) $mdc(3027, 1224)$
   f) $mdc(7469, 2464)$

9) Um prédio possui duas escadas; uma delas com 780 degraus e a outra com 700 degraus. Sabendo que os degraus das duas escadas só estão no mesmo nível quando conduzem a um andar, descubra quantos andares tem o prédio?

10) A Capoeira é a manifestação da cultura popular afro-brasileira, que combina harmoniosamente luta, jogo e dança, realizado com o acompanhamento de instrumentos musicais. Dois grupos estão participando de uma roda de capoeira. O Grupo A tem 84 participantes e o Grupo B tem 66 participantes. O mestre deseja formar subgrupos com o maior número possível de pessoas,

garantindo que todos os subgrupos tenham o mesmo número de participantes e sejam formados apenas por integrantes de um mesmo grupo.

Qual será a quantidade de subgrupos do Grupo A?

1.4 Equações Diofantinas

Esses tipos de equações recebem esse nome por causa de *Diofanto de Alexandria*, matemático grego do século III. É considerado um dos matemáticos mais influentes de sua época e considerado o pai da Álgebra e da Teoria dos Números.

Uma *Equação Diofantina Linear* é é qualquer equação polinomial que tenha coeficientes inteiros, com uma ou mais incógnitas.

Ela é é da forma:

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b$$

Onde $a_1, a_2, \ldots, a_n$ são números inteiros, b também é, chamado de *termo independente* e $x_1, \ldots, x_n$ são as incógnitas.

Iremos ver com mais detalhe as equações com duas incógnitas, que são da forma $ax + by = c$, através do seguinte *problema*:

"Um jogo eletrônico tem o seguinte funcionamento: A máquina exibe um número inteiro positivo, que corresponde a pontuação exata que o jogador deverá marcar para vencer a partida. Os pontos são marcados cada vez que o jogador abate um invasor, que o fica desafiando na tela. Existem dois tipos de invasores: os marcianos (na cor vermelha), valendo cada um 14 pontos e os jupiterianos (na cor verde), com o valor individual de 10 pontos. Suponha que você vai participar deste jogo e a máquina lhe exibe o número 420. De quantas maneiras você pode vencer o jogo? Quantos invasores de cada cor você deverá abater?"

Deveremos procurar saber qual o número de marcianos e qual o número de jupiterianos que devem ser abatidos de modo a chegar exatamente nessa pontuação. Denotaremos, respectivamente por x e y essas quantidades. Relacionando as variáveis temos a equação: $14x + 10y = 420$.

Toda resolução de uma equação diofantina consiste de seguirmos três passos:

i) Verificar se a equação possui solução.

ii) Encontrar uma solução particular dessa equação.

iii) Determinar o seu conjunto solução.

Nem toda equação diofantina dessa forma admite solução. Para que uma solução exista, é necessário que $mdc(a, b) \mid c$. Na equação presente no problema acima, temos que $mdc(14, 10) = 2$ e que $2 \mid 420$, pois $420 = 2 \cdot 210$. Com isso, essa equação possui solução.

O próximo passo é encontrarmos uma solução particular dessa equação, ou seja, achar um par ordenado (x, y), com coordenadas inteiras, que resolva essa equação. Em alguns casos, se consegue achar um par diretamente, em outros casos, uma solução é encontrada atráves de um método chamado de *Algoritmo de Euclides Estendido*.

Este algoritmo, publicado pela primeira vez em 1963 por *D.E. Knuth*, calcula, ao mesmo tempo, o mdc de dois números inteiros a e b e determina inteiros x e y tal que $ax + by = mdc(a, b)$. Esse algoritmo é realizando usando matrizes.

O algoritmo detalhado é o seguinte:

SPG, suponha $a \geq b$. Para calcular $mdc(a, b)$ montamos a matriz:

$$A = \begin{bmatrix} b & 1 & 0 \\ a & 0 & 1 \end{bmatrix}$$

Efetuando-se a divisão euclidiana entre a e b, temos $a = bq_1 + r_1$. O primeiro passo do algoritmo consiste em diminuir da segunda linha q_1 vezes a primeira linha, obtendo a matriz:

$$A_1 = \begin{bmatrix} b & 1 & 0 \\ a - bq_1 & -q_1 & 1 \end{bmatrix} = \begin{bmatrix} b & 1 & 0 \\ r_1 & -q_1 & 1 \end{bmatrix}$$

Efetuando-se agora a divisão euclidiana entre b e r_1, temos $b = r_1q_2 + r_2$. O segundo passo do algoritmo consiste em diminuir da primeira linha q_2 vezes a segunda linha, obtendo a matriz:

$$A_2 = \begin{bmatrix} b - q_2r_1 & 1 + q_1q + 2 & -q_2 \\ a - bq_1 & -q_1 & 1 \end{bmatrix} = \begin{bmatrix} r_2 & 1 + q_1q_2 & -q_2 \\ r_1 & -q_1 & 1 \end{bmatrix}$$

O processo repete-se, seguindo esses dois passos, reproduzindo o algoritmo de Euclides efetuado, agora, sobre as duas linhas da matriz, até obtermos no final uma matriz B, da forma:

$$B = \begin{bmatrix} d & y & x \\ 0 & k & l \end{bmatrix} \text{ ou } B = \begin{bmatrix} 0 & k & l \\ d & y & x \end{bmatrix}$$

Nessas matrizes, $d = mdc(a, b)$ e x e y são inteiros tais que $d = ax + by$. Importante não se esquecer da ordem: Na matriz final, o primeiro elemento é o mdc, o segundo elemento é o valor de y e o terceiro elemento é o valor de x.

OBS: O fato desse algoritmo existir **não** significa que vocês devem usar esse algoritmo para achar uma solução particular de toda e qualquer equação diofantina que exista. Algumas equações tem soluções de fácil identificação e outras equações podem ter soluções encontradas por pura tentativa e erro. Se você não conseguir identificar uma solução facilmente, você deve usar esse algoritmo.

Para podermos usar esse algoritmo no problema anterior, precisamos achar uma solução para $14x + 10y = 2$, pois, $2 = mdc(14, 10)$. Vamos lá:

$$\begin{bmatrix}10 & 1 & 0\\ 14 & 0 & 1\end{bmatrix} \Rightarrow \begin{bmatrix}10 & 1 & 0\\ 14-1\cdot 10 & 0-1\cdot 1 & 1-1\cdot 0\end{bmatrix} \Rightarrow \begin{bmatrix}10 & 1 & 0\\ 4 & -1 & 1\end{bmatrix} \Rightarrow$$
$$\Rightarrow \begin{bmatrix}10-2\cdot 4 & 1-2\cdot(-1) & 0-2\cdot 1\\ 4 & -1 & 1\end{bmatrix} \Rightarrow \begin{bmatrix}2 & 3 & -2\\ 4 & -1 & 1\end{bmatrix} \Rightarrow$$
$$\Rightarrow \begin{bmatrix}2 & 3 & -2\\ 4-2\cdot 2 & -1-2\cdot(3) & 1-2\cdot(-2)\end{bmatrix} \Rightarrow \begin{bmatrix}2 & 3 & -2\\ 0 & -7 & 5\end{bmatrix}$$

Pelo algoritmo, uma solução particular é $(-2, 3)$, ou seja, $14 \cdot (-2) + 10 \cdot 3 = 2$. Foi visto anteriormente que $420 = 2 \cdot 210$, então multiplicando a equação nos dois lados por 210, obtemos:

$$14 \cdot (-420) + 10 \cdot (630) = 420$$

Com isso, $(-420, 630)$ é uma solução particular de $14x + 10y = 420$.

O último passo da resolução dessa equação é determinarmos seu *Conjunto Solução*. De um modo geral, se uma equação diofantina possui alguma solução, então ela possui *infinitas* soluções. Se (x_0, y_0) for uma solução de uma equação diofantina $ax + by = c$ então sua solução geral é dada por:

$$S = \left\{ \left(x_0 + \frac{b}{d}t, y_0 - \frac{a}{d}t \right) \mid t \in \mathbb{Z} \right\}$$

Onde $t \in \mathbb{Z}$ e $d = mdc(a, b)$.

Determinando o conjunto solução da equação diofantina do problema, obtemos:

$$S = \{(-420 + 5t, 630 - 7t) \,| t \in \mathbb{Z}\}$$

Isso resolve nosso problema? **Não**, pois nos é interessado apenas as soluções que sejam inteiros não-negativos (não deve existir uma quantidade negativa de invasores destruídos). Assim, devemos impor a condição:

$$-420 + 5t \geq 0, \qquad 630 - 7t \geq 0$$

Resolvendo essas inequações, obtemos $t \geq 84$ e $t \leq 90$. Como $t \in \mathbb{Z}$, então $t = 84, 85, 86, 87, 88, 89, 90$. Para saber as soluções, precisamos substituir os valores de t acima na solução geral:

- $t = 84 \Rightarrow (-420 + 5 \cdot 84, 630 - 7 \cdot 84) = (0, 42)$
- $t = 85 \Rightarrow (-420 + 5 \cdot 85, 630 - 7 \cdot 85) = (5, 35)$
- $t = 86 \Rightarrow (-420 + 5 \cdot 86, 630 - 7 \cdot 86) = (10, 28)$
- $t = 87 \Rightarrow (-420 + 5 \cdot 87, 630 - 7 \cdot 87) = (15, 21)$

- $t = 88 \Rightarrow (-420 + 5 \cdot 88, 630 - 7 \cdot 88) = (20, 14)$
- $t = 89 \Rightarrow (-420 + 5 \cdot 89, 630 - 7 \cdot 89) = (25, 7)$
- $t = 90 \Rightarrow (-420 + 5 \cdot 90, 630 - 7 \cdot 90) = (30, 0)$

Assim, para ganhar o jogo, deve-se fazer as combinações acima de marcianos e jupiterianos destruídos, respectivamente.

Vamos ver outro exemplo:

Exemplo 7. Determine o conjunto solução da equação diofantina $14x + 9y = 51$.

Resolução. Primeiro passo, ver se ela tem solução. $mdc(14, 9) = 1$ e como $1|51$, ela possui solução.

Segundo passo, encontrar uma solução particular. Usando o algoritmo **estendido**:

$$\begin{bmatrix} 9 & 1 & 0 \\ 14 & 0 & 1 \end{bmatrix} \Rightarrow \begin{bmatrix} 9 & 1 & 0 \\ 14 - 1 \cdot 9 & 0 - 1 \cdot 1 & 1 - 1 \cdot 0 \end{bmatrix} \Rightarrow \begin{bmatrix} 9 & 1 & 0 \\ 5 & -1 & 1 \end{bmatrix} \Rightarrow$$

$$\Rightarrow \begin{bmatrix} 9 - 1 \cdot 5 & 1 - 1 \cdot (-1) & 0 - 1 \cdot 1 \\ 5 & -1 & 1 \end{bmatrix} \Rightarrow \begin{bmatrix} 4 & 2 & -1 \\ 5 & -1 & 1 \end{bmatrix} \Rightarrow$$

$$\Rightarrow \begin{bmatrix} 4 & 2 & -1 \\ 5 - 1 \cdot 4 & -1 - 1 \cdot (2) & 1 - 1 \cdot (-1) \end{bmatrix} \Rightarrow \begin{bmatrix} 4 & 2 & -1 \\ 1 & -3 & 2 \end{bmatrix}$$

Com isso, uma solução particular para $14x + 9y = 1$ é $(2, -3)$, ou seja, $14 \cdot 2 + 9 \cdot (-3) = 1$. Multiplicando a equação nos dois lados por 51, obtemos:

$$14 \cdot 102 + 9 \cdot (-153) = 51$$

Com isso, $(102, -153)$ é uma solução particular de $14x + 9y = 51$.

Para finalizar, o conjunto solução é:

$$S = \{(102 + 9t, -153 - 14t) \,|t \in \mathbb{Z}\}$$

OBS: Se quiséssemos uma solução completamente positiva, teríamos que fazer que nem o problema anterior e impor uma condição para as duas componentes do conjunto solução:

$$102 + 9t \geq 0, \qquad -153 - 14t \geq 0$$

Resolvendo essas inequações, obtemos $t \geq -11,333\ldots$ e $t \leq -10,92$. Como $t \in \mathbb{Z}$, então $t = -11$.

Substituindo t por -11, nós encontraremos o único par positivo desse conjunto solução:

$$(x, y) = (102 + 9 \cdot (-11), -153 - 14 \cdot (-11)) = (102 - 99, -153 + 154) = (3, 1)$$

O único par positivo desse conjunto solução é o par $(3, 1)$.

1.4.1 Exercícios

11) Para as equações diofantinas abaixo, verifique se cada uma delas possui solução e, em caso positivo, determine o conjunto solução:

    a) $18x + 2y = 52$
    b) $72x + 56y = 40$
    c) $44x + 12y = 78$
    d) $27x + 15y = 309$
    e) $102x + 3y = 34$

12) Determine as soluções positivas das equações diofantinas do exercício anterior que admitem solução.

13) Deseja-se comprar 225 bolas de gude que são vendidas em saquinhos que contém 6 ou 15 bolinhas. Determine as quantidades necessárias de saquinhos para efetivação da compra.

14) Um caixa eletrônico tem apenas notas de $R\$20,00$ e $R\$50,00$. De quantas maneiras este caixa pode liberar um saque de $R\$530,00$?

1.5 Números Primos

Um número natural, maior do que 1, é chamado de *primo* se os únicos divisores dele forem o número um e o próprio número. Se um número natural não é primo, então ele é chamado de *composto*.

Os primeiros números primos são:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, \ldots$$

Um resultado bem importante que envolve os números primos, que também é um dos pilares da Teoria dos Números, é o **Teorema Fundamental da Aritmética (TFA)**. Formalmente, ele é definido da forma:

"Todo número natural a, maior do que 1, pode ser escrito de forma ***única****, a menos da ordem dos fatores, como um produto de primos. De outra forma, isso significa que:*

$$a = p_1 p_2 \dots p_n,$$

onde $p_1 p_2 \dots p_n$ são primos, não necessariamente distintos."

Definindo de outra forma, todo número natural pode ser *fatorado* (via divisões sucessivas), em um produto de números primos. Essa fatoração tem o nome de *Fatoração Canônica*

Exemplo 8. Faça a fatoração do número 300.

Resolução.

300	2
150	2
75	3
25	5
5	5
1	$2^2 \cdot 3 \cdot 5^2$

Ou seja, $300 = 2^2 \cdot 3 \cdot 5^2$

Os números primos não necessariamente precisam estar em ordem na fatoração.

Um resultado extremamente importante sobre números primos é que*existem infinitos deles.* Mesmo que não consigamos determinar todos os números primos existentes (e talvez nunca consigamos), pelo menos nós sabemos que existem infinitos números primos. Vamos mostrar agora uma demonstração que prova exatamente isso.

Vamos mostrar que, dado um conjunto finito qualquer $\mathscr{P}$ de primos, tem que existir um primo fora de $\mathscr{P}$.

Digamos que $\mathscr{P} = \{p_1, \dots, p_s\}$, é um conjunto finito formado apenas por números primos e consideremos o número $\mathscr{N} = p_1 \dots p_s$, que é igual ao produto de todos os primos em $\mathscr{P}$. Como $\mathscr{N}$ e $\mathscr{N} + 1$ não podem ter nenhum fator próprio comum, um primo que divide $\mathscr{N}$ não pode dividir $\mathscr{N} + 1$. Mas, todos os primos em $\mathscr{P}$ dividem $\mathscr{N}$; logo nenhum primo em $\mathscr{P}$ pode dividir $\mathscr{N} + 1$. Contudo, pelo **Teorema Fundamental da Aritmética**, o número inteiro $\mathscr{N} + 1$ tem que ter algum fator primo. Como estes fatores não podem dividir $\mathscr{N}$, então são primos que não pertencem a $\mathscr{P}$, provando assim o que queríamos.

Com isso, existem infinitos números primos.

Existem muitos métodos para determinar, ou se determinado número é primo (chamado *testes de primalidade*), ou uma forma de se encontrar sua fatoração (chamados de métodos de fatoração ou de algoritmos de fatoração). Vamos ver uma delas a seguir.

1.5.1 Método de Fermat

Esse é um dos métodos mais elementares que existem. Ele funciona da forma:

Se um número n for um número ímpar composto, ele é possível de se escrever na forma $a^2 - b^2$, com a e b sendo inteiros positivos. Então, n pode ser fatorado como $(a+b)(a-b)$, e com isso, $(a+b)$ e $(a-b)$ serão fatores de n.

Mas como achar esses números a e b? Na prática é o seguinte:

Assumamos que $a = [\sqrt{n}]$, que é a **"função parte inteira"** da raíz quadrada de n.

A função parte inteira é uma função que retorna o maior inteiro que seja igual ou menor que o número de entrada, em outras palavras, ele "pega a parte inteira" do número de entrada.

Após definirmos a, verificamos se $b = \sqrt{a^2 - n}$ é um número inteiro. Se for inteiro, ótimo, encontramos a e b e determinamos nossos fatores. Se não for inteiro, aumentamos o valor de a em uma unidade e fazemos a verificação novamente, até que b seja encontrado.

Se a for incrementado sem sucesso até que ele seja igual a $\dfrac{n+1}{2}$, então ele será primo.

Exemplo 9. Vamos testar esse método para um n composto, $n = 1717$

Resolução. Vamos determinar a: $a = [\sqrt{1717}] = [41{,}43] = 41$. Vamos verificar se b é inteiro: $b = \sqrt{a^2 - n} = \sqrt{1681 - 1717} = \sqrt{-36}$. Como b não é inteiro, devemos incrementar a, ou seja, testarmos para $a + 1 = 42$. Devemos fazer isso quantas vezes forem necessárias até encontrarmos b inteiro. A tabela contém todas as iterações a partir do 42.

a	$b = \sqrt{a^2 - 1717}$	a	$b = \sqrt{a^2 - 1717}$
42	6,8557	51	29,7321
43	11,4891	52	31,4165
44	14,7986	53	33,0454
45	17,5499	54	34,6266
46	19,9749	55	36,1666
47	22,1810	56	37,6699
48	24,2280	57	39,1408
49	26,1534	58	40,5826
50	27,9821	59	42

Após todos esses passos, encontramos nosso b inteiro. Como $a = 59$ e $b = 42$, podemos encontrar nossos fatores: $(a + b) = 59 + 42 = 101$ e $(a - b) = 59 - 42 = 17$, que são os fatores de 1717.

Exemplo 10. Vamos testar esse método agora para um número que seja um quadrado perfeito, digamos $n = 2209$.

Resolução. Se n for um quadrado perfeito, então $a = \sqrt{n}$, $b = 0$ e $a + b = a - b$. Então:

a	$b = \sqrt{a^2 - 2209}$
47	0

Assim $a = 47$ e $b = 0$. Com isso, $(a + b) = 47$ e $(a - b) = 47$, que são os fatores de n. Com isso, n é um quadrado perfeito.

1.5.2 Exercícios

15) Realize a fatoração dos números abaixo:

a) 294
b) 440
c) 1350
d) 1764
e) 3168
f) 10800

16) Realize a fatoração dos números abaixo **via Método de Fermat**:

a) 5913
b) 6887
c) 7663
d) 10117

Capítulo 2

Aritmética Modular

2.1 Congruências

Vamos entrar num território desconhecido, mas não menos interessante. Seja n um número inteiro positivo. Dizemos que dois inteiros a e b são **congruentes módulo** n se eles tiverem o mesmo resto na divisão por n. Pensando em um relógio, que vai de 1 a 12, a $13^{\underline{a}}$ hora e a $85^{\underline{a}}$ hora são congruentes, pois ambos deixam resto 1 na divisão por 12. Ou seja, essas horas são congruentes a hora "1".

Uma definição mais formal é a seguinte: "Dizemos que dois inteiros a e b são **congruentes módulo** n se $a - b$ for um múltiplo de n."

Sua notação é dada por $a \equiv b$ (mod n). Ou seja, $a \equiv b$ (mod n) $\Rightarrow a - b = k \cdot n, k \in \mathbb{Z}$. Caso eles não sejam congruentes, ou seja, se $a - b$ não for um múltiplo de n, escrevemos $a \not\equiv b$ (mod n)

Exemplo 11. i) $25 \equiv 1$ (mod 3), pois $25 - 1 = 24 = 8 \cdot 3$

ii) $26 \equiv -4$ (mod 5), pois $26 - (-4) = 30 = 6 \cdot 5$

iii) $-3 \equiv 4$ (mod 7), pois $-3 - 4 = -7 = (-1) \cdot 7$

iv) $30 \not\equiv 2$ (mod 3), pois $30 - 2 = 28$ e 28 não é múltiplo de 3.

v) $24 \not\equiv 3$ (mod 5), pois $24 - 3 = 21$ e 21 não é múltiplo de 5.

Nós iremos convencionar $n \geq 2$. Embora exista congruência módulo 0 e congruência módulo 1, eles são casos bem particulares que não valem para quaisquer par de inteiros a e b.

Uma consequência dessa definição é o seguinte: $a \equiv b$ (mod n) se, e somente se, a e b tem o mesmo resto quando divididos por n.

Podemos usar essa consequência para definir a **transitividade**: Se $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n}$ então $a \equiv c \pmod{n}$.

Um exemplo é $44 \equiv 19$ (mod 5). Ao fazermos a divisão de 44 por 5, obtemos resto igual a 4. Ao fazermos a mesma coisa com o número 19, também obtemos resto igual a 4. Usando a transitividade, podemos escrever $44 \equiv 4 \pmod{5}$.

Algumas *propriedades* das congruências:

i) Para quaisquer $a, b \in \mathbb{Z}$, se temos $a \equiv b$ (mod n) então temos

$$a \pm c \equiv b \pm c \text{ (mod n) e } ac \equiv bc \text{ (mod n) , para todo } c \in \mathbb{Z}$$

ii) Para quaisquer $a, b, c, d \in \mathbb{Z}$, se temos $a \equiv b$ (mod n) e $c \equiv d$ (mod n) então temos

$$a \pm c \equiv b \pm d \text{ (mod n) e } ac \equiv bd \text{ (mod n)}$$

iii) Para quaisquer $a, b \in \mathbb{Z}$, se $a \equiv b$ (mod n) então

$$a^r \equiv b^r \text{ (mod n), para todo } r \in \mathbb{Z}, r \geq 1$$

iv) (**Lei do cancelamento aditivo**) Para quaisquer $a, b, c \in \mathbb{Z}$, se $a + c \equiv b + c$ (mod n) então $a \equiv b$ (mod n)

v) Para quaisquer $a, b, c \in \mathbb{Z}$, se $ac \equiv bc$ (mod n) então $a \equiv b \left(\text{ mod } \frac{n}{mdc(c,n)} \right)$

vi) (**Lei do cancelamento multiplicativo**) Para quaisquer $a, b, c \in \mathbb{Z}$, se $ac \equiv bc$ (mod n) e $mdc(c, n) = 1$ então $a \equiv b$ (mod n)

Vamos ver alguns exemplos bem interessantes que são resolvidos via congruências:

Exemplo 12. Determine o resto de 3^{333} por 25.

Resolução. Precisamos achar um número "x" tal que $3^{333} \equiv x$ (mod 25). Vamos calcular as primeiras potências de 3 para determinarmos um bom ponto de partida:

$$\begin{cases} 3^1 \equiv 3 \text{ (mod 25)} \\ 3^2 \equiv 9 \text{ (mod 25)} \\ 3^3 \equiv 2 \text{ (mod 25)} \\ 3^4 \equiv 6 \text{ (mod 25)} \\ 3^5 \equiv -7 \text{ (mod 25)} \end{cases}$$

Dessas primeiras potências, um bom ponto de partida é a congruência $3^3 \equiv 2$ (mod 25). Como queremos 3^{333}, podemos aplicar a **propriedade iii)**, e reescrever essa congruência como:

$$(3^3)^{111} \equiv 3^{333} \equiv 2^{111} \text{ (mod 25)}$$

Agora , pela transitividade, temos que $2^{111} \equiv x$ (mod 25), então, precisamos lidar com essa potência 2^{111}. Vamos fazer a mesma coisa feita com as potências de 3:

$$\begin{cases} 2^1 \equiv 2 \pmod{25} \\ 2^2 \equiv 4 \pmod{25} \\ 2^3 \equiv 8 \pmod{25} \\ 2^4 \equiv 16 \pmod{25} \\ 2^5 \equiv 7 \pmod{25} \\ 2^6 \equiv 14 \pmod{25} \\ 2^7 \equiv 3 \pmod{25} \\ 2^8 \equiv 6 \pmod{25} \\ 2^9 \equiv 12 \pmod{25} \\ 2^{10} \equiv -1 \pmod{25} \end{cases}$$

Dessas potências acima, um bom candidato é $2^{10} \equiv -1 \pmod{25}$. Como queremos 2^{111}, podemos aplicar a **propriedade iii)** e reescrever essa congruência como:

$$(2^{10})^{11} \equiv 2^{110} \equiv (-1)^{11} \equiv -1 \pmod{25}$$

Como temos $2^{110} \equiv -1 \pmod{25}$, pela **propriedade i)**, temos que $2^{110} \cdot 2 \equiv (-1) \cdot 2 \pmod{25}$, o que é equivalente a $2^{111} \equiv -2 \pmod{25}$. Como nosso resto deve ser positivo, note que $-2 \equiv 23 \pmod{25}$, pois $-2 - 23 = -25 = 25 \cdot (-1)$.

Concluindo, **o resto da divisão de 3^{333} por 25 é 23**.

Exemplo 13. O dias da semana de um calendário seguem uma relação de congruência módulo 7. Normalmente convenciona-se que o primeiro dia da semana (domingo) é congruente a 0 módulo 7, e assim por diante até o sábado ser congruente a 6 módulo 7. Outra convenção é o dia atual ser congruente a 0 módulo 7 e assim por diante. Seguindo essa ordem, se hoje é quarta-feira, que dia da semana será daqui a 132 dias?

Resolução. Se hoje é quarta-feira, então podemos considerá-lo como "dia 0" e podemos fazer com que ele seja congruente a 0 módulo 7. Então, para acharmos o dia da semana daqui a 132 dias, precisamos primeiramente ver qual será o número congruente a 132, módulo 7. Uma forma segura é através da divisão euclidiana de 132 por 7:

$$132 = 7 \cdot 18 + 6$$

Então $132 \equiv 6 \pmod{7}$. Com isso, se hoje é o "dia 0", daqui a 132 dias, ele será o "dia 132". E como $132 \equiv 6 \pmod{7}$, temos que ver qual dia da semana é congruente a 6 módulo 7. Ora, se quarta-feira é congruente a 0 módulo 7, então:

- Quinta-feira é congruente a 1 módulo 7.
- Sexta-feira é congruente a 2 módulo 7.
- Sábado é congruente a 3 módulo 7.
- Domingo é congruente a 4 módulo 7.
- Segunda-feira é congruente a 5 módulo 7.
- Terça-feira é congruente a 6 módulo 7.

Portanto, o "dia 132" é uma terça-feira.

2.1.1 Exercícios

1) Utilizando as propriedades das congruências, encontre o resto da divisão de:

   a) 3^{40} por 7
   b) 12^{12} por 5
   c) 2^{101} por 11
   d) 14^{256} por 6
   e) $100^{33} + 33^{100}$ por 7
   f) $99^5 + 100^5$ por 4

2) Determine o algarismo das unidades de 2^{70}. [Dica: Analise este número módulo 10]

3) Determine os dois últimos algarismos de 7^{999999}. [Dica: Analise este número módulo 100].

4) (Use o exemplo do calendário como referência) Se hoje é sábado, que dia da semana será daqui a 303 dias? e daqui a 997 dias? e daqui a 1492 dias?

2.2 Teorema de Euler e Pequeno Teorema de Fermat

Vimos anteriormente quando que dois números são co-primos (quando o *mdc* deles é igual a 1). Para cada número natural $n \geq 1$, indiquemos por $\varphi(n)$ o número de inteiros positivos menores ou iguais a n que são co-primos com n. A função φ assim definida é chamada de **Função φ de Euler** (ou Função Totiente de Euler).

Para cada $n \in \mathbb{N}$, considerando o conjunto:

$$A_n = \{m \in \mathbb{N} | 1 \leq m \leq n \text{ e } mdc(m, n) = 1\}$$

temos que $\varphi(n) = \#(A_n)$, em que $\#(A_n)$ é a cardinalidade de A_n. Por exemplo, para $n = 20$, os inteiros positivos menores do que 20 e co-primos com ele são $1, 3, 7, 9, 11, 13, 17, 19$. Ou seja, $\varphi(20) = 8$.

Se n for *primo*, então $\varphi(n) = n - 1$. Para n naturais em geral, há uma expressão própria para calcular $\varphi(n)$:

Se $n > 1$ e $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ é sua **fatoração canônica**, então

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\dots\left(1 - \frac{1}{p_r}\right) \tag{2.2.1}$$

Exemplo 14. Calcule $\varphi(86400)$

Resolução. A fatoração canônica de 86400 é $2^7 \cdot 3^3 \cdot 5^2$. Então, pela expressão 2.2.1, temos que

$$\varphi(86400) = 86400\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right) = 86400\left(\frac{1}{2}\right)\left(\frac{2}{3}\right)\left(\frac{4}{5}\right)$$
$$= 86400 \cdot \frac{4}{15} = 4 \cdot 5760 = \mathbf{23040}$$

O teorema que dá nome a essa seção, o **Teorema de Euler**, relaciona a função definida acima com as congruências. Ela é a seguinte:

Teorema de Euler: Sejam a e n inteiros, com $n \geq 1$ e $mdc(a, n) = 1$. Então

$$a^{\varphi(n)} \equiv 1(\pmod{n})$$

Uma consequência direta desse teorema é o chamado **Pequeno Teorema de Fermat**, que é definido da forma:

Pequeno Teorema de Fermat: Seja p primo e $a \in \mathbb{Z}$ de modo que $p \nmid a$. Então

$$a^{p-1} \equiv 1 \pmod{p}$$

Os exemplos apresentados na seção anterior também podem ser resolvidos utilizando a função de Euler e esses dois teoremas. Vamos ver mais alguns:

Exemplo 15. Determine o resto da divisão de 3^{2026} por 8.

Resolução. Como $mdc(3, 8) = 1$, o Teorema de Euler pode ser usado. Como $\varphi(8) = 4$, segue que:

$$3^4 \equiv 1 \pmod{8}$$

Efetuando a divisão euclidiana de 2026 por 4, obtemos: $2026 = 4 \cdot 506 + 2$, ou seja, elevando ambos os membros da congruência por 506, obtemos:

$$\left(3^4\right)^{506} \equiv 1^{506} \pmod{8} \Rightarrow 3^{2024} \equiv 1 \pmod{8}$$

Como $3^2 \equiv 1 \pmod{8}$, segue que:

$$3^{2024} \cdot 3^2 \equiv 1 \cdot 1 \pmod{8} \Rightarrow 3^{2026} \equiv 1 \pmod{8}$$

Portanto, o resto da divisão de 3^{2026} por 8 é igual a 1.

Exemplo 16. Determine o resto da divisão de 11^{111} por 24.

Resolução. Como $mdc(11, 24) = 1$, o Teorema de Euler pode ser usado. Como $\varphi(24) = \varphi(2^3 \cdot 3) = 24\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 24\left(\frac{1}{2}\right)\left(\frac{2}{3}\right) = 24 \cdot \frac{1}{3} = 8$, segue que:

$$11^8 \equiv 1 \pmod{24}$$

Efetuando a divisão euclidiana de 111 por 8, obtemos: $11 = 8 \cdot 13 + 7$, ou seja, elevando ambos os membros da congruência por 13, obtemos:

$$\left(11^8\right)^{13} \equiv 1^{13} \pmod{24} \Rightarrow 11^{104} \equiv 1 \pmod{24}$$

Como $11^2 \equiv 1 \pmod{24}$, segue que $\left(11^2\right)^3 \equiv 1^3 \pmod{24} \Rightarrow 11^6 \equiv 1 \pmod{24}$ e $11^7 \equiv 11 \pmod{24}$. Com isso:

$$11^{104} \cdot 11^7 \equiv 1 \cdot 11 \pmod{24} \Rightarrow 11^{111} \equiv 11 \pmod{24}$$

Portanto, o resto da divisão de 11^{111} por 24 é igual a 11.

2.2.1 Exercícios

5) Determine:

a) $\varphi(225)$ b) $\varphi(20480)$ c) $\varphi(10!)$

6) Utilizando os Teoremas de Euler e Fermat, apresentados nessa seção, encontre o resto da divisão de:

a) 12^{12} por 5
b) 15^{256} por 8
c) 25^{2025} por 16
d) 39^{135} por 23
e) $100^{33} + 33^{100}$ por 7
f) $2^{70} + 3^{70}$ por 15

7) Determine os dois últimos algarismos de $9^{7777777}$.

2.3 Congruências Lineares

O que são congruências lineares? Pense numa equação do primeiro grau, com coeficientes inteiros e com incógnita x, do tipo $ax + c = d$. Essa equação pode ser reescrita da forma $ax = d - c$. Chamando "$d - c$" de b, obtemos $ax = b$. Congruências Lineares é uma congruência que é o equivalente a essa equação mostrada, só que ao invés do sinal de igual ($=$), teremos o sinal de congruência ($\equiv$). Numa equação como a acima, só existe uma solução. No caso das congruências lineares, isso nem sempre acontece.

Dados a e b inteiros, com $a \neq 0$, e $n \in \mathbb{N}, n \geq 2$, uma congruência da forma $ax \equiv b \pmod{n}$ é chamada uma congruência **linear**, onde x é uma incógnita.

Determinar as soluções de uma congruência linear, caso elas existam, significa achar todos os x_0 inteiros de modo que $ax_0 \equiv b \pmod{n}$. Uma congruência linear admite solução se, e somente se, $mdc(a, n)|b$.

Caso ela admita solução, e sendo x_0 uma dessas soluções, todas as soluções dessa congruência linear serão da forma:

$$x = x_0 + \frac{n}{d}k, \qquad \text{com } k \in \mathbb{Z} \text{ e } d = mdc(a, n)$$

Podemos determinar infinitas soluções para a congruência $ax \equiv b \pmod{n}$ seguindo a expressão acima, mas se quisemos encontrar soluções que sejam **incongruentes** duas a duas, também podemos encontrar. Esse número de soluções incongruentes duas a duas é **finito** e será igual ao valor de $d = mdc(a, n)$. Se x_0 for uma solução particular da congruência, então essas soluções serão da forma:

$$x_0, \quad x_0 + \frac{n}{d}, \quad x_0 + \frac{2n}{d}, \ldots, x_0 + \frac{(d-1)n}{d}$$

Todos esses resultados apresentados pressupõem que uma solução particular já é conhecida ou que é obtida com relativa facilidade. Agora, a pergunta que nos interessa é: **Como resolver** uma congruência linear $ax \equiv b \pmod{n}$?

Considere $d = mdc(a, n)$. Assumindo que essa congruência admite solução, então nós temos que $d|b$. Então, precisamos primeiramente usar o *Algoritmo de Euclides estendido* para obter inteiros r e s tais que $d = ar + ns$. Como $d|b$, então existe um inteiro t tal que $b = dt$. Com isso, segue que $x_0 = rt$ é uma solução de $ax \equiv b \pmod{n}$. Então, resumindo, sua solução geral será

$$x = x_0 + \frac{n}{d}k, \qquad \text{com } k \in \mathbb{Z} \text{ e } d = mdc(a, n)$$

Além disso,

$$x_0, \quad x_0 + \frac{n}{d}, \quad x_0 + \frac{2n}{d}, \ldots, x_0 + \frac{(d-1)n}{d}$$

são as soluções da congruência linear que são duas a duas incongruentes módulo n.

Exemplo 17. Resolva a congruência linear: $6x \equiv 15 \pmod{21}$

Resolução. Nesse caso, $d = mdc(6, 21) = 3$ e $3|15, 15 = 3 \cdot 5, t = 5$, logo essa congruência tem solução. Para achar uma solução particular, devemos achar r e s tal que

$$6r + 21s = 3$$

Usando o *Algoritmo de Euclides Estendido*, obtemos $6 \cdot (-3) + 21 \cdot 1 = 3$, ou seja, $r = -3$. Com $r = -3$ e $t = 5$, temos que $x_0 = rt = (-3) \cdot 5 = -15$ é uma sol. particular da congruência.

Sua solução geral é $x = -15 + \frac{21}{3}k = -15 + 7k, \quad k \in \mathbb{Z}$. Como $d = 3$, temos **três** soluções incongruentes módulo 21, que são

$$-15, \quad -15 + \frac{21}{3}, \quad -15 + \frac{42}{3} \Rightarrow -15, -15 + 7, -15 + 14 \Rightarrow -15, -8, -1$$

Se quisermos apenas soluções positivas, temos que $-15, -8$ e -1 são congruentes modulo 21 a $6, 13$ e 20, respectivamente.

OBS: Poderíamos ter obtido as soluções positivas diretamente, dado que $-15 \equiv 6 \pmod{21}$, aonde a solução geral seria $x = 6 + 7k$, e as três soluções incongruentes seriam $6, 13$ e 20, como encontramos anteriormente.

Exemplo 18. Resolva a congruência linear: $18x \equiv 60 \pmod{16}$

Resolução. Nesse caso, $d = mdc(18, 16) = 2$ e $2|60, 60 = 2 \cdot 30, t = 30$, logo essa congruência tem solução. Para achar uma solução particular, devemos achar r e s tal que

$$18r + 16s = 2$$

Usando o *Algoritmo de Euclides Estendido*, obtemos $18 \cdot 1 + 16 \cdot (-1) = 2$, ou seja, $r = 1$. Com $r = 1$ e $t = 30$, temos que $x_0 = rt = (1) \cdot 30 = 30$ é uma sol. particular da congruência, com $30 \equiv 14 \pmod{16}$.

Sua solução geral é $x = 14 + \frac{16}{2}k = 14 + 8k, \quad k \in \mathbb{Z}$. Como $d = 2$, temos **duas** soluções incongruentes módulo 16, que são

$$14, \quad 14 + \frac{16}{2} \Rightarrow 14, 14 + 8 \Rightarrow 14, 22$$

Como $22 \equiv 6 \pmod{16}$, as duas soluções incongruentes são 6 e 14.

2.3.1 Inversos Módulo n

Um caso especial de congruência linear, e que será muito relevante nos próximos capítulos, é os dos inversos módulo n. Dado um inteiro a, um outro inteiro x é o inverso módulo n de a se $ax \equiv 1 \pmod{n}$. Normalmente chamamos esse x de a^{-1}, donde $x \equiv a^{-1} \pmod{n}$. Essa congruência possui solução se, e somente se, $mdc(a, n) = 1$. Isso significa que nem todo elemento possui inverso. Por exemplo, se $n = 8$, os números $2, 4$ e 6 não possuem inverso módulo 8, pois $mdc(2, 8) = 2, mdc(4, 8) = 2, mdc(6, 8) = 2$.

Um resultado relacionado a isso é o seguinte: Se $mdc(a, n) = 1$ então a congruência linear $ax \equiv 1 \pmod{n}$ só terá **uma solução** módulo n. Qualquer outra solução será congruente módulo n a solução encontrada.

Então, se pegarmos um n primo, todo inteiro a irá admitir um inverso módulo n.

Podemos resolver esses tipos de congruências lineares da mesma forma que foi apresentada anteriormente:

Exemplo 19. Obtenha o inverso de 5 módulo 17 pelo método visto anteriormente.

Resolução. Para obtermos esse inverso, queremos achar um x tal que $5x \equiv 1 \pmod{17}$. Precisamos resolver essa congruência linear, sabendo que ela terá somente uma solução módulo 17.

Como $d = mdc(5, 17) = 1$, segue essa congruência possui solução e que $t = 1$. Para achar uma solução particular, que será a **única**, devemos encontrar r e s tal que

$$5r + 17s = 1$$

Usando o *Algoritmo de Euclides Estendido*, obtemos $5 \cdot 7 + 17 \cdot (-2) = 1$, ou seja, $r = 7$. Com $r = 7$ e $t = 1$, temos que $x_0 = rt = 7$. Com isso, a solução da congruência é $x_0 = 7$. Com efeito, temos que $5 \cdot 7 = 35$ e $35 \equiv 1 \pmod{17}$.

Portanto, o inverso de 5 módulo 17 é igual a 7.

Além desse método, também podemos resolver utilizando o *Teorema de Euler* e o *Pequeno Teorema de Fermat*, fazendo uma pequena modificação às respectivas congruências.

Se n for primo, o *Pequeno Teorema de Fermat* nos diz que, dado a inteiro:

$$a^{n-1} \equiv 1 \pmod{n}$$

Se multiplicarmos ambos os lados da congruência por a^{-1} (podemos fazer isso, pela **propriedade i)** das congruências), obtemos:

$$a^{n-2} \equiv a^{-1} \pmod{n}$$

Exemplo 20. Obter o inverso de 5 módulo 19 pelo método acima.

Resolução. Como 19 é primo, usando o que acabamos de ver, temos que $5^{19-2} \equiv 5^{-1} \pmod{9}$, ou seja, $5^{-1} \equiv 5^{17} \pmod{19}$.

Em outras palavras, o inverso de 5 módulo 19 é o resto da divisão de 5^{17} por 19.

Vamos ver as potências de 5 no módulo 19, fazendo cálculos envolvendo congruências e suas propriedades, para obtermos esse resto:

$$\begin{aligned}
5^1 &\equiv 5 \pmod{19} \\
5^2 &\equiv 25 \equiv 6 \pmod{19} \\
5^4 &\equiv 6^2 \equiv 36 \equiv -2 \pmod{19} \\
5^8 &\equiv (-2)^2 \equiv 4 \pmod{19} \\
5^{16} &\equiv 4^2 \equiv 16 \equiv -3 \pmod{19} \\
5^{17} &\equiv -3 \cdot 5 \equiv -15 \equiv 4 \pmod{19}
\end{aligned}$$

Ou seja, o inverso de 5 módulo 19 é igual a 4. Logicamente pois $5 \cdot 4 = 20$ e $20 \equiv 1 \pmod{19}$.

Se n for composto, o *Teorema de Euler* nos diz que, dado a inteiro:

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

Se multiplicarmos ambos os lados da congruência por a^{-1} (podemos fazer isso, pela **propriedade i)** das congruências), obtemos:

$$a^{\varphi(n)-1} \equiv a^{-1} \pmod{n}$$

Exemplo 21. Obter o inverso de 5 módulo 18 pelo método acima.

Resolução. Como 18 é composto, precisamos calcular $\varphi(18)$. Usando o método já visto nessa apostila (expressão 2.2.1), como $18 = 3^2 \cdot 2$, então $\varphi(18) = 18 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) = 18 \cdot \left(\frac{1}{2}\right) \cdot \left(\frac{2}{3}\right) = \frac{18}{3} = 6$. Usando o resultado acima, temos que $5^{6-1} \equiv 5^{-1} \pmod{18}$, ou seja, $5^{-1} \equiv 5^5 \pmod{18}$

Em outras palavras, o inverso de 5 módulo 18 é o resto da divisão de 5^5 por 18.

Vamos ver as potências de 5 no módulo 18, fazendo cálculos envolvendo congruências e suas propriedades, para obtermos esse resto:

$$\begin{aligned}
5^1 &\equiv 5 \pmod{18} \\
5^2 &\equiv 25 \equiv 7 \pmod{18} \\
5^3 &\equiv 7 \cdot 5 \equiv 35 \equiv -1 \pmod{18} \\
5^5 &\equiv 5^2 \cdot 5^3 \equiv 7 \cdot (-1) \equiv -7 \equiv 11 \pmod{18}
\end{aligned}$$

Ou seja, o inverso de 5 módulo 18 é igual a 11. Logicamente pois $5 \cdot 11 = 55$ e $55 \equiv 1 \pmod{18}$.

Exemplo 22. Dado n natural, $n \geq 2$, é verdade que o inverso de $n - 1$ módulo n é ele mesmo? Se sim, prove.

Resolução. Sim é verdade. Vamos provar:

Queremos mostrar que $(n-1)\cdot(n-1) \equiv 1 \pmod{n}$. Vamos primeiro trabalhar com o lado esquerdo da congruência. Esse lado esquerdo é um *produto notável*, e é igual a $n^2 - 2n + 1$. Vamos ver o resto da divisão dessa expressão por n.

Está claro para nós que n^2 é um múltiplo de n e que $-2n$ também é, ou seja, temos $n^2 \equiv 0 \pmod{n}$ e $-2n \equiv 0 \pmod{n}$. Além disso, segue que $1 \equiv 1 \pmod{n}$ Ou seja, pela **propriedade ii)** das congruências, podemos "somar" essas três congruências, obtendo $n^2 - 2n + 1 \equiv 0 + 0 + 1 \equiv 1 \pmod{n}$

Portanto, temos que $(n-1)\cdot(n-1) \equiv 1 \pmod{n}$, o que prova que o inverso de $n-1$ módulo é ele mesmo.

2.3.2 Exercícios

8) Resolva, quando possível, as congruências:

a) $8x \equiv 26 \pmod{6}$
b) $18x \equiv 60 \pmod{26}$
c) $6x \equiv 21 \pmod{18}$
d) $12x \equiv 36 \pmod{28}$
e) $13x \equiv 4 \pmod{42}$
f) $24x \equiv 9 \pmod{59}$

9) Obtenha os inversos módulo n em cada situação a seguir:

a) O inverso de 5 módulo 23.
b) O inverso de 11 módulo 31.
c) O inverso de 4 módulo 15.
d) O inverso de 42 módulo 55.
e) O inverso de 7 módulo 40.
f) O inverso de 19 módulo 97.

2.4 Sistema de Congruências e o Teorema Chinês dos Restos

Como já sabemos determinar a solução de uma congruência linear, nos convém saber como determinar soluções de sistemas de congruências lineares, que, tal como em sistemas de equações lineares, consiste em resolver simultaneamente duas (ou mais) congruências lineares. Vamos resolver um exemplo:

Exemplo 23. Resolva o sistema de congruências:

$$\begin{cases} x \equiv 4 \pmod{7} \\ x \equiv 9 \pmod{15} \end{cases}$$

Resolução. Resolver esse sistema significa determinar todos os inteiros x que satisfazem ambas as congruências.

Nessa situação, em que temos um sistema de duas congruências, podemos achar uma solução geral via o método da substituição, que funciona de modo semelhante ao usado para resolver sistemas de equações lineares.

Da primeira congruência, obtemos $x = 7y + 4, y \in \mathbb{Z}$. Como esse valor de x deve fazer a segunda congruência também, devemos substituir esse x na segunda congruência, obtendo $7y + 4 \equiv 9 \pmod{15}$,

o que equivale em $7y \equiv 5 \pmod{15}$. Como $mdc(7, 15) = 1$ e $1|5$, essa congruência tem solução inteira. Resolvendo da forma vista na seção anterior, se obtém $y = 5 + 15k, k \in \mathbb{Z}$. Agora, substituindo esse valor de y em $x = 7y + 4$, obtemos:

$$x = 7(5 + 15k) + 4 = 35 + 105k + 4 = 105k + 39$$

Ou seja, a solução geral desse sistema é $x = 39 + 105k$ ou $x \equiv 39 \pmod{105}$.

Caso fosse um sistema de 3 ou 4 congruências, o ideal, por evitar confusão de incógnita, usar a incógnita k somente na última congruência.

Esse método não é o único, e nem é recomendado em sistemas de 3 ou mais congruências. Outro método será descrito na sequência, chamado de *Teorema Chinês dos Restos*.

2.4.1 Teorema Chinês dos Restos

O problema mais antigo envolvendo restos foi descoberto num tratado chinês do século III d.C chamado de *Sun Ji Suanjing*, cuja tradução é *O Clássico Matemático de Sun Zi*, de autor desconhecido. O problema envolvendo restos neste tratado é chamado atualmente de **Teorema Chinês dos Restos**.

O problema, encontrado no Capítulo 3, página 26 do *Sun Ji Suanjing*, diz o seguinte:

> *Agora há um número desconhecido de objetos.*
> *Se os contarmos de três em três, resta 2;*
> *se os contarmos de cinco em cinco, resta 3;*
> *se os contarmos de sete em sete, resta 2.*
> *Encontre o número de objetos.*

Ao lado do problema, o autor de *Sun Ji Suanjing* trouxe a resposta:

> *Resposta: 23.*
> *Método: Se contarmos de três em três e o resto for 2, anote 140.*
> *Se contarmos de cinco em cinco e o resto for 3, anote 63.*
> *Se contarmos de sete em sete e o resto for 2, anote 30.*
> *Some os valores para obter 233 e subtraia 210 para encontrar a resposta.*
> *Se contarmos de três em três e o resto for 1, anote 70.*
> *Se contarmos de cinco em cinco e o resto for 1, anote 21.*
> *Se contarmos de sete em sete e o resto for 1, anote 15.*
> *Quando [um número] excede 106, o resultado é obtido subtraindo 105.*

Mais adiante iremos resolver esse problema via o Teorema. Antes, precisamos mostrar alguns resultados preliminares.

De um modo geral, nossa intenção é resolver sistemas de congruências da forma

$$\begin{cases} a_1x \equiv b_1 \pmod{n_1} \\ a_2x \equiv b_2 \pmod{n_2} \\ \vdots \\ a_kx \equiv b_k \pmod{n_k} \end{cases} \tag{2.4.1}$$

Cada uma dessas congruências pode ser expressa de uma forma equivalente, da forma $x \equiv c_i \pmod{m_i}, i = 1, \ldots, k$, podendo transformar o sistema 2.4.1 em um outro sistema mais "simples" e que contém as mesmas soluções. De modo geral, a congruência linear $ax \equiv b \pmod{n}$, em que $d = mdc(a, n)$, com $d|b$ é **equivalente** a

$$x \equiv rb^* \pmod{m}$$

sendo $b^* = \dfrac{b}{d}$, $d = ar + sn$ e $m = \dfrac{n}{d}$. Ao fazermos essa "transformação", o sistema presente em 2.4.1 é equivalente ao sistema:

$$\begin{cases} x \equiv c_1 \pmod{m_1} \\ x \equiv c_2 \pmod{m_2} \\ \vdots \\ x \equiv c_k \pmod{m_k} \end{cases} \tag{2.4.2}$$

E, para resolver esse sistema, usaremos o *Teorema Chinês dos Restos*, descrito a seguir:

Sejam $m_1, m_2, \ldots, m_k$ números naturais tais que $mdc(m_i, m_j) = 1$, para $m_i \neq m_j$. Então, o sistema de congruências lineares presente em 2.4.2 (acima) possui uma solução, que é única módulo $m = m_1m_2 \ldots m_k$.

Se $m = m_1m_2 \ldots m_k$, então defina $M_i = \dfrac{m}{m_i} = m_1m_2 \ldots m_{i-1}m_{i+1} \ldots m_k$, onde M_i é o produto de todos os inteiros $m_1, m_2, \ldots, m_k$, excluindo m_i. Como m_k e M_k são co-primos, existem r_i e s_i tais que: $r_iM_i + s_im_i = 1$, para cada $i = 1, \ldots, k$. Com isso, o inteiro

$$x_0 = c_1r_1M_1 + c_2r_2M_2 + \cdots + c_kr_kM_k$$

é uma solução do sistema. E sua solução geral será $x = x_0 + km, k \in \mathbb{Z}$.

A seguir, um passo-a-passo para resolver um sistema de congruências da mesma estrutura que o presente em 2.4.2, via o Teorema Chinês dos Restos:

- Verificar se $mdc(m_i, m_j) = 1$, para $m_i \neq m_j$.
- Determinar m, que é igual ao produto de todos os m_i, $i = 1, \ldots, k$.
- Determinar cada M_i, que é o produto de todos os inteiros $m_1, m_2, \ldots, m_k$, excluindo m_i.
- Para cada m_i e M_i, determinar r_i e s_i tal que $r_i M_i + s_i m_i = 1$. Destaque cada r_i obtido.
- Reunir todos os c_i, r_i e M_i, para calcular $x_0 = c_1 r_1 M_1 + c_2 r_2 M_2 + \cdots + c_k r_k M_k$.
- Após obter x_0, determinar a solução geral, que é da forma $x = x_0 + km, k \in \mathbb{Z}$.

Vamos agora resolver o problema presente no início da seção:

Exemplo 24. Determine a solução do sistema do inicio da seção, via o Teorema Chinês dos Restos:

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7 \end{cases}$$

Resolução. Uma vez que $mdc(3,5) = mdc(3,7) = mdc(5,7) = 1$, o teorema pode ser usado. Como $m_1 = 3$, $m_2 = 5$, $m_3 = 7$, então $m = 3 \cdot 5 \cdot 7 = 105$ e

$$M_1 = \frac{m}{m_1} = 35 \qquad M_2 = \frac{m}{m_2} = 21 \qquad M_3 = \frac{m}{m_3} = 15$$

Vamos determinar agora inteiros r_i e s_i tais que $r_i M_i + s_i m_i = 1$ para $i = 1, 2, 3$. Temos:

$$\begin{aligned} 1 &= (-1) \cdot 35 + 3 \cdot 12 \Rightarrow r_1 = -1 \\ 1 &= 1 \cdot 21 + 5 \cdot (-4) \Rightarrow r_2 = 1 \\ 1 &= 1 \cdot 15 + 7 \cdot (-2) \Rightarrow r_3 = 1 \end{aligned}$$

Como $c_1 = 2, c_2 = 3$ e $c_3 = 2$, podemos determinar x_0:

$$x_0 = c_1 r_1 M_1 + c_2 r_2 M_2 + c_3 r_3 M_3 = 2 \cdot (-1) \cdot 35 + 3 \cdot 1 \cdot 21 + 2 \cdot 1 \cdot 15 = 23$$

Portanto, $x_0 = 23$ e a solução geral do sistema é:

$$x = 23 + 105k, k \in \mathbb{Z}.$$

Verificando, $23 = 3 \cdot 7 + 2$, $23 = 5 \cdot 4 + 3$, $23 = 7 \cdot 3 + 2$.

Exemplo 25. Um general conta o número de soldados sobreviventes de uma batalha alinhando-os sucessivamente em linhas de certos tamanhos. Toda vez, ele conta o número de soldados que faltam para completar uma linha inteira. O general, antes da batalha, disponha de 1200 soldados. Depois da batalha, tivemos:

- 3 soldados restantes se alinharmos em linhas de cinco soldados.
- 3 soldados restantes se alinharmos em linhas de seis soldados.
- 1 soldado restante se alinharmos em linhas de sete soldados.
- Nenhum soldado restante se alinharmos em linhas de onze soldados.

Quantos soldados sobreviveram a batalha?

Resolução. Resolver esse problema significa resolver o sistema:

$$\begin{cases} x \equiv 3 \pmod 5 \\ x \equiv 3 \pmod 6 \\ x \equiv 1 \pmod 7 \\ x \equiv 0 \pmod{11} \end{cases}$$

Vamos resolvê-lo do mesmo jeito que o exemplo anterior.

Uma vez que $mdc(5,6) = mdc(5,7) = mdc(5,11) = mdc(6,7) = mdc(6,11) = mdc(7,11) = 1$, o teorema pode ser usado. Como $m_1 = 5$, $m_2 = 6$, $m_3 = 7$, $m_4 = 11$, então $m = 5 \cdot 6 \cdot 7 \cdot 11 = 2310$ e

$$M_1 = \frac{m}{m_1} = 462 \qquad M_2 = \frac{m}{m_2} = 385 \qquad M_3 = \frac{m}{m_3} = 330 \qquad M_4 = \frac{m}{m_4} = 210$$

Vamos determinar agora inteiros r_i e s_i tais que $r_i M_i + s_i m_i = 1$ para $i = 1, 2, 3, 4$. Temos:

$$\begin{aligned} 1 &= 3 \cdot 462 + 5 \cdot (-277) \Rightarrow r_1 = 3 \\ 1 &= 1 \cdot 385 + 6 \cdot (-64) \Rightarrow r_2 = 1 \\ 1 &= 1 \cdot 330 + 7 \cdot (-47) \Rightarrow r_3 = 1 \\ 1 &= 1 \cdot 210 + 11 \cdot (-19) \Rightarrow r_4 = 1 \end{aligned}$$

Como $c_1 = 3, c_2 = 3$, $c_3 = 1$ e $c_4 = 0$, podemos determinar x_0:

$$\begin{aligned} x_0 &= c_1 r_1 M_1 + c_2 r_2 M_2 + c_3 r_3 M_3 + c_4 r_4 M_4 = 3 \cdot 3 \cdot 462 + 3 \cdot 1 \cdot 385 + 1 \cdot 1 \cdot 330 + 0 \cdot (1) \cdot 210 \\ &= 4158 + 1175 + 330 = 5643 \end{aligned}$$

Portanto, $x_0 = 5643 \equiv 1023 \pmod{2310}$ e a solução geral do sistema é:

$$x = 1023 + 2310k, k \in \mathbb{Z}.$$

Como existiam 1200 soldados, então colocando $k = 0$ na solução acima, obtemos 1023 soldados sobreviventes.

2.4.2 Exercícios:

10) Resolva os sistemas a seguir:

a) $\begin{cases} x \equiv 3 \pmod{8} \\ x \equiv 8 \pmod{11} \end{cases}$ b) $\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 5 \pmod{7} \\ x \equiv 9 \pmod{17} \end{cases}$ c) $\begin{cases} 3x \equiv 1 \pmod{7} \\ 5x \equiv 2 \pmod{11} \\ 4x \equiv 3 \pmod{13} \end{cases}$

11) Berenice tem uma cesta cheia de ovos. Quando ela retira esses ovos da cesta, de 2 em 2, há um ovo sobrando. Quando ela retira de 3 em 3, há dois ovos sobrando. Quando ela retira os ovos de de 5 em 5 , há dois ovos sobrando. E quando ele retira os ovos de 7 em 7, sobra cinco ovos. Qual a menor quantidade de ovos que poderia estar na cesta de Berenice?

12) Três fazendeiros cultivavam juntos todo o seu arroz e o dividiam igualmente entre si no tempo da colheita. Em um certo ano, cada um deles foi a um mercado diferente vender o seu arroz. Cada um desses mercados só comprava arroz em múltiplos de um peso padrão, que diferia em cada um dos mercados. O primeiro fazendeiro vendeu o seu arroz em um mercado onde o peso padrão era $5Kg$. Ele vendeu tudo o que podia e voltou para casa com $3Kg$ de arroz. O segundo fazendeiro vendeu todo o arroz que podia em um mercado onde o peso padrão era $14Kg$ e voltou para casa com $8Kg$. O terceiro fazendeiro vendeu todo o arroz que podia em um mercado onde o peso padrão era $17Kg$ e voltou (ao mesmo tempo que os dois) com $11Kg$. Qual a quantidade mínima de arroz que eles podem ter cultivado, no total?

Capítulo 3

Criptografia

A palavra *Criptografia* vem do grego, fusão das palavras *kryptos* (que significa secreto ou oculto) e *graphein* (que significa escrita ou escrever), ou seja, de um modo bem simplista, criptografia significa *Escrita em Códigos*. Segundo o autor *Simon Singh*, "o intuito da criptografia não é ocultar a existência de uma mensagem, mas esconder seu significado." Esse ato de "esconder" tem um nome: Codificação. E o ato de "descobrir" o conteúdo dessa mensagem tem outro nome: Decodificação.

Ao longo da história, codificadores e decodificadores travam uma batalha, e tal batalha inspiravam muitas descobertas cientificas, com os codificadores criando códigos cada vez mais fortes enquanto que os decodificadores buscam encontrar fraquezas nesses códigos que os permitiam desvendá-los. Tal batalha acelerou o desenvolvimento da tecnologia, incluindo os computadores mais modernos.

Vamos descrever brevemente as principais técnicas de codificação.

3.1 Cifras de Transposição e Substituição

3.1.1 Cifra de Transposição

Esse tipo de cifra consiste em embaralhar as letras das mensagens, gerando um anagrama. Embora essa cifra seja bem difícil de ser interceptada por um inimigo, ela também será bem difícil de ser decifrada pelo destinatário, a não ser que esse embaralhamento siga um acordo previamente estabelecido entre as partes, o que deve ser feito em segredo.

Há dois métodos relativamente simples que usam essa técnica. Um deles é a transposição via **"Cerca de Ferrovia"**. Trata-se de escrever uma mensagem em uma sequência de diagonais, alterando elas de forma a deixá-las em linhas alternadas, onde o texto cifrado é formado pela sequência de letras na linha superior seguida pela sequência de letras na linha inferior. Vejamos um exemplo: Se a mensagem original é "DEPOIS DE AMANHÃ", essa mensagem na cerca de ferrovia seria da forma:

Figura 3.1: Cerca de Ferrovia

D		P		I		D		A		A		H	
	E		O		S		E		M		N		A

Fonte: Elaborado pelo autor.

Portanto, a mensagem cifrada é DPIDAAHEOSEMNA.

Para recuperar a mensagem, o caminho contrário deve ser feito, o que torna um processo bastante

vulnerável.

Um outro método pode ser usado, esse um pouco mais seguro, que usa um "método retangular" (segundo o autor). Primeiramente, é definida uma chave, que é uma palavra qualquer e depois se ordena alfabeticamente as colunas ocupadas por cada letra dessa chave. Em seguida, escreve-se a mensagem a ser cifrada linha por linha, sob a chave preenchendo todos os espaços da tabela. Caso haja espaços, normalmente se coloca o símbolo do jogo da velha. (#) Para cifrar a mensagem, é retirada a sequencia das letras das colunas na ordem crescente das letras da chave. Vejamos um exemplo: Se a mensagem original é "DEPOIS DE AMANHÃ" e a chave é "QUATRO", a tabela retangular será da forma:

Figura 3.2: Método Retangular.

ORDEM	3	6	1	5	4	2
CHAVE	Q	U	A	T	R	O
MENSAGEM	D	E	P	O	I	S
	D	E	A	M	A	N
	H	A	#	#	#	#

Fonte: Elaborado pelo autor.

A mensagem cifrada será PA#SN#DDHIA#OM#EEA.

Para decifrar a mensagem, o receptor faz o processo inverso, ou seja, o receptor deve escrever em colunas e decodificar em linhas.

3.1.2 Cifra de Substituição

Esse tipo de cifra consiste em trocar uma letra ou conjunto de letra por outras letras, símbolos e/ou números. Um dos métodos de criptografar mensagens mais antigos que existem é a chamada **"Cifra de César"**. Segundo o autor, para produzir o texto cifrado, Júlio César substituía cada letra do alfabeto por outra que fica três posições adiante no alfabeto (A $\rightarrow$ D, B $\rightarrow$ E, etc). Se seguirmos essa lógica, a mensagem "DEPOIS DE AMANHÃ" seria cifrada em GHSRLVDPDQKD.

Esse método é um dos mais antigos mas também um dos mais rápidos de serem decifrados. Se soubermos que foi usada a Cifra de César, como há somente 25 valores possíveis para as chaves, levaríamos pouco tempo para quebrar o código.

Um aprimoramento da Cifra de César é a **Cifra de Substituição Monoalfabética**, onde cada um dos caracteres da mensagem original é substituída por outro caractere, baseado numa tabela pré-estabelecida ou de acordo com uma chave, que nesse caso será um número que indica quantas posições deve-se avançar no alfabeto para obter o texto cifrado.

Embora esse método seja um aprimoramento da Cifra de César, ele ainda é fácil de ser quebrado.

Isso porque, no alfabeto, cada letra tem uma "frequência" fixa em que elas são geralmente usadas. Uma tabela contém essas frequências:

Figura 3.3: Tabela das Frequências das Letras em Português

Letra	%	Letra	%	Letra	%	Letra	%
A	14,64	G	1,30	N	5,05	T	4,34
B	1,04	H	1,28	O	10,73	U	4,64
C	3,88	I	6,18	P	2,52	V	1,70
D	4,10	J	0,40	Q	1,20	X	0,21
E	12,57	L	2,78	R	6,53	Z	0,47
F	1,02	M	4,75	S	7,81		

Fonte: Severino Collier Coutinho, 2015

Assim, apenas analisando a frequência de cada símbolo na mensagem, podemos descobrir a que letra correspondem os símbolos mais frequentes.

Com o tempo, essa cifra foi ficando cada vez mais ineficiente e sendo quebrada cada vez mais facilmente. Coube aos criptográficos criarem uma cifra mais resistente a quebra.

Uma dessas cifras é a **Cifra de Substituição Polialfabética**, que passou por muitos intelectuais para ser aperfeiçoada gradativamente. Entre esses intelectuais, estavam o abade alemão *Johannes Trithemius (1462-1516))*, o cientista italiano *Giovanni Porta (1535-1615)* e o diplomata Francês *Blaise de Vigenère (1523-1596)*. Este último chegou a misturar as ideias dos três para formar uma nova cifra, coerente e poderosa. Essa cifra, portanto, ficou conhecida como **Cifra de Vigenère**.

Em 1586, Vigenère publica um tratado sobre a escrita secreta, chamada *"Traicté des chiffres"*, que descreve seu método: Uma matriz 26x26 com 26 alfabetos, chamada tabela de Vigenère ou **Tabula Recta**.

Figura 3.4: Tabula Recta

		Letra da Mensagem																							
		A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
Letra da palavra-chave	**A**	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
	C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
	D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
	E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
	F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
	G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
	H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
	I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
	J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
	K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
	L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
	M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
	N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
	O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
	P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
	Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
	R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
	S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
	T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
	U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
	V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
	W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
	X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
	Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
	Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Fonte: Produzido pelo autor.

Portanto, para enviar uma mensagem por esse método deve ser feito o seguinte: escreve-se a palavra-chave sobre a mensagem original repetidamente até que cada letra da mensagem original fique associada a uma determinada letra da palavra-chave. A letra da mensagem cifrada será onde se intercepta a letra da palavra-chave (linha da tabela acima) com a letra da mensagem original (coluna da tabela acima) e dessa forma se prossegue até concluir a cifragem.

Por exemplo: Se a mensagem for “DEPOIS DE AMANHÃ” e a palavra-chave for “COISA” então a cifragem fica da forma:

Palavra-Chave	COISAC	OI	SACOIS
Mensagem Original	DEPOIS	DE	AMANHA
Mensagem Cifrada	FSXGIU	RM	SMCBPS

Para decifrar a mensagem, se procede de modo parecido. Essa cifra é imune à análise de frequência, a letra com mais frequência na mensagem cifrada nem sempre irá representar a mesma letra na

mensagem original. E descobrir a chave é um processo quase que literalmente impossível pois a palavra-chave pode ser qualquer palavra no dicionário ou uma palavra inventada.

Outra cifra foi inventada pelo arquiteto italiano *Leon Alberti (1404-1472)*, que foi a primeira cifra a ter uma máquina criptográfica, que é o disco de cifra, chamado de *"Disco de Alberti"*:

Figura 3.5: Disco de Alberti

Fonte: Wikimédia Commons

Esse disco foi construído da seguinte maneira: Alberti tomou dois círculos de cobre com uma pequena diferença de diâmetro entre eles e escreveu um alfabeto ao longo da borda de cada círculo. Em seguida, colocou-se o círculo menor no interior do círculo maior de modo que uma agulha passada pelos dois centros seja usada como eixo comum. Os círculos podiam girar independentemente, de modo que os dois alfabetos mudavam suas posições relativas e assim eram usados para cifrar a mensagem. O alfabeto do círculo maior representava a mensagem original enquanto que o alfabeto do círculo menor representava a mensagem cifrada. Cada letra na mensagem original era extraída do círculo maior com a correspondente no círculo menor, sendo esta a letra na mensagem cifrada.

3.2 Criptografia nos séculos XIX e XX

Em 1830 houve um avanço na área de comunicação com a invenção do telégrafo e do código Morse, ambos inventados por *Samuel Morse (1791-1872)*. O código Morse foi a primeira representação binária (ponto e traço) do alfabeto com grande aplicação. Após suas respectivas invenções, o código e o telégrafo chegaram a exercer um importante papel na comunicação em geral. Mas havia preocupação quanto a segurança e a sigilosidade das mensagens enviadas, isso porque a mensagem escrita em código Morse era entregue ao operador do telégrafo, que a lia antes de transmitir ela adiante. Para evitar que segredos sentimentais, comerciais, importantes, etc de serem revelados ao operador, uma solução adotada foi cifrar essas mensagens antes de passá-las ao operador. Com a estabilidade do código

Morse, o interesse de se quebrar a cifra de Vigenère foi diminuindo com o tempo. Mas existiram duas pessoas que contribuíram a esse "interesse": Babbage e Kasiski.

Charles Babbage (1791-1871) foi um matemático e inventor inglês mais conhecido por conceber a primeira ideia de um computador. Entre outras obras, Babbage ficou inreressado na cifra de Vigenère e de como quebrá-la.

Trabalhando paralelamente a Babbage, o oficial da reserva do exército prussiano, *Friedrich Wilhelm Kasiski (1805-1881)*, publicou em 1863 um trabalho, cujo nome era *"Die Geheimschriften und die Dechiffer-Kunst"* (A Escrita Secreta e a Arte de Decifrá-la) que descreve uma técnica de como quebrar a cifra de Vigenère, conhecida como "Teste de Kasiski". Essa publicação acabou dando os créditos da quebra da cifra de Vigenère somente a Kasiski e não se sabe ao certo porque que Babbage não chegou a publicar seu trabalho sobre a quebra da cifra (foram encontrados documentos após sua morte). Há uma teoria para isso, porém: Segundo relatos, Babbage descobriu a quebra logo depois do início da Guerra da Criméia (1853-1856), e essa descoberta deu aos britânicos uma vantagem sobre os russos, e isso pode ser significado que, Babbage provavelmente tenha sido "obrigado" a manter em segredo o seu trabalho pela segurança britânica.

Graças a descoberta de Babbage e Kasiski, a cifra de Vigenère não era mais segura e não houve nenhum avanço no sentido de novas cifras na segunda metade do século XIX. Nesse período de insegurança, na virada do século, o físico italiano *Guglielmo Marconi (1874-1937)* realizou um feito poderoso para a comunicação: A transmissão via **rádio**. Esse equipamento era capaz de transmitir e recber pulsos elétricos a uma distância de até 2,5 Km com a vantagem de não haver a necessidade de um fio para transportar a mensagem entre o emissor e o receptor. Tal invenção encantou os militares, que sentiram ao mesmo tempo euforia e medo. De uma forma, a comunicação via rádio permitiu que generais mantivessem contato com seus batalhões independentemente de seus movimentos. Mas, essa facilidade de comunicação também significava que essa mensagem poderiam chegar aonde não deveria, a chamada **interceptação**. Por causa disso, era necessário uma codificação confiável para que terceiros, ao interceptar as mensagens, não conseguissem decifrá-las.

Toda essa indefinição acerca da comunicação via rádio foi posta em prova na *Primeira Guerra Mundial (1914-1918)*, onde as nações envolvidas queriam utilizar esse poder do rádio, mas não conseguiam garantir sua segurança. Não houve nenhum avanço na criptografia nesse período, no sentido de se criarem cifras que sejam difíceis de serem quebradas. Por mais que houvesse essa insegurança, a quantidade de mensagens transmitidas pelo rádio durante a Guerra foi enorme e todas corriam risco de serem interceptadas.

No período entre guerras, a procura por um sistema eficiente e seguro que possa ser usado nos conflitos seguintes continuou. Isso felizmente aconteceu, com os criptográficos deixando de usar lápis e papel e passando a explorar a tecnologia da época. Na década de 1920, o engenheiro alemão *Arthur Scherbius (1878-1929)* desenvolveu uma máquina criptográfica que era uma versão elétrica do Disco de Alberti. Ele patentou essa máquina e deu a ela o nome de **Enigma**. Essa invenção se tornaria o mais complicado sistema de cifragem da história e a partir de 1926, o exército alemão passou a desfrutar desse sistema.

Com a *Segunda Guerra Mundial (1939-1945)*, os alemães acreditavam que a máquina Enigma teria um papel vital na vitória do Eixo, mas isso não aconteceu. Uma equipe de milhares de matemáticos trabalhavam anonimamente para conseguir quebrar a máquina Enigma, entre eles *Alan Turing (1912-1954)*. Antes de trabalhar nessa equipe, Turing era professor de matemática em Cambridge,

onde em 1937, publicou um trabalho científico intitulado *"On Computable Numbers"* (Os Números Computáveis), onde descreve uma máquina imaginária que poderia efetuar de forma automática os processos que são desenvolvidos por um matemático. Essas máquinas, chamadas de "Máquinas de Turing", foram as precursoras dos primeiros computadores, que surgiram décadas depois.

Em 1939, Turing recebe um convite da Escola de Cifras e Códigos do Governo da Inglaterra para se tornar um **Criptoanalista** (especialista em quebrar cifras), e interrompe sua carreira em Cambridge. Essa escola tinha sede na Mansão Bletchley Park e seu único objetivo era quebrar as chaves da máquina Enigma.

Os ingleses já tinham uma réplica da máquina Enigma, mas não conseguiam decifrar as mensagens cifradas porque o segredo era saber como a máquina era ajustada, pois a chave permanecia em segredo. Essa busca pela quebra da cifra continuou até que Turing, seguindo os caminhos do matemático polonês *Marian Rejewski (1905-1980)*, que havia quebrado uma versão mais simples da máquina Enigma, e em conjunto com os outros pesquisadores em Bletchley Park, conseguiram quebrar a versão atual e mais avançada da Enigma, o que alterou o curso da guerra (estima-se que isso antecipou o término da guerra em três anos).

3.3 Criptografia no pós-guerra: Diffie-Hellman e RSA

Após a segunda guerra, o uso da tecnologia e dos computadores passaram a ser cada vez mais presentes na criptografia e na criptoanálise. Começando com a *máquina Colossus*, os criptoanalistas continuaram a desenvolver tecnologias computacionais para auxiliá-los na quebra de todas as cifras, enquanto que os criptógrafos começaram a contra-atacar, usando os computadores para desenvolver cifras mais complexas.

Na década de 1960, os computadores ficaram mais poderosos, em maior quantidade e mais baratos. O que era algo que somente o governo e os militares teriam, agora estava presente também em empresas, e com isso as cifragens ficaram cada vez mais difundidas. Um dos fatores que determinam a "força" de uma cifra é a quantidade de chaves possíveis. Quanto maior for o número de chaves, maior será o número de possibilidades e consequentemente o tempo para encontrar a chave certa será maior.

Quando duas pessoas querem conversar "em segredo", essas pessoas tinham que combinar entre elas uma chave. O problema é que, a não ser que essa chave seja combinada numa conversa pessoal, essa chave teria que ser combinada via computador ou via outro método, e a chance dessa chave ser interceptada ou roubada era relativamente alta. Esse problema é chamado de *Problema da Distribuição de Chaves*. Um dos criptógrafos interessados em resolver esse problema era *Whitfield Diffie (1944-presente)*, graduado pelo Instituto de Técnologia de Massachussets (MIT). Em 1974, em uma palestra apresentada por ele sobre as suas tentativas em resolver o problema da distribuição de chaves, ele acaba conhecendo outro criptógrafo, *Martin Hellman (1945-presente)*. Os dois acabaram por trabalhar juntos para tentar resolver o problema da distribuição de chaves. Mais tarde se junta a eles o pesquisador *Ralph Merkle (1952-presente)*. A ideia trabalhada por eles era a ligação entre a criptografia e a teoria dos números, que atualmente é uma ligação irreversível. Ela pode ser exemplificada na seguinte situação:

João e Maria querem trocar entre si uma chave secreta por telefone. Eles escolhem, em comum acordo, dois números naturais a e m, e os tornam públicos. João escolhe outro número natural α_J e o mantém secreto. Com esse número ele calcula o **único** número $\beta_j < m$ tal que $a^{\alpha_J} \equiv \beta_J \pmod{m}$, e o envia para Maria. Maria, por sua vez, escolhe um número natural a^{α_M}, também mantendo-o

secreto, e com ele calcula o único número $\beta_M < m$ tal que $a^{\alpha_M} \equiv \beta_M \pmod{m}$ e o envia para João.

Em seguida, João calcula $\beta_M^{\alpha_J}$, obtendo:

$$\beta_M^{\alpha_J} \equiv (a^{\alpha_M})^{\alpha_J} \equiv a^{\alpha_M \alpha_J} \equiv \alpha \text{ (mod m), com } \alpha < m$$

Por sua vez, Maria calcula $\beta_J^{\alpha_M}$, obtendo:

$$\beta_J^{\alpha_M} \equiv (a^{\alpha_J})^{\alpha_M} \equiv a^{\alpha_J \alpha_M} \equiv \alpha \text{ (mod m), com } \alpha < m$$

Pronto! Está trocada a chave secreta (α) entre João e Maria. São públicas as informações a, m, β_J, β_M e são secretas as informações α_J, que só João conhece, α_M, que só Maria conhece e α, que ambos conhecem.

Exemplo 26. Pegue a situação acima e considere $a = 52$ e $m = 271$. Além disso, João escolhe $\alpha_J = 5$ e Maria escolhe $\alpha_M = 7$. Qual será a chave secreta?

Resolução. João faz o seguinte cálculo para determinar β_J e enviá-lo a Maria:

$$52^2 \equiv 2704 \equiv 265(\text{mod}271)$$
$$52^4 \equiv 265^2 \equiv 36(\text{mod}271)$$
$$52^7 = 52^4 \times 52^2 \times 52 \equiv 36 \times 265 \times 52 \equiv 150(\text{mod}271).$$

Logo, $\beta_J = 150$. Por sua vez, Maria faz a seguinte conta para determinar β_M e enviá-lo a João:

$$52^5 = 52^4 \times 52 \equiv 36 \times 52 \equiv 246(\text{mod}271).$$

Logo, $\beta_M = 246$. Para determinar a chave α, João tem que reduzir $\beta_M^{\alpha_J} = 246^7$ módulo 271. Logo,

$$246^2 = 60516 \equiv 83(\text{mod}271)$$
$$246^4 = 246^2 \times 246^2 \equiv 83 \times 83 \equiv 114(\text{mod}271)$$
$$246^7 = 246^4 \times 246^2 \times 246 \equiv 114 \times 83 \times 246 \equiv 33(\text{mod}271)$$

João encontra então $\alpha = 33$. Agora é a vez de Maria calcular o resíduo de $\beta_J^{\alpha_M} = 150^5$ módulo 271. Mas, $150^2 = 22500 \equiv 7(\text{mod}271)$

$$150^5 = 150^2 \times 150^2 \times 150 = 7 \times 7 \times 150 \equiv 33(\text{mod}271)$$

encontrando também, como era de se esperar, $\alpha = 33$.

O sucesso deste método reside no fato de ser difícil descobrir qualquer dos três números α_J, α_M ou α, conhecendo apenas os dados públicos a, m, β_J e β_M. De fato, dado $x \in \mathbb{N}$, relativamente fácil calcular o resto da divisão de a^x por m, mas é difícil fazer o caminho oposto, ou seja, dado $y \in \mathbb{N}$ é difícil encontrar $x \in \mathbb{N}$ tal que y é o resto da divisão de a^x por m. Os restos da divisão de a^x por m,

ao variar x, comportam-se de modo caótico. Assim, dado y, para resolver em x a equação $a^x \equiv y \pmod{m}$ é necessário construir a tabela dos valores da função

$$\begin{aligned} \mathbb{N} &\to \mathbb{Z}_m \\ x &\to [a^x] \end{aligned}$$

o que pode ser computacionalmente inviável, dependendo de uma boa escolha de a e de m.

Todos os métodos descritos até agora são de cifras simétricas, ou seja, usa-se a mesma chave para codificar e decodificar uma mensagem. O contrário desse método é o método de cifras assimétricas, onde a chave de codificar é diferente da chave de decodificar uma mensagem. Essa distinção é o que torna essa cifra tão especial, que revolucionaria o mundo da criptografia. Diffie e Hellman tinham convencido ao mundo que o problema de distribuição de chaves havia solução mas nunca conseguiram tornar em realidade a cifra assimétrica. **O método exemplificado acima resolve esse problema no caso particular de troca entre duas pessoas de cada vez**.

Essa "corrida" foi vencida por um trio de pesquisadores:

- *Ron **R**ivest (1947-presente)*
- *Adi **S**hamir (1952-presente)*
- *Leonard **A**dleman (1945-presente)*

Rivest e Shamir eram os responsáveis pelas ideias e pela formalização das mesmas, enquanto que Adleman era o responsável em detectar falhas nas ideias de Rivest e Shamir, garantindo que eles não perdessem tempo em ideias que não chegariam a lugar nenhum. A primeira versão foi feita em abril de 1977 e a versão final foi publicada em setembro de 1977 (disponível nesse link. Rivest foi quem fez essa descoberta, com a contribuição de Shamir e de Adleman, aos quais citou na sua primeira versão. Adleman não concordou em ser considerado um dos autores pois não foi ele quem fez a descoberta e sim quem identificava as falhas. Após discussão, Adleman concorda em ser citado como o terceiro autor. E assim esse método acabou sendo chamado de **RSA** (Rivest, Shamir e Adleman), tornando-se a cifra mais influente da criptografia moderna e hoje mais conhecida como criptografia de chave pública.

O próximo capítulo será dedicado à ele.

Capítulo 4

Criptografia RSA

Tudo (ou quase tudo) o que foi visto nos capítulos anteriores será usado nesse capítulo, para (finalmente) mostrarmos como que a criptografia RSA funciona e como descrever ela. Além de mostrar esse funcionamento, precisamos ver se de fato ela é segura. Esse procedimento consiste em codificar e decodificar uma mensagem qualquer, tomando cuidado com o fato de que, decodificar significa passar da mensagem codificada à mensagem original. Ou seja, tão importante quando mostrar como que é feita a codificação e a decodificação, é mostrar que, de fato, ao codificar uma mensagem especifica, sua decodificação irá retornar a mensagem original.

Cada seção desse capítulo irá conter exercícios relacionados ao conteúdo para serem feitos em sala em conjunto com a explicação do método.

4.1 Pré-Codificação

Para codificarmos uma mensagem, é necessário fazer um procedimento preliminar para podermos fazer a codificação, que é converter a mensagem em uma sequência de números.

Suponhamos, para simplificar, que a mensagem original é um texto onde não há números, apenas palavras, e no qual todas as letras são maiúsculas. Portanto, em última análise a mensagem é constituída pelas letras que formam as palavras e pelos espaços entre palavras. Chamaremos esta primeira etapa de pré-codificação, para distingui-la do processo de codificação propriamente dito.

Na pré-codificação convertemos as letras em números usando a seguinte tabela de conversão:

A	B	C	D	E	F	G	H	I	J	K	L	M
10	11	12	13	14	15	16	17	18	19	20	21	22
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
23	24	25	26	27	28	29	30	31	32	33	34	35

O espaço entre duas palavras será substituído pelo número 99, quando for feita a conversão. Por exemplo, a frase AMO GATOS é convertida no número

$$102224991610292428$$

Exercício. Construa uma frase curta e faça a conversão como feito acima.

Observe que precisamos fazer cada letra corresponder a um número de, pelo menos, dois algarismos para evitar ambiguidades. Se fizéssemos A corresponder ao número 1, B ao 2 , e assim por diante, não teríamos como saber se 19 representa AI ou S, já que esta última é a décima nona letra do alfabeto.

Antes de continuar precisamos determinar os parâmetros do sistema RSA que vamos usar. Estes parâmetros são dois primos distintos, que vamos denotar por p e q. Escolhidos esses primos p e q, faça

$n = p \cdot q$. A "lógica" desse sistema e o porquê dele ser tão eficiente (por enquanto) é que normalmente esses primos contém centenas (ou até milhares) de algarismos, de modo que, ao pegarmos o produto deles, não é um processo fácil e rápido "dividir" esse número no produto de dois primos (mesmo usando um supercomputador). Por uma questão didática, iremos usar como exemplo, primos bem menores.

A parte final da pré-codificação consiste de separar a mensagem original em "blocos", onde cada bloco deve ser menor que o número n e não pode começar com o número 0. Por exemplo, se escolhermos $p = 3$ e $q = 17$, teremos $n = 51$. A mensagem acima convertida em números seria dividida nos blocos abaixo:

$$10 - 22 - 2 - 49 - 9 - 16 - 10 - 29 - 24 - 28$$

Note que essa divisão dos blocos não é única (ao invés de fazermos $2 - 49$, poderíamos ter feito $24 - 9$), desde que se tome o cuidado de não começar nenhum bloco com o número 0. Além disso, nenhum desses blocos representam uma unidade linguística (da tabela), ou seja, é quase que literalmente impossível decifrar essa mensagem pelo método de frequência.

Por que "quase que literalmente impossível"?
Por exemplo, a frase "O alcance da república é imenso" convertida em números, seria:

24 99 10211210231214 99 1310 99 271425301121181210 99 14 182214232824

Se formos fazer a divisão em blocos, teríamos algo do tipo:

$$\cdots - 102 - 112 - \cdots - 30 - 112 - 118 - \ldots$$

Dois blocos representados pelo número 112*, mas que foram gerados por sequências de letras diferentes. O primeiro através da sequência "LC" e o segundo através da sequência "BL".*

4.2 Codificação

Para codificarmos a mensagem, precisamos de n, o produto dos primos definido na pré-codificação e de um número inteiro positivo e que seja um *inverso módulo* $\varphi(n)$, ou seja, $mdc(e, \varphi(n)) = 1$. Como visto anteriormente, já que n é um produto de primos p e q, distintos, então:

$$\varphi(n) = \varphi(pq) = \varphi(p) \cdot \varphi(q) = (p-1) \cdot (q-1)$$

Exercício. Usando os "primeiros primos" $(2, 3, 5, 7, 11, 17, 19, etc)$ construa uma chave pública para usar na codificação. (**Algumas escolhas de primos tornam a determinação do inverso módulo φ(n) mais fácil. Tente descobrir quais são elas**)

O par (n, e) é chamado de *chave de codificação* do sistema RSA que estamos usando. Esta chave pode ser tornada pública; isto é, podemos enviá-la a qualquer um que queira nos mandar uma mensagem, sem preocupação de mantê-la secreta. Por isso a chave de codificação também é conhecida

como chave pública do sistema. Supondo que já submetemos a mensagem à pré-codificação, temos uma sequência de números que, como na seção anterior, chamaremos de blocos. Codificaremos cada bloco separadamente. A mensagem codificada será a sequência dos blocos codificados. Isto é muito importante porque depois de codificados os blocos não podem mais ser reunidos de modo a formar um longo número.

Então, se a chave de codificação for um par (n, e), como codificar um bloco b qualquer? Por construção, b deve ser menor que n. Denotando o bloco codificado por $\mathbf{C}(b)$, ele é calculado da forma:

$$\mathbf{C}(b) = \text{ resto da divisão de } b^e \text{ por } n.$$

Em termos de aritmética modular, $b^e \equiv \mathbf{C}(b) (\text{mod } n)$, com $0 \leq \mathbf{C}(b) < n$.

Vamos retornar ao nosso caso: $p = 3$, $q = 17$, $n = 51$. Com isso, $\varphi(n) = 2 \cdot 16 = 32$. Precisamos agora encontrar um valor para e, sabendo que e é um inverso módulo 32. Uma forma simples de encontrar esse número é encontrar o menor primo que não divide 32, esse número é o número 3. Assim, o primeiro bloco da mensagem a ser codificada, 10, será codificado como o resto da divisão de 10^3 por 32. Vamos fazer as contas:

$$10^3 \equiv 10^2 \cdot 10 \equiv 49 \cdot 10 \equiv 490 \equiv 31 \text{ (mod 51)}$$

Codificando toda a mensagem, bloco a bloco, obtemos:

$$\begin{aligned}
22^3 &\equiv 22^2 \cdot 22 \equiv 25 \cdot 22 \equiv 550 \equiv 40 \text{ (mod 51)} \\
2^3 &\equiv 8 \text{ (mod 51)} \\
49^3 &\equiv 49^2 \cdot 49 \equiv 4 \cdot 49 \equiv 196 \equiv 43 \text{ (mod 51)} \\
9^3 &\equiv 9^2 \cdot 9 \equiv 30 \cdot 9 \equiv 270 \equiv 15 \text{ (mod 51)} \\
16^3 &\equiv 16^2 \cdot 16 \equiv 1 \cdot 16 \equiv 16 \text{ (mod 51)} \\
10^3 &\equiv 10^2 \cdot 10 \equiv 49 \cdot 10 \equiv 490 \equiv 31 \text{ (mod 51)} \\
29^3 &\equiv 29^2 \cdot 29 \equiv 25 \cdot 29 \equiv 725 \equiv 11 \text{ (mod 51)} \\
24^3 &\equiv 24^2 \cdot 24 \equiv 15 \cdot 24 \equiv 360 \equiv 3 \text{ (mod 51)} \\
28^3 &\equiv 28^2 \cdot 28 \equiv 19 \cdot 28 \equiv 532 \equiv 22 \text{ (mod 51)}
\end{aligned}$$

Portanto, a mensagem codificada será:

$$31 - 40 - 43 - 15 - 16 - 31 - 11 - 3 - 22$$

Exercício. Codifique a mensagem criada no primeiro exercício usando a chave criada no segundo exercício, seguindo o procedimento acima.

4.3 Decodificação

Com a codificação feita e os blocos enviados para o destinatário, cabe a esse destinatário decodificar a mensagem feita. Ou seja, queremos saber qual é o procedimento que nos permite, de posse de um bloco codificado e da chave pública, reconstruir o bloco original, antes da codificação.

Do que precisamos? Do número n e do **inverso de** e módulo $\varphi(n)$, o qual chamaremos de d. Esse par (n, d) é chamado de **par de decodificação**. Se a for um bloco da mensagem codificada, então $\mathbf{D}(a)$ será o resultado do processo de decodificação. Tal como na codificação, $\mathbf{D}(a)$ é calculado da forma:

$$\mathbf{D}(a) = \text{ resto da divisão de } a^d \text{ por } n$$

Em termos de aritmética modular, $a^d \equiv \mathbf{D}(a) (\text{mod } n)$, com $0 \leq \mathbf{D}(a) < n$.

Tendo em posse os valores de "e" e de $\varphi(n)$, para encontramos d de um modo geral, precisamos usar o *algoritmo de Euclides estendido*. Para casos onde esses valores são pequenos, esse algoritmo não é absolutamente necessário. Por outro lado, se queremos decodificar um bloco já codificado, o esperado é que o resultado seja o bloco original, ou seja $\mathbf{D}(\mathbf{C}(b)) = b$. Será feita uma seção dedicada para mostrar que isso sempre acontece.

Vamos encontrar d. No nosso caso, temos $n = 51$, $\varphi(n) = 32$ e $e = 3$. Então, como d é um inverso de 3 módulo 32, temos $3d \equiv 1 (\text{mod } 32)$, o que equivale em $3d - 32k = 1 \Rightarrow 3d + 32(-k) = 1$. Como dito anteriormente, nesse caso não é absolutamente necessário usarmos o algoritmo completamente, pois para $d = 43$ e $k = 4$, temos $3 \cdot 43 + 32 \cdot (-4) = 129 - 128 = 1$. Ou seja, $d = 43$. Assim, para decodificarmos o primeiro bloco, 31, precisamos encontrar o resto da divisão de 31^{43} por 51.

Até poderíamos usar o mesmo método da codificação para encontrar esse resto, mas ele nem sempre será recomendado, principalmente para casos onde n, b e d são números maiores. Ao invés disso, podemos usar o *Teorema Chinês dos Restos* e o *Pequeno Teorema de Fermat* para aliviar as contas.

Como $51 = 17 \cdot 3$, com 17 e 3 sendo números primos, então $\varphi(17) = 16$ e $\varphi(3) = 2$. Podemos usar o *Pequeno Teorema de Fermat* para calcularmos os restos de 31^{43} módulo 17 e módulo 3, respectivamente. Primeiramente, $31 \equiv 1 (\text{mod } 3)$. Então $31^{43} \equiv 1^{43} \equiv 1 (\text{mod } 3)$. Com isso, precisamos aplicar o *Pequeno Teorema de Fermat* apenas na primeira congruência:

$$\begin{aligned} 31^{16} &\equiv 1 (\text{mod } 17) \\ (31^{16})^2 &\equiv 1^2 (\text{mod } 17) \\ 31^{32} &\equiv 1 (\text{mod } 17) \\ 31^{32} \cdot 31^9 &\equiv 31^9 (\text{mod } 17) \\ 31^{43} &\equiv 31^{11} (\text{mod } 17) \end{aligned}$$

Precisamos lidar com o 31^9. Como $31 \equiv 14 (\text{mod } 17)$, então $31^2 \equiv 14^2 \equiv 9 (\text{mod } 17) \Rightarrow (31^2)^5 \equiv 9^5 (\text{mod } 17) \Rightarrow 31^10 \equiv 9^5 \equiv 8 (\text{mod } 17) \Rightarrow 31^10 \cdot 31 \equiv 8 \cdot 31 \equiv 10 (\text{mod } 17)$. Por transitividade, $31^{43} \equiv 10 (\text{mod } 17)$.

Dos dois resultados obtidos, $31^{43} \equiv 10 (\text{mod } 17)$ e $31^{43} \equiv 1 (\text{mod } 3)$, eles são correspondentes ao sistema:

$$\begin{cases} x \equiv 10 (\text{mod } 17) \\ x \equiv 1 (\text{mod } 3) \end{cases}$$

O que é possível de se resolver via *Teorema Chinês dos Restos*:

(**OBS:** Nesse caso específico, usar o Teorema pode não ser a opção mais eficaz, mas ele será resolvido pelo Teorema para mostrar como que é ele resolvido num caso geral, caso seja com valores maiores)

Para usarmos o teorema, iremos encontrar $c_1, c_2, n_1, n_2, M_1, M_2$. Nesse sistema, $c_1 = 10, c_2 = 1, m_1 = 17, m_2 = 3, M_1 = 3, M_2 = 17$. Como $mdc(17, 3) = mdc(3, 17) = 1$, precisamos determinar inteiros x e y tais que $17x + 3y = 1$. Para $x = -1$ e $y = 6$, essa equação diofantina é resolvida. Portanto:

$$1 = 17 \cdot (-1) + 3 \cdot 6 \Rightarrow r_1 = 6$$
$$1 = 3 \cdot (6) + 17 \cdot (-1) \Rightarrow r_2 = -1$$

Como $c_1 = 10$ e $c_2 = 1$, uma solução é:

$$x_0 = 10 \cdot 6 \cdot 3 + 1 \cdot (-1) \cdot 17 = 180 - 17 = 163$$

Portanto, $x_0 = 163 \equiv 10 (\text{mod } 51)$. Com isso, ao decodificar o bloco 31, é retornado o bloco 10, o que é o esperado. A decodificação dos outros oito blocos será deixada como exercício ao leitor.

Exercício. Dada a chave pública que você determinou, calcule o valor de d. Em seguida, passe a codificação e a chave (n, d) para o colega e peça para ele tentar decodificar e descobrir a frase que você escreveu. (e vice-versa, claro)

Iremos agora mostrar que esse método de codificação e de decodificação de fato funciona.

4.4 Funcionamento

Essa seção é mais "rigorosa" em relação as outras porque iremos ver, de certa forma, uma "demonstração" desse método. Não é obrigatório apresentar essa parte aos alunos se você, professor, não estiver confortável.

Como foi visto nos cálculos anteriores, nós tínhamos um bloco pré-codificado (10), que codificado retornou o bloco 31 e que decodificado retornou o bloco 10 novamente. O método exposto acima só será útil se o que aconteceu nos cálculos de fato acontecer com **qualquer** bloco. Digamos que temos um sistema RSA de parâmetros p e q, onde $n = pq$. Então para codificarmos, precisamos de "n" e "e", e para decodificarmos, precisamos de "n" e "d". Na notação que usamos anteriormente, precisamos mostrar que se temos um bloco b, $1 \leq b \leq n - 1$, então $\mathbf{DC}(b) = b$.

Na verdade só precisamos mostrar que $\mathbf{DC}(b) \equiv b \ (\text{mod } n)$ pois, ambos os números $\mathbf{DC}(b)$ e b estão no intervalo entre 1 e $n - 1$, e eles só serão congruentes módulo n se forem iguais. **Isso é o**

motivo de, na pré-codificação, os blocos serem formados de forma a cada bloco ser menor que n e que esses blocos tenham que ficar separados mesmo após a codificação.

Da definição de **D** e de **C** temos que

$$\mathbf{DC}(b) \equiv (b^e)^d \equiv b^{ed} \pmod{n} \tag{4.4.1}$$

Porém d é o inverso de e módulo $\varphi(n)$, ou seja, $ed = 1 + k\varphi(n), k \in \mathbb{Z}$. Como d e e são inteiros maiores do que 2 e $\varphi(n) > 0$, então $k > 0$. Substituindo ed em 4.4.1, temos:

$$b^{ed} \equiv b^{1+k\varphi(n)} \equiv (b^{\varphi(n)})^k b \pmod{n}$$

Como $b^{\phi(n)} \equiv 1 \pmod{n}$, pelo Teorema de Euler, nos resta $b^{ed} \equiv b \pmod{n}$. Portanto, $\mathbf{DC}(b) \equiv b \pmod{n}$, o que resolveria nossa demonstração, mas, para podermos usar o Teorema de Euler, estaríamos assumindo que $mdc(b, n) = 1$, o que não necessariamente é verdade. Para evitarmos isso, teremos que demonstrar sem usar o Teorema de Euler.

Para isso, lembre-se que $n = pq$ em que p e q são primos distintos. Vamos calcular a forma reduzida de b^{ed} módulo p e módulo q (são análogos). Vamos começar com a forma reduzida de b^{ed} módulo p.

Sabemos que existe $k \in \mathbb{Z}$ tal que $ed = 1 + k\phi(n)$, mas como $\phi(n) = (p-1)(q-1)$ então $ed = 1 + k(p-1)(q-1)$. Logo:

$$b^{ed} \equiv b \cdot (b^{p-1})^{k(q-1)} \pmod{p}$$

Parece ser o momento para usarmos o Pequeno Teorema de Fermat, mas para isso, precisamos supor que p não divide b. Caso isso aconteça, então $b^{p-1} \equiv 1 \pmod{p}$ pelo Pequeno Teorema de Fermat, o que implica em $b^{ed} \equiv b \pmod{p}$.

Falta ainda mostrar o caso onde p divide b. Como p é primo, se p divide b então $b \equiv 0 \pmod{p}$ e a congruência é imediatamente verificada. Assim, $b^{ed} \equiv b \pmod{p}$ vale para **qualquer valor de b**.

Analogamente, mostra-se que $b^{ed} \equiv b \pmod{q}$. Com isso, temos que $b^{ed} - b$ é divisível tanto por p quanto por q. Como p e q são primos distintos, então $mdc(p, q) = 1$. Existe uma propriedade relevante relacionada a isso:

"Dados $a, b \in \mathbb{Z}$. Então se $a|c$, $b|c$ e $mdc(a, b) = 1$ então $ab|c$."

Aplicando isso a nossa situação, temos que pq divide $b^{ed} - b$. Como $n = pq$, concluímos que $b^{ed} \equiv b \pmod{n}$, para qualquer inteiro b. Isto encerra a demonstração que o método funciona, ou seja, que $\mathbf{DC}(b) = b$.

4.5 Segurança

Como já sabemos, a criptografia RSA é uma criptografia de *chave pública*, onde a chave de codificação, (n, e) corresponde à chave pública do sistema e, por causa disso, é acessível a qualquer usuário. A segurança do RSA depende da dificuldade de se calcular d quando n e e são conhecidos. Como nós vimos anteriormente, d é o inverso de e módulo $\varphi(n)$, e, para obtê-lo, teríamos que aplicar o algoritmo de Euclides estendido. Mas, para obtermos $\varphi(n)$, teríamos que fatorar n para obtermos p e q. O segredo para "quebrarmos" o código é conseguirmos fatorar n. Por isso, o ideal é que n seja um número grande, pois não existe um algoritmo rápido de fatoração que permita "quebrar" n em dois fatores, independentemente da quantidade de algarismos de n.

Embora não exista uma demonstração de que quebrar o RSA e fatorar n sejam problemas equivalentes (um depender do outro), geralmente se acredita nisso. O próprio **Ron Rivest** afirma isso em um de seus artigos.

Mas se uma fatoração difícil/impossível de n é o segredo para assegurar a segurança do RSA, *como escolher* os primos p e q? Claro que se ambos forem pequenos, é fácil fatorar n. Ainda, se ambos forem grandes mas $\mid p - q \mid$ for pequeno, também será fácil fatorar n usando o *Algoritmo de Fermat*, cujo método foi visto no capítulo 1.

O sistema RSA está em uso faz-se muitos anos e uma escolha adequada de primos p e q torna o sistema muito seguro. Além desse, existem outros métodos, em que a fatoração se torna possível se $p-1$ ou $q-1$ tiverem fatores primos pequenos, chamado de método *p-1 de Pollard*, e um método em que a fatoração se torna possível se $p+1$ ou $q+1$ tiverem fatores primos pequenos, chamado método de *p+1 de Williams*.

Normalmente, para uso pessoal, uma chave deve ter tamanho da ordem 10^{231} aproximadamente, com 231 algarismos, ou seja, os primos p e q deveriam ter, por exemplo, 110 e 121 algarismos, respectivamente. Para importantes transações bancárias esse número seria ainda maior, da ordem 10^{308} aproximadamente, com 308 algarismos. Com o passar do tempo, essas ordens irão aumentar, mas, para valores suficientemente frandes de p e de q, o RSA é invencível... por enquanto.

Nunca saberemos o que o futuro nos reserva, mas é possível que, em alguma época no futuro, alguém possa encontrar um modo rápido de fatorar qualquer n, o que tornaria o RSA inútil. Mas até agora não existe nenhum método de fatoração realmente rápida, pois matemáticos acreditam que fatorar é uma tarefa *inerentemente difícil*. Por enquanto, o RSA é seguro. Não se sabe por quanto tempo. Quem sabe até o dia em que os computadores quânticos forem completamente desenvolvidos.

4.5.1 Exercícios

Esses exercícios tratam de todo o capítulo.

1. Discuta sobre a seguinte situação: "Se as chaves públicas de duas pessoas diferentes têm um primo em comum, então é fácil quebrar o RSA destas duas pessoas."

2. Sabemos que se n é a chave pública de uma implementação do RSA, então $n = pq$, onde p e q são primos positivos distintos. Imagine que alguém lhe emprestou um computador (que você

não tem a menor ideia de como funciona) que, ao receber a chave pública n calcula o número $m = (p-1)(q-1)$. Mostre que é possível determinar p e q a partir de n e m.

3. Sabendo que $n = 3552377$ é igual ao produto de dois números primos e que $\varphi(n) = 3548580$, fatore n.

4. A chave pública utilizada pelo Banco de Toulouse para codificar suas mensagens é a seguinte: $n = 10403$ e $e = 8743$. Recentemente os computadores do banco receberam, se local indeterminado, a seguinte mensagem:

$$4746 - 8214 - 9372 - 9009 - 4453 - 8198$$

O que diz a mensagem mandada ao Banco de Toulouse?

Referências Bibliográficas

[1] M. d. N. C. BEZERRA *et al.*, *Teoria dos números: um curso introdutório*. Editora Universitária da Assessoria de Educação a Distância-EditAedi, 2018.

[2] B. C. of Engineering, "Unit 4: Congruences and its applications," 2022. Acesso em: 8 jun. 2025.

[3] M. Carvalho, "Problemas aritmética c4n2 – algoritmo da divisão e análise dos restos." `https://portaldaobmep.impa.br/uploads/msg/5hbq58op1uw48.pdf`, 2023. Material elaborado para o programa OBMEP na Escola.

[4] Equipe Programa Cientista-Chefe em Educação Básica, "Aritmética elementar i." `https://www.ced.seduc.ce.gov.br/wp-content/uploads/sites/82/2022/03/caderno01_deAluno.pdf`, 2022. Caderno de atividades elaborado em parceria entre UFC, FUNCAP e SEDUC-CE.

[5] S. C. Coutinho, *Números inteiros e criptografia RSA*. IMPA, 1997.

[6] S. C. Coutinho, "Criptografia," *Rio de Janeiro, Programa de Iniciação Científica da OBMEP (PIC-OBMEP)*, 2015.

[7] L. R. Dante, *Tudo é matemática 6. ano*. Ática, 2011.

[8] F. J. F. Carneiro, *Criptografia e Teoria dos números*. Rio de Janeiro: Editora Ciência Moderna Ltda., 2017.

[9] A. Hefez, *Aritmética*. Rio de Janeiro: SBM, 2016.

[10] L. H. Ing, "The history of the chinese remainder theorem," *Mathematical Medley*, 2003.

[11] H. H. DOMINGUES, *Fundamentos da aritmética*. Florianópolis: Editora da UFSC, 2021.

[12] D. E. Knuth, *The art of computer programming*, vol. 3. Pearson Education, 1997.

[13] H. H. P. Nucci and G. R. Grosch, "Um estudo teórico e prático dos métodos de fatoração de inteiros de fermat e pollard p-1," 1 2009. Orientadora: Profa. MSc. Adriana Betânia de Paula Molgora.

[14] Secretaria da Educação do Estado do Espírito Santo (SEDU-ES), "Rotina pedagógica escolar – matemática – 6º ano – quinzena 7." `https://curriculo.sedu.es.gov.br/curriculo/wp-content/uploads/2025/01/RPE_MAT_6_Q_07_29_01_25.pdf`, 2025. Material elaborado pela Gerência de Currículo da Educação Básica (GECEB).

[15] S. Singh, *The code book*, vol. 7. Doubleday New York, 1999.

[16] V. L. Vieira, *Um curso básico em teoria dos números*. Editora Livraria da Física, 2020.

[17] Y. Hui, *Xiangjie Jiuzhang Suanfa*. Unknown, 1265. Inclui a história de Han Xin contando soldados, associada ao Teorema Chinês dos Restos.

Resolução dos Exercícios

Neste capítulo estarão as resoluções dos exercícios. É recomendado que somente o professor aplicador dessa apostila tenha acesso à essas resoluções, que serão feitas de um jeito mais "formal".

Resoluções – Capítulo 1

Divisibilidade

1) Para ver se as afirmações são verdadeiras ou falsas, precisamos efetuar as divisões e verificar se seus restos são iguais ou diferentes do que zero.

a) $\begin{array}{r|l} 495 & 9 \\ \hline 45 & 55 \\ 45 & \\ \hline 0 & \end{array}$

é **VERDADEIRO** que $9 \mid 495$.

b) $\begin{array}{r|l} 1.260 & 7 \\ \hline 7 & 180 \\ 56 & \\ \hline 56 & \\ \hline 00 & \end{array}$

é **VERDADEIRO** que $7 \mid 1260$.

c) $\begin{array}{r|l} 349 & 8 \\ \hline 32 & 43 \\ 29 & \\ \hline 24 & \\ \hline 5 & \end{array}$

é **FALSO** que $8 \mid 349$.

d) $\begin{array}{r|l} 378 & 12 \\ \hline 36 & 31 \\ 18 & \\ \hline 12 & \\ \hline 6 & \end{array}$

é **VERDADEIRO** que $12 \nmid 378$.

e) $\begin{array}{r|l} 182 & 14 \\ \hline 14 & 13 \\ 42 & \\ \hline 42 & \\ \hline 0 & \end{array}$

é **VERDADEIRO** que $14 \mid 182$.

f) $\begin{array}{r|l} 46.809 & 3 \\ \hline 3 & 15.603 \\ 16 & \\ 15 & \\ \hline 1\,8 & \\ 1\,8 & \\ \hline 009 & \\ 9 & \\ \hline 0 & \end{array}$

é **FALSO** que $3 \nmid 46809$.

2) Para verificar cada caso se ela consegue colocar as 255 balas nos saquinhos de modo que não sobre nenhum, precisamos calcular as divisões necessárias:

$\begin{array}{r|l} 255 & 8 \\ \hline 24 & 31 \\ \hline 15 & \\ 8 & \\ \hline 7 & \end{array}$ $\quad$ $\begin{array}{r|l} 255 & 12 \\ \hline 24 & 21 \\ \hline 15 & \\ 12 & \\ \hline 3 & \end{array}$ $\quad$ $\begin{array}{r|l} 255 & 15 \\ \hline 15 & 17 \\ \hline 105 & \\ 105 & \\ \hline 0 & \end{array}$

Como o resto na divisão por 8 e na divisão por 12 não são iguais a zero, então Dona Augusta não conseguiria colocar as balas sem que sobre nenhuma. A divisão por 15, porém, tem resto

zero, então Dona Augusta consegue consegue colocar as balas nesses saquinhos, sem que sobre nenhum. O número de saquinhos necessários é igual a 17.

Divisão Euclidiana

3) Precisamos encontrar "n" tal que $n = 12 \cdot 8 + r$, sendo "r" o resto. Mas, como o resto é o "maior possível", então $r = b - 1$. Como $b = 12$, segue que $r = 12 - 1 = 11$ e a partir daí, podemos encontrar n:

$$n = 12 \cdot 8 + 11 = 96 + 11 = 107$$

O número encontrado é 107.

4) Temos que "a" é o dividendo, "b" é o divisor, $q = 23$ e "r" é o resto. Como o resto é o maior possível, $r = b - 1$. Pela hipótese, $a - b = 206$. Podemos resolver esse problema da forma:

$$a = 23b + b - 1 \Rightarrow a - b = 23b - 1 \Rightarrow 206 = 23b - 1 \Rightarrow$$
$$23b = 207 \Rightarrow b = \frac{207}{23} \Rightarrow b = 9$$

O divisor é igual a 9. Como $r = b - 1$, então o resto é igual a 8.

5) Temos que $a = 463$, $q = 15$ e $r = b - 1$. Para encontrarmos b, devemos fazer o seguinte:

$$463 = 15b + b - 1 \Rightarrow 463 = 16b - 1 \Rightarrow 16b = 464 \Rightarrow b = \frac{464}{16} = 29$$

O divisor é igual a 29.

6) Vamos resolver via decomposição: Decompondo o número 26877 em números que sabemos ser divisíveis por 9:

$$26877 = 18000 + 8877 = 18000 + 8100 + 777 =$$
$$= 18000 + 8100 + 720 + 57 = 18000 + 8100 + 720 + 54 + 3$$

Como as quatro primeiras parcelas são divisíveis por 9 e a última não é, segue que o resto da divisão é igual a 3.

7) Do enunciado, aplicando o conceito da divisão euclidiana, temos que $b = 7q + 5$, com $q \in \mathbb{Z}$. Então:

$$b^2 + b + 11 = (7q + 5)^2 + 7q + 5 + 11 = 49q^2 + 70q + 25 + 7q + 16 = 49q^2 + 77q + \underbrace{41}_{35+6} =$$
$$= 7(7q^2 + 11q + 5) + 6$$

Chamando $7q^2 + 11q + 5$ de q', temos $b^2 + b + 11 = 7q' + 6$. Portanto, o resto da divisão de $b^2 + b + 11$ por 7 é igual a 6.

mdc e Algoritmo de Euclides

8) Vamos fazer as divisões sucessivas para cada item.

a)
$$\begin{cases} 202 &= 28 \times 7 + 6 \\ 28 &= 6 \times 4 + 4 \\ 6 &= 4 \times 1 + 2 \\ 4 &= 2 \times 2 + 0 \end{cases}$$

$mdc(202, 28) = 2$

b)
$$\begin{cases} 389 &= 167 \times 2 + 55 \\ 167 &= 55 \times 3 + 2 \\ 55 &= 2 \times 27 + 1 \\ 2 &= 1 \times 2 + 0 \end{cases}$$

$mdc(389, 167) = 1$

c)
$$\begin{cases} 3387 &= 637 \times 5 + 202 \\ 637 &= 202 \times 3 + 31 \\ 202 &= 31 \times 6 + 15 \\ 31 &= 15 \times 2 + 1 \\ 15 &= 1 \times 15 + 0 \end{cases}$$

$mdc(3387, 637) = 1$

d)
$$\begin{cases} 874 &= 551 \times 1 + 323 \\ 551 &= 323 \times 1 + 228 \\ 323 &= 228 \times 1 + 95 \\ 228 &= 95 \times 2 + 38 \\ 95 &= 38 \times 2 + 19 \\ 38 &= 19 \times 2 + 0 \end{cases}$$

$mdc(874, 551) = 19$

e)
$$\begin{cases} 3027 &= 1224 \times 2 + 579 \\ 1224 &= 579 \times 2 + 66 \\ 579 &= 66 \times 8 + 51 \\ 66 &= 51 \times 1 + 15 \\ 51 &= 15 \times 3 + 6 \\ 15 &= 6 \times 2 + 3 \\ 6 &= 3 \times 2 + 0 \end{cases}$$

$mdc(3027, 1224) = 3$

f)
$$\begin{cases} 7469 &= 2464 \times 3 + 77 \\ 2464 &= 77 \times 32 + 0 \end{cases}$$

$mdc(7469, 2464) = 77$

9) Como as duas escadas começam juntas e terminam juntas no último andar e além disso, elas ficam no mesmo nível somente quando conduzem a um andar, então precisamos achar um número "k" que seja divisor de 700 e de 780 e que também seja o maior deles. Ora, esse é o $mdc(780, 700)$, que precisamos calcular.

$$\begin{cases} 780 &= 700 \times 1 + 80 \\ 700 &= 80 \times 8 + 60 \\ 80 &= 60 \times 1 + 20 \\ 60 &= 20 \times 3 + 0 \end{cases}$$

Com isso, $k = mdc(780, 700) = 20$ e o prédio tem 20 andares.

Por curiosidade, a escadaria com 700 degraus possui $\dfrac{700}{20} = 35$ degraus por andar e a escadaria com 780 degraus possui $\dfrac{780}{20} = 39$ degraus por andar.

10) Para determinar a maior quantidade possível de integrantes presente em cada subgrupo que respeite o que o mestre deseja, devemos calcular o *mdc* de 84 e 66. Então:

$$\begin{cases} 84 &= 66 \times 1 + 18 \\ 66 &= 18 \times 3 + 12 \\ 18 &= 12 \times 1 + 6 \\ 12 &= 6 \times 2 + 0 \end{cases}$$

Com isso, $mdc(84, 66) = 6$ e cada subgrupo terá 6 integrantes. Para determinarmos a quantidade de subgrupos do Grupo A, precisamos calcular $\frac{84}{6} = 14$. Portanto, o grupo A terá 14 subgrupos, cada um com 6 integrantes.

Equações Diofantinas

11) Para cada equação, será visto primeiro se ela possui solução e, em caso positivo, iremos encontrar uma solução particular via o algoritmo **estendido**:

a) $mdc(18, 2) = 2$ e $2 \mid 52$, logo essa equação tem solução. Vamos encontrar uma solução particular de $18x + 2y = 2$ via algoritmo estendido:

$$\begin{bmatrix} 2 & 1 & 0 \\ 18 & 0 & 1 \end{bmatrix} \Rightarrow \begin{bmatrix} 2 & 1 & 0 \\ 18 - 2 \cdot 9 & 0 - 1 \cdot 9 & 1 - 0 \cdot 9 \end{bmatrix} \Rightarrow \begin{bmatrix} 2 & 1 & 0 \\ 0 & -9 & 1 \end{bmatrix}$$

Portanto, uma solução particular para $18x + 2y = 2$ é o par $(0, 1)$ (*eu sei que essa solução parece óbvia, mas para manter o padrão de resolução, foi seguido o algoritmo mesmo assim*). Para a equação original, basta multiplicar essa solução por 26. A solução particular será $(0, 26)$.

Seu conjunto solução será: $S = \{(t, 26 - 9t) \mid t \in \mathbb{Z}\}$

b) $mdc(72, 56) = 8$ e $8 \mid 40$, logo essa equação tem solução. Vamos encontrar uma solução particular de $72x + 56y = 8$ pelo algoritmo estendido:

$$\begin{bmatrix} 56 & 1 & 0 \\ 72 & 0 & 1 \end{bmatrix} \Rightarrow \begin{bmatrix} 56 & 1 & 0 \\ 72 - 56 \cdot 1 & 0 - 1 \cdot 1 & 1 - 0 \cdot 1 \end{bmatrix} \Rightarrow \begin{bmatrix} 56 & 1 & 0 \\ 16 & -1 & 1 \end{bmatrix}$$

$$\Rightarrow \begin{bmatrix} 56 - 16 \cdot 3 & 1 - (-1) \cdot 3 & 0 - 1 \cdot 3 \\ 16 & -1 & 1 \end{bmatrix} \Rightarrow \begin{bmatrix} 8 & 4 & -3 \\ 16 & -1 & 1 \end{bmatrix}$$

$$\Rightarrow \begin{bmatrix} 8 & 4 & -3 \\ 16 - 8 \cdot 2 & -1 - 4 \cdot 2 & 1 - (-3) \cdot 2 \end{bmatrix} \Rightarrow \begin{bmatrix} 8 & 4 & -3 \\ 0 & -9 & 7 \end{bmatrix}$$

Portanto, uma solução particular é $(-3, 4)$. Para a equação original, basta multiplicar essa solução por 5. A solução particular será $(-15, 20)$.

Seu conjunto solução será: $S = \{(-15 + 7t, 20 - 9t) \mid t \in \mathbb{Z}\}$

c) $mdc(44, 12) = 4$ e $4 \nmid 78$, logo essa equação **não** tem solução.

d) $mdc(27, 15) = 3$ e $3 \mid 309$, logo essa equação tem solução. Vamos encontrar uma solução particular de $27x + 15y = 3$ pelo algoritmo estendido:

$$\begin{bmatrix} 15 & 1 & 0 \\ 27 & 0 & 1 \end{bmatrix} \Rightarrow \begin{bmatrix} 15 & 1 & 0 \\ 27 - 15 \cdot 1 & 0 - 1 \cdot 1 & 1 - 0 \cdot 1 \end{bmatrix} \Rightarrow \begin{bmatrix} 15 & 1 & 0 \\ 12 & -1 & 1 \end{bmatrix}$$

$$\Rightarrow \begin{bmatrix} 15 - 12 \cdot 1 & 1 - (-1) \cdot 1 & 0 - 1 \cdot 1 \\ 12 & -1 & 1 \end{bmatrix} \Rightarrow \begin{bmatrix} 3 & 2 & -1 \\ 12 & -1 & 1 \end{bmatrix}$$

$$\Rightarrow \begin{bmatrix} 3 & 2 & -1 \\ 12 - 3 \cdot 4 & 2 - 1 \cdot 4 & 1 - (-1) \cdot 4 \end{bmatrix} \Rightarrow \begin{bmatrix} 3 & 2 & -1 \\ 0 & -2 & 5 \end{bmatrix}$$

Portanto, uma solução particular é $(-1, 2)$. Para a equação original, basta multiplicar essa solução por 103. A solução particular será $(-103, 206)$.

Seu conjunto solução será: $S = \{(-103 + 5t, 206 - 9t) \mid t \in \mathbb{Z}\}$

e) $mdc(102, 3) = 3$ e $3 \nmid 34$, logo essa equação **não** tem solução.

12) Da questão anterior, apenas a letra *a*), *b*) e *d*) continham equações com solução. Para determinarmos as soluções positivas de cada conjunto solução, precisamos restringir os valores de x e de y para que eles sejam maiores ou iguais a zero.

a) O conjunto solução é $S = \{(t, 26 - 9t) \mid t \in \mathbb{Z}\}$. Precisamos que

$$t \geq 0 \qquad \text{e} \qquad 26 - 9t \geq 0$$

o que implica em $t \geq 0$ e $t \leq 2{,}888\ldots$. Como $t \in \mathbb{Z}$, então $t \geq 0$ e $t \leq 2$. As três únicas soluções positivas dessa equação serão aquelas em que $t = 0$, $t = 1$ e $t = 2$. Calculando:

- $t = 0 \Rightarrow (0, 26 - 9 \cdot 0) = (0, 26)$
- $t = 1 \Rightarrow (1, 26 - 9 \cdot 1) = (1, 17)$
- $t = 2 \Rightarrow (2, 26 - 9 \cdot 2) = (2, 8)$

b) O conjunto solução é $S = \{(-15 + 7t, 20 - 9t) \mid t \in \mathbb{Z}\}$. Precisamos que

$$-15 + 7t \geq 0 \qquad \text{e} \qquad 20 - 9t \geq 0$$

o que implica em $t \geq 2{,}142$ e $t \leq 2{,}222\ldots$. Como $t \in \mathbb{Z}$, então não existe nenhum número inteiro que seja ao mesmo tempo maior que 2,142 e menor que 2,222. Logo, essa equação não admite soluções positivas.

d) O conjunto solução é $S = \{(-103 + 5t, 206 - 9t) \mid t \in \mathbb{Z}\}$. Precisamos que

$$-103 + 5t \geq 0 \qquad \text{e} \qquad 206 - 9t \geq 0$$

o que implica em $t \geq 20{,}6$ e $t \leq 22{,}888\ldots$. Como $t \in \mathbb{Z}$, então $t \geq 21$ e $t \leq 22$. As duas únicas soluções positivas dessa equação serão aquelas em que $t = 21$ e $t = 22$. Calculando:

- $t = 21 \Rightarrow (-103 + 5 \cdot 21, 206 - 9 \cdot 21) = (2, 17)$

- $t = 22 \Rightarrow (-103 + 5 \cdot 22, 206 - 9 \cdot 22) = (7, 8)$

13) Para resolver o problema, precisamos encontrar as soluções positivas da equação $15x + 6y = 225$. Como $mdc(15, 6) = 3$ e $3 \mid 225$, logo essa equação tem solução. Vamos encontrar uma solução particular de $15x + 6y = 3$. Por observação, identificamos que o par $(1, -2)$ resolve a equação acima. Para a equação original, basta multiplicar essa solução por 75. A solução particular será $(75, -150)$ e seu conjunto solução será $S = \{(75 + 2t, -150 - 5t) \mid t \in \mathbb{Z}\}$. Como queremos somente as soluções **positivas**, precisamos que

$$75 + 2t \geq 0 \qquad \text{e} \qquad -150 - 5t \geq 0$$

o que implica em $t \geq -37{,}5$ e $t \leq -30$. Como $t \in \mathbb{Z}$, então $t \geq -37$ e $t \leq -30$. As soluções positivas dessa equação serão aquelas em que $t = -37, \ldots, -30$. Calculando:

- $t = -37 \Rightarrow (75 + 2 \cdot (-37), -150 - 5 \cdot (-37)) = (1, 35)$
- $t = -36 \Rightarrow (75 + 2 \cdot (-36), -150 - 5 \cdot (-36)) = (3, 30)$
- $t = -35 \Rightarrow (75 + 2 \cdot (-35), -150 - 5 \cdot (-35)) = (5, 25)$
- $t = -34 \Rightarrow (75 + 2 \cdot (-34), -150 - 5 \cdot (-34)) = (7, 20)$
- $t = -33 \Rightarrow (75 + 2 \cdot (-33), -150 - 5 \cdot (-33)) = (9, 15)$
- $t = -32 \Rightarrow (75 + 2 \cdot (-32), -150 - 5 \cdot (-32)) = (11, 10)$
- $t = -31 \Rightarrow (75 + 2 \cdot (-31), -150 - 5 \cdot (-31)) = (13, 5)$
- $t = -30 \Rightarrow (75 + 2 \cdot (-30), -150 - 5 \cdot (-30)) = (15, 0)$

14) Para resolver o problema, precisamos encontrar as soluções positivas da equação $50x + 20y = 530$. Como $mdc(50, 20) = 10$ e $10 \mid 530$, essa equação tem solução. Vamos encontrar uma solução particular de $50x + 20y = 10$. Por observação, identificamos que o par $(1, -2)$ resolve a equação acima. Para a equação original, basta multiplicar essa solução por 53. A solução particular será $(53, -106)$ e seu conjunto solução será $S = \{(53 + 2t, -106 - 5t) \mid t \in \mathbb{Z}\}$. Como queremos somente as soluções **positivas**, precisamos que

$$53 + 2t \geq 0 \qquad \text{e} \qquad -106 - 5t \geq 0$$

o que implica em $t \geq -26{,}5$ e $t \leq -21{,}2$. Como $t \in \mathbb{Z}$, então $t \geq -26$ e $t \leq -22$. As soluções positivas dessa equação serão aquelas em que $t = -26, \ldots, -22$. Calculando:

- $t = -26 \Rightarrow (53 + 2 \cdot (-26), -106 - 5 \cdot (-26)) = (1, 24)$
- $t = -25 \Rightarrow (53 + 2 \cdot (-25), -106 - 5 \cdot (-25)) = (3, 19)$
- $t = -24 \Rightarrow (53 + 2 \cdot (-24), -106 - 5 \cdot (-24)) = (5, 14)$
- $t = -23 \Rightarrow (53 + 2 \cdot (-23), -106 - 5 \cdot (-23)) = (7, 9)$
- $t = -22 \Rightarrow (53 + 2 \cdot (-22), -106 - 5 \cdot (-22)) = (9, 4)$

Números Primos

15) Vamos fatorar esses números.

a)

294	2
147	3
49	7
7	7
1	$2 \cdot 3 \cdot 7^2$

b)

440	2
220	2
110	2
55	5
11	11
1	$2^3 \cdot 5 \cdot 11$

c)

1350	2
675	3
225	3
75	3
25	5
5	5
1	$2 \cdot 3^3 \cdot 5^2$

d)

1764	2
882	2
441	3
147	3
49	7
7	7
1	$2^2 \cdot 3^2 \cdot 7^2$

e)

3168	2
1584	2
792	2
396	2
198	2
99	3
33	3
11	11
1	$2^5 \cdot 3^2 \cdot 11$

f)

10800	2
5400	2
2700	2
1350	2
675	3
225	3
75	3
25	5
5	5
1	$2^4 \cdot 3^3 \cdot 5^2$

16) Vamos fazer o procedimento explicado para cada número.

a) Para o número 5913 :

- $a = [\sqrt{5913}] \cong [76, 89] = 76 \Rightarrow b = \sqrt{5776 - 5913} = \sqrt{-137}$ (não deu certo)
- $a = 77 \Rightarrow b = \sqrt{5929 - 5913} = \sqrt{16} = 4$

Com $a = 77$ e $b = 4$, podemos encontrar nossos fatores: $(a + b) = 77 + 4 = 81$ e $(a - b) = 77 - 4 = 73$. Portanto, os fatores são 81 e 73.

b) Para o número 6887 :

- $a = [\sqrt{6887}] \cong [82, 98] = 82 \Rightarrow b = \sqrt{6724 - 6887} = \sqrt{-163}$ (não deu certo)
- $a = 83 \Rightarrow b = \sqrt{6889 - 6887} = \sqrt{2} \cong 1{,}4142$ (não deu certo)
- $a = 84 \Rightarrow b = \sqrt{7056 - 6887} = \sqrt{169} = 13$

Com $a = 84$ e $b = 13$, podemos encontrar nossos fatores: $(a + b) = 84 + 13 = 97$ e $(a - b) = 84 - 13 = 71$. Portanto, os fatores são 97 e 71.

c) Para o número 7663 :

- $a = [\sqrt{7663}] \cong [87, 53] = 87 \Rightarrow b = \sqrt{7569 - 7663} = \sqrt{-94}$ (não deu certo)
- $a = 88 \Rightarrow b = \sqrt{7744 - 7663} = \sqrt{81} = 9$

Com $a = 88$ e $b = 9$, podemos encontrar nossos fatores: $(a + b) = 88 + 9 = 97$ e $(a - b) = 88 - 9 = 79$. Portanto, os fatores são 97 e 79.

d) Para o número 10117 :

- $a = [\sqrt{10117}] \cong [100{,}58] = 100 \Rightarrow b = \sqrt{10000 - 10117} = \sqrt{-117}$ (não deu certo)

- $a = 101 \Rightarrow b = \sqrt{10201 - 10117} = \sqrt{84} \cong 9{,}16$ (não deu certo)
- $a = 102 \Rightarrow b = \sqrt{10404 - 10117} = \sqrt{287} \cong 16{,}94$ (não deu certo)
- $a = 103 \Rightarrow b = \sqrt{10609 - 10117} = \sqrt{492} \cong 22{,}18$ (não deu certo)
- $a = 104 \Rightarrow b = \sqrt{10816 - 10117} = \sqrt{699} \cong 26{,}43$ (não deu certo)
- $a = 105 \Rightarrow b = \sqrt{11025 - 10117} = \sqrt{908} \cong 30{,}13$ (não deu certo)
- $a = 106 \Rightarrow b = \sqrt{11236 - 10117} = \sqrt{1119} \cong 33{,}45$ (não deu certo)
- $a = 107 \Rightarrow b = \sqrt{11449 - 10117} = \sqrt{1332} \cong 36{,}49$ (não deu certo)
- $a = 108 \Rightarrow b = \sqrt{11664 - 10117} = \sqrt{1547} \cong 39{,}33$ (não deu certo)
- $a = 109 \Rightarrow b = \sqrt{11881 - 10117} = \sqrt{1764} = 42$

Com $a = 109$ e $b = 42$, podemos encontrar nossos fatores: $(a + b) = 109 + 42 = 151$ e $(a - b) = 109 - 42 = 67$. Portanto, os fatores são 151 e 67.

Resoluções – Capítulo 2

Congruências

1) Vamos calcular:

a) Precisamos achar um número "x" tal que $3^{40} \equiv x \pmod 7$. Sabemos que $3^3 = 27 \equiv -1 \pmod 7$. Usando a **propriedade iii** e elevando os dois termos à potência 13, obtemos $3^{39} \equiv (-1)^{13} \equiv -1 \pmod 7$. Usando agora a **propriedade i** e multiplicando os termos por 3, obtemos $3^{40} \equiv -3 \pmod 7$. Para lidarmos com esse -3, note que $-3 \equiv 4 \pmod 7$ pois $-3 - 4 = -7 = 7 \cdot (-1)$.

Logo, $3^{40} \equiv 4 \pmod 7$ e o resto da divisão de 3^{40} por 7 é igual a 4.

b) Precisamos achar um número "x" tal que $12^{12} \equiv x \pmod 5$. Sabemos que $12 \equiv 2 \pmod 5$. Usando a **propriedade iii** e elevando os dois termos à potência 4, obtemos $12^4 \equiv 2^4 \equiv 16 \equiv 1 \pmod 5$. Usando novamente essa propriedade e elevando à potência 3, obtemos $12^{12} \equiv 1^3 \equiv 1 \pmod 5$.

O resto da divisão de 12^{12} por 5 é igual a 1.

c) Precisamos achar um número "x" tal que $2^{101} \equiv x \pmod{11}$. Sabemos que $2^5 = 32 \equiv -1 \pmod{11}$. Usando a **propriedade iii** e elevando os dois termos à potência 50, obtemos $2^{100} \equiv (-1)^{50} \equiv 1 \pmod{11}$. Usando agora a **propriedade i** e multiplicando os termos por 2, obtemos $2^{101} \equiv 2 \pmod{11}$.

O resto da divisão de 2^{101} por 11 é igual a 2.

d) Precisamos achar um número "x" tal que $14^{256} \equiv x \pmod 6$. Sabemos que $14 \equiv 2 \pmod 6$. Usando a **propriedade iii** e elevando os dois termos à potência 4, obtemos $14^4 \equiv 2^4 \equiv 16 \equiv -2 \pmod 6$. Repetindo o passo anterior, $14^{16} \equiv (-2)^4 \equiv 16 \equiv -2 \pmod 6$. Repetindo novamente, $14^{64} \equiv (-2)^4 \equiv 16 \equiv -2 \pmod 6$. Repetindo uma última vez, $14^{256} \equiv (-2)^4 \equiv 16 \equiv -2 \pmod 6$. Para lidarmos com esse -2, note que $-2 \equiv 4 \pmod 6$ pois $-1 - 4 = -6 = 6 \cdot (-1)$.

Logo, $14^{256} \equiv 4 \pmod 6$ e o resto da divisão de 14^{256} por 6 é igual à 4.

e) Precisamos achar um número "x" tal que $100^{33} + 33^{100} \equiv x \pmod 7$. Vamos fazer cada parcela separadamente e usarmos a **propriedade ii** no final.

Para a primeira parcela, sabemos que $100 \equiv 2 \pmod 7$. Usando a **propriedade iii** e elevando os dois termos à potência 3, obtemos $100^3 \equiv 2^3 \equiv 8 \equiv 1 \pmod 7$. Usando novamente essa propriedade e elevando à potência 11, obtemos $100^{33} \equiv 1^{11} \equiv 1 \pmod 7$. Logo, a primeira parcela é congruente à 1 módulo 7.

Para a segunda parcela, sabemos que $33 \equiv -2 \pmod 7$. Usando a **propriedade iii** e elevando os dois termos à potência 6, obtemos $33^6 \equiv 2^6 \equiv 64 \equiv 1 \pmod 7$. Usando novamente essa propriedade e elevando à potência 16, obtemos $33^{96} \equiv 1^{16} \equiv 1 \pmod 7$. Agora usando a **propriedade i** e multiplicando os dois termos por 33^4, obtemos $33^{100} \equiv 33^4 \equiv (-2)^4 \equiv 16 \equiv 2$. Logo, a segunda parcela é congruente à 2 módulo 7.

Usando a **propriedade ii**, com $100^{33} \equiv 1 \pmod 7$ e $33^{100} \equiv 2 \pmod 7$, obtemos $100^{33} + 33^{100} \equiv 3 \pmod 7$ e o resto da divisão de $100^{33} + 33^{100}$ por 7 é igual a 3.

f) Precisamos achar um número "x" tal que $99^5 + 100^5 \equiv x \pmod 4$. Vamos fazer cada parcela separadamente e usarmos a **propriedade ii** no final.

Para a primeira parcela, sabemos que $99 \equiv -1 \pmod 4$. Usando a **propriedade iii** e elevando os dois termos à potência 5, obtemos $99^5 \equiv (-1)^5 \equiv -1 \pmod 4$. Para lidarmos com esse -1, note que $-1 \equiv 3 \pmod 4$ pois $-1 - 3 = -4 = 4 \cdot (-1)$. Logo a primeira parcela é congruente à 3 módulo 4.

Para a segunda parcela, sabemos que $100 \equiv 0 \pmod 4$. Usando a **propriedade iii** e elevando os dois termos à potência 5, obtemos $100^5 \equiv 0^5 \equiv 0 \pmod 4$. Logo, a segunda parcela é congruente à 0 módulo 4.

Usando a **propriedade ii**, com $99^5 \equiv 3 \pmod 4$ e $100^5 \equiv 0 \pmod 4$, obtemos $99^5 + 100^5 \equiv 3 \pmod 4$ e o resto da divisão de $99^5 + 100^5$ por 4 é igual a 3.

2) Seguindo a dica, para resolver esse problema precisamos, na prática, encontrar o resto da divisão de 2^{70} por 10. Podemos seguir o mesmo caminho da questão anterior.

Precisamos achar um número "x" tal que $2^{70} \equiv x \pmod{10}$. Sabemos que $2^5 \equiv 2 \pmod{10}$. Usando a **propriedade iii** e elevando os dois termos à potência 7, obtemos $2^{35} \equiv 2^7 \equiv -2 \pmod{10}$. Usando a mesma propriedade com a potência 2 anterior, obtemos $2^{70} \equiv (-2)^2 \equiv 4 \pmod{10}$.

Logo, $2^{70} \equiv 4 \pmod{10}$ e o algarismo das unidades de 2^{70} é 4.

3) É o mesmo do exercício anterior, só que agora é $(\mathrm{mod}\, 100)$ ao invés de $(\mathrm{mod}\, 10)$.

Precisamos achar um número "x" tal que $7^{999999} \equiv x \pmod{100}$. Vamos ver as primeiras potências de 7:

- $7^2 = 49$
- $7^3 = 343$
- $7^4 = 2401$

Opa! $7^4 = 2401$, ou seja, $7^4 \equiv 1 \pmod{100}$. Para chegarmos na potência 999999, devemos usar a **propriedade iii** e para isso precisamos determinar em qual potência devemos elevar o 7^4. Para isso, basta dividir 999999 por 4 e pegar seu quociente. $999999 = 4 \cdot 249999 + 3$. Ou seja, a potência para ser elevada é 249999. Fazendo isso, obtemos $7^{999996} \equiv 1^{999996} \equiv 1 \pmod{100}$. Usando agora a **propriedade i** e multiplicando os termos por 7^3, obtemos $7^{999999} \equiv 7^3 \equiv 343 \equiv 43 \pmod{100}$.

Logo, $7^{999999} \equiv 43 \pmod{100}$ e os dois últimos algarismos de 7^{999999} é o número 43.

4) Seguindo o exemplo presente na apostila, vamos fazer as divisões euclidianas de $303, 997$ e 1492, cada um por 7:

- $303 = 7 \cdot 43 + 2$
- $997 = 7 \cdot 142 + 3$
- $1492 = 7 \cdot 213 + 1$

Então, dessas divisões, temos que $303 \equiv 2 \pmod 7$, $997 \equiv 3 \pmod 7$ e $1492 \equiv 1 \pmod 7$. Precisamos agora ver quais dias são congruentes a $1, 2, 3$ considerando o dia 0 ser o Sábado.

- Domingo é congruente a 1 módulo 7, então daqui a 1492 dias, será um domingo.
- Segunda-feira é congruente a 2 módulo 7, então daqui a 303 dias, será uma segunda-feira.
- Terça-feira é congruente a 3 módulo 7, então daqui a 997 dias, será uma terça-feira.

Teorema de Euler e Pequeno Teorema de Fermat

5) Para determinar esses valores, você precisa fazer a fatoração canônica do número e usar a expressão 2.2.1.

   a) $225 = 3^2 \cdot 5^2$. Então:

$$\varphi(225) = 225\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 225 \cdot \frac{2}{3} \cdot \frac{4}{5} = 225 \cdot \frac{8}{15} = 8 \cdot 15 = 120$$

   b) Parece complicado, mas ao fazer a fatoração, você obtém: $20480 = 2^{12} \cdot 5$. Então:

$$\varphi(20480) = 20480\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 20480 \cdot \frac{1}{2} \cdot \frac{4}{5} = 20480 \cdot \frac{4}{10} = 2048 \cdot 4 = 8192$$

   c) O desafio principal é fatorarmos $10! = 3628800$. Sabemos que $10! = 10 \times 9 \times 8 \times 7 \times 6 \times 5 \times 4 \times 3 \times 2 \times 1$. Então:

$$10! = 2 \times 5 \times 3^2 \times 2^3 \times 7 \times 2 \times 3 \times 5 \times 2^2 \times 3 \times 2 = 2^8 \times 3^4 \times 5^2 \times 7$$

   Com isso, temos:

$$\varphi(10!) = 3628800\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right)\left(1 - \frac{1}{7}\right) = 3628800 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} \cdot \frac{6}{7} =$$
$$= 3628800 \cdot \frac{8}{35} = 103680 \cdot 8 = 829440$$

6) Vamos calcular (o exercício pede para usar os dois teoremas mas não impede que as propriedades sejam usadas também):

   a) Como 5 é primo e $5 \nmid 12$, podemos usar o Pequeno Teorema de Fermat, obtendo $12^4 \equiv 1 \pmod 5$. Disso, usando a **propriedade iii** e elevando os dois termos à potência 3, obtemos $12^{12} \equiv 1 \pmod 5$. O resto da divisão de 12^{12} por 5 é igual a 1.

   b) Como $mdc(15, 8) = 1$, o Teorema de Euler pode ser usado. Como $\varphi(8) = 4$, temos que $15^4 \equiv 1 \pmod 8$. Disso, usando a **propriedade iii** e elevando os dois termos à potência 64, obtemos $15^{256} \equiv 1 \pmod 8$. O resto da divisão de 15^{256} por 8 é igual a 1.

c) Como $mdc(25, 16) = 1$, o Teorema de Euler pode ser usado. Como $\varphi(16) = 8$, temos que $25^8 \equiv 1 \pmod{16}$. Disso, usando a **propriedade iii** e elevando os dois termos à potência 253, obtemos $25^{2024} \equiv 1 \pmod{16}$. Agora, usando a **propriedade i** e multiplicando os dois termos por 25, obtemos $25^{2025} \equiv 25 \equiv 9 \pmod{16}$. O resto da divisão de 25^{2025} por 16 é igual a 9.

d) Como 23 é primo e $23 \nmid 39$, podemos usar o Pequeno Teorema de Fermat, obtendo $39^{22} \equiv 1 \pmod{23}$. Disso, usando a **propriedade iii** e elevando os dois termos à potência 6, obtemos $39^{132} \equiv 1 \pmod{23}$. Precisamos agora usar a **propriedade i** e multiplicar os dois termos por 39^3, mas antes, note que $39 \equiv 16 \pmod{23}$. Então $39^3 \equiv 16^3 \pmod{23}$. Vamos lidar com o 16^3. Sabemos que $16^2 = 256$ e $256 \equiv 3 \pmod{23}$. Então, $16^3 \equiv 16^2 \cdot 16 \equiv 3 \cdot 16 \equiv 48 \equiv 2 \pmod{23}$. Com isso, usando a **propriedade i**, obtemos $39^{135} \equiv 2 \pmod{23}$ O resto da divisão de 39^{135} por 23 é igual a 2.

e) Esse exercício é idêntico ao da seção anterior, que precisamos resolver de modo diferente. Como 7 é primo, $100 \nmid 7$ e $33 \nmid 7$, podemos usar o podemos usar o Pequeno Teorema de Fermat, obtendo $100^6 \equiv 1 \pmod{7}$ e $33^6 \equiv 1 \pmod{7}$. Vamos usar a **propriedade iii** nas duas congruências. Na primeira, vamos elevar os dois termos à potência 5 e na segunda, à potência 16, obtendo $100^{30} \equiv 1 \pmod{7}$ e $33^{96} \equiv 1 \pmod{7}$. Para chegarmos as congruências necessárias, precisamos multiplicar os termos da primeira por 100^3 e os termos da segunda por 33^4. Note que, $100 \equiv 2 \pmod{7}$ e $33 \equiv -2 \pmod{7}$. Então, $100^3 \equiv 2^3 \equiv 8 \equiv 1 \pmod{7}$ e $33^4 \equiv (-2)^4 \equiv 16 \equiv 2 \pmod{7}$. Então, usando a **propriedade i**, obtemos $100^{33} \equiv 1 \pmod{7}$ e $33^{100} \equiv 2 \pmod{7}$. Para finalizar, vamos usar a **propriedade ii** e somar essas duas congruências, obtendo $100^{33} + 33^{100} \equiv 1 + 2 \equiv 3 \pmod{7}$. O resto da divisão de $100^{33} + 33^{100}$ por 7 é igual a 3.

f) Só conseguimos usar o Teorema de Euler na primeira parcela pois $mdc(3, 15) \neq 1$, então teremos que usar somente as propriedades na segunda parcela. Vamos então tratar cada parcela separadamente.

Na primeira parcela, como $\varphi(15) = 8$, pelo Teorema de Euler, $2^8 \equiv 1 \pmod{15}$. Usando a **propriedade iii** e elevando os dois termos à potência 8, obtemos $2^{64} \equiv 1 \pmod{15}$. Ainda falta usar a **propriedade i** e multiplicarmos os termos por 2^6, mas note que $2^6 = 64$ e $64 \equiv 4 \pmod{15}$. Então, $2^{70} \equiv 4 \pmod{15}$.

Na segunda parcela, vamos ver as primeiras potências de 3 em relação à congruência:

- $3^1 = 3 \equiv 3 \pmod{15}$
- $3^2 = 9 \equiv 9 \pmod{15}$
- $3^3 = 27 \equiv 12 \pmod{15}$
- $3^4 = 81 \equiv 6 \pmod{15}$
- $3^5 = 243 \equiv 3 \pmod{15}$

Ou seja, de 4 em 4 expoentes, o resto é sempre igual a 3, e esse ciclo se repete indefinidamente, ao ponto de uma potência da forma 3^t, com t sendo um número que deixe resto 1 na divisão por 4 sempre ser congruente a 3 módulo 15. Então, qual o número de deixa resto 1 na divisão por 4 e que esteja mais próximo de 70? Esse número é o 69, pois $69 = 4 \cdot 17 + 1$. Com isso, $3^{69} \equiv 3 \pmod{15}$. Agora, usando a **propriedade i** e multiplicando os termos por 3, obtemos $3^{70} \equiv 9 \pmod{15}$.

Usando a **propriedade ii**, com $2^{70} \equiv 4 \pmod{15}$ e $3^{70} \equiv 9 \pmod{15}$, obtemos $2^{70} + 3^{70} \equiv 4 + 9 \equiv 13 \pmod{15}$ e o resto da divisão de $2^{70} + 3^{70}$ por 15 é igual a 13.

7) Esse exercício é semelhante ao exercício 3) da seção anterior. Como $mdc(9, 100) = 1$, podemos usar o Teorema de Euler. Como $100 = 2^2 \cdot 5^2$, então

$$\varphi(100) = 100\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right) = 100\cdot\frac{1}{2}\cdot\frac{4}{5} = 100\cdot\frac{4}{10} = 4\cdot 10 = 40$$

Com isso, pelo Teorema, $9^{40} \equiv 1 \pmod{100}$. Para chegarmos na potência 7777777, devemos usar a **propriedade iii** e para isso precisamos determinar em qual potência devemos elevar o 9^{40}. Para isso, basta dividir 7777777 por 0 e pegar seu quociente. $7777777 = 40\cdot 194444 + 17$. Ou seja, a potência para ser elevada é 194444. Fazendo isso, obtemos $9^{7777760} \equiv 1^{7777760} \equiv 1 \pmod{100}$. Para chegarmos no expoente procurado, precisamos usar a **propriedade i** e multiplicar os termos por 9^{17}, o que não é algo simples. Vamos passo-a-passo, usando as propriedades quando necessário:

- $9^2 = 81 \equiv 81 \pmod{100}$
- $9^4 \equiv 81^2 \equiv 6561 \equiv 61 \pmod{100}$
- $9^8 \equiv 61^2 \equiv 3721 \equiv 21 \pmod{100}$
- $9^{16} \equiv 21^2 \equiv 441 \equiv 41 \pmod{100}$
- $9^{17} \equiv 41\cdot 9 \equiv 369 \equiv 69 \pmod{100}$

Com isso, obtemos $9^{17} \equiv 69 \pmod{100}$. Agora sim, usando a **propriedade i**, obtemos $9^{7777777} \equiv 69 \pmod{100}$.

Logo, os dois últimos algarismos de $9^{7777777}$ é o número 69.

Congruências Lineares

8) Vamos resolver:

a) $mdc(8,6) = 2$ e $2 \mid 26$, com $26 = 2\cdot 13 \quad (t = 13)$. Essa congruência tem solução. Para achar uma solução particular, devemos achar r e s tal que $8r + 6s = 2$. Resolvendo essa equação, obtemos $8\cdot 1 + 6\cdot(-1) = 2$, ou seja, $r = 1$. Com $r = 1$ e $t = 13$, temos que $x_0 = rt = 1\cdot 13 = 13$, que é uma solução particular da congruência. Note que $13 \equiv 1 \pmod{6}$.

Sua solução geral é $x = 1 + \frac{6}{2}k = 1 + 3k, k \in \mathbb{Z}$. Como $d = 2$, temos 2 soluções incongruentes módulo 6, que são: $1, 1+3 \Rightarrow 1, 4$.

b) $mdc(18,26) = 2$ e $2 \mid 60$, com $30 = 2\cdot 30 \quad (t = 30)$. Essa congruência tem solução. Para achar uma solução particular, devemos achar r e s tal que $18r + 26s = 2$. Resolvendo essa equação, obtemos $18\cdot 3 + 26\cdot(-2) = 2$, ou seja, $r = 3$. Com $r = 3$ e $t = 30$, temos que $x_0 = rt = 3\cdot 30 = 90$, que é uma solução particular da congruência. Note que $90 \equiv 12 \pmod{26}$.

Sua solução geral é $x = 12 + \frac{26}{2}k = 12 + 13k, k \in \mathbb{Z}$. Como $d = 2$, temos 2 soluções incongruentes módulo 26, que são: $12, 12+13 \Rightarrow 12, 25$.

c) $mdc(6,18) = 6$ e $6 \nmid 21$, ou seja, essa congruência **não tem solução**.

d) $mdc(12,28) = 4$ e $4 \mid 36$, com $36 = 4\cdot 9 \quad (t = 9)$. Essa congruência tem solução. Para achar uma solução particular, devemos achar r e s tal que $12r + 28s = 4$. Resolvendo essa equação, obtemos $12\cdot(-2) + 28\cdot(1) = 4$, ou seja, $r = -2$. Com $r = -2$ e $t = 9$, temos que $x_0 = rt = (-2)\cdot 9 = -18$, que é uma solução particular da congruência. Note que $-18 \equiv 10 \pmod{28}$.

Sua solução geral é $x = 10 + \frac{28}{4}k = 10 + 7k, k \in \mathbb{Z}$. Como $d = 4$, temos 4 soluções incongruentes módulo 28, que são: $10, 10+7, 10+14, 10+21 \Rightarrow 10, 17, 24, 31 \Rightarrow 3, 10, 17, 24$, pois $31 \equiv 3 \pmod{28}$.

e) $mdc(13, 42) = 1$ e $1 \mid 4$, com $4 = 1 \cdot 4 \quad (t = 4)$. Essa congruência tem solução. Para achar uma solução particular, devemos achar r e s tal que $13r + 42s = 1$. Resolvendo essa equação, obtemos $13 \cdot (13) + 28 \cdot (-4) = 1$, ou seja, $r = 13$. Com $r = 13$ e $t = 4$, temos que $x_0 = rt = 13 \cdot 4 = 52$, que é uma solução particular da congruência. Note que $52 \equiv 10 \pmod{42}$.

Sua solução geral é $x = 10 + \frac{42}{1}k = 10 + 42k, k \in \mathbb{Z}$. Como $d = 1$, temos somente 1 solução incongruente módulo 42, que é 10.

f) $mdc(24, 59) = 1$ e $1 \mid 9$, com $9 = 1 \cdot 9 \quad (t = 9)$. Essa congruência tem solução. Para achar uma solução particular, devemos achar r e s tal que $24r + 59s = 1$. Resolvendo essa equação, obtemos $24 \cdot (-27) + 59 \cdot 11 = 1$, ou seja, $r = -27$. Com $r = -27$ e $t = 9$, temos que $x_0 = rt = (-27) \cdot 9 = -243$, que é uma solução particular da congruência. Note que $-243 \equiv 52 \pmod{59}$.

Sua solução geral é $x = 52 + \frac{59}{1}k = 52 + 59k, k \in \mathbb{Z}$. Como $d = 1$, temos somente 1 solução incongruente módulo 42, que é 52.

9) Vamos resolver:

a) Como 23 é primo, temos que $5^{23-2} \equiv 5^{-1} \pmod{23} \Rightarrow 5^{-1} \equiv 5^{21} \pmod{23}$.
O inverso procurado é o resto da divisão de 5^{21} por 23. Vamos encontrá-lo via propriedades das congruências:

$$\begin{aligned} 5^2 &\equiv 25 \equiv 2 \pmod{23} \\ 5^{10} &\equiv 2^5 \equiv 32 \equiv 9 \pmod{23} \\ 5^{20} &\equiv 9^2 \equiv 81 \equiv 12 \pmod{23} \\ 5^{21} &\equiv 12 \cdot 5 \equiv 60 \equiv 14 \pmod{23} \end{aligned}$$

O inverso de 5 módulo 23 é igual a 14. Prova real: $5 \times 14 = 70$ e $70 \equiv 1 \pmod{23}$.

b) Como 31 é primo, temos que $11^{31-2} \equiv 11^{-1} \pmod{31} \Rightarrow 11^{-1} \equiv 11^{29} \pmod{31}$.
O inverso procurado é o resto da divisão de 11^{29} por 31. Vamos encontrá-lo via propriedades das congruências:

$$\begin{aligned} 11^2 &\equiv 121 \equiv 28 \pmod{31} \\ 11^4 &\equiv 28^2 \equiv 784 \equiv 9 \pmod{31} \\ 11^{28} &\equiv 9^7 \equiv 4782969 \equiv 10 \pmod{31} \\ 11^{29} &\equiv 10 \cdot 11 \equiv 110 \equiv 17 \pmod{31} \end{aligned}$$

O inverso de 11 módulo 31 é igual a 17. Prova real: $11 \times 17 = 187$ e $187 \equiv 1 \pmod{31}$.

c) Como 15 é composto, precisamos calcular $\varphi(15)$. Como $15 = 3 \cdot 5$, então $\varphi(15) = \varphi(3) \cdot \varphi(5) = 2 \cdot 4 = 8$. Com isso, $4^{\varphi(15)-1} \equiv 4^{-1} \pmod{15}$, ou seja, $4^{-1} \equiv 4^7 \pmod{15}$.

O inverso procurado é o resto da divisão de 4^7 por 15. Vamos encontrá-lo via propriedades das congruências:

$$\begin{aligned} 4^2 &\equiv 16 \equiv 1 \pmod{15} \\ 4^6 &\equiv 1^3 \equiv 1 \pmod{15} \\ 4^7 &\equiv 1 \cdot 4 \equiv 4 \pmod{15} \end{aligned}$$

O inverso de 4 módulo 15 é igual a 4. Prova real: $4 \times 4 = 16$ e $16 \equiv 1 \pmod{15}$.

d) Como 55 é composto, precisamos calcular $\varphi(55)$. Como $55 = 5 \cdot 11$, então $\varphi(55) = \varphi(5) \cdot \varphi(11) = 4 \cdot 10 = 40$. Com isso, $42^{\varphi(55)-1} \equiv 42^{-1} \pmod{55}$, ou seja, $42^{-1} \equiv 42^{39} \pmod{55}$.

O inverso procurado é o resto da divisão de 42^{39} por 55. Vamos encontrá-lo via propriedades das congruências:

$$\begin{aligned} 42^3 &\equiv 74088 \equiv 3 \pmod{55} \\ 42^{12} &\equiv 3^4 \equiv 81 \equiv 26 \pmod{55} \\ 42^{36} &\equiv 26^3 \equiv 17576 \equiv 31 \pmod{55} \\ 42^{39} &\equiv 42^{36} \cdot 42^3 \equiv 31 \cdot 3 \equiv 93 \equiv 38 \pmod{55} \end{aligned}$$

O inverso de 42 módulo 55 é igual a 38. Prova real: $42 \times 38 = 1596$ e $1596 \equiv 1 \pmod{55}$.

e) Como 40 é composto, precisamos calcular $\varphi(40)$. Como $40 = 2^3 \cdot 5$, então $\varphi(40) = 40 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{5}\right) = 40 \cdot \left(\frac{1}{2}\right) \cdot \left(\frac{4}{5}\right) = 4 \cdot 4 = 16$. Com isso, $7^{\varphi(40)-1} \equiv 7^{-1} \pmod{40}$, ou seja, $7^{-1} \equiv 7^{15} \pmod{40}$.

O inverso procurado é o resto da divisão de 7^{15} por 40. Vamos encontrá-lo via propriedades das congruências:

$$\begin{aligned} 7^2 &\equiv 49 \equiv 9 \pmod{40} \\ 7^4 &\equiv 9^2 \equiv 81 \equiv 1 \pmod{40} \\ 7^{12} &\equiv 1^3 \equiv 1 \pmod{40} \\ 7^{15} &\equiv 1 \cdot 7^3 \equiv 243 \equiv 23 \pmod{40} \end{aligned}$$

O inverso de 7 módulo 40 é igual a 23. Prova real: $7 \times 23 = 161$ e $161 \equiv 1 \pmod{40}$.

f) Como 97 é primo, temos que $19^{97-2} \equiv 19^{-1} \pmod{97} \Rightarrow 19^{-1} \equiv 19^{95} \pmod{97}$.

O inverso procurado é o resto da divisão de 19^{95} por 97. Vamos encontrá-lo via propriedades das congruências:

$$19^2 \equiv 361 \equiv 70 \pmod{97}$$
$$19^4 \equiv 70^2 \equiv 4900 \equiv 50 \pmod{97}$$
$$19^8 \equiv 50^2 \equiv 2500 \equiv 75 \pmod{97}$$
$$19^{16} \equiv 75^2 \equiv 5625 \equiv -1 \pmod{97}$$
$$19^{32} \equiv (-1)^2 \equiv 1 \pmod{97}$$
$$19^{64} \equiv 1^2 \equiv 1 \pmod{97}$$
$$19^{80} \equiv 19^{64} \cdot 19^{16} \equiv 1 \cdot (-1) \equiv -1 \pmod{97}$$
$$19^{95} \equiv 19^{80} \cdot 19^8 \cdot 19^4 \cdot 19^2 \cdot 19 \equiv -1 \cdot 75 \cdot 50 \cdot 70 \cdot 19 \equiv -4987500 \equiv 46 \pmod{97}$$

O inverso de 19 módulo 97 é igual a 46. Prova real: $19 \times 46 = 874$ e $874 \equiv 1 \pmod{97}$.

Sistema de Congruências e o Teorema Chinês dos Restos

10) Vamos resolver:

a) Esse sistema nós resolveremos via método da substituição:
Da primeira congruência, $x \equiv 3 \pmod 8$, obtemos $x = 3 + 8y$, $y \in \mathbb{Z}$. Substituindo x na segunda congruência, obtemos $3 + 8y \equiv 8 \pmod{11}$, o que equivale a $8y \equiv 5 \pmod{11}$. Precisamos resolver essa congruência linear, o que é possível dado que $mdc(8, 11) = 1$ e $1 \mid 5$, com $5 = 1 \cdot 5 \quad (t = 5)$. Essa congruência tem solução. Para achar uma solução particular, devemos achar r e s tal que $8r + 11s = 1$. Resolvendo essa equação, obtemos $8 \cdot 7 + 11 \cdot (-5) = 1$, ou seja, $r = 7$. Com $r = 7$ e $t = 5$, temos que $y_0 = rt = 5 \cdot 7 = 35$, que é uma solução particular da congruência. Note que $35 \equiv 2 \pmod{11}$
Sua solução geral é $y = 2 + \dfrac{11}{1}k = 2 + 11k, k \in \mathbb{Z}$.
Voltando pro sistema, vamos substituir esse y em $x = 3+8y$, obtendo $x = 3+8\cdot(2+11k) = 3 + 16 + 88k = 19 + 88k$. Ou seja, a solução geral desse sistema é $x = 88k + 19$ ou $x \equiv 19 \pmod{88}$.

b) Uma vez que $mdc(3, 7) = mdc(3, 17) = mdc(7, 7) = 1$, o teorema pode ser usado. Como $m_1 = 3$, $m_2 = 7$, $m_3 = 17$, então $m = 3 \cdot 7 \cdot 17 = 357$ e

$$M_1 = \frac{m}{m_1} = 119 \qquad M_2 = \frac{m}{m_2} = 51 \qquad M_3 = \frac{m}{m_3} = 21$$

Vamos determinar agora inteiros r_i e s_i tais que $r_i M_i + s_i m_i = 1$ para $i = 1, 2, 3$. Temos:

$$1 = (-1) \cdot 119 + 40 \cdot 3 \Rightarrow r_1 = -1$$
$$1 = (-3) \cdot 51 + 22 \cdot 7 \Rightarrow r_2 = -3$$
$$1 = (-4) \cdot 21 + 5 \cdot 17 \Rightarrow r_3 = -4$$

Como $c_1 = 2, c_2 = 5$ e $c_3 = 9$, podemos determinar x_0:

$$x_0 = c_1r_1M_1 + c_2r_2M_2 + c_3r_3M_3 = 2 \cdot (-1) \cdot 119 + 5 \cdot (-3) \cdot 51 + 9 \cdot (-4) \cdot 21 = -1759$$

Portanto, $x_0 = -1759 \equiv 26 \pmod{357}$ e a solução geral do sistema é:

$$26 + 357k, k \in \mathbb{Z}$$

c) Precisamos primeiramente determinar um sistema equivalente (seguindo o que foi explicado na página 27), que é possível aplicar o Teorema Chinês dos Restos.
Da primeira congruência, $3x \equiv 1 \pmod{7}$, nós temos $d = mdc(3, 7) = 1$, $b^* = 1$, $m = 7$ e $1 = 3 \cdot 5 + 7 \cdot (-2) \Rightarrow r = 5$. Disso, segue que $x \equiv 5 \pmod{7}$.
Da segunda congruência, $5x \equiv 2 \pmod{11}$, nós temos $d = mdc(5, 11) = 1$, $b^* = 2$, $m = 11$ e $1 = 5 \cdot 9 + 11 \cdot (-4) \Rightarrow r = 9$. Disso, segue que $x \equiv 18 \equiv 7 \pmod{11}$.
Da terceira congruência, $4x \equiv 3 \pmod{13}$, nós temos $d = mdc(4, 13) = 1$, $b^* = 3$, $m = 13$ e $1 = 4 \cdot 10 + 13 \cdot (-3) \Rightarrow r = 10$. Disso, segue que $x \equiv 30 \equiv 4 \pmod{13}$.
O sistema é então equivalente ao sistema:

$$\begin{cases} x \equiv 5 \pmod{7} \\ x \equiv 7 \pmod{11} \\ x \equiv 4 \pmod{13} \end{cases}$$

Uma vez que $mdc(7, 11) = mdc(7, 13) = mdc(11, 13) = 1$, o teorema pode ser usado. Como $m_1 = 7$, $m_2 = 11$, $m_3 = 13$, então $m = 7 \cdot 11 \cdot 13 = 1001$ e

$$M_1 = \frac{m}{m_1} = 143 \qquad M_2 = \frac{m}{m_2} = 91 \qquad M_3 = \frac{m}{m_3} = 77$$

Vamos determinar agora inteiros r_i e s_i tais que $r_iM_i + s_im_i = 1$ para $i = 1, 2, 3$. Temos:

$$\begin{aligned} 1 &= (-2) \cdot 143 + 41 \cdot 7 \Rightarrow r_1 = -2 \\ 1 &= 4 \cdot 91 + (-33) \cdot 11 \Rightarrow r_2 = 4 \\ 1 &= (-1) \cdot 77 + 6 \cdot 13 \Rightarrow r_3 = -1 \end{aligned}$$

Como $c_1 = 5, c_2 = 7$ e $c_3 = 4$, podemos determinar x_0:

$$x_0 = c_1r_1M_1 + c_2r_2M_2 + c_3r_3M_3 = 5 \cdot (-2) \cdot 143 + 7 \cdot 4 \cdot 91 + 4 \cdot (-1) \cdot 77 = 810$$

Portanto, $x_0 = 810$ e a solução geral do sistema é:

$$x = 810 + 1001k, k \in \mathbb{Z}$$

11) A situação presente no problema representa o seguinte sistema de congruências:

$$\begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 2 \pmod{3} \\ x \equiv 2 \pmod{5} \\ x \equiv 5 \pmod{7} \end{cases}$$

Uma vez que $mdc(2,3) = mdc(2,5) = mdc(2,7) = mdc(3,5) = mdc(3,7) = mdc(5,7) = 1$, o teorema pode ser usado. Como $m_1 = 2$, $m_2 = 3$, $m_3 = 5$, $m_4 = 7$, então $m = 2 \cdot 3 \cdot 5 \cdot 7 = 210$ e

$$M_1 = \frac{m}{m_1} = 105 \qquad M_2 = \frac{m}{m_2} = 70 \qquad M_3 = \frac{m}{m_3} = 42 \qquad M_4 = \frac{m}{m_4} = 30$$

Vamos determinar agora inteiros r_i e s_i tais que $r_i M_i + s_i m_i = 1$ para $i = 1, 2, 3, 4$. Temos:

$$\begin{aligned}
&1 = 1 \cdot 105 + (-52) \cdot 2 \Rightarrow r_1 = 1 \\
&1 = 1 \cdot 70 + (-23) \cdot 3 \Rightarrow r_2 = 1 \\
&1 = (-2) \cdot 42 + 17 \cdot 5 \Rightarrow r_3 = (-2) \\
&1 = (-3) \cdot 30 + (13) \cdot 7 \Rightarrow r_4 = (-3)
\end{aligned}$$

Como $c_1 = 1, c_2 = 2$, $c_3 = 2$ e $c_4 = 5$, podemos determinar x_0:

$$\begin{aligned}
x_0 &= c_1 r_1 M_1 + c_2 r_2 M_2 + c_3 r_3 M_3 + c_4 r_4 M_4 = \\
&= 1 \cdot 1 \cdot 105 + 2 \cdot 1 \cdot 70 + 2 \cdot (-2) \cdot 42 + 5 \cdot (-3) \cdot 30 = \\
&= 105 + 140 - 168 - 450 = -373
\end{aligned}$$

Portanto, $x_0 = -373 \equiv 47 \pmod{210}$ e a solução geral do sistema é:

$$x = 47 + 210k, k \in \mathbb{Z}.$$

Como o problema pede a menor quantidade de ovos, colocando $k = 0$ na solução acima, obtemos 47 ovos presentes na cesta de Berenice.

12) A situação presente no problema representa o seguinte sistema de congruências:

$$\begin{cases} x \equiv 3 \pmod{5} \\ x \equiv 8 \pmod{14} \\ x \equiv 11 \pmod{17} \end{cases}$$

Uma vez que $mdc(5,14) = mdc(5,17) = mdc(14,17) = 1$, o teorema pode ser usado. Como $m_1 = 5$, $m_2 = 14$, $m_3 = 17$, então $m = 5 \cdot 14 \cdot 17 = 1190$ e

$$M_1 = \frac{m}{m_1} = 238 \qquad M_2 = \frac{m}{m_2} = 85 \qquad M_3 = \frac{m}{m_3} = 70$$

Vamos determinar agora inteiros r_i e s_i tais que $r_i M_i + s_i m_i = 1$ para $i = 1, 2, 3$. Temos:

$$\begin{aligned}
&1 = 2 \cdot 238 + (-95) \cdot 5 \Rightarrow r_1 = 2 \\
&1 = 1 \cdot 85 + (-6) \cdot 14 \Rightarrow r_2 = 1 \\
&1 = (-8) \cdot 70 + 33 \cdot 17 \Rightarrow r_3 = (-8)
\end{aligned}$$

Como $c_1 = 3, c_2 = 8$ e $c_3 = 11$, podemos determinar x_0:

$$\begin{aligned} x_0 &= c_1 r_1 M_1 + c_2 r_2 M_2 + c_3 r_3 M_3 = 3 \cdot 2 \cdot 238 + 8 \cdot 1 \cdot 85 + 11 \cdot (-8) \cdot 70 \\ &= 1428 + 680 - 6160 = -4052 \end{aligned}$$

Portanto, $x_0 = -4052 \equiv 708 \pmod{1190}$ e a solução geral do sistema é:

$$x = 708 + 1190k, k \in \mathbb{Z}$$

Como o problema pede a quantidade **mínima** de arroz, colocando $k = 0$ na solução acima, obtemos uma quantidade de arroz igual à $708Kg$ para cada fazendeiro. A quantidade **total** é de $708 \times 3 = 2124Kg$.

Resoluções – Capítulo 4

1) Se essas chaves públicas, digamos n e m, tem um primo em comum, digamos p, então $mdc(n, m) = p$. Com isso, é possível fazer $\frac{n}{p} = q_1$ e $\frac{m}{p} = q_2$ e com isso podemos quebrar o código dessas duas pessoas.

2) Se conhecemos n e m então :

$$m = (p-1)(q-1) = pq - (p+q) + 1 = n - (p+q) + 1 \Rightarrow (p+q) = n - m + 1$$

Sabemos que $pq = n$ e $p + q = n - m + 1$. Podemos usar a regra da soma e produto (da equação do $2^{\underline{o}}$ grau) para acharmos p e q dados esses valores.

Usando a regra da soma e do produto, $x^2 - Sx + P = 0$, onde S é a soma das raízes, $S = n - m + 1$ e P é o produto das raízes, $P = n$, temos, via fórmula de *Bháskara*, que:

$$p = \frac{n - m + 1 + \sqrt{(n-m+1)^2 - 4n}}{2} \quad q = \frac{n - m + 1 - \sqrt{(n-m+1)^2 - 4n}}{2}$$

3) Precisamos usar o exercício anterior para resolver isso, com $n = 3552377$ e $m = \varphi(n) = 3548580$:

- $S = p + q = n - m + 1 = 3552377 - 3548580 + 1 = 3798$
- $P = pq = n = 3552377$
- $x^2 - Sx + P = 0 \Rightarrow x^2 - 3798x + 3552377 = 0$

Calculando o Δ:

$$\Delta : 3798^2 - 4 \cdot 1 \cdot 3552377 = 14424804 - 14209508 = 215296$$

Calculando p e q:

$$p = \frac{3798 + \sqrt{215296}}{2} \quad q = \frac{3798 - \sqrt{215296}}{2} \Rightarrow p = \frac{3798 + 464}{2} \quad q = \frac{3798 - 464}{2}$$

$$p = \frac{4262}{2} = 2131 \qquad q = \frac{3334}{2} = 1667$$

Portanto, n é fatorado como $2131 \cdot 1667$.

4) Fatorando $n = 10403$, obtemos $n = 103 \cdot 101$, ou seja, $\varphi(n) = 102 \cdot 100 = 10200$. Sabemos que d é o inverso de $e = 8743$ módulo 10200, ou seja: $8743d \equiv 1 \pmod{10200}$. Como $mdc(8743, 10200) = 1$ e $1 \mid 1$ ($t = 1$). Devemos encontrar r e s tal que $8743r + 10200s = 1$. Vamos encontrar via **Algoritmo de Euclides Estendido**:

$$\begin{bmatrix} 8743 & 1 & 0 \\ 10200 & 0 & 1 \end{bmatrix} \Rightarrow \begin{bmatrix} 8743 & 1 & 0 \\ 10200 - 8743 & 0 - 1 & 1 - 0 \end{bmatrix} = \begin{bmatrix} 8743 & 1 & 0 \\ 1457 & -1 & 1 \end{bmatrix}$$

$$\Rightarrow \begin{bmatrix} 8743 - 1457 \cdot 6 & 1 - (-1) \cdot 6 & 0 - 1 \cdot 6 \\ 1457 & -1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 7 & -6 \\ 1457 & -1 & 1 \end{bmatrix}$$

$$\Rightarrow \begin{bmatrix} 1 & 7 & -6 \\ 1457 - 1457 \cdot 1 & -1 - 1457 \cdot 7 & 1 - 1457 \cdot (-6) \end{bmatrix} = \begin{bmatrix} 1 & 7 & -6 \\ 0 & -10200 & 8743 \end{bmatrix}$$

Portanto, achamos uma solução particular $(7, -6)$, e com isso, $r = 7$. Com $t = 1$ e $r = 7$, concluímos que $d = 7 \cdot 1 = 7$.

Agora precisamos decodificar cada bloco da mensagem codificada para encontrarmos a mensagem original, usando a chave $(10403, 7)$

- Para o bloco 4746

$$\begin{aligned} 4746^2 &\equiv 2021 \pmod{10403} \\ 4746^4 &\equiv 2021^2 \equiv 6465 \pmod{10403} \\ 4746^6 &\equiv 4746^4 \cdot 4746^2 \equiv 2021 \cdot 6465 \equiv 10000 \pmod{10403} \\ 4746^7 &\equiv 10000 \cdot 4746 \equiv 1514 \pmod{10403} \\ D(4746) &= 1514 \end{aligned}$$

- Para o bloco 8214

$$\begin{aligned} 8214^2 &\equiv 6341 \pmod{10403} \\ 8214^4 &\equiv 6341^2 \equiv 686 \pmod{10403} \\ 8214^6 &\equiv 8214^4 \cdot 8214^2 \equiv 6341 \cdot 686 \equiv 1472 \pmod{10403} \\ 8214^7 &\equiv 1472 \cdot 8214 \equiv 2722 \pmod{10403} \\ D(8214) &= 2722 \end{aligned}$$

- Para o bloco 9372

$$
\begin{aligned}
9372^2 &\equiv 1855 \pmod{10403} \\
9372^4 &\equiv 1855^2 \equiv 8035 \pmod{10403} \\
9372^6 &\equiv 9372^4 \cdot 9372^2 \equiv 1855 \cdot 8035 \equiv 7829 \pmod{10403} \\
9372^7 &\equiv 7829 \cdot 9372 \equiv 1029 \pmod{10403} \\
D(9372) &= 1029
\end{aligned}
$$

- Para o bloco 9009

$$
\begin{aligned}
9009^2 &\equiv 8278 \pmod{10403} \\
9009^4 &\equiv 8278^2 \equiv 723 \pmod{10403} \\
9009^6 &\equiv 9009^4 \cdot 9009^2 \equiv 723 \cdot 8278 \equiv 484 \pmod{10403} \\
9009^7 &\equiv 484 \cdot 9009 \equiv 1831 \pmod{10403} \\
D(9009) &= 1831
\end{aligned}
$$

- Para o bloco 4453

$$
\begin{aligned}
4453^2 &\equiv 1091 \pmod{10403} \\
4453^4 &\equiv 1091^2 \equiv 4339 \pmod{10403} \\
4453^6 &\equiv 4453^4 \cdot 4453^2 \equiv 4339 \cdot 1091 \equiv 484 \pmod{10403} \\
4453^7 &\equiv 484 \cdot 4453 \equiv 1831 \pmod{10403} \\
D(4453) &= 1831
\end{aligned}
$$

- Para o bloco 8198

$$
\begin{aligned}
8198^2 &\equiv 3824 \pmod{10403} \\
8198^4 &\equiv 3824^2 \equiv 6761 \pmod{10403} \\
8198^6 &\equiv 8198^4 \cdot 8198^2 \equiv 6761 \cdot 3824 \equiv 2609 \pmod{10403} \\
8198^7 &\equiv 2609 \cdot 8198 \equiv 14 \pmod{10403} \\
D(8198) &= 14
\end{aligned}
$$

A mensagem original recebida pelo banco foi $1514 - 2722 - 1029 - 9931 - 1831 - 14$, que pode ser dividida em:

$$15 - 14 - 27 - 22 - 10 - 29 - 99 - 31 - 18 - 31 - 14$$

Seguindo a tabela presente na página 41, a mensagem é **FERMAT VIVE**.