Universidade Federal de São Paulo

Instituto de Ciência e Tecnologia

Mestrado Profissional em Matemática em Rede Nacional - PROFMAT

Decifrando a Aritmética para o Ensino Fundamental

Lais Aline Casagrande Pires de Melo

Orientadora: Prof[a]. Dr[a]. Grasiele Cristiane Jorge

São José dos Campos
Março, 2017

PROFMAT

Título: *Decifrando a Aritmética para o Ensino Fundamental*

Dissertação apresentada ao Instituto de Ciência e Tecnologia da UNIFESP, campus São José dos Campos/SP, como parte dos requisitos exigidos para a obtenção do título de Mestre pelo Programa de Mestrado Profissional em Matemática em Rede Nacional – PROFMAT.

São José dos Campos
Março, 2017

de Melo, Lais Aline Casagrande Pires

Decifrando a Aritmética para o Ensino Fundamental, Lais Aline Casagrande Pires de Melo – São José dos Campos, 2017.

viii, 73f.

Dissertação (Mestrado) – Universidade Federal de São Paulo. Instituto de Ciência e Tecnologia. Programa de Pós-Graduação em Matemática em Rede Nacional (PROFMAT).

Deciphering Arithmetic for Middle School

1. Aritmética Modular. 2. Criptografia. 3. RSA. 4. Livro Digital.

UNIVERSIDADE FEDERAL DE SÃO PAULO

INSTITUTO DE CIÊNCIA E TECNOLOGIA

Mestrado Profissional em Matemática em Rede Nacional
PROFMAT

Chefe de departamento:

Prof. Dr. Carlos Marcelo Gurjão de Godoy

Coordenador do Programa de Pós-Graduação:

Prof. Dr. Angelo Calil Bianchi

LAIS ALINE CASAGRANDE PIRES DE MELO

DECIFRANDO A ARITMÉTICA PARA O ENSINO FUNDAMENTAL

Presidente da banca: Profª. Drª. Grasiele Cristiane Jorge

Banca examinadora:

Prof. Dr. Agnaldo José Ferrari

Profª. Drª. Cláudia Aline Azevedo dos Santos Mesquita

Profª. Drª. Vanessa Gonçalves Paschoa Ferraz

Data da Defesa: 03 de março de 2017

"A felicidade só é real quando compartilhada."
(Christopher McCandless)

AGRADECIMENTOS

Primeiramente a Deus por tudo.

Aos meus pais e irmã, pelo apoio incondicional, em especial a minha mãe por cuidar tão bem de mim e do meu lar para que eu pudesse estudar.

Ao meu marido e colega de curso, Rodrigo, por acreditar em mim em todos os momentos. A jornada PROFMAT foi muito mais leve com você ao meu lado.

A minha orientadora, professora Dr^{a}. Grasiele Cristiane Jorge, por toda disponibilidade e atenção mesmo em período de férias e por me conduzir no desenvolvimento de toda a dissertação.

A todos os professores do programa PROFMAT, por compartilharem seus conhecimentos.

Ao professor Dr. José Silvério Edmundo Germano e toda equipe do curso de formação de professores em Tecnologias Digitais da Informação e Comunicação, por me inspirar e ensinar a utilizar novos objetos educacionais digitais em minhas aulas.

Aos colegas do PROFMAT, por dividirem comigo inseguranças, angústias e alegrias ao longo do curso.

Ao ICT-Unifesp, por nos proporcionar um ambiente favorável aos estudos.

À CAPES pelo apoio financeiro, sem o qual não seria possível concluir este mestrado.

RESUMO

Neste trabalho estudamos tópicos relacionados à aritmética modular e ao sistema de criptografia RSA. Como uma proposta didática para estimular os alunos criamos um livro digital contextualizado, onde os alunos irão utilizar o algoritmo RSA e, com a ajuda do professor, irão entender todos os resultados matemáticos envolvidos em sua estrutura.

Palavras-chave: Aritmética Modular, Criptografia, RSA, Livro Digital.

ABSTRACT

In this work we study topics related to modular arithmetic and RSA cryptographic system. As a didactic proposal to stimulate students we create a contextualized digital book, where students will use the algorithm RSA and, with the help of the teacher, they will understand all mathematics results involved in its structure.

Keywords: Modular Arithmetic, Cryptografhy, RSA, Digital Book.

SUMÁRIO

1

INTRODUÇÃO

Desde os tempos remotos o homem vem desenvolvendo e utilizando técnicas que possibilitam a troca de mensagens secretas que podem ser lidas facilmente pelo receptor autorizado, mas dificilmente por aqueles que as interceptam sem autorização [4]. O estudo do processo de enviar uma mensagem secreta em que apenas o verdadeiro destinatário consegue compreender é feito pela criptografia. Em grego, as palavras "*cryptos*" e "*graphein*" significam "*oculto*" e "*escrever*", respectivamente, e então, a palavra criptografia significa "escrita oculta".

A criptografia por muito tempo esteve predominantemente associada aos segredos militares, de Estado, de diplomacia e de comércio. Foi devido ao uso crescente dos computadores e da internet como meio de comunicação que a criptografia foi deixando de ser empregada somente por grandes empresas e governos e começou também a ser utilizada em grande escala em várias operações realizadas via internet, como, por exemplo, transações bancárias, compras com cartões de crédito, aplicativos para mensagens em celulares e envio de e-mails. Com todo esse progresso tecnológico, métodos mais elaborados e confiáveis de sistemas criptográficos tornaram-se necessários. O sistema de criptografia RSA que será abordado neste trabalho figura entre um dos mais utilizados atualmente.

O avanço tecnológico das últimas décadas não somente impulsionou o desenvolvimento da criptografia como também transformou toda a sociedade. Hoje constituímos a chamada sociedade da informação, caracterizada pelas inúmeras formas de adquirir conhecimento através de novas tecnologias, que permitem acessar de maneira simples e incrivelmente rápida uma enorme quantidade de informações. Diante desta realidade, o aluno do século XXI não possui apenas a escola como o único referencial para buscar o conhecimento. Para se adequar a este novo perfil de aluno, é necessário deixar o ambiente escolar em sintonia com essas novas tecnologias. Um dos recursos a ser utilizado neste sentido é o livro digital. O livro digital se assemelha ao livro tradicional, porém ele pode ser lido em equipamentos eletrônicos como computadores, tablets e celulares e possui uma interatividade com o leitor, podendo ter imagens, animações, sons, vídeos e endereços eletrônicos para o leitor acessar e expandir sua experiência ao ler o livro.

Tendo em mente utilizar tecnologias digitais para tornar o ambiente escolar mais atrativo, neste trabalho foi elaborado um livro digital intitulado *"Ataque à Séquia*

- *Missão T55"*, que em seu desenrolar apresentará o sistema de criptografia RSA e atividades de codificação e decodificação de mensagens a serem desenvolvidas pelos estudantes.

Além do uso do livro digital, o estudo do sistema de criptografia RSA também é um elemento motivador para o aluno, pois está ligado com a questão tecnológica atual. Mais interessante do que aprender apenas a aplicar o algoritmo do RSA é entender por que ele funciona e, desta forma, o presente texto contém toda a fundamentação teórica necessária para o uso e o entendimento do RSA.

Assuntos como aritmética modular e criptografia não estão nos Parâmetros Curriculares Nacionais (PCNs) de Matemática (BRASIL, 1997). Contudo, segundo os PCNs, a potencialidade do conhecimento matemático deve ser explorada da forma mais ampla possível no ensino fundamental. Diante disso, a proposta que apresentamos pode ser aplicada através de uma atividade extracurricular com os alunos do 9º ano.

Nosso texto é dividido como se segue. No Capítulo 2 apresentamos resultados envolvendo números inteiros e naturais e focando em divisibilidade, máximo divisor comum e números primos. No Capítulo 3 falamos sobre aritmética dos restos e os Teoremas de Fermat e Euler. No Capítulo 4 descrevemos o sistema de criptografia RSA e explicamos como utilizar o sistema livre PARI/GP para fazer os cálculos utilizados no algoritmo do RSA. Finalmente, no Capítulo 5 apresentamos o livro digital *"Ataque à Séquia - Missão T55"* e a resolução das atividades nele contidas. Destacamos que o texto contém alguns conteúdos suplementares relacionados a números primos, que são o Crivo de Erastótenes e critérios de divisibilidade. O intuito de colocar estes tópicos foi para que o aluno pudesse se familiarizar com os números primos antes de estudar o RSA, uma vez que estes são os principais elementos que compõe tal sistema criptográfico.

2

NÚMEROS NATURAIS E NÚMEROS INTEIROS

Neste capítulo falaremos sobre divisibilidade no conjunto dos números inteiros, algoritmo euclidiano da divisão, máximo divisor comum, números primos e compostos, Teorema Fundamental da Aritmética e Crivo de Eratóstenes. Em nosso texto admitimos que o leitor esteja familiarizado com o *conjunto dos números inteiros*

$$\mathbb{Z} = \{\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots\},$$

com o *conjunto dos números naturais*

$$\mathbb{N} = \{1, 2, 3, \cdots\},$$

com as operações de adição e multiplicação e suas propriedades, com a ordenação dos inteiros, com a exponenciação e com o conceito de módulo de um número inteiro. Caso o leitor queira rever tais conceitos sugerimos [3, 7, 8]. Para os resultados apresentados neste capítulo utilizamos [7, 9].

2.1 MÚLTIPLOS E DIVISORES

Definição 2.1.1 *Dado um número inteiro a, o conjunto dos* **múltiplos inteiros** *de a é:*

$$a\mathbb{Z} = \{ad;\ d \in \mathbb{Z}\}.$$

Definição 2.1.2 *Diremos que um número inteiro d é um* **divisor** *de outro número inteiro a, se a é múltiplo de d, ou seja, se $a = dc$, para algum inteiro c. Neste caso, dizemos também que a é* **divisível** *por d ou que d* **divide** *a.*

Representaremos o fato de um número d ser divisor de um número a pelo símbolo $d \mid a$. Caso d não divida a, escreveremos $d \nmid a$.

Estabeleceremos a seguir algumas propriedades da divisibilidade:

Proposição 2.1.1 *Sejam $a, b, c \in \mathbb{Z}$. Temos que:*

(i) $1 \mid a$, $a \mid a$ *e* $a \mid 0$.

(ii) $0 \mid a \Leftrightarrow a = 0$.

(iii) *se* $a \mid b$ *e* $b \mid a \Rightarrow |a| = |b|$.

(iv) *se* $a \mid b$ *e* $b \mid c \Rightarrow a \mid c$.

(v) *se* $a \mid b$ *e* $b \neq 0 \Rightarrow |a| \leq |b|$.

(vi) *se* $a \mid b \Rightarrow a \mid bc$.

Demonstração:

(i) Decorre das igualdades $a = a.1$ e $0 = 0.a$.

(ii) Suponhamos que $0 \mid a$. Logo, existe $c \in \mathbb{Z}$ tal que $a = c.0 = 0$. Para a recíproca basta observar que $0 \mid 0$, que foi provado no item anterior.

(iii) Se $a = 0$, então $b = 0$ e $a = b$. Suponha agora $a \neq 0$. Como $a \mid b$ e $b \mid a$, existem inteiros p_1 e p_2 tais que $b = ap_1$ e $a = bp_2$. Substituindo o valor de b em $a = bp_2$ temos $a = ap_1p_2$, ou seja, $a(1 - p_1p_2) = 0$. Como $a \neq 0$, temos $p_1p_2 = 1$. Deste modo, ou $p_1 = p_2 = 1$ ou $p_1 = p_2 = -1$. Portanto, ou $a = b$ ou $a = -b$. Assim $|a| = |b|$.

(iv) Como $a \mid b$ e $b \mid c$, existem inteiros k_1 e k_2 tais que $b = k_1a$ e $c = k_2b$. Substituindo o valor de b na equação $c = k_2b$ temos $c = k_2(k_1a) = (k_2k_1)a$, o que nos mostra que $a \mid c$.

(v) De fato, se $a \mid b$, existe $c \in \mathbb{Z}$ tal que $b = ca$. Aplicando o módulo, temos que $|b| = |c||a|$. Como $b \neq 0$, temos que $c \neq 0$. Logo, $1 \leq |c|$ e, consequentemente, $|a| \leq |a||c| = |b|$.

(vi) Se $a \mid b$, existe $k \in \mathbb{Z}$ tal que $b = ka$. Multiplicando por c a equação $b = ka$, temos que $bc = kac = (kc)a$, o que nos mostra que $a \mid bc$. ■

Proposição 2.1.2 *Sejam* $a, b, c \in \mathbb{Z}$ *tais que* $a \mid b$ *e* $a \mid c$. *Então, para todo* x,y $\in \mathbb{Z}$ *temos que*

$$a \mid (xb + yc).$$

Demonstração: Como $a \mid b$ e $a \mid c$ então existem f, $g \in \mathbb{Z}$ tais que $b = fa$ e $c = ga$. Logo,

$$xb + yc = x(fa) + y(ga) = (xf + yg)a,$$

o que prova o resultado. ■

Exemplo 2.1.1 *Sabemos que* $3 \mid 9$ *e* $3 \mid 6$. *Então,* $3 \mid (9x + 6y)$ *para todo* $x,y \in \mathbb{Z}$. *Por exemplo,* $3 \mid 102$ *pois* $102 = 9 \times 4 + 6 \times 11$.

2.2 ALGORITMO EUCLIDIANO DA DIVISÃO

Sejam p, q dois números inteiros com $p < q$. Usaremos a notação $[p, q)$ para representar os números inteiros maiores ou iguais a p e menores do que q.

Teorema 2.2.1 *(Algoritmo Euclidiano da Divisão) Dados dois inteiros* a *e* b *com* $a \neq 0$, *existe um único par de inteiros* q *e* r *tais que* $b = qa + r$ *com* $0 \leq r < |a|$.

Demonstração: Suponhamos primeiro $a > 0$. Queremos comparar o número b com os múltiplos do número a. Para isto, consideremos todos os intervalos de inteiros da forma $[na, (n+1)a)$, para n um número inteiro qualquer. Isto nos dá uma partição de $\mathbb{Z}$:

$$\mathbb{Z} = \cdots \cup [-10a, -9a) \cup \cdots \cup [-3a, -2a) \cup [-2a, -a) \cup [-a, 0) \cup [0, a) \cup [a, 2a) \cup [2a, 3a) \cup \cdots \cup [10a, 11a) \cup \cdots.$$

O número b estará em um e apenas um dos intervalos acima. Digamos que b pertença ao intervalo $[qa, (q+1)a)$ para algum $q \in \mathbb{Z}$. Logo, $qa \leq b < (q+1)a$ e então $0 \leq b - qa < a$. Desta forma, fazendo $r = b - qa$ temos que $b = qa + r$ e $0 \leq r < a$, o que garante a existência de q e r.

Para mostrarmos a unicidade, suponhamos $b = qa + r = q_1 a + r_1$ com $q_1, r_1 \in \mathbb{Z}$ e $0 \leq r_1 < a$. Assim, $(q - q_1)a = r_1 - r$, o que implica que a divide $r_1 - r$. Mas, notemos que $0 \leq |r_1 - r| < a$, pois $0 \leq r < a$ e $0 \leq r_1 < a$. Logo, a única possibilidade em que a divide $(r_1 - r)$ é $|r_1 - r| = 0$, ou seja, $r_1 = r$. Desta forma, $a(q - q_1) = r_1 - r = 0$ e então $q - q_1 = 0$ (pois $a \neq 0$). Portanto, $q_1 = q$.

Para o caso $a < 0$, devemos particionar $\mathbb{Z}$ em intervalos de inteiros disjuntos do tipo $[na, (n-1)a)$ para $n \in \mathbb{Z}$. Assim,

$$\mathbb{Z} = \cdots \cup [10a, 9a) \cup \cdots \cup [3a, 2a) \cup [2a, a) \cup [a, 0) \cup [0, -a) \cup [-a, -2a) \cup [-2a, -3a) \cup \cdots \cup [-10a, -11a) \cup \cdots$$

e então o número b estará em apenas um dos intervalos acima. Digamos que b pertença ao intervalo $[qa, (q-1)a)$. Logo, $qa \leq b < (q-1)a$ e então $0 \leq b - qa <$

$-a$. Desta forma, fazendo $r = b - qa$ temos que $b = qa + r$ e $0 \leq r < -a = |a|$, o que garante a existência de q e r. A unicidade é mostrada de forma análoga ao que foi feito no caso $a > 0$. ■

Definição 2.2.1 *O número b do Teorema 2.2.1 é chamado de **dividendo**, o número a **divisor** e os números q e r são chamados, respectivamente, **quociente** e **resto** da divisão de b por a.*

Exemplo 2.2.1 *Vejamos alguns exemplos:*

- *Se $b = 24$ e $a = 5$, então $24 = 4 \times 5 + 4$ e $0 \leq 4 < 5$.*
- *Se $b = 24$ e $a = -5$, então $24 = (-4) \times (-5) + 4$ e $0 \leq 4 < |-5|$.*

Note que dados dois números inteiros a e b, nem sempre b é múltiplo de a. Este será o caso se, e somente se, $r = 0$.

Exemplo 2.2.2 *Quando $a > 0$ e $b > 0$ temos três casos para determinar os números q e r na divisão euclidiana, que são:*

(i) $b < a$*:*

Como $b = 0.a + b$, temos que $q = 0$ e $r = b$.

(ii) $b = a$*:*

Como $b = 1.a + 0$, neste caso tomamos $q = 1$ e $r = 0$.

(iii) $b > a$*:*

Podemos considerar a sequência

$$b - a, b - 2a, b - 3a, \cdots$$

até encontrar um número natural q tal que $b - (q+1)a < 0$ com $b - qa \geq 0$. Assim, obtemos $b = qa + r$, onde $r = b - qa$ e $0 \leq r < a$.

Por exemplo, para dividir o número 49 por 11, determinamos os resultados da subtração de 49 pelos múltiplos de 11:

$49 - 11 = 38$,
$49 - 2 \times 11 = 27$,
$49 - 3 \times 11 = 16$,
$49 - 4 \times 11 = 5$ *e*
$49 - 5 \times 11 = -6 < 0$.

Assim, a divisão euclidiana de 49 por 11 se expressa como:

$$49 = 4 \times 11 + 5.$$

2.3 MÁXIMO DIVISOR COMUM

Definição 2.3.1 *Dados dois números inteiros a e b não simultaneamente nulos, o maior divisor comum de a e b será chamado de* **máximo divisor comum** *de a e b e denotado por $mdc(a, b)$.*

Observação 2.3.1 *Note que $mdc(a, b) = mdc(b, a)$. Observe também que dados a, $b \in \mathbb{Z}$, temos que*

$$mdc(a, b) = mdc(-a, b) = mdc(a, -b) = mdc(-a, -b) = mdc(|a|, |b|).$$

Assim, para efeito do cálculo do máximo divisor comum de dois números inteiros, podemos sempre calcular o máximo divisor comum dos seus módulos.

O problema de determinar o máximo divisor comum de dois números é bem simples quando os números são pequenos, pois neste caso podemos listar todos os divisores comuns positivos desses números e escolher o maior deles, que será o seu máximo divisor comum.

Exemplo 2.3.1 *Para calcular $mdc(10, 15)$, determinamos todos os divisores positivos de 10, que são:*

$$1, 2, 5, 10;$$

e todos os divisores positivos de 15, que são:

$$1, 3, 5, 15.$$

Tomando o maior divisor comum, obtemos $mdc(10, 15) = 5$.

No entanto, quando um dos dois números for grande, esse método fica impraticável, pois achar divisores de um número grande é mais trabalhoso. Três séculos antes de Cristo, Euclides deu uma solução para este problema descrevendo um algoritmo muito eficiente para fazer o cálculo do máximo divisor comum. Este método é conhecido como *Algoritmo de Euclides* [7].

Lema 2.3.1 *(Lema de Euclides) Dados dois inteiros a e b, os divisores comuns de a e b são exatamente os divisores comuns de a e $b - ca$, para todo número inteiro c fixado.*

Demonstração: Se d é um divisor comum de a e b, é claro que d é divisor comum de a e de $b - ca$ pela Proposição 2.1.2.

Reciprocamente, suponhamos que d seja divisor comum de a e de $b - ca$. Logo, d também é divisor de ca pois $d \mid a$. Portanto, pela Proposição 2.1.2, temos que d é divisor de $b = (b - ca) + ca$. Assim, d é divisor comum de a e b. ∎

O Lema de Euclides nos diz que os divisores comuns de a e b são os mesmos divisores comuns de a e $b - ac$ para todo $c \in \mathbb{Z}$. Logo, tomando o maior divisor comum em ambos os casos, obtemos:

$$mdc(b, a) = mdc(a, b - ac).$$

Do Lema de Euclides podemos tirar um modo prático para calcular o máximo divisor comum de dois números que será enunciado no Teorema 2.3.1. Vejamos primeiro um exemplo do método.

Exemplo 2.3.2 *Vamos calcular o máximo divisor comum de a e b, onde $a = 108$ e $b = 294$.*

Pelo Lema de Euclides, sabemos que o máximo divisor comum de a e b é o mesmo que o de a e de b menos um múltiplo qualquer de a. Vamos tomar o menor dos números não negativos da forma b menos um múltiplo de a. Este número é obtido pelo algoritmo euclidiano da divisão:

$$294 = 108 \times 2 + 78.$$

Assim,

$$mdc(294, 108) = mdc(108, 294 - 108 \times 2) = mdc(108, 78).$$

Apliquemos o mesmo argumento ao par $a_1 = 78$ e $b_1 = 108$. Primeiro dividimos 108 por 78, obtendo:

$$108 = 78 \times 1 + 30.$$

Assim,

$$mdc(294, 108) = mdc(108, 78) = mdc(78, 108 - 78 \times 1) = mdc(78, 30).$$

Apliquemos novamente o mesmo argumento ao par $a_2 = 30$ e $b_2 = 78$. Primeiro dividimos 78 por 30, obtendo:

$$78 = 30 \times 2 + 18.$$

Assim,

$$mdc(294, 108) = mdc(78, 30) = mdc(30, 78 - 30 \times 2) = mdc(30, 18).$$

Mais uma vez, aplicamos o mesmo argumento para o par $a_3 = 18$ *e* $b_3 = 30$. *Temos que*

$$30 = 18 \times 1 + 12.$$

Assim,

$$mdc(294, 108) = mdc(30, 18) = mdc(18, 30 - 18 \times 1) = mdc(18, 12).$$

Aplicando o mesmo argumento pela penúltima vez, obtemos

$$mdc(294, 108) = mdc(18, 12) = mdc(12, 18 - 12 \times 1) = mdc(12, 6).$$

E finalmente encontramos o máximo divisor comum aplicando o argumento pela última vez:

$$mdc(294, 108) = mdc(12, 6) = mdc(6, 12 - 6 \times 2) = mdc(6, 0) = 6.$$

Logo,

$$mdc(294, 108) = 6.$$

Teorema 2.3.1 *Sejam* $r_0 = b$, $r_1 = a$ *inteiros não negativos com* $a \neq 0$. *Se o algoritmo da divisão for aplicado sucessivamente para se obter*

$$r_j = q_{j+1} r_{j+1} + r_{j+2}, \;\; 0 \leq r_{j+2} < r_{j+1}$$

para $j = 0, 1, 2, \cdots, n-1$ *e* r_{n+1} *for o primeiro resto igual a zero, então* $mdc(a, b) = r_n$.

Demonstração: Vamos inicialmente dividir b por a, ou seja, r_0 por r_1, obtendo $r_0 = q_1 r_1 + r_2$. Em seguida, dividimos r_1 por r_2 obtendo $r_1 = q_2 r_2 + r_3$ e assim, sucessivamente, até a obtenção do resto $r_{n+1} = 0$. É claro que vai existir um resto zero pois a sequência de restos inteiros $r_1 > r_2 > r_3 > \cdots \geq 0$ é decrescente e limitada inferiormente por zero. Até chegarmos ao resto zero obtemos as seguintes equações:

$$r_0 = q_1 r_1 + r_2 \text{ com } 0 < r_2 < r_1,$$

$$r_1 = q_2 r_2 + r_3 \text{ com } 0 < r_3 < r_2,$$

$$r_2 = q_3 r_3 + r_4 \text{ com } 0 < r_4 < r_3,$$

$$\vdots$$

$$r_{n-3} = q_{n-2} r_{n-2} + r_{n-1} \text{ com } 0 < r_{n-1} < r_{n-2},$$

$$r_{n-2} = q_{n-1} r_{n-1} + r_n \text{ com } 0 < r_n < r_{n-1} \text{ e}$$

$$r_{n-1} = q_n r_n + 0.$$

Pela última equação temos que $mdc(r_{n-1}, r_n) = r_n$ e, pelo Lema de Euclides, na penúltima equação temos que $mdc(r_{n-2}, r_{n-1}) = mdc(r_{n-1}, r_n) = r_n$. Prosseguindo desta maneira temos que $r_n = mdc(r_{n-1}, r_n) = mdc(r_{n-2}, r_{n-1}) = \cdots = mdc(r_1, r_2) = mdc(r_0, r_1) = mdc(a, b)$. ■

Exemplo 2.3.3 *No Exemplo 2.3.2 vimos que:*

$6 = 18 - 12 \times 1$,
$12 = 30 - 18 \times 1$,
$18 = 78 - 30 \times 2$,
$30 = 108 - 78 \times 1$ *e*
$78 = 294 - 108 \times 2$.

Juntando essas equações temos o seguinte:

$$\begin{aligned} 6 = 18 - 12 \times 1 &= 18 - (30 - 18 \times 1) \times 1 \\ &= 18 \times 2 - 30 \\ &= (78 - 30 \times 2) \times 2 - 30 \\ &= 78 \times 2 - 30 \times 5 \\ &= 78 \times 2 - (108 - 78 \times 1) \times 5 \\ &= 78 \times 7 - 108 \times 5 \\ &= (294 - 108 \times 2) \times 7 - 108 \times 5 \\ &= 294 \times 7 - 108 \times 19. \end{aligned}$$

Assim, podemos escrever:

$$6 = mdc(294, 108) = 294 \times 7 + 108 \times (-19).$$

No Teorema 2.3.2 veremos que o que ocorreu no Exemplo 2.3.3 ocorre sempre, ou seja, o máximo divisor comum de a e b pode ser expresso com $an + bm$ para inteiros apropriados n e m. Para a demonstração que se segue usaremos uma técnica um pouco diferente do que foi usado no Exemplo 2.3.3 acima com o intuito de obter uma demonstração simplificada.

Teorema 2.3.2 *(Relação de Bézout). Dados dois inteiros a e b, quaisquer, mas não ambos nulos, existem dois inteiros n e m tais que*

$$mdc(a,b) = an + bm.$$

Demonstração: Consideremos o conjunto $A = \{na + mb;\ m, n \in \mathbb{Z}\}$. Este conjunto contém números positivos, negativos e também o zero. Sejam n_0 e m_0 inteiros tais que $c = n_0a + m_0b$ seja o menor inteiro positivo do conjunto. Vamos provar que c é o máximo divisor comum entre a e b. Primeiro, mostremos que $c \mid a$ e $c \mid b$. Suponhamos que c não divide a. Neste caso, pelo algoritmo euclidiano da divisão, existem q e r inteiros tais que $a = qc + r$ com $0 < r < c$. Daí, $r = a - qc = a - q(n_0a + m_0b) = (1 - qn_0)a + (-qm_0)b$. Isso mostra que $r \in A$ pois $1 - qn_0$ e $-qm_0$ são inteiros. Mas, $0 < r < c$ e c é o menor elemento positivo do conjunto A. Logo, temos uma contradição e, portanto, $c \mid a$. De forma análoga mostramos que $c \mid b$. Seja d o máximo divisor comum de a e b. Logo, existem $k_1, k_2 \in \mathbb{Z}$ tais que $a = k_1d$ e $b = k_2d$. Desta forma, $c = n_0a + m_0b = n_0(k_1d) + m_0(k_2)d = (n_0k_1 + m_0k_2)d$, o que implica que $d \mid c$. Como $d \mid c$ e d e c são positivos temos que $d \leq c$. Como d é o máximo divisor de a e de b, então $c \leq d$. Logo, $d = c = n_0a + m_0b$. ∎

Observação 2.3.2 *Uma propriedade do máximo divisor comum que decorre da Relação de Bézout é a seguinte: se d é um divisor comum de dois números a e b, não simultaneamente nulos, então d divide $mdc(a,b)$.*

Da demonstração do Teorema 2.3.2 decorre o seguinte corolário:

Corolário 2.3.1 *Dados dois inteiros a e b, não ambos nulos, o menor elemento positivo do conjunto $a\mathbb{Z} + b\mathbb{Z}$ é $mdc(a,b)$.*

Definição 2.3.2 *Dois inteiros a e b são ditos* **primos entre si** *ou* **coprimos** *ou* **relativamente primos** *se $mdc(a,b) = 1$.*

Proposição 2.3.1 *Dois números inteiros a e b são primos entre si se, e somente se, existem inteiros m e n tais que $an + bm = 1$.*

Demonstração: Suponhamos que a e b sejam primos entre si, isto é, $mdc(a,b) = 1$. Pela Relação de Bézout existem inteiros n e m tais que $an + bm = mdc(a,b) = 1$. Reciprocamente, se existem inteiros n e m tais que $an + bm = 1$, segue que 1 é o menor elemento positivo do conjunto $a\mathbb{Z} + b\mathbb{Z}$. Logo, ele é o máximo divisor comum de a e b. Portanto, a e b são primos entre si. ∎

Proposição 2.3.2 *Para todo inteiro positivo t, $mdc(ta, tb) = t\,mdc(a, b)$.*

Demonstração: Pela Relação de Bézout e pelo Corolário 2.3.1, temos que $mdc(ta, tb)$ é o menor valor positivo de $\{tan + tbm;\ m, n \in \mathbb{Z}\}$, que é igual a t vezes o menor valor positivo de $\{an + bm;\ m, n \in \mathbb{Z}\}$. ■

Proposição 2.3.3 *Se $c > 0$ e a e b são divisíveis por c, então*

$$mdc\left(\frac{a}{c}, \frac{b}{c}\right) = \frac{1}{c} mdc(a, b).$$

Demonstração: Como a e b são divisíveis por c, temos que $\frac{a}{c}$ e $\frac{b}{c}$ são inteiros. Basta, então, substituir na Proposição 2.3.2 a por $\frac{a}{c}$ e b por $\frac{b}{c}$ tomando $t = c$. Daí, teremos $mdc(a, b) = c\,mdc\left(\frac{a}{c}, \frac{b}{c}\right)$ e o resultado segue. ■

Corolário 2.3.2 *Se $mdc(a, b) = d$, temos que $mdc\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.*

Demonstração: Se tomarmos c como sendo o máximo divisor comum d na Proposição 2.3.3, teremos o resultado desejado. ■

Proposição 2.3.4 *Se $a \mid bc$ e $mdc(a, b) = 1$, então $a \mid c$.*

Demonstração: Como $mdc(a, b) = 1$ pela Proposição 2.3.1 existem inteiros n e m tais $na + mb = 1$. Multiplicando os dois lados desta igualdade por c temos $(na)c + (mb)c = n(ac) + m(bc) = c$. Como $a \mid ac$ e, por hipótese, $a \mid bc$ então, pela Proposição 2.1.2, $a \mid c$. ■

Exemplo 2.3.4 *Temos que $4 \mid (27 \times 20)$. Como $mdc(4, 27) = 1$, então $4 \mid 20$.*

2.4 NÚMEROS PRIMOS E COMPOSTOS

Definição 2.4.1 *Um número natural $n > 1$ possuindo somente dois divisores positivos (n e 1) é chamado* **primo**. *Se $n > 1$ não é primo, dizemos que é* **composto**.

Exemplo 2.4.1 *O número 210 é composto pois possui como divisores positivos 1, 2, 3, 5 e 7. De fato, 210 pode ser representado pelo produto de dois números naturais menores, o 21 e o 10 ($210 = 21 \times 10$). Mas, os números 21 e 10 também são compostos, pois $21 = 3 \times 7$ e $10 = 2 \times 5$. Dessa forma, temos que $210 = 21 \times 10 = 3 \times 7 \times 2 \times 5$. Esta é a decomposição completa de nosso número (sua representação como produto de números primos está na Figura 1.*

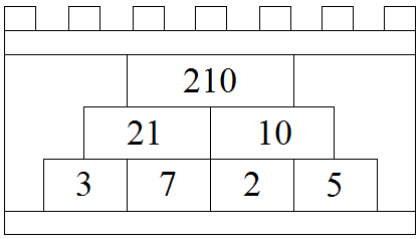

Figura 1: Torre da fatoração de 210

Proposição 2.4.1 *Sejam p, a, b inteiros. Se p é primo e $p \mid ab$, então $p \mid a$ ou $p \mid b$.*

Demonstração: Se $p \not| a$, então $mdc(a, p) = 1$. Logo, pela Proposição 2.3.4, temos que $p \mid b$. ■

Corolário 2.4.1 *Sejam $p, a_1, \cdots, a_n$ inteiros. Se p é primo e $p \mid a_1 \cdots a_n$, então $p \mid a_i$ para algum i.*

Números primos são como tijolos com os quais você pode construir todos os números naturais maiores do que 1 como veremos no próximo teorema.

Teorema 2.4.1 *(Teorema Fundamental da Aritmética) Todo inteiro n maior do que 1 pode ser representado de maneira única (a menos da ordem) como um produto de fatores primos.*

Demonstração: Se n é primo não há nada a ser demonstrado. Suponhamos, pois, n composto. Seja p_1 o menor dos divisores positivos de n diferente de 1 ($p_1 > 1$). Afirmamos que p_1 é primo. Isto é verdade, pois, caso contrário existiria $p, 1 < p < p_1$ com $p \mid p_1$ e então $p \mid n$, contradizendo a escolha de p_1. Logo, $n = p_1 n_1$ com p_1 primo.
Se n_1 for primo a prova está completa. Caso contrário, tomamos p_2 como o menor fator de n_1 diferente de 1. Pelo argumento anterior, p_2 é primo e temos que $n = p_1 p_2 n_2$ com p_1, p_2 primos.
Repetindo esse procedimento, obtemos uma sequência decrescente de inteiros positivos $n_1, n_2, \cdots$. Como todos estes inteiros são maiores do que 1, este processo deve terminar e então $n = p_1 p_2 \cdots p_k$ para algum $k \geq 2$. Como os primos $p_1, p_2, \cdots, p_k$ não são, necessariamente, distintos, n terá, em geral, a forma:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}.$$

Para mostrarmos a unicidade usamos indução em n. Para $n = 2$ a afirmação é verdadeira. Assumimos, então, que ela se verifica para todos os inteiros maiores do

que 1 e menores do que n. Vamos provar que ela também é verdadeira para n. Se n é primo, não há nada a provar. Vamos supor, então, que n seja composto e que tenha duas fatorações, isto é,

$$n = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_r.$$

Vamos provar que $s = r$ e que cada p_i é igual a algum q_j. Como p_1 é primo e divide o produto $q_1 q_2 \cdots q_r$, pelo Corolário 2.4.1 ele divide pelo menos um dos fatores q_j. Sem perda de generalidade podemos supor que $p_1 \mid q_1$. Como são ambos primos, isto implica $p_1 = q_1$. Logo $n/p_1 = p_2 \cdots p_s = q_2 \cdots q_r$. Como $1 < n/p_1 < n$, a hipótese de indução nos diz que as duas fatorações são idênticas, isto é, $s = r$ e, a menos da ordem, as fatorações $p_1 p_2 \cdots p_s$ e $q_1 q_2 \cdots q_r$ são iguais.

■

Teorema 2.4.2 *(Euclides) A sequência dos números primos é infinita.*

Demonstração: Suponhamos que a sequência dos números primos seja finita. Seja $p_1, p_2, \cdots, p_n$ a lista de todos os primos. Consideremos o número $R = p_1 p_2 \cdots p_n + 1$. É claro que R não é divisível por nenhum dos p_i de nossa lista pois se fosse divisível por alguns deles, o número 1 também seria, o que não acontece. Além disso, R é maior do que qualquer p_i. Agora, pelo Teorema Fundamental da Aritmética, ou R é primo ou possui algum fator primo e isto implica na existência de um primo que não pertence à nossa lista. Portanto a sequência dos números primos não pode ser finita. ■

2.5 CRIVO DE ERATÓSTENES

Um método muito antigo para verificar se um número é primo é o chamado *Crivo de Eratóstenes*, devido ao matemático grego Eratóstenes. O método será descrito através do Exemplo 2.5.1. A eficiência do método é baseada no seguinte teorema:

Teorema 2.5.1 *Se um número natural n não é primo, então n possui, necessariamente, um fator primo menor do que ou igual a $\sqrt{n}$.*

Demonstração: Sendo n composto, então $n = n_1 n_2$ onde $1 < n_1 < n$ e $1 < n_2 < n$. Sem perda de generalidade vamos supor $n_1 < n_2$. Logo, $n_1 \leq \sqrt{n}$ pois, caso contrário, teríamos $n = n_1 n_2 > \sqrt{n}\sqrt{n} = n$, o que é um absurdo. Portanto, pelo Teorema Fundamental da Aritmética, se n_1 possui algum fator primo p, este deve ser $\leq \sqrt{n}$. Como p, sendo um fator primo de n_1 é também um fator de n, a demonstração está completa. ■

Exemplo 2.5.1 *Vamos analisar todos os números primos menores ou iguais a* 97. *Os números primos menores ou iguais a* $\sqrt{97} \simeq 9,85$ *são* $2, 3, 5,$ *e* 7. *Criemos uma tabela com os números de* 2 *até* 97 *como a Tabela* 1.

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97			

Tabela 1: Exemplo Crivo de Eratóstenes

O primeiro desses números, o 2, *é primo, pois ele não é múltiplo de nenhum número anterior diferente de* 1. *Risquemos todos os demais múltiplos de* 2 *na tabela, pois esses não são primos.*

	2	3	~~4~~	5	~~6~~	7	~~8~~	9	~~10~~
11	~~12~~	13	~~14~~	15	~~16~~	17	~~18~~	19	~~20~~
21	~~22~~	23	~~24~~	25	~~26~~	27	~~28~~	29	~~30~~
31	~~32~~	33	~~34~~	35	~~36~~	37	~~38~~	39	~~40~~
41	~~42~~	43	~~44~~	45	~~46~~	47	~~48~~	49	~~50~~
51	~~52~~	53	~~54~~	55	~~56~~	57	~~58~~	59	~~60~~
61	~~62~~	63	~~64~~	65	~~66~~	67	~~68~~	69	~~70~~
71	~~72~~	73	~~74~~	75	~~76~~	77	~~78~~	79	~~80~~
81	~~82~~	83	~~84~~	85	~~86~~	87	~~88~~	89	~~90~~
91	~~92~~	93	~~94~~	95	~~96~~	97			

Tabela 2: Exemplo Crivo de Eratóstenes

O primeiro número não riscado na nova tabela, a Tabela 2*, é o* 3 *que é primo, pois não é múltiplo de nenhum número anterior diferente de* 1*. Risquemos todos os demais múltiplos de* 3 *na tabela, pois esses não são primos.*

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	25	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	35	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	49	~~50~~
~~51~~	~~52~~	53	~~54~~	55	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	65	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	77	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	85	~~86~~	~~87~~	~~88~~	89	~~90~~
91	~~92~~	~~93~~	~~94~~	95	~~96~~	97			

Tabela 3: Exemplo Crivo de Eratóstenes

O primeiro número não riscado na nova tabela, a Tabela 3*, é o* 5 *que é primo, pois não é múltiplo de nenhum número anterior diferente de* 1*. Risquemos todos os demais múltiplos de* 5 *na tabela, pois esses não são primos.*

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	49	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	77	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
91	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97			

Tabela 4: Exemplo Crivo de Eratóstenes

O primeiro número maior do que 5 *e que não foi riscado na Tabela* 4 *é o* 7*, que é primo. Risquemos os demais múltiplos de* 7 *na tabela.*

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97			

Tabela 5: Exemplo Crivo de Eratóstenes

Logo, os primos entre 2 *e* 97 *são todos aqueles que não foram riscados na Tabela* 5*, pois se tais números não fossem primos eles teriam como fator* 2*,* 3*,* 5 *ou* 7*. Em particular, o número* 97 *é primo.*

3

A ARITMÉTICA DOS RESTOS

A grande ideia de Gauss (1777-1855) de desenvolver uma aritmética dos restos da divisão por um certo número fixado será apresentada neste capítulo. Falaremos sobre congruências, classes residuais, inversos modulares, equações diofantinas, Teorema de Fermat, Teorema de Euler e critérios de divisibilidade. Para os resultados apresentados neste capítulo utilizamos [1, 7, 8, 9].

3.1 CONGRUÊNCIAS

Definição 3.1.1 *Seja dado um número inteiro m maior do que 1. Diremos que dois números inteiros a e b são* **congruentes módulo** *m se a e b possuírem mesmo resto quando divididos por m e simbolizaremos por:*

$$a \equiv b \ mod \ m.$$

Quando a e b não forem congruentes módulo m, escreveremos

$$a \not\equiv b \ mod \ m.$$

Exemplo 3.1.1 *Alguns exemplos de inteiros congruentes módulo m:*

(1) $23 \equiv 5 \ mod \ 3$*, pois os restos das divisões de* 23 *e de* 5 *por* 3 *são os mesmos (iguais a* 2*).*

(2) $33 \equiv 18 \ mod \ 5$*, pois os restos das divisões de* 33 *e* 18 *por* 5 *são os mesmos (iguais a* 3*).*

(3) $29 \not\equiv 9 \ mod \ 7$*, pois o resto da divisão de* 29 *por* 7 *é* 1*, enquanto que o resto da divisão de* 9 *por* 7 *é* 2*.*

A menos que se diga o contrário, no que se segue m será um número inteiro maior do que 1.

Para mostrar que $a \equiv b \bmod m$ não é necessário efetuar a divisão de a e de b por m, como mostrado a seguir.

Proposição 3.1.1 *Sejam a e b dois números inteiros. Temos que $a \equiv b \ mod \ m$ se, e somente se, m divide $b - a$.*

Demonstração: De fato, pelo algoritmo euclidiano da divisão, podemos escrever

$$a = mq_1 + r_1 \text{ e } b = mq_2 + r_2,$$

onde $0 \leq r_1 < m$ e $0 \leq r_2 < m$. Sem perda de generalidade, podemos supor $r_1 \leq r_2$ (se o contrário ocorrer, basta considerar $a - b$ ao invés de $b - a$ na equação a seguir). Assim, podemos escrever

$$b - a = m(q_2 - q_1) + r_2 - r_1.$$

Logo, pela Proposição 2.1.2 temos que m divide $b - a$ se, e somente se, m divide $r_2 - r_1$. Por ser $0 \leq r_2 - r_1 < m$, segue que m divide $b - a$ se, e somente se, $r_2 - r_1 = 0$, ou seja, se, e somente se, $r_2 = r_1$. ■

Proposição 3.1.2 *Se a e b são inteiros, temos que $a \equiv b \ mod \ m$ se, e somente se, existir um inteiro k tal que $a = b + km$.*

Demonstração: Se $a \equiv b \bmod m$, então $m \mid (a - b)$ o que implica na existência de um inteiro k tal que $a - b = km$, isto é, $a = b + km$. A recíproca é trivial pois na existência de k satisfazendo $a = b + km$, temos $km = a - b$, ou seja, que $m \mid (a - b)$ isto é, $a \equiv b \bmod m$. ■

Proposição 3.1.3 *Para todo $a, b, c \in \mathbb{Z}$, temos que:*

(i) $a \equiv a \ mod \ m$ (propriedade reflexiva).

(ii) se $a \equiv b \ mod \ m$, então $b \equiv a \ mod \ m$ (propriedade simétrica).

(iii) se $a \equiv b \ mod \ m$ e $b \equiv c \ mod \ m$, então $a \equiv c \ mod \ m$ (propriedade transitiva).

Demonstração:

(i) Como $m \mid 0$, então $m \mid (a - a)$, o que implica $a \equiv a \bmod m$.

(ii) Se $a \equiv b \bmod m$, então $a = b + km$ para algum inteiro k. Logo $b = a - km$, o que implica, pela Proposição 3.1.2, $b \equiv a \bmod m$.

(iii) Se $a \equiv b \bmod m$ e $b \equiv c \bmod m$, então existem inteiros k_1 e k_2 tais que $a - b = k_1 m$ e $b - c = k_2 m$. Somando, membro a membro, estas últimas equações, obtemos $a - c = (k_1 + k_2)m$, o que implica pela Proposição 3.1.2 que $a \equiv c \bmod m$. ■

Definição 3.1.2 *Se h e k são dois inteiros com $h \equiv k \ mod \ m$, dizemos que h é um* **resíduo de k módulo m.**

Definição 3.1.3 *O conjunto de inteiros* $\{r_1, \cdots, r_s\}$ *é chamado um* **sistema completo de resíduos módulo** m *se:*

1. $r_i \not\equiv r_j \ mod\ m$ *para* $i \neq j$;

2. *para todo inteiro* n *existe um* r_i *tal que* $n \equiv r_i \ mod\ m$.

Proposição 3.1.4 *O conjunto* $\{0, 1, ..., m-1\}$ *é um sistema completo de resíduos módulo* m.

Demonstração: Para um dado inteiro a, pela divisão euclidiana, existem q e r inteiros tais que $a = mq + r$, onde $0 \leq r < m$. Daí, $mq = a - r$, o que implica que $m \mid (a - r)$, ou seja, $a \equiv r \mod m$. Se $r_1, r_2 \in \{0, 1, ..., m-1\}$ e $r_1 < r_2$, então $0 < r_2 - r_1 < m$. Logo, m não divide $r_2 - r_1$, o que implica que r_1 e r_2 não são congruentes módulo m. ■

3.1.1 *Congruências e Somas*

Proposição 3.1.5 *Sejam* a_1, a_2, b_1 *e* b_2 *inteiros quaisquer. Se* $a_1 \equiv b_1 \ mod\ m$ *e* $a_2 \equiv b_2 \ mod\ m$, *então* $a_1 + a_2 \equiv b_1 + b_2 \ mod\ m$ *e* $a_1 - a_2 \equiv b_1 - b_2 \ mod\ m$.

Demonstração: De fato, como $a_1 \equiv b_1 \mod m$ e $a_2 \equiv b_2 \mod m$, então m divide $b_1 - a_1$ e divide $b_2 - a_2$. Logo,

$$m \text{ divide } (b_1 - a_1) + (b_2 - a_2) = (b_1 + b_2) - (a_1 + a_2),$$

mostrando que $b_1 + b_2 \equiv a_1 + a_2 \mod m$. O caso $a_1 - a_2 \equiv b_1 - b_2 \mod m$ é similar. ■

Pela Proposição 3.1.5 temos que as congruências de mesmo módulo somam-se e subtraem-se membro a membro tal qual as igualdades.

Proposição 3.1.6 *Sejam* $a, b, c, m \in \mathbb{Z}$. *Temos que:*

$$a + c \equiv b + c \ mod\ m \text{ se, e somente se, } a \equiv b \ mod\ m.$$

Demonstração: Se $a \equiv b \mod m$, segue imediatamente da Proposição 3.1.5 que $a + c \equiv b + c \mod m$, pois $c \equiv c \mod m$. Reciprocamente, se $a + c \equiv b + c \mod m$, então m divide $(b + c) - (a + c)$, o que implica que m divide $b - a$ e, consequentemente, $a \equiv b \mod m$. ■

Pela Proposição 3.1.6 temos que para as congruências, vale o cancelamento com relação à adição.

3.1.2 *Congruências e Produtos*

Proposição 3.1.7 *Sejam a_1, a_2, b_1 e b_2 inteiros quaisquer. Se $a_1 \equiv b_1$ mod m e $a_2 \equiv b_2$ mod m, então $a_1a_2 \equiv b_1b_2$ mod m.*

Demonstração: De fato, como $a_1 \equiv b_1 \bmod m$ e $a_2 \equiv b_2 \bmod m$, então m divide $a_1 - b_1$ e $a_2 - b_2$. Por outro lado, como

$$a_1a_2 - b_1b_2 = a_1a_2 - b_1b_2 + a_1b_2 - a_1b_2 = a_1(a_2 - b_2) + b_2(a_1 - b_1),$$

segue, pela Proposição 2.1.2, que m divide $a_1a_2 - b_1b_2$, o que prova o resultado. ■

Pela Proposição 3.1.7 temos que as congruências de mesmo módulo multiplicam-se membro a membro tal qual as igualdades.

Repetidas aplicações da Proposição 3.1.7 fornecem o seguinte resultado:

Corolário 3.1.1 *Se $a \equiv b$ mod m, então $a^n \equiv b^n$ mod m, para todo n natural.*

3.2 CLASSES RESIDUAIS

Definição 3.2.1 *Dado um inteiro a denotaremos por $\overline{a}$ o conjunto*

$$\overline{a} = \{x \in \mathbb{Z} \text{ tal que } x \equiv a \bmod m\}.$$

Tal conjunto será chamado de **classe residual de a módulo m.**

Observação 3.2.1 *Dados dois números inteiros a e b temos que $\overline{a} = \overline{b}$ se, e somente se, os restos da divisão de a e de b por m são iguais, ou seja,*

$$\overline{a} = \overline{b} \text{ se, e somente se, } a \equiv b \bmod m.$$

Consideremos as classes residuais

$$\begin{aligned}
\overline{0} &= \{x \in \mathbb{Z};\ x \equiv 0 \bmod m\},\\
\overline{1} &= \{x \in \mathbb{Z};\ x \equiv 1 \bmod m\},\\
&\vdots\\
\overline{m-1} &= \{x \in \mathbb{Z};\ x \equiv m-1 \bmod m\}.
\end{aligned}$$

Sendo todos os possíveis restos da divisão por m os números $0, 1, 2, \cdots, m-1$, temos que a união dos conjuntos $\overline{0}, \overline{1}, \cdots, \overline{m-1}$ contém todos os inteiros e tais conjuntos são dois a dois disjuntos.

Acabamos de particionar o conjunto $\mathbb{Z}$ dos números inteiros em subconjuntos, onde cada um deles é formado por todos os números inteiros que possuem o mesmo resto quando divididos por m. Isso nos dá uma partição de $\mathbb{Z}$.

O conjunto de todas as classes residuais disjuntas módulo m será representado por

$$\mathbb{Z}_m = \{\overline{0}, \overline{1}, \cdots, \overline{m-1}\}.$$

Exemplo 3.2.1 *Seja $m = 2$. Então,*

$\overline{0} = \{x \in \mathbb{Z};\ x \equiv 0\ mod\ 2\} = \{x \in \mathbb{Z};\ x\ é\ par\ \}$ *e*

$\overline{1} = \{x \in \mathbb{Z};\ x \equiv 1\ mod\ 2\} = \{x \in \mathbb{Z};\ x\ é\ ímpar\ \}$.

Temos portanto que $\overline{a} = \overline{0}$ se, e somente se, a é par e $\overline{a} = \overline{1}$ se, e somente se, a é ímpar.

Exemplo 3.2.2 *Seja $m = 3$. Então,*

$\overline{0} = \{3x;\ x \in \mathbb{Z}\}$, $\overline{1} = \{3x+1;\ x \in \mathbb{Z}\}$ *e* $\overline{2} = \{3x+2;\ x \in \mathbb{Z}\}$.

Queremos definir agora duas operações no conjunto $\mathbb{Z}_m$: uma operação de adição $\oplus$ e uma operação de multiplicação $\odot$.

Sejam dados $\overline{a}, \overline{b} \in \mathbb{Z}_m$. Definimos então

$$\overline{a} \oplus \overline{b} = \overline{a+b}$$

e

$$\overline{a} \odot \overline{b} = \overline{a.b},$$

onde $+$ e $.$ denotam, respectivamente, a adição e a multiplicação em $\mathbb{Z}$.

Temos que tais operações estão bem definidas pois dados $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ tais que $\overline{a_1} = \overline{a_2}$ e $\overline{b_1} = \overline{b_2}$, então segue das Proposições 3.1.5 e 3.1.7 que $\overline{a_1} \oplus \overline{b_1} = \overline{a_2} \oplus \overline{b_2}$ e $\overline{a_1} \odot \overline{b_1} = \overline{a_2} \odot \overline{b_2}$.

Exemplo 3.2.3 ***Aritmética módulo*** 4

Em $\mathbb{Z}_4$, temos apenas as classes residuais $\overline{0}, \overline{1}, \overline{2}$ e $\overline{3}$. Observe as operações de adição e multiplicação em $\mathbb{Z}_4$ dadas pela Tabela 6*:*

$\oplus$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

$\odot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Tabela 6: Tabelas de adição e multiplicação de $\mathbb{Z}_4$

Note que diferentemente da aritmética dos números inteiros, surge um novo fenômeno: $\overline{2} \neq \overline{0}$ *e, no entanto,* $\overline{2} \odot \overline{2} = \overline{0}$.

Exemplo 3.2.4 ***Aritmética módulo*** 5

Em $\mathbb{Z}_5$*, temos as classes residuais* $\overline{0}, \overline{1}, \overline{2}, \overline{3}$ *e* $\overline{4}$*. Observe as operações de adição e multiplicação em* $\mathbb{Z}_5$ *dadas pela Tabela* 7*:*

$\oplus$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

$\odot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Tabela 7: Tabelas de adição e multiplicação de $\mathbb{Z}_5$

No que se segue para simplificar a notação usaremos os símbolos $+$ e $.$ para representar a adição $\oplus$ e a multiplicação $\odot$ em $\mathbb{Z}_m$, respectivamente.

3.3 INVERSOS MODULARES

Definição 3.3.1 *Diremos que* a *e* a' *são* ***inversos módulo*** m *se*

$$aa' \equiv 1 \ mod \ m.$$

Neste caso, também dizemos que a' *é o* ***inverso de*** a ***módulo*** m *e vice-versa. Ou ainda, usando os símbolos apresentados anteriormente, dizemos que um elemento* $\overline{a} \in \mathbb{Z}_m$ *é* ***invertível*** *(ou* ***inversível****), quando existir* $\overline{b} \in \mathbb{Z}_m$ *tal que* $\overline{a}.\overline{b} = 1$.

Exemplo 3.3.1 *A Tabela* 8 *representa a multiplicação em* $\mathbb{Z}_2$.

.	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$

Tabela 8: Tabela da multiplicação em $\mathbb{Z}_2$

Temos que todo elemento não nulo de $\mathbb{Z}_2$ é invertível pois neste caso, temos apenas o elemento $\overline{1}$ não nulo e ele é o inverso dele mesmo.

A Tabela 9 *representa a multiplicação em $\mathbb{Z}_3$.*

.	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

Tabela 9: Tabela da multiplicação em $\mathbb{Z}_3$

Todo elemento não nulo de $\mathbb{Z}_3$ é invertível pois $\overline{1}.\overline{1} = \overline{1}$ e $\overline{2}.\overline{2} = \overline{1}$.

Observe na Tabela 6 *que os únicos elementos invertíveis de $\mathbb{Z}_4$ são $\overline{1}$ e $\overline{3}$. Já pela Tabela* 7*, vemos que em $\mathbb{Z}_5$ ocorre o mesmo que em $\mathbb{Z}_2$ e $\mathbb{Z}_3$, ou seja, todo elemento distinto de $\overline{0}$ é invertível.*

Vamos analisar o que ocorre em $\mathbb{Z}_6$ através da Tabela 10*.*

.	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Tabela 10: Tabela da multiplicação em $\mathbb{Z}_6$

Os únicos elementos não nulos de $\mathbb{Z}_6$ que são invertíveis são o $\overline{1}$ e o $\overline{5}$.

Vimos no Exemplo 3.3.3 que em $\mathbb{Z}_2$, $\mathbb{Z}_3$ e $\mathbb{Z}_5$ todo elemento não nulo é invertível e que $\mathbb{Z}_4$ e $\mathbb{Z}_6$ não seguem esta regra. Isto ocorre pois $2, 3$ e 5 são números primos, ao passo que 4 e 6 são números compostos. Essa observação vem da seguinte proposição:

Proposição 3.3.1 *Um elemento $\overline{a} \in \mathbb{Z}_m$ é invertível se, e somente se, $mdc(a, m) = 1$.*

Demonstração: Se $\overline{a}$ é invertível, então existe $\overline{b} \in \mathbb{Z}_m$ tal que $\overline{1} = \overline{a}.\overline{b} = \overline{a.b}$. Logo, $a.b \equiv 1 \bmod m$, isto é, existe um inteiro t tal que $a.b + t.m = 1$ e, consequentemente, $mdc(a, m) = 1$ pela Proposição 2.3.1. Reciprocamente, se $mdc(a, m) = 1$, existem inteiros b e t tais que $a.b + m.t = 1$ e, consequentemente, $\overline{1} = \overline{a.b + m.t} = \overline{a}.\overline{b} + \overline{0} = \overline{a}.\overline{b}$. Portando, $\overline{a}$ é invertível. ∎

Exemplo 3.3.2 *Em* $\mathbb{Z}_{12} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{9}, \overline{10}, \overline{11}\}$ *os elementos inversíveis são* $\{\overline{1}, \overline{5}, \overline{7}, \overline{11}\}$.

Observação 3.3.1 *Notemos que* $\overline{3}$ *é inversível em* $\mathbb{Z}_4$, *em* $\mathbb{Z}_5$ *e em* $\mathbb{Z}_7$. *O inverso de* $\overline{3}$ *em* $\mathbb{Z}_4$ *é* $\overline{3}$, *em* $\mathbb{Z}_5$ *é* $\overline{2}$ *e em* $\mathbb{Z}_7$ *é* $\overline{5}$. *Isso mostra que para diferentes valores de* m, *os inversos de* $\overline{3}$ *em* $\mathbb{Z}_m$ *são diferentes. Esta observação é bem importante para entendermos o sistema de criptografia RSA.*

Proposição 3.3.2 *Suponhamos que* a *tem inverso módulo* m. *Se* $ab \equiv ac \ mod \ m$, *para* $b, c \in \mathbb{Z}$, *então* $b \equiv c \ mod \ m$.

Demonstração: Seja a' o inverso de a módulo m. Multiplicando a congruência $ab \equiv ac \bmod m$ por a', obtemos

$$(a'a).b \equiv (a'a)c \bmod m, \text{ ou seja, } a'a(b - c) = km \text{ para algum } k \in \mathbb{Z}.$$

Como $a'a \equiv 1 \bmod m$ então $a'a = 1 + \tilde{k}m$ para algum $\tilde{k} \in \mathbb{Z}$. Daí $(1 + \tilde{k}m)(b - c) = km$, o que implica $m \mid b - c$. Logo, $b \equiv c \bmod m$, mostrando que o cancelamento pode ser feito neste caso. ∎

Foi visto na Proposição 3.3.1 como verificar quando um elemento é invertível, mas não mostramos como calcular o inverso modular de um número sem construir a tabela da multiplicação das classes residuais, ou seja, sem ficar testando até encontrar o inverso modular. Esse processo pode ser bastante demorado e cansativo como veremos no exemplo que se segue.

Exemplo 3.3.3 *Qual o inverso de* 14 *módulo* 45*? Sabemos que ele existe, pois* $mdc(14, 45) = 1$. *Podemos ficar tentando até encontrar um número inteiro* x *tal que* $14x \equiv 1 \ mod \ 45$. *Comecemos as contas:*

$$x = 1 \longrightarrow 14.1 \equiv 14 \ mod \ 45,$$
$$x = 2 \longrightarrow 14.2 \equiv 28 \ mod \ 45,$$
$$x = 3 \longrightarrow 14.3 \equiv 42 \ mod \ 45,$$
$$x = 4 \longrightarrow 14.4 \equiv 56 \equiv 11 \ mod \ 45,$$
$$x = 5 \longrightarrow 14.5 \equiv 70 \equiv 25 \ mod \ 45,$$
$$x = 6 \longrightarrow 14.6 \equiv 84 \equiv 39 \ mod \ 45 \ e$$
$$x = 7 \longrightarrow 14.7 \equiv 98 \equiv 8 \ mod \ 45.$$

Se continuarmos, só encontraremos o inverso de 14 *módulo* 45 *para* $x = 29$*, isto é,* $14.29 \equiv 406 \equiv 1 \ mod\ 45$.

Como vimos no Exemplo 3.3.3, o processo de encontrar o inverso pode ser demorado. Vamos então estudar um outro método para resolver uma **congruência linear** $ax \equiv b \bmod m$ onde x é uma incógnita. Essa congruência pode ser representada através da equação

$$ax + my = b,$$

para $x, y \in \mathbb{Z}$. Tais equações são chamadas **equações diofantinas lineares** em homenagem ao matemático grego Diofanto de Alexandria (aprox. 300 d.C.).

Então, resolver a congruência $ax \equiv b \bmod m$ é equivalente a encontrar um par de inteiros x e y que satisfaçam a equação diofantina $ax + my = b$.

Teorema 3.3.1 *Sejam* a*,* b *e* c *inteiros e* $d = mdc(a, b)$*. Se* d *não divide* c*, então a equação* $ax + by = c$ *não possui solução inteira. Se* d *divide* c*, então ela possui infinitas soluções e se* $x = x_0$ *e* $y = y_0$ *é uma solução particular, então todas as soluções são dadas por*

$$x = x_0 + (b/d)k \ e$$
$$y = y_0 - (a/d)k$$

para $k \in \mathbb{Z}$.

Demonstração: Se $d \nmid c$, então a equação $ax + by = c$, não possui solução pois, como $d \mid a$ e $d \mid b$, d deveria dividir c, o qual é uma combinação de a e b. Suponhamos que $d \mid c$. Pelo Teorema 2.3.2, existem inteiros n_0 e m_0, tais que

$$an_0 + bm_0 = d. \tag{1}$$

Como $d \mid c$, existe um inteiro k tal que $c = kd$. Se multiplicarmos, ambos os membros de (1) por k, teremos $a(n_0k) + b(m_0k) = kd = c$. Isto nos diz que o par (x_0, y_0) com $x_0 = n_0k$ e $y_0 = m_0k$ é uma solução de $ax + by = c$. É fácil a verificação de que os pares da forma

$$x = x_0 + (b/d)k \text{ e}$$
$$y = y_0 - (a/d)k$$

são soluções, uma vez que

$$\begin{aligned} ax + by &= a(x_0 + (b/d)k) + b(y_0 - (a/d)k) \\ &= ax_0 + \frac{ab}{d}k + by_0 - \frac{ab}{d}k \\ &= ax_0 + by_0 = c. \end{aligned}$$

O que acabamos de mostrar é que, conhecida uma solução particular (x_0, y_0) de $ax + by = c$ podemos, a partir dela, gerar infinitas soluções. Precisamos, agora, mostrar que toda solução da equação $ax + by = c$ é da forma $x = x_0 + (b/d)k$ e $y = y_0 - (a/d)k$. Vamos supor que (x, y) seja uma solução, isto é, $ax + by = c$. Mas, como $ax_0 + by_0 = c$, obtemos, subtraindo membro a membro, que

$$ax + by - ax_0 - by_0 = a(x - x_0) + b(y - y_0) = 0,$$

o que implica $a(x - x_0) = b(y_0 - y)$. Como $d = mdc(a, b)$ temos, pelo Corolário 2.3.2 que

$$mdc\left(\frac{a}{d}, \frac{b}{d}\right) = 1.$$

Portanto, dividindo os dois membros da igualdade $a(x - x_0) = b(y_0 - y)$ por d, teremos

$$\frac{a}{d}(x - x_0) = \frac{b}{d}(y_0 - y). \tag{2}$$

Logo, pela Proposição 2.3.4, $(b/d) \mid (x - x_0)$ e portanto existe um inteiro k satisfazendo $x - x_0 = k(b/d)$, ou seja, $x = x_0 + (b/d)k$. Substituindo este valor de x na Equação (2) temos $y = y_0 - (a/d)k$, o que conclui a demonstração. ∎

Exemplo 3.3.4 *Retomando a congruência* $14x \equiv 1$ *mod* 45 *do Exemplo 3.3.3, podemos reescrevê-la como uma equação diofantina linear*

$$14x - 45y = 1,$$

com x *e* y *inteiros.*

Como $mdc(14, 45) = 1$ *que divide* 1*, então a equação possui solução. Vamos primeiramente encontrar* n_0 *e* m_0 *inteiros tais que* $14n_0 + 45m_0 = 1$*. Em seguida, vamos encontrar uma solução particular* (x_0, y_0)*. Temos que:*

$45 = 3 \times 14 + 3$,
$14 = 4 \times 3 + 2$ *e*
$3 = 1 \times 2 + 1$.

Substituindo as equações acima umas nas outras, obtemos

$$14.(-16) - 45.(-5) = 1.$$

Logo, $n_0 = -16$ *e* $m_0 = -5$ *e* $x_0 = -16$ *e* $y_0 = -5$ *é solução particular da equação diofantina* $14x - 45y = 1$*. Consequentemente, as soluções da equação são*

$$x = -16 - 45k \text{ e}$$
$$y = -5 - 14k$$

com $k \in \mathbb{Z}$*.*

Para que possamos obter uma solução inteira positiva para a congruência $14x \equiv 1$ *mod* 45*, basta tomarmos* $k = -1$ *e obtemos* $x = 29$*. Portanto, o inverso modular de* 14 *módulo* 45 *é* 29*.*

3.4 TEOREMAS DE FERMAT E DE EULER

Nesta seção serão apresentados dois teoremas de muita relevância e suas respectivas demonstrações.

3.4.1 *Teorema de Fermat*

Exemplo 3.4.1 *[1] Com tudo que vimos sobre congruências, vamos tentar descobrir o resto da divisão do número* 3^{64} *por* 31*. Calculando os restos das potências de* 3 *encontramos*

$$3^3 \equiv 27 \equiv -4 \ mod\ 31.$$

Mas $4 = 2^2$*, de modo que*

$$3^3 \equiv -2^2 \ mod\ 31.$$

A vantagem de trabalhar com 2 *é que* $2^5 \equiv 32 \equiv 1$ *mod* 31*. Agora, dividindo* 64 *por* 3 *obtemos* $64 = 21.3 + 1$ *e daí*

$$3^{64} \equiv (3^3)^{21}3 \equiv -(2)^{42}3 \ mod\ 31.$$

Como $42 = 8.5 + 2$*, temos que:*

$$2^{42} \equiv (2^5)^8 2^2 \equiv 4 \ mod\ 31.$$

Assim,

$$3^{64} \equiv -(2)^{42}3 \equiv -4.3 \equiv -12 \ mod\ 31.$$

Como $-12 \equiv 19$ *mod* 31*, o resto da divisão de* 3^{64} *por* 31 *é* 19*.*

O problema que acabamos de resolver pode ser facilmente solucionado se conhecermos o famoso *Teorema de Fermat* cuja demonstração aqui apresentada foi descoberta pelo matemático suíço Leonard Euler no século XVIII [1].

Teorema 3.4.1 *(Teorema de Fermat) Se* p *é um número primo e* a *é um inteiro que não é divisível por* p*, então*

$$a^{p-1} \equiv 1 \ mod\ p.$$

Demonstração: Um sistema completo de resíduos módulo p é $\{0, 1, \cdots, p-1\}$. Consideremos apenas os resíduos não nulos multiplicados por a, isto é,

$$a.1, a.2, a.3, \cdots, a.(p-1).$$

Sejam

$$\begin{gathered} r_1 \equiv a.1 \bmod p, \\ r_2 \equiv a.2 \bmod p, \\ \cdots \\ r_{p-1} \equiv a.(p-1) \bmod p, \end{gathered}$$

com $0 \leq r_i < p$ para todo $i = 1, \cdots, p-1$.

Multiplicando os r_i's obtemos:

$$r_1.r_2.\cdots.r_{p-1} \equiv (a.1).(a.2)\cdots(a.(p-1)) \bmod p$$

Contudo,

$$(a.1).(a.2).(a.3)\cdots(a.(p-1)) = a^{p-1}.(1.2.3\cdots(p-1)).$$

Desta forma,

$$r_1.r_2.\cdots.r_{p-1} \equiv a^{p-1}.(1.2.3\cdots(p-1)) \bmod p. \tag{3}$$

Agora, notemos que não pode haver dois elementos congruentes módulo p no conjunto $\{r_1, r_2, \cdots, r_{p-1}\}$. Para provar isto, suponhamos que $r_k \equiv r_l \bmod p$ para dois inteiros k e l, com $1 \leq k, l \leq p-1$. Daí, teríamos que

$$a.k \equiv r_k \equiv r_l \equiv a.l \bmod p,$$

isto é,

$$a.k \equiv a.l \bmod p.$$

Entretanto, como p não divide a e p é primo, então $mdc(a,p) = 1$. Mas isto implica que a é inversível módulo p de forma que, pela Proposição 3.3.2, podemos cancelá-lo na congruência acima, obtendo

$$k \equiv l \bmod p.$$

Mas, k e l são inteiros positivos menores que p e só podem ser congruentes se forem iguais. Logo,

$$\text{se } r_k \equiv r_l \bmod p, \text{ então } k = l.$$

Isto nos mostra que os resíduos $\{r_1, \cdots, r_{p-1}\}$ são não nulos (pois p não divide a) e dois a dois não congruentes. Acontece que só há $p-1$ resíduos não nulos diferentes módulo p no sistema completo de resíduos $\{0, 1, 2, \cdots, p-1\}$. Isso nos permite deduzir que a sequência de classes residuais $\overline{r_1}, \overline{r_2}, \cdots, \overline{r_{p-1}}$ é apenas um embaralhamento de $\overline{1}, \overline{2}, \overline{3}, \cdots, \overline{p-1}$.

Em particular,

$$\overline{r_1}.\overline{r_2}.\overline{r_3}\cdots\overline{r_{p-1}} = \overline{1}.\overline{2}.\overline{3}\cdots\overline{(p-1)}. \tag{4}$$

Concluindo, temos que por (3),

$$r_1.r_2...r_{p-1} \equiv a^{p-1}.(1.2.3...(p-1)) \bmod p.$$

e por (4)

$$r_1.r_2.r_3...r_{p-1} \equiv 1.2.3...(p-1) \bmod p.$$

Portanto,

$$a^{p-1}.(1.2.3...(p-1)) \equiv 1.2.3...(p-1) \bmod p.$$

Agora, notemos que $1.2.3...(p-1)$ é o produto de elementos inversíveis módulo p. Logo é, ele próprio, um elemento inversível módulo p. Com isto podemos cancelá-lo dos dois lados da congruência, o que nos dá

$$a^{p-1} \equiv 1 \bmod p,$$

que é o que precisávamos demonstrar. ■

Voltando ao problema de achar o resto da divisão de 3^{64} por 31, vamos resolvê-lo utilizando o Teorema de Fermat no exemplo seguinte.

Exemplo 3.4.2 *Primeiro observamos que* 31 *é um número primo e que* $mdc(3, 31) = 1$ *e então aplicamos o Teorema de Fermat. Assim,*

$$3^{30} \equiv 1 \ mod\ 31.$$

Como $64 = 2.30 + 4$, *temos*

$$3^{64} \equiv (3^{30})^2.3^4 \equiv 1.81 \equiv 19 \ mod\ 31,$$

confirmando o resultado dos cálculos anteriores de uma maneira bem mais simples.

3.4.2 *Teorema de Euler*

Para enunciarmos o Teorema de Euler é necessário apresentarmos alguns resultados preliminares. Além disso estes resultados serão de grande importância no RSA.

Definição 3.4.1 *Se* m *é um inteiro positivo, a* **função** ϕ **de Euler**, *denotada por* $\phi(m)$, *é definida como sendo o número de inteiros positivos menores do que ou iguais a* m *que são relativamente primos com* m.

Definimos a *função fi de Euler* então como $\phi : \mathbb{N} \to \mathbb{N}$ tal que $\phi(m) = \#\{a \in \mathbb{N},\ a < m;\ mdc(a, m) = 1\}$. Pela definição, temos que $\phi(m) \leq m - 1$, para todo $m \geq 2$.

Proposição 3.4.1 *Se* p *é um número primo, então* $\phi(p) = p - 1$.

Demonstração: De fato, neste caso todos os inteiros positivos menores que m são coprimos com m. ■

Proposição 3.4.2 *Se* p *e* q *são primos distintos, então* $\phi(pq) = (p - 1)(q - 1)$.

Demonstração: Temos que $\phi(pq)$ é quantidade de inteiros positivos menores ou iguais a pq que são coprimos com pq. Para que um inteiro não seja coprimo com pq ele deve ser múltiplo de p ou múltiplo de q pois os únicos divisores de pq maiores do que 1 são p e q. A quantidade de múltiplos de p menores ou iguais a pq é $\frac{pq}{p} = q$ e a quantidade de múltiplos de q menores ou iguais a pq é $\frac{pq}{q} = p$. Entre os múltiplos de p e os múltiplos de q menores ou iguais a pq o único elemento em comum é o pq. Desta forma, temos que $\phi(pq)$ é igual ao total de inteiros positivos menores que pq menos a quantidade de múltiplos de p somados ao múltiplos de q mais a quantidade da intersecção dos múltiplos de p e q, isto é,

$$\phi(pq) = pq - (p + q) + 1 = (p - 1)(q - 1).$$

■

Definição 3.4.2 *Um* **sistema reduzido de resíduos módulo** m *é um conjunto de* $\phi(m)$ *inteiros* $r_1, r_2, ..., r_{\phi(m)}$*, tais que:*

1. *cada elemento do conjunto é relativamente primo com* m*;*

2. *se* $i \neq j$*, então* $r_i \neq r_j \ mod\ m$*.*

Exemplo 3.4.3 *O conjunto* $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$ *é um sistema completo de resíduos módulo* 12*. Já* $\{1, 5, 7, 11\}$ *é um sistema reduzido de resíduos módulo* 12*.*

A fim de se obter um sistema reduzido de resíduos módulo m, basta retirar os elementos do sistema completo que não são relativamente primos com m.

Proposição 3.4.3 *Seja* a *um inteiro positivo tal que* $mdc(a, m) = 1$*. Se* $r_1, r_2, \cdots, r_{\phi(m)}$ *é um sistema reduzido de resíduos módulo* m*, então* $a.r_1, a.r_2, \cdots, a.r_{\phi(m)}$ *é, também, um sistema reduzido de resíduos módulo* m*.*

Demonstração: Como na sequência $a.r_1, a.r_2, \cdots, a.r_{\phi(m)}$ temos $\phi(m)$ elementos, devemos mostrar que todos eles são relativamente primos com m e dois a dois não congruentes módulo m.

Primeiramente, como $mdc(a, m) = 1$ e $mdc(r_i, m) = 1$, pela Proposição 2.3.1, existem x_1, x_2, y_1 e y_2 inteiros, tais que

$$x_1 a + y_1 m = 1 \text{ e } x_2 r_i + y_2 m = 1.$$

Agora,

$$x_1 a + y_1 m = 1 \Leftrightarrow x_1 a(x_2 r_i + y_2 m) + y_1 m = 1$$
$$\Leftrightarrow x_1 x_2 a r_i + x_1 y_2 a m + y_1 m = 1 \Leftrightarrow x_1 x_2 a r_i + m(x_1 y_2 a + y_1) = 1.$$

Logo, existem $x_3 = x_1 x_2$ e $y_3 = x_1 y_2 a + y_1$ inteiros tais que

$$x_3 a r_i + y_3 m = 1,$$

concluindo assim que $mdc(ar_i, m) = 1$, ou seja, na sequência $a.r_1, a.r_2, \cdots, a.r_i$ todos os elementos são relativamente primos com m.

Nos resta mostrar que $a.r_i \not\equiv a.r_j \mod m$ se $i \neq j$. Como $mdc(a, m) = 1$, se $a.r_i \equiv a.r_j \mod m$ teríamos que $r_i \equiv r_j \mod m$, o que implicaria $i = j$, uma vez que $r_1, , r_2, ..., r_{\phi(m)}$ é um sistema reduzido de resíduos módulo m. ■

Exemplo 3.4.4 *Sejam* $m = 10$ *e* $a = 3$. *Temos que o conjunto* $\{1, 3, 7, 9\}$ *é um sistema reduzido de resíduos módulo* 10. *Consideremos o conjunto formado por* $\{3.1, 3.3, 3.7, 3.9\}$. *Pelo Proposição 3.4.3 este conjunto também constitui um sistema reduzido de resíduos módulo* 10. *Isto significa que cada um dos elementos* $\{3.1, 3.3, 3.7, 3.9\}$ *é congruente módulo* 10 *a exatamente um dos elementos* $1, 3, 7$ *e* 9. *Temos, na realidade que*

$$3.1 \equiv 3 \equiv 3 \ mod\ 10,$$
$$3.3 \equiv 9 \equiv 9 \ mod\ 10,$$
$$3.7 \equiv 21 \equiv 1 \ mod\ 10 \ e$$
$$3.9 \equiv 27 \equiv 7 \ mod\ 10.$$

Multiplicando, membro a membro, estas congruências obtemos

$$3^4(1.3.7.9) \equiv (1.3.7.9) \ mod\ 10.$$

Como $mdc(1.3.7.9, 10) = 1$ *podemos cancelar o fator* $(1.3.7.9)$ *obtendo*

$$3^4 \equiv 1 \ (mod\ 10).$$

Observe que $4 = \phi(10)$, *ou seja, provamos que* $3^{\phi(10)} \equiv 1 \ mod\ 10$.

Teorema 3.4.2 *(Teorema de Euler) Se* m *é um inteiro positivo e* a *um inteiro com* $mdc(a, m) = 1$, *então*

$$a^{\phi(m)} \equiv 1 \ mod\ m.$$

Demonstração: Na Proposição 3.4.3 mostramos que os elementos $a.r_1, a.r_2, \cdots, a.r_{\phi(m)}$ constituem um sistema reduzido de resíduos módulo m se $mdc(a, m) = 1$ e $r_1, r_2, ..., r_{\phi(m)}$ for um sistema reduzido de resíduos módulo m. Isto significa que $a.r_i$ é congruente a exatamente um dos r_j, $1 \leq j \leq \phi(m)$, e portanto o produto dos $a.r_i$ deve ser congruente ao produto dos r_j módulo m, isto é,

$$(a.r_1).(a.r_2) \cdots (a.r_{\phi(m)}) \equiv r_1.r_2 \cdots r_{\phi(m)} \bmod m,$$

ou seja,

$$a^{\phi(m)} r_1.r_2 \cdots r_{\phi(m)} \equiv r_1.r_2 \cdots r_{\phi(m)} \bmod m.$$

Como $mdc(r_1.r_2...r_{\phi(m)}, m) = 1$, podemos cancelar o produto $r_1.r_2...r_{\phi(m)}$ em ambos os lados para obter $a^{\phi(m)} \equiv 1 \bmod m$. ■

Como para p primo $\phi(p) = p - 1$, o Teorema de Euler é uma generalização do Teorema de Fermat que diz que $a^{p-1} \equiv 1 \bmod p$ quando $mdc(a, p) = 1$.

3.5 CRITÉRIOS DE DIVISIBILIDADE

Vamos estabelecer alguns critérios de divisibilidade por números primos utilizando o que aprendemos sobre congruências.

Se n for um inteiro positivo, então um critério de divisibilidade por n é uma regra que nos permite determinar se um dado inteiro é, ou não divisível por n, a um custo menor que o de efetuar a divisão [1].

Para obtermos esses critérios de divisibilidade devemos primeiro entender a expansão de um número inteiro no sistema decimal.

Seja dado um número n escrito no sistema decimal. Sua expansão decimal será:

$$n = n_r \cdots n_2 n_1 n_0 = n_r 10^r + \cdots + n_2 10^2 + n_1 10^1 + n_0,$$

onde
n_0 é o algarismo das unidades de n,
n_1 é o algarismo das dezenas de n,
n_2 é o algarismo das centenas de n,
e assim por diante até chegar no algarismo n_r.

Exemplo 3.5.1 *O número* 8759 *é representado como*

$$8759 = 8.10^3 + 7.10^2 + 5.10 + 9.$$

Divisibilidade por 2

O critério de divisibilidade por 2 é um dos mais conhecidos, pois dado um inteiro qualquer basta verificarmos se o algarismo da unidade é $0, 2, 4, 6$ ou 8, que o mesmo será divisível por 2, ou seja, verificamos se o algarismo da unidade é *par*. Temos então nosso primeiro critério de divisibilidade:

Proposição 3.5.1 *Um número inteiro é divisível por* 2 *se, e somente se, seu algarismo da unidade é* $0, 2, 4, 6$ *ou* 8.

Demonstração: Usaremos a congruência módulo 2 para provar este critério. Seja a o número inteiro que queremos descobrir se é ou não divisível por 2. Podemos representar o número a em sua expansão decimal como:

$$a = a_n \cdots a_1 a_0 = a_n.10^n + \cdots + a_1.10 + a_0.$$

Temos que, $10 \equiv 0 \bmod 2$. Também, $10^2 = 10.10 \equiv 0.0 \equiv 0 \bmod 2$ pela Proposição 3.1.7 e pela mesma proposição $10^3 = 10.10^2 \equiv 0 \bmod 2$. Continuando este raciocínio, este procedimento nos permite concluir que $10^k \equiv 0 \bmod 2$ qualquer que seja o inteiro $k > 0$ escolhido.

Assim, $a_k 10^k \equiv a_k 0 \equiv 0 \bmod 2$ para todo inteiro $k > 0$ e então

$$a = a_n.10^n + \cdots + a_1.10 + a_0 \equiv a_0 \bmod 2.$$

Portanto, para saber se a é divisível por 2 basta analisar o algarismo das unidades deste número. Como a_0 é um número entre 0 e 9, para que tenhamos $a \equiv 0 \bmod 2$, a_0 poderá assumir apenas os valores $0, 2, 4, 6$ ou 8. ■

Divisibilidade por 3

Um outro critério bastante conhecido é o de divisibilidade por 3:

Proposição 3.5.2 *Um número inteiro é divisível por* 3 *se, e somente se, a soma de seus algarismos é divisível por* 3*.*

Demonstração: Usaremos a congruência módulo 3 para provar este critério. Vamos representar o inteiro a em sua expansão decimal assim como fizemos na divisibilidade por 2, isto é:

$$a = a_n \cdots a_1 a_0 = a_n.10^n + \cdots + a_1.10 + a_0.$$

Temos que $10 \equiv 1 \bmod 3$. Também, $10^2 \equiv 10.10 \equiv 1.1 \equiv 1 \bmod 3$ e $10^3 \equiv 10^2.10 \equiv 1.1 \equiv 1 \bmod 3$. Acabamos de aplicar as propriedades da multiplicação de congruências vistas na Seção 3.1.2. Continuando este raciocínio, este procedimento nos permite concluir que $10^k \equiv 1 \bmod 3$ qualquer que seja o inteiro $k > 0$ escolhido.

Assim, $a_k 10^k \equiv a_k 1 \equiv a_k \bmod 3$ para todo inteiro $k > 0$ e então

$$a \equiv a_n.10^n + \cdots + a_1.10 + a_0 \equiv a_n + \cdots + a_1 + a_0 \bmod 3,$$

que é exatamente o que precisamos para podermos concluir o critério de divisibilidade por 3. De fato, dizer que a é divisível por 3 é o mesmo que dizer que $a \equiv 0 \bmod 3$. Como

$$a \equiv a_n + \cdots + a_1 + a_0 \bmod 3$$

a transitividade nos garante que $a \equiv 0 \bmod 3$ ocorre exatamente quando

$$a_n + \cdots + a_1 + a_0 \equiv 0 \bmod 3$$

que, por sua vez, equivale a dizer

$$a_n + \cdots + a_1 + a_0 \text{ é divisível por } 3.$$

Mas,

$$a_n + \cdots + a_1 + a_0$$

é a soma dos algarismos de a. Portanto, a é divisível por 3 se, e somente se, a soma $a_n + \cdots + a_1 + a_0$ dos seus algarismos for divisível por 3. ■

Divisibilidade por 5

O critério de divisibilidade por 5 é percebido quando observamos os múltiplos de 5, que são todos os números terminados em 0 ou 5, ou seja, basta verificarmos o algarismo das unidades para sabermos se um número é ou não divisível por 5. Este critério se assemelha com o critério de divisibilidade por 2:

Proposição 3.5.3 *Um número inteiro é divisível por* 5 *se, e somente se, seu algarismo da unidade é* 5 *ou* 0*.*

Demonstração: Para provar este critério é necessário os mesmos argumentos e propriedades já apresentadas na divisibilidade por 2, mas com congruências módulo 5.

Seguindo os mesmos passos, chegaremos na seguinte conclusão:

$$a \equiv a_n.10^n + \cdots + a_1.10 + a_0 \equiv a_0 \bmod 5,$$

pois $10 \equiv 0 \bmod 5$ e $a_n.10^k \equiv 0 \bmod 5$ para todo $k > 0$.

Portanto, para saber se a é divisível por 5 basta analisar o algarismo das unidades deste número. Como a_0 é um número entre 0 e 9, para que tenhamos $a \equiv 0 \bmod 5$, a_0 poderá assumir apenas os valores 0 ou 5. ■

Divisibilidade por 7 [1]

O critério de divisibilidade por 7 não é tão conhecido como os critérios anteriores (por $2, 3$ e 5). Primeiro vamos analisar o que foi feito nos casos anteriores para o caso 7. Vamos começar expressando um inteiro a como

$$a = a_n.10^n + \cdots + a_1.10 + a_0.$$

Aplicando a mesma estratégia já usada nos critérios anteriores, temos as seguintes congruências módulo 7:

$10 \equiv 3 \bmod 7$,
$10^2 \equiv 3^2 \equiv 2 \bmod 7$,
$10^3 \equiv 10.10^2 \equiv 3.2 \equiv 6 \bmod 7$,
$10^4 \equiv 10.10^3 \equiv 3.(-1) \equiv -3 \equiv 4 \bmod 7$,
$10^5 \equiv 10.10^4 \equiv 3.4 \equiv 12 \equiv 5 \bmod 7$ e
$10^6 \equiv 10.10^5 \equiv 3.5 \equiv 15 \equiv 1 \bmod 7$

Para efetuar estes cálculos usamos as propriedades da congruência que já conhecemos. Paramos na sexta potência simplesmente porque, daí em diante os restos vão se repetir. De fato,

$10^7 \equiv 10.10^6 \equiv 3.1 \equiv 3 \bmod 7$,
$10^8 \equiv 10.10^7 \equiv 3.3 \equiv 9 \equiv 2 \bmod 7$,
$10^9 \equiv 10.10^8 \equiv 3.6 \equiv 6 \bmod 7$

e assim por diante. Mais precisamente, se m é um inteiro qualquer e q e r são seu quociente e seu resto na divisão por 6, então

$$10^m = 10^{6q+r} = (10^6)^q.10^r \bmod 7.$$

Como $10^6 \equiv 1 \bmod 7$, concluímos que

$$10^m = (10^6)^q.10^r \equiv 10^r \bmod 7.$$

Mas isto é ótimo porque, sendo um resto da divisão por 6, r satisfaz a desigualdade $0 \leq r \leq 5$, de modo que 10^r pode ser facilmente determinado das potências módulo 7 calculadas acima para $0 \leq r \leq 5$.

Fazendo isto, e escrevendo as potências da maior para a menor, temos

$$a \equiv a_0 + a_1.3 + a_2.2 + a_3.6 + a_4.4 + a_5.5 + a_6 + a_7.3 + \cdots + a_n.10^r \bmod 7,$$

onde r é o resto da divisão de n por 6. Infelizmente, este procedimento não é mais simples que efetuar a divisão do número por 7 e verificar se o resto é 0 ou não, o que torna este método inviável. Mas, há outra maneira de enunciar o critério de divisibilidade por 7. Porém, precisamos de uma preparação.

Isolando o algarismo das unidades de a e colocando o 10 em evidência na expansão da base 10, podemos escrever

$$a = (a_n.10^{n-1} + \cdots + a_1).10 + a_0.$$

e fazendo $\hat{a} = (a_n.10^{n-1} + \cdots + a_1)$, escrevemos

$$a = \hat{a}.10 + a_0.$$

Exemplo 3.5.2 *Por exemplo, digamos que* $a = 124567$ *que tem como algarismo da unidade* $a_0 = 7$*. Assim,* $a = 12456.10 + 7$*, de modo que, neste caso,* $\hat{a} = 12456$*.*

Uma vez que tenhamos escrito a na forma $a = \hat{a}.10 + a_0$ aplicamos a congruência módulo 7. Como $10 \equiv 3 \bmod 7$, temos que

$$a = \hat{a}.10 + a_0 \equiv 3.\hat{a} + a_0 \bmod 7$$

isto é, a é divisível por 7 se, e somente se, $3.\hat{a} + a_0$ também for.

Exemplo 3.5.3 *Por exemplo, digamos que desejamos saber se* 128 *é divisível por* 7*. Se* $a = 128$*, então* $a_0 = 8$ *e* $\hat{a} = 12$*. Temos que*

$$3.\hat{a} + a_0 = 3.12 + 8 = 44.$$

Como 44 *não é divisível por* 7*, o critério acima nos garante que* 128 *também não pode ser.*

Podemos reformular este critério afim de deixá-lo mais simples e com o seguinte enunciado:

Proposição 3.5.4 *Um número inteiro* a *é divisível por* 7 *se, e somente se,* 7 *divide* $-\hat{a} + 2.a_0$*, onde* $\hat{a} = (a_n.10^{n-1} + \cdots + a_1)$*.*

Demonstração: Para provarmos este critério, começamos multiplicando a congruência $a \equiv 3.\hat{a} + a_0 \bmod 7$ por 2, o que nos dá

$$2.a \equiv 2(3.\hat{a} + a_0) \equiv 6.\hat{a} + 2.a_0 \bmod 7.$$

Mas, como $6 \equiv -1 \bmod 7$, temos

$$2.a \equiv -\hat{a} + 2.a_0 \bmod 7.$$

Se 7 divide a, ou seja, se $a \equiv 0 \bmod 7$, então

$$-\hat{a} + 2.a_0 \equiv 0 \bmod 7$$

pela transitividade da congruência, ou seja, se 7 divide $-\hat{a} + 2.a_0$.

Agora, se 7 divide $-\hat{a} + 2.a_0$, ou seja, se $-\hat{a} + 2.a_0 \equiv 0 \bmod 7$, então $a \equiv 0 \bmod 7$. De fato, para mostrar isso precisamos desfazer o que fizemos quando multiplicamos a equação por 2. Como $2.3 \equiv -1 \bmod 7$, devemos multiplicar ambos os lados da equação $-\hat{a} + 2.a_0 \equiv 0 \bmod 7$ por 3. Vejamos:

$$3.(-\hat{a} + 2.a_0) \equiv 3.0 \bmod 7 \iff -3.\hat{a} + 6.a_0 \equiv 0 \bmod 7.$$

Como $6 \equiv -1 \bmod 7$, então

$$-3.\hat{a} - a_0 \equiv 0 \bmod 7.$$

Pondo -1 em evidência, ficamos com

$$-(3.\hat{a} + a_0) \equiv 0 \bmod 7.$$

Acontece que

$$3.\hat{a} + a_0 \equiv a \bmod 7$$

de modo que a equação $-(3.\hat{a} + a_0) \equiv 0 \bmod 7$ pode ser reescrita na forma

$$-a \equiv 0 \bmod 7,$$

que é o mesmo que dizer que 7 divide a. ■

Exemplo 3.5.4 *Digamos que queremos saber se $a = 10794$ é ou não é divisível por 7. Neste caso,*

$$a_0 = 4 \text{ e } \hat{a} = 1079.$$

Pelo critério estabelecido acima, basta descobrir se 7 divide ou não

$$-\hat{a} + 2.a_0 = -1079 + 2.4 = -1071.$$

Como isto ainda não é fácil de determinar, vamos usar o critério novamente, só que desta vez para $b = 1071$. Temos que $b_0 = 1$ e $\hat{b} = 107$. Assim,

$$-\hat{b} + 2.b_0 = -107 + 2.1 = -105.$$

Aplicando mais uma vez o critério para $c = 105$ temos que $c_0 = 5$ e $\hat{c} = 10$. Como

$$-\hat{c} + 2.c_0 = -10 + 2.5 = 0$$

é claramente divisível por 7*, então* 7 *divide* $c = 105$*. Mas isto implica, pelo critério, que* 7 *divide* $b = 1071$ *que, por sua vez, implica que* 7 *divide* $a = 10794$*, que é o que queríamos saber.*

Observe que no Exemplo 3.5.4 aplicamos a regra dada pelo critério a números sucessivamente menores, até obter um caso em que sabíamos a resposta sem fazer sequer uma conta. Temos, assim, uma regra *recursiva*, isto é, uma regra que reduz um dado problema a um problema análogo mas com dados menores [1].

Divisibilidade por 11

Proposição 3.5.5 *Um número inteiro é divisível por* 11 *se, e somente se, a soma dos algarismos de posição par subtraídos da soma dos algarismos de posição ímpar, resultar em um número divisível por* 11*.*

Demonstração: O critério de divisibilidade por 11 será provado assim como fizemos para o critério por 3. Utilizaremos a expansão decimal e a congruência módulo 11. Assim, dado o inteiro a queremos encontrar um critério que facilite descobrir se a é ou não divisível por 11.

Como $10 \equiv -1 \bmod 11$, aplicando as propriedades de congruência na expansão $a = a_n.10^n + \cdots + a_2.10^2 + a_1.10 + a_0$ temos que

$$a \equiv a_n.(-1)^n + \cdots + a_2.(-1)^2 + a_1.(-1) + a_0 \bmod 11,$$

isto é,

$$a \equiv a_n.(-1)^n + \cdots + a_2 - a_1 + a_0 \bmod 11.$$

Observe que os termos em posições pares ficaram com sinal positivo e os de posições ímpares com sinal negativo. Isso nada mais é que uma alternância dos sinais dos termos. Em outras palavras, o número a só é divisível por 11 se a soma alternada de seus termos também for divisível por 11. ■

4

CRIPTOGRAFIA

Neste capítulo falaremos sobre o funcionamento do sistema de criptografia RSA e apresentaremos o sistema livre PARI/GP. Para este capítulo utilizamos as referências [1, 2, 4, 5, 8].

4.1 SISTEMA DE CRIPTOGRAFIA RSA

O mais conhecido dos métodos de criptografia de chave pública é o RSA. Ele foi inventado em 1977 por R. L. Rivest, A. Shamir e L. Adleman, que na época trabalhavam no Massachussets Institute of Technology (M.I.T.). As letras RSA correspondem às iniciais dos inventores do método. Há vários outros sistemas de criptografia de chave pública, mas o RSA continua sendo o mais usado atualmente em aplicações comerciais [1].

O sistema de criptogragia RSA se baseia na relativa facilidade em encontrar números primos grandes e ao mesmo tempo na enorme dificuldade prática em fatorar um número natural grande como produto de dois primos. O sistema possui duas chaves, uma pública e outra privada, para que qualquer pessoa possa cifrar uma mensagem e somente o seu legítimo destinatário possa decifrá-la.

Grande parte das mensagens transmitidas são textos e para que seja aplicada a criptografia RSA é necessário a transformação dessas mensagens em sequências numéricas. Para isto é utilizado o código numérico ASCII que significa Código Padrão Americano para o Intercâmbio de Informação. Este código traduz todas as informações em códigos binários (código o qual os computadores "entendem").

Criaremos dois personagens fictícios para explicar o funcionamento do sistema de criptografia RSA: Alice e Bob.

Bob quer utilizar o sistema criptográfico em que qualquer pessoa possa lhe enviar uma mensagem cifrada segundo uma chave pública e que ele, e somente ele, possa decifrá-la com a sua chave secreta.

Criação das chaves pública e secreta

1º Passo: Bob deve escolher dois números primos distintos p e q muito grandes e efetuar o seu produto $m = pq$.

Observação 4.1.1 *Note que é fácil calcular o número m, mas, é extremamente difícil e computacionalmente muito demorado desfazer essa operação, ou seja, fatorar m. Esse é o ponto mais importante do sistema: uma operação fácil de fazer mas difícil de desfazer.*

Note também que Bob pode gerar infinitos $m's$, pois existem infinitos números primos como vimos no Teorema 2.4.2.

2º Passo: Bob calcula $\phi(m)$.

Observação 4.1.2 *Note que Bob sabe calcular $\phi(m)$ pois como p e q são primos distintos, então $\phi(m) = \phi(pq) = (p-1)(q-1)$.*

3º Passo: Bob escolhe um par de números a e b tais que $mdc(a, \phi(m)) = mdc(b, \phi(m)) = 1$ e

$$ab \equiv 1 \bmod \phi(m).$$

Observação 4.1.3 *Bob pode escolher inicialmente um a tal que $mdc(a, \phi(m)) = 1$ e em seguida resolver a congruência $ab \equiv 1$ mod $\phi(m)$ para encontrar b.*

4º Passo: Bob então torna público os números m e b, que são a sua chave pública. A chave secreta de Bob é constituída pelos primos p e q, o número $\phi(m)$ e a.

Codificando a mensagem

Alice ou qualquer outra pessoa que conheça a chave pública de Bob (m, b) pode cifrar uma mensagem.

5º Passo: Alice deve usar uma tabela de conversão a fim de transformar a mensagem de texto, se for o caso, em uma sequência numérica. A sequência numérica gerada x será particionada em blocos $x = x_1x_2 \cdots x_s$ de modo que cada número x_i dessa sequência seja menor que m.

6º Passo: Para cada x_i da sequência Alice deve fazer x_i^b e calcular o resíduo $C(x_i)$ de x_i^b módulo m tal que $0 \leq C(x_i) < m$, isto é,

$$x_i^b \equiv C(x_i) \bmod m,\ 0 \leq C(x_i) < m.$$

7º Passo: Alice envia $C(x) = C(x_1)C(x_2)\cdots C(x_s)$ para Bob.

Decodificando a mensagem

8º Passo: Bob, ao receber $C(x)$, usa o inverso de b módulo $\phi(m)$, que é o elemento a guardado na sua chave privada e calcula $D(C(x_i))$, que é o resíduo de $C(x_i)^a$ módulo m, e faz

$$C(x_i)^a \equiv D(C(x_i)) \equiv x_i \bmod m \text{ onde } 0 \leq D(C(x_i)) < m,$$

para cada $i = 1, 2, \cdots, s$.

9º Passo: Após recuperar a sequência numérica x criada por Alice, Bob consulta a mesma tabela de conversão que Alice utilizou para saber qual foi a mensagem enviada.

A matemática escondida na decodificação

Como $ab \equiv 1 \bmod \phi(m)$, então existe $k \in \mathbb{Z}$ tal que $ab = 1 + k\phi(m)$. Daí, para cada i,

$$D(C(x_i)) \equiv C(x_i)^a \equiv (x_i^b)^a \equiv x_i^{ab} \equiv x_i^{k\phi(m)+1} \equiv x_i.(x_i^{\phi(m)})^k \bmod m.$$

Pelo Teorema de Euler, se $mdc(x_i, m) = 1$, então $x_i^{\phi(m)} \equiv 1 \bmod m$. Portanto,

$$D(C(x_i)) \equiv x_i.(x_i^{\phi(m)})^k \equiv x_i \bmod m.$$

Ambos $D(C(x_i))$ e x_i são menores do que m, então $D(C(x_i)) = x_i$.

Em aplicações práticas do RSA há muitas contas a serem feitas e isso só é possível com o uso de computadores. Por exemplo, é necessário ter acesso a números primos muito grandes para gerar as chaves.

Observação 4.1.4 *A RSA Data Security, que é responsável pela padronização do RSA, recomenda que se utilizem chaves de* 2048 *bits, o que resulta em um número com* 617 *dígitos.*

Exemplo 4.1.1 *Para que possamos compreender o funcionamento do sistema de criptografia RSA com um pouco mais de facilidade, iremos escolher dois números*

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

Tabela 11: Tabela de conversão

primos pequenos, pois queremos realizar todos os cálculos necessários apenas com o auxílio de uma calculadora. Usaremos a Tabela 11 como tabela de conversão.

O espaço entre duas palavras será substituído pelo número 99 *quando for feita a conversão. Poderíamos ter escolhido outros números para representar cada letra, porém devemos apenas escolher números de dois algarismos, pois se algumas letras fossem representadas por números de dois algarismos e outras por números de um algarismo poderíamos ter problemas em identificar as letras. Por exemplo, se a letra A correspondesse ao número* 1*, a letra B ao número* 2 *e a letra L ao número* 12*, não saberíamos se a sequência* 12 *é a conversão de AB ou L.*

Seguindo os passos já apresentados:

1^o ***Passo:*** *Bob escolhe os números primos distintos* $p = 3$ *e* $q = 7$*. Logo,*

$$m = pq = 3 \times 7 = 21.$$

2^o ***Passo:*** *Bob calcula* $\phi(m) = \phi(pq) = (p-1)(q-1) = (3-1)(7-1) = 12$.

3^o ***Passo:*** *Bob escolhe* $a = 17$*, pois* $mdc(\phi(m), a) = mdc(12, 17) = 1$*. Agora ele deve encontrar o inverso multiplicativo de* $a = 17$ *resolvendo a congruência* $17b \equiv 1 \mod 12$*, isto é, solucionando a equação diofantina* $17b - 12y = 1$*, para* $b, y \in \mathbb{Z}$*. Feito isto, ele encontra* $b = 5$*.*

Temos então as duas chaves:

- ***Chave pública:*** $(m, b) = (21, 5)$.
- ***Chave secreta:*** $(m, a) = (21, 17)$.

4^o ***Passo:*** *Bob torna púbica a chave* (m, b).

Suponhamos que Alice queira enviar a mensagem BOM DIA para Bob.

5^o ***Passo:*** *Utilizando a Tabela 11, a sequência numérica que Alice deve codificar é* 11242299131810. *Ela então divide a mensagem em blocos, que podem ser de tamanhos variáveis, desde que cada bloco x_i seja menor que m. Assim,*

$$11242299131810 \leftrightarrow 11-2-4-2-2-9-9-13-18-10.$$

6^o ***Passo:*** *Para cada x_i ela encontra um $C(x_i)$ tal que $x_i^b \equiv C(x_i)\ mod\ m$ da seguinte forma:*

1^o *Bloco:* $11 \rightarrow 11^5 \equiv 2\ mod\ 21$,
$2^o, 4^o$ *e* 5^o *Bloco:* $2 \rightarrow 2^5 \equiv 11\ mod\ 21$,
3^o *Bloco:* $4 \rightarrow 4^5 \equiv 16\ mod\ 21$,
6^o *e* 7^o *Bloco:* $9 \rightarrow 9^5 \equiv 18\ mod\ 21$,
8^o *Bloco:* $13 \rightarrow 13^5 \equiv 13\ mod\ 21$,
9^o *Bloco:* $18 \rightarrow 18^5 \equiv 9\ mod\ 21$ *e*
10^o *Bloco:* $10 \rightarrow 10^5 \equiv 19\ mod\ 21$

7^o ***Passo:*** *Após codificar toda a mensagem, Alice envia a seguinte sequência de blocos para Bob:*

$$C(x) = 2-11-16-11-11-18-18-13-9-19.$$

A decodificação da mensagem consiste em uma nova exponenciação, desta vez usando a chave secreta, que só Bob conhece.

8^o ***Passo:*** *Para decifrar a mensagem $C(x)$, Bob faz $C(x_i)^a\ mod\ m$ para cada bloco enviado por Alice. Vejamos:*

1^o *Bloco:* $2 \rightarrow 2^{17} \equiv 11\ mod\ 21$,
$2^o, 4^o$ *e* 5^o *Bloco:* $11 \rightarrow 11^{17} \equiv 2\ mod\ 21$,
3^o *Bloco:* $16 \rightarrow 16^{17} \equiv 4\ mod\ 21$,
6^o *e* 7^o *Bloco:* $18 \rightarrow 18^{17} \equiv 9\ mod\ 21$,
8^o *Bloco:* $13 \rightarrow 13^{17} \equiv 13\ mod\ 21$,
9^o *Bloco:* $9 \rightarrow 9^{17} \equiv 18\ mod\ 21$ *e*
10^o *Bloco:* $19 \rightarrow 19^{17} \equiv 10\ mod\ 21$

9^o ***Passo:*** *Sendo assim, Bob obtém a sequência numérica* 11242299131810 *e consulta de dois em dois algarismos a Tabela 11. Finalmente Bob chega na mensagem BOM DIA enviada por Alice.*

4.2 SISTEMA PARI/GP

Embora número escolhido ($m = 21$) no Exemplo 4.1.1 é muito pequeno, as contas de exponenciação são bastante grandes para serem feitas à mão. Por essa razão mostraremos como usar um sistema de computação algébrica, o PARI/GP, que é capaz de fazer cálculos com números grandes em alta velocidade.

O PARI/GP possui versões para diversos sistemas operacionais. Para obtê-lo basta acessar o link `https://pari.math.u-bordeaux.fr/download.html` e realizar o download.

No que se segue vamos exemplificar como utilizar o PARI/GP com os cálculos que precisamos fazer no RSA.

Exemplo 4.2.1 *Vamos criptografar e descriptografar apenas a letra A como exemplo para compreendermos a ordem dos cálculos realizados no sistema PARI/GP.*

A Figura 2 mostra a captura de tela das operações realizadas no sistema.

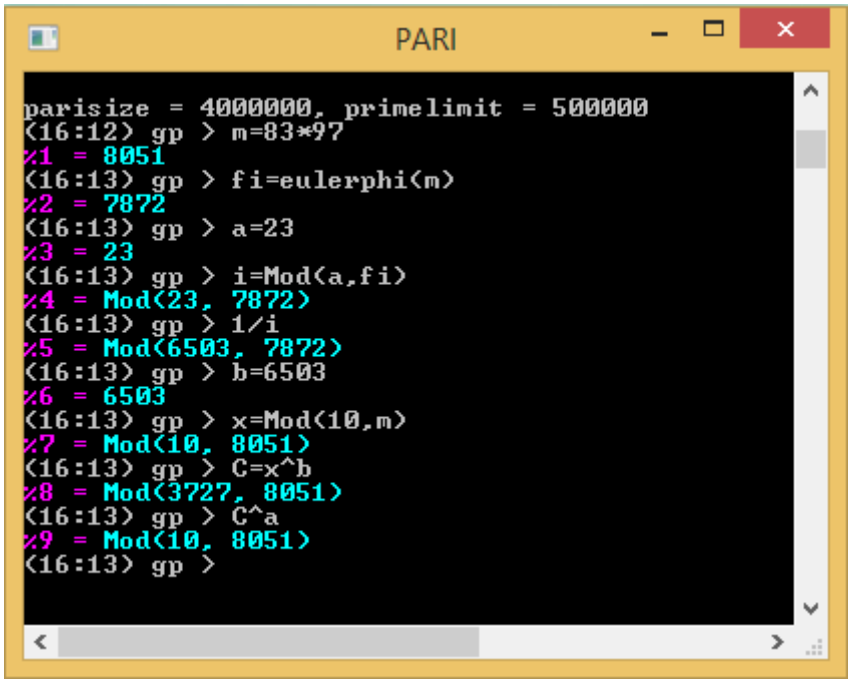

Figura 2: Cálculos realizados no PARI/GP

Vamos descrever, passo a passo, as operações realizadas:

Linha 1***:*** *Primeiramente escolhemos dois primos distintos* ($p = 83$ *e* $q = 97$*). Então, no sistema, definimos* $m = 83 * 97$*. A multiplicação é representada pelo símbolo* $*$ *. Observe que o sistema numera os resultados obtidos* ($\%1, \%2, \cdots$)*. O valor* 8051 *está agora armazenado na variável* m*.*

Linha 2***:*** *Armazenamos, na variável* fi*, o valor eulerphi(m). Este comando calcula a função* $\phi(m)$*. Assim,* $fi = 7872 = \phi(8051)$*.*

Linha 3***:*** *Escolhemos* $a = 23$*, pois* $mdc(\phi(m), a) = mdc(7872, 23) = 1$*.*

Linha 4***:*** *Definimos* $i = Mod(a, fi) = Mod(23, 7872)$*. O comando "Mod" é utilizado para aritmética modular. Assim, o que fizemos foi definir* $i = 23$ *mod* 7872*.*

Linha 5***:*** *Para calcular o inverso multiplicativo de* 23 *módulo* 7872*, pedimos o valor* $1/i$*, que o sistema entende como o inverso de* 23 *mod* 7872*. O resultado obtido é* 6503 *mod* 7872*.*

Linha 6***:*** *Definimos* $b = 6503$*.*

Acabamos de determinar as chaves:

- ***Chave pública:*** $(m, b) = (8051, 6503)$*.*
- ***Chave secreta:*** $(m, a) = (8051, 23)$*.*

Vamos agora criptografar a letra A. De acordo com a Tabela de Conversão 11*, temos que a letra A corresponde ao número* 10*. Assim:*

Linha 7***:*** *Definimos* $x = Mod(10, m)$*, que corresponde a* 10 *mod* 8051*.*

Linha 8***:*** *A mensagem criptografada é* $C = x^b$ *mod* m*. A exponenciação no PARI/GP é dada pelo símbolo* $\hat{}$ *. Obtivemos* $C = 3727$ *mod* 8051*.*

***Linha** 9: Para decifrar a mensagem fazemos C^a mod m, que resulta em 10 mod 8051, que é a mensagem original x.*

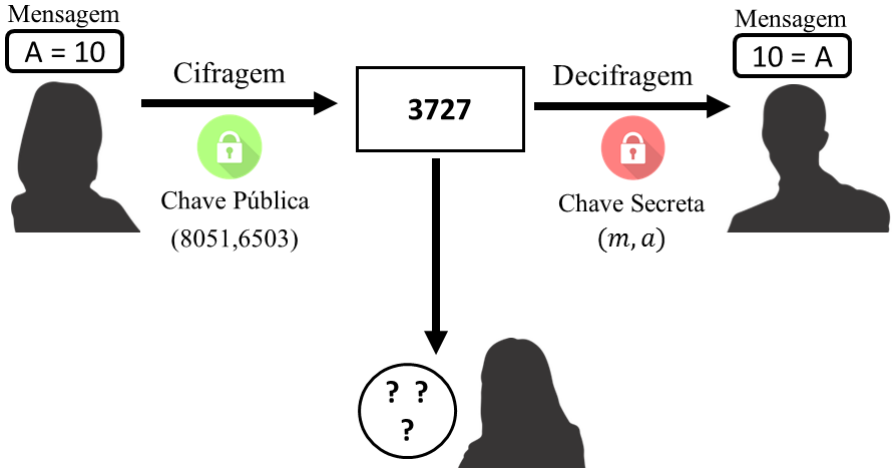

Figura 3: Alice enviando a mensagem A para Bob

4.3 SEGURANÇA DO RSA

A segurança do RSA se fundamenta na enorme dificuldade prática em fatorar um número natural grande como produto de dois primos em tempo polinomial, pois se conseguíssemos fatorar o número natural m como produto de primos $m = pq$, poderíamos facilmente calcular o valor de $\phi(m) = (p-1)(q-1)$ e resolver a congruência $ab \equiv 1 \mod \phi(m)$, já que possuímos o valor de b que está na chave pública. Assim, determinando o valor de a descobriríamos a chave secreta.

Até o momento, não se conhece um algoritmo para fatoração de naturais grandes em um computador clássico que funcione em tempo polinomial, mas também não se provou que um algoritmo deste tipo não pode existir.

Exemplo 4.3.1 *A chave pública de Bob é $(m, b) = (77, 37)$. Alice utiliza esta chave para criptografar uma mensagem para Bob. Alice envia a mensagem $C(x) = 63$. Vamos quebrar o código descobrindo a chave secreta de Bob e revelar a mensagem original enviada por Alice.*

I. Utilizando os critérios de divisibilidade tentamos fatorar o número m. Como 77 não é um número natural grande concluímos com certa facilidade que $77 = 7 \times 11$. Logo, $p = 7$ e $q = 11$.

II. Calculamos $\phi(m) = \phi(77) = (7-1)(11-1) = 60$.

III. *Encontramos o valor de a resolvendo a congruência* $37a \equiv 1 \ mod\ 60$*, ou seja, determinando o inverso de b módulo* $\phi(m)$*. Feito isso, encontramos* $a = 13$*.*

IV. *Portanto, a chave secreta de Bob é o par* $(m, a) = (77, 13)$*.*

V. *Com posse da chave secreta, podemos descriptografar a mensagem* $C(x)$ *enviada por Alice. Para isso, devemos encontrar o resíduo de* $C(x)^a$ *módulo* m*. Assim,* $63^{13} \equiv 28 \ mod\ 77$*.*

VI. *Suponhamos que Alice tenha utilizado a Tabela de Conversão* 11*, então a mensagem enviada para Bob foi a letra R já que o número* 28 *corresponde à letra R na tabela.*

5

PROPOSTA DIDÁTICA

Neste capítulo apresentamos uma proposta didática para o ensino do sistema de criptografia RSA no ensino fundamental, especificamente com alunos que cursam o último ano deste ciclo, o 9º ano.

A proposta tem como objetivo motivar o aluno a entender o funcionamento do RSA e com isso proporcionar um estudo mais aprofundado de aritmética. Por isso, sugerimos que os conteúdos desta dissertação sejam abordados com os alunos na seguinte ordem:

- Capítulo 2: Números naturais e Números Inteiros.
- Seção 3.1 do Capítulo 3: Congruências.
- Noções básicas de Criptografia.
- Uso do sistema PARI/GP para cálculo de congruências.
- Livro Digital.
- Seções 3.2, 3.3, 3.4 e 3.5 do Capítulo 3.
- Capítulo 4: Sistema de Criptografia RSA.

5.1 LIVRO DIGITAL

O centro desta proposta é um objeto educacional digital, o livro digital intitulado *"Ataque à Séquia - Missão T55"* (`http://online.flipbuilder.com/vejn/unlf/`).

No que se segue apresentamos todas as páginas do livro com suas atividades propostas.

Figura 4: Capa do Livro

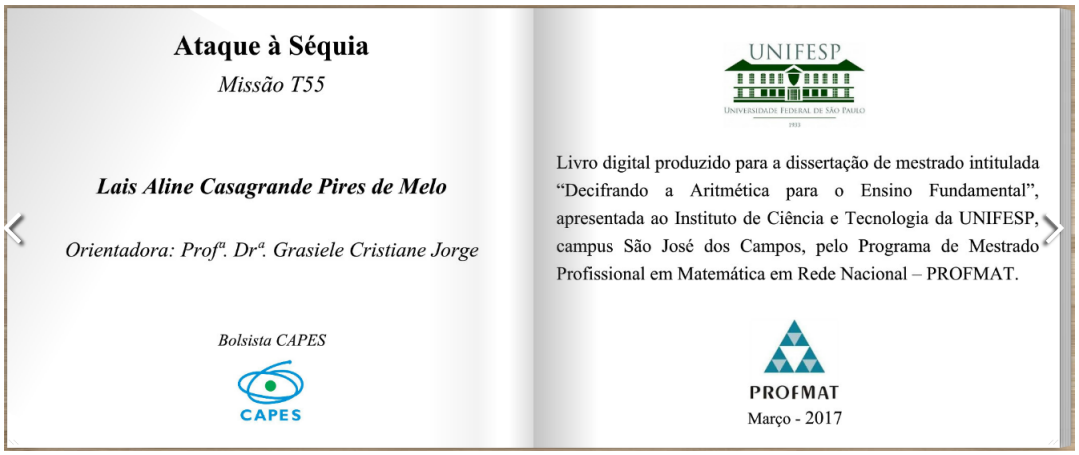

Figura 5: Folha de rosto

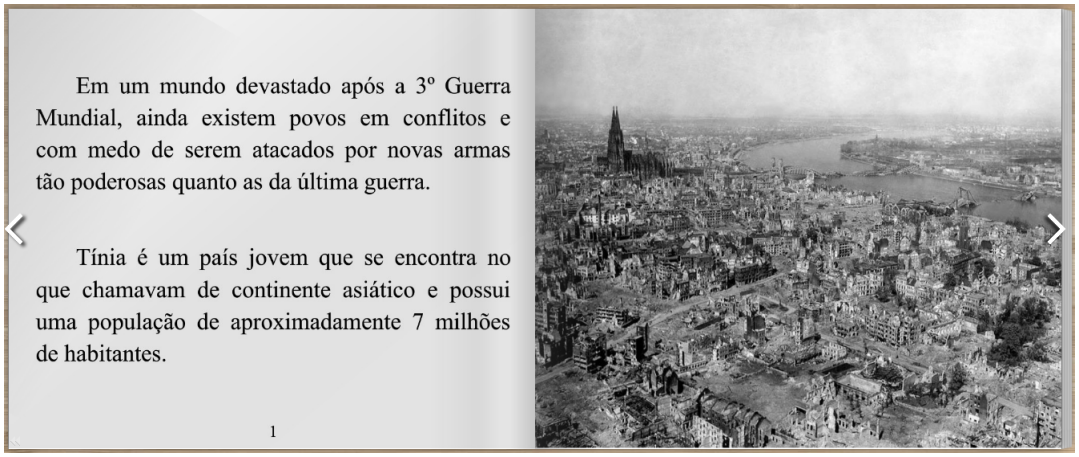

Figura 6: Páginas 1 e 2

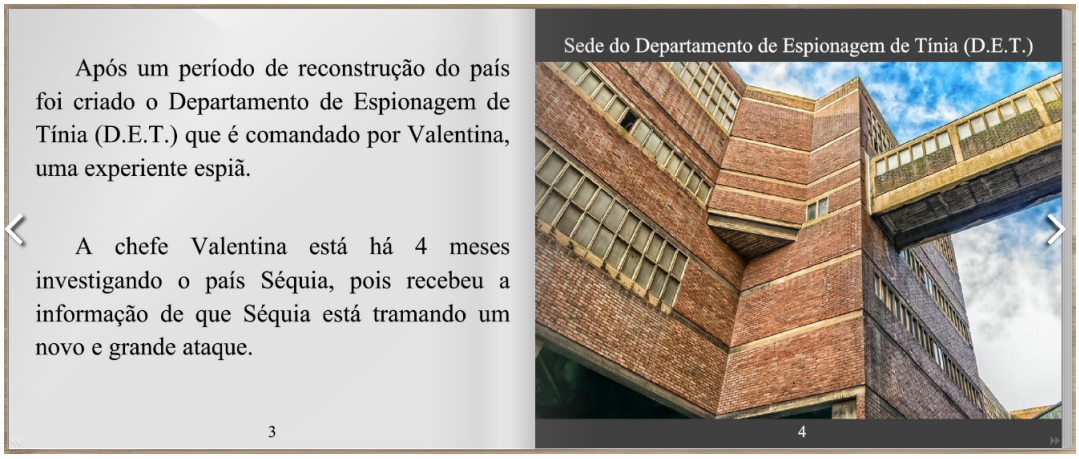

Figura 7: Páginas 3 e 4

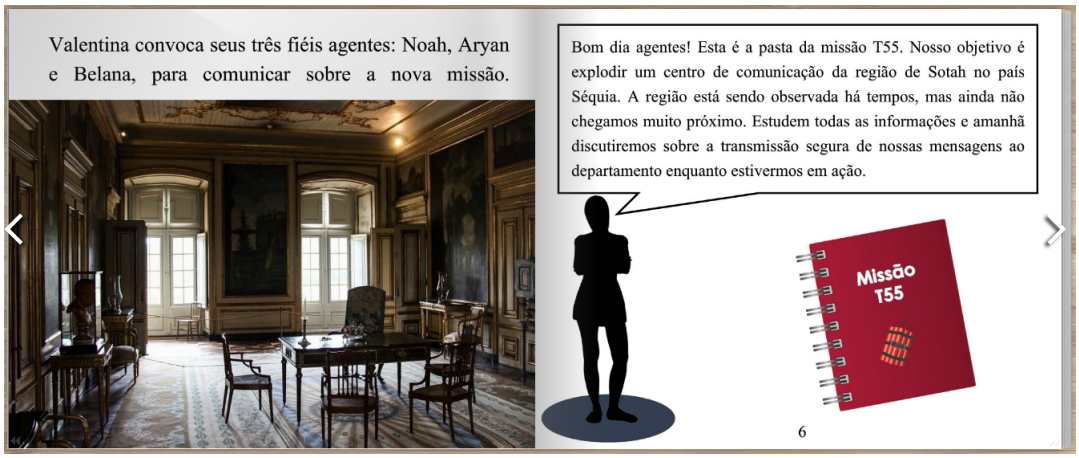

Figura 8: Páginas 5 e 6

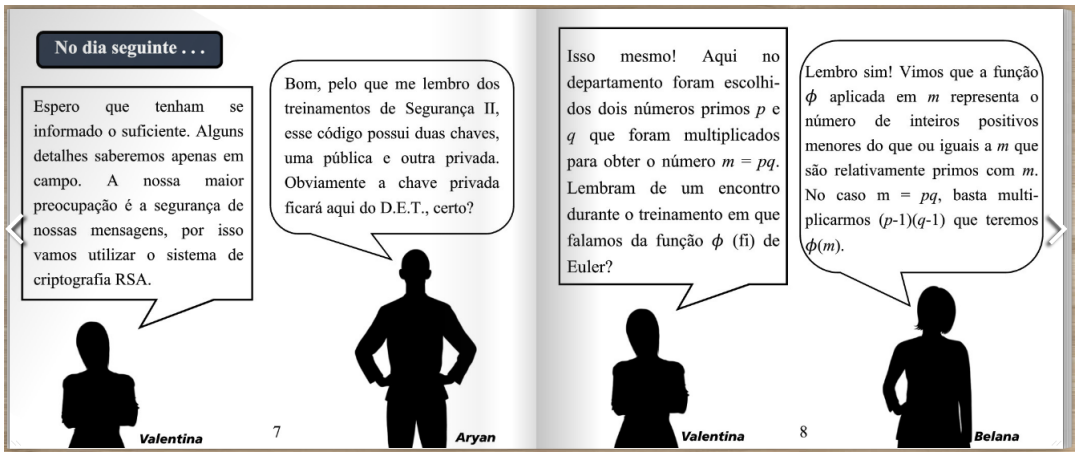

Figura 9: Páginas 7 e 8

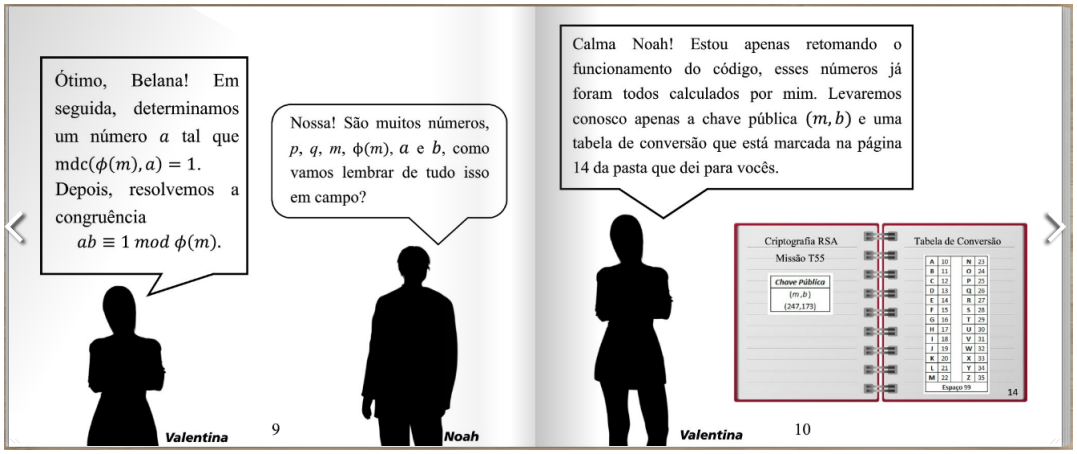

Figura 10: Páginas 9 e 10

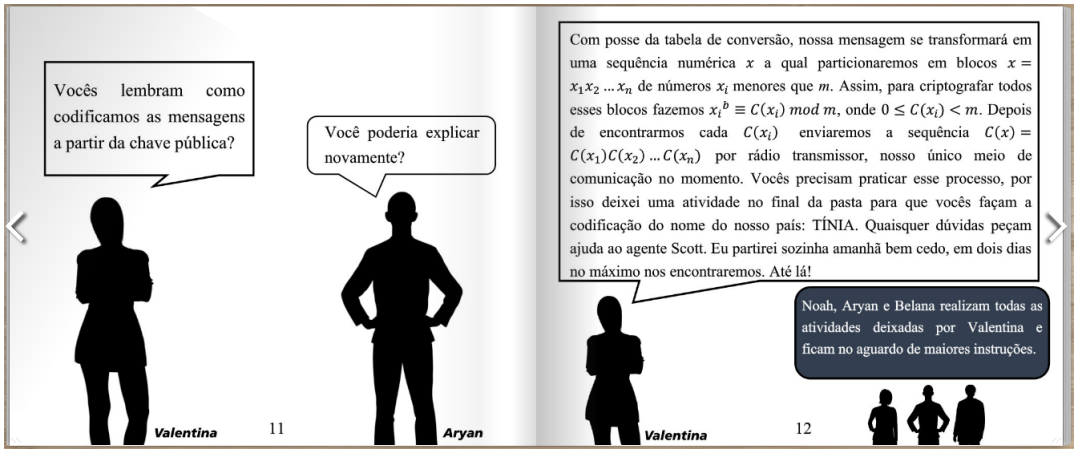

Figura 11: Páginas 11 e 12

Figura 12: Páginas 13 e 14

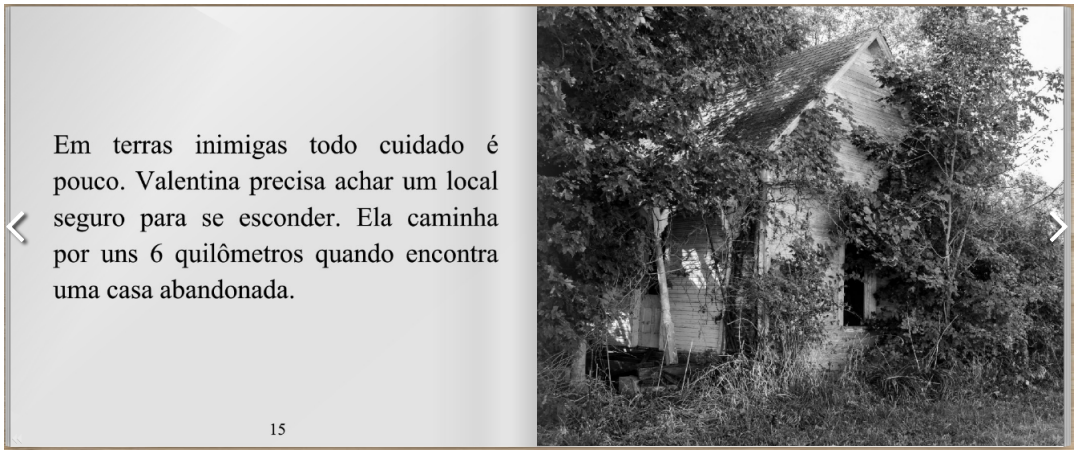

Figura 13: Páginas 15 e 16

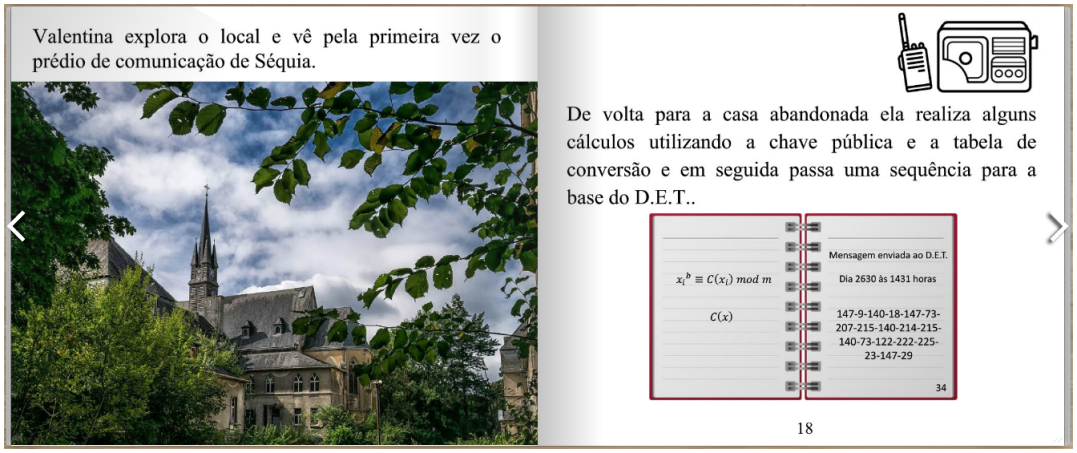

Figura 14: Páginas 17 e 18

Figura 15: Páginas 19 e 20

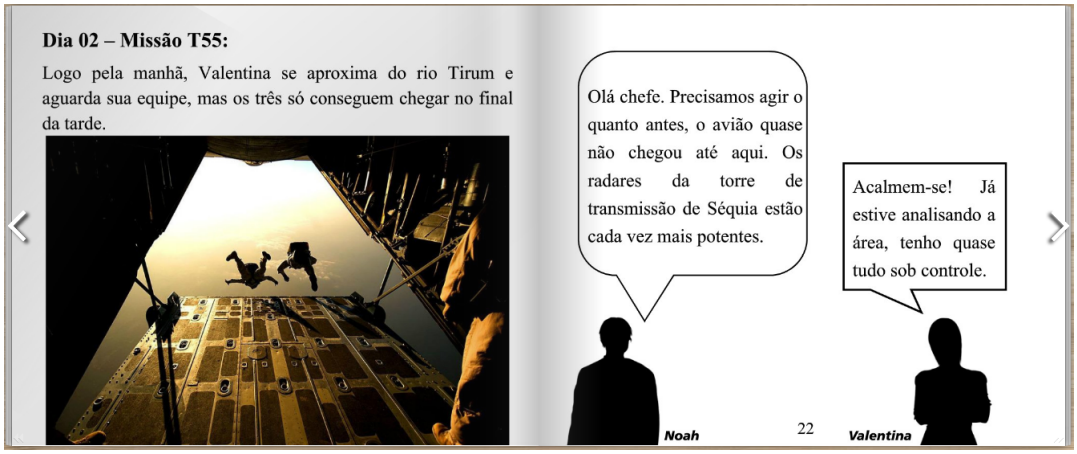

Figura 16: Páginas 21 e 22

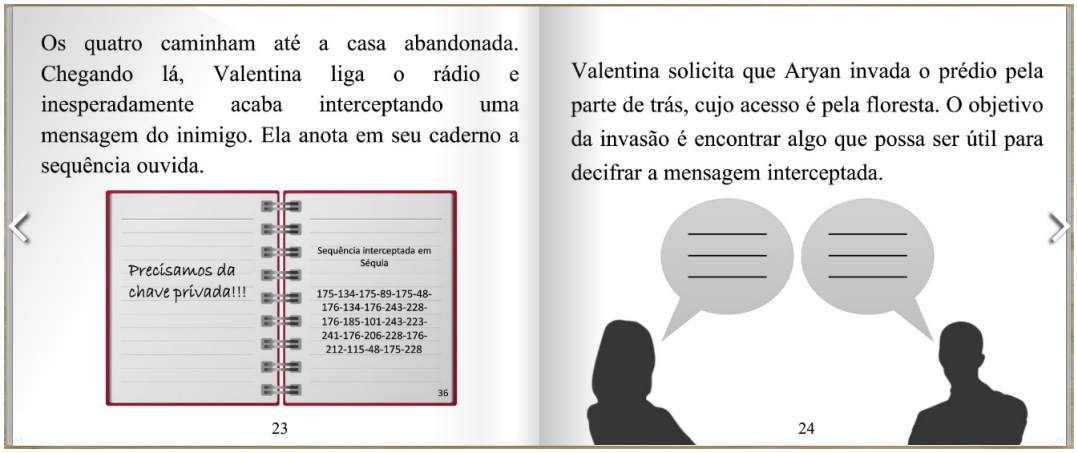

Figura 17: Páginas 23 e 24

Figura 18: Páginas 25 e 26

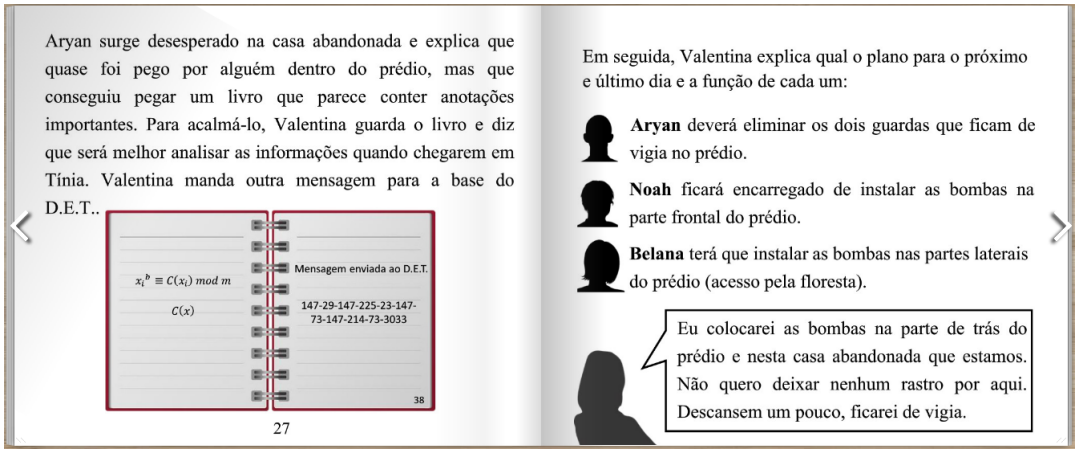

Figura 19: Páginas 27 e 28

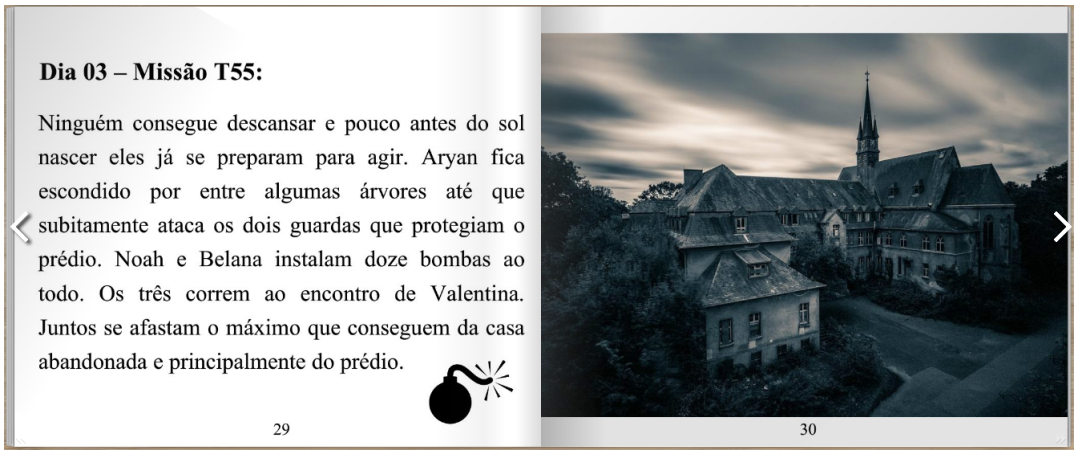

Figura 20: Páginas 29 e 30

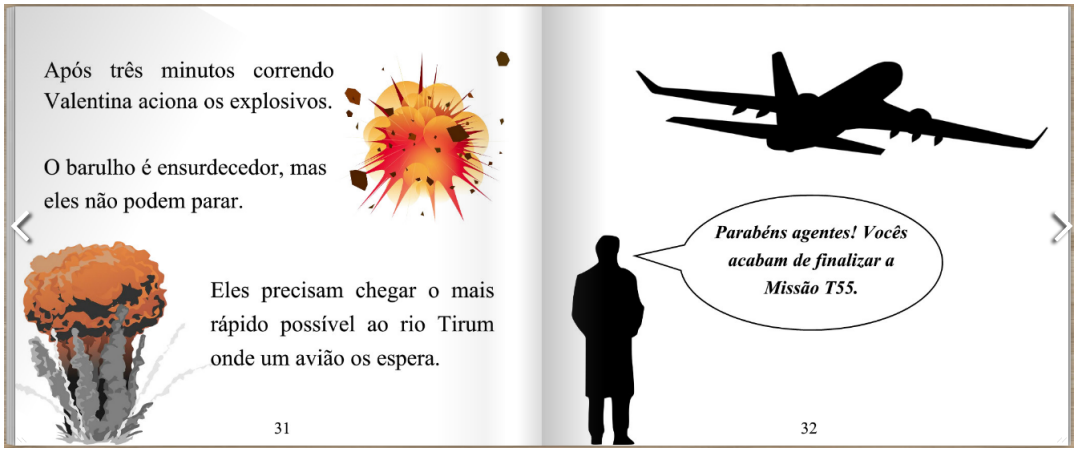

Figura 21: Páginas 31 e 32

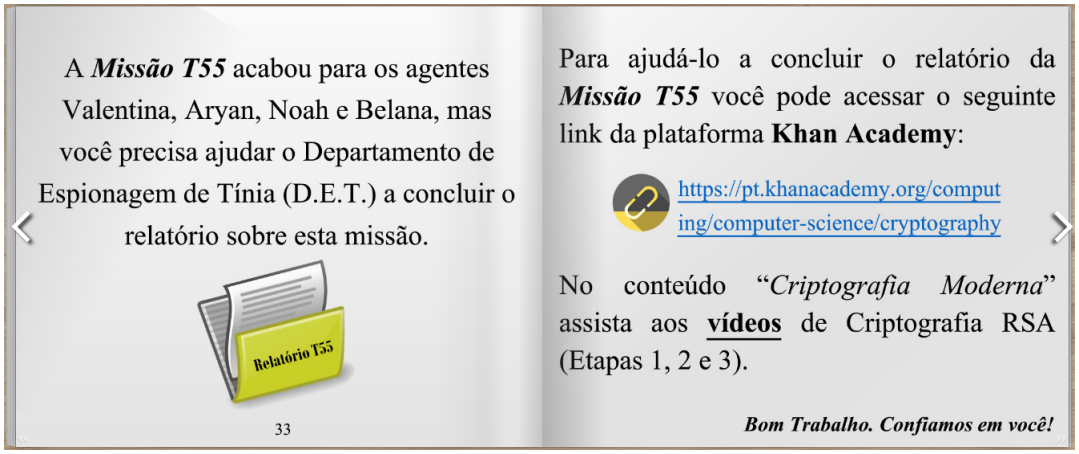

Figura 22: Páginas 33 e 34

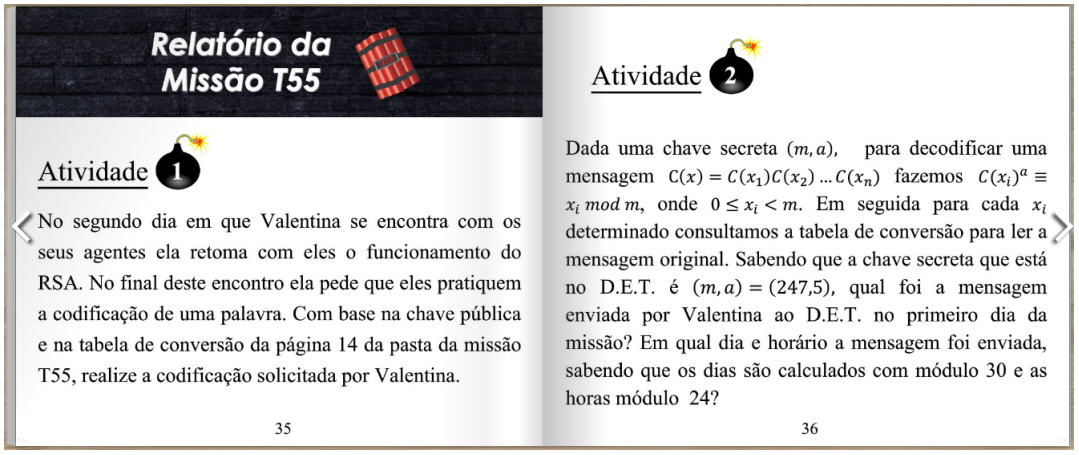

Figura 23: Atividades 1 e 2

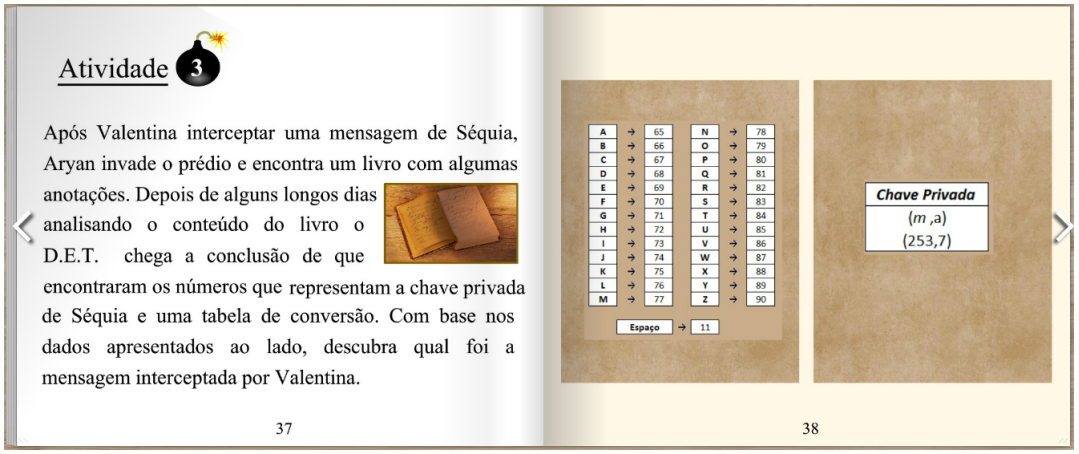

Figura 24: Atividade 3

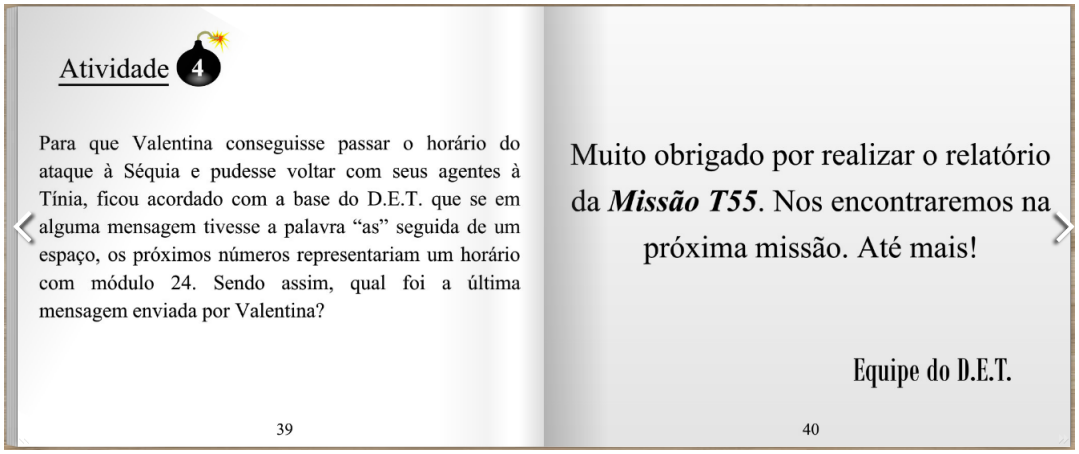

Figura 25: Atividade 4

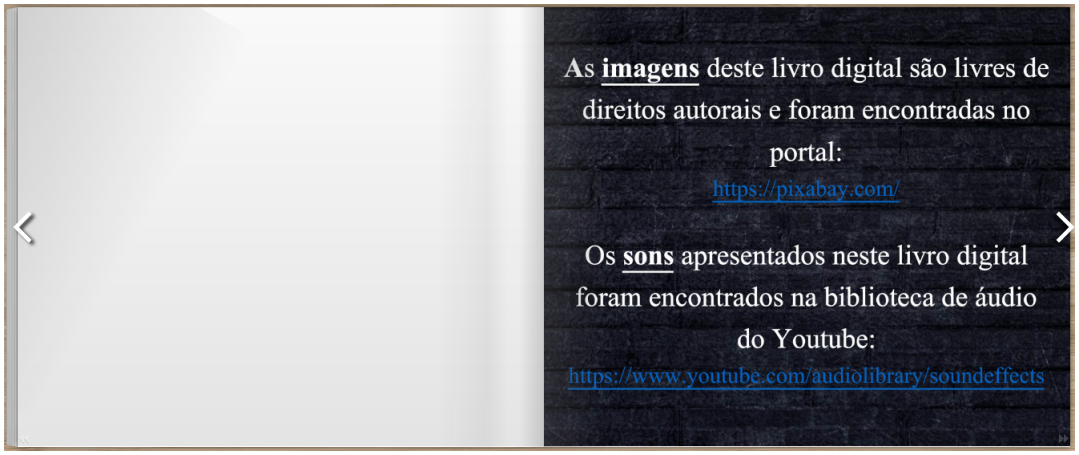

Figura 26: Páginas finais

5.2 RESOLUÇÃO DAS ATIVIDADES

Nesta seção, apresentamos as soluções das Atividades 1, 2, 3 e 4 que constam no livro digital. Para resolvermos tais atividades utilizaremos o sistema PARI/GP.

Atividade 1

Vamos codificar o nome do país dos agentes: TÍNIA. Utilizando a tabela de conversão e a chave pública $(m, b) = (247, 173)$ registrada na Página 14 da pasta da missão, temos

$$\text{TINIA} \rightarrow x = 2918231810.$$

Separamos em blocos a sequência x, tal que cada bloco x_i seja menor do que ou igual a $m = 247$ e obtemos a sequência

$$\text{TINIA} \rightarrow x = 29 - 18 - 23 - 18 - 10.$$

Para cada bloco x_i fazemos $x_i^b \equiv C(x_i) \bmod 247$, a fim de encontrarmos $C(x)$.

No sistema PARI/GP registramos $b = 173$, $m = 247$ e $x = Mod(x_i, m)$. Em seguida calculamos $C = x_i\hat{}b$, para cada x_i da sequência x.

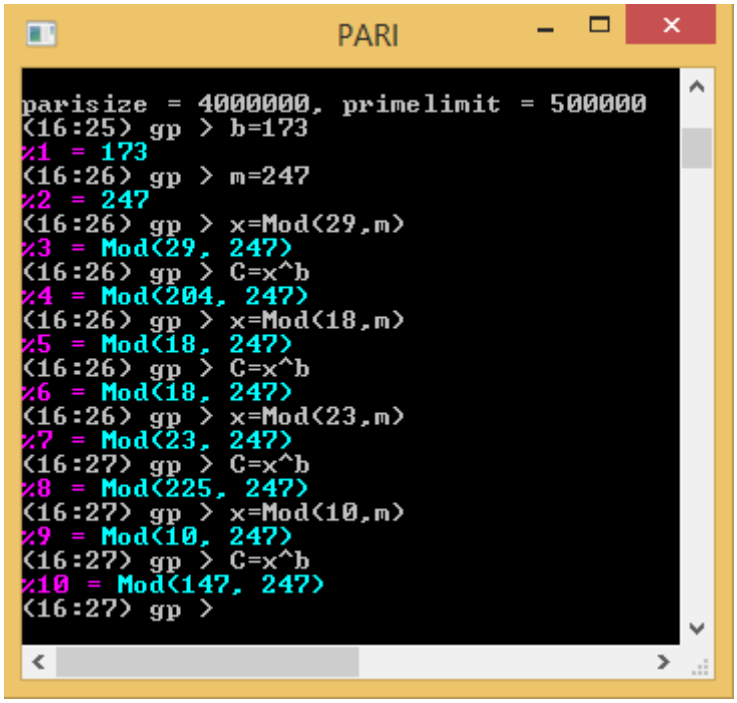

Figura 27: Resolução da Atividade 1

Assim, a codificação de cada x_i é

$$29^b \equiv 204 \bmod m,$$
$$18^b \equiv 18 \bmod m,$$
$$23^b \equiv 225 \bmod m \text{ e}$$
$$10^b \equiv 147 \bmod m.$$

Portanto, o nome TINIA codificado gera a sequência

$$C(x) = 204 - 18 - 225 - 18 - 147.$$

Atividade 2

Vamos primeiramente decodificar a mensagem enviada por Valentina. Temos:

$$C(x) = 147 - 9 - 140 - 18 - 147 - 73 - 207 - 215 - 140 - 214 - 215 - 140 - 73 - 122 - 222 - 225 - 23 - 147 - 29.$$

Sabendo que a chave privada é $(m, a) = (247, 5)$, fazemos $C(x_i)^a \equiv x_i \bmod m$, a fim de encontrarmos cada x_i que corresponde a mensagem enviada.

Sendo assim, no sistema PARI/GP registramos $a = 5$, $m = 247$ e $C = Mod(C(x_i), m)$. Em seguida calculamos $x = C(x_i)\hat{}a$, para cada $C(x_i)$ da sequência $C(x)$.

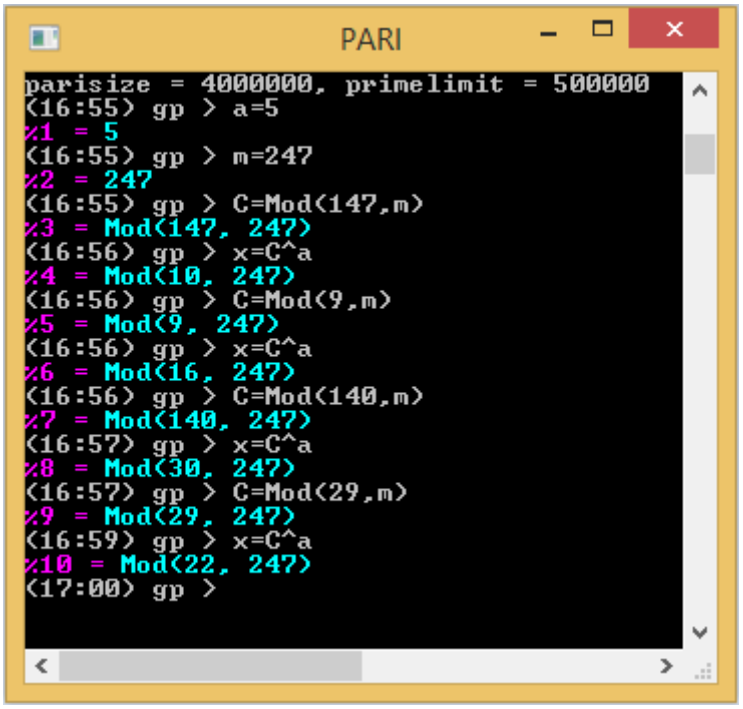

Figura 28: Resolução da Atividade 2

Assim, a decodificação de cada $C(x_i)$ é

$$147^a \equiv 10 \bmod m,$$
$$9^a \equiv 16 \bmod m,$$
$$140^a \equiv 30 \bmod m,$$
$$\vdots$$
$$29^a \equiv 22 \bmod m.$$

E por fim consultamos a tabela de conversão. Portanto, a mensagem enviada por Valentina ao D.E.T. no primeiro dia da missão foi "AGUIA POUSOU VENHAM".

Para responder a outra pergunta sobre o dia e o horário em que a mensagem foi enviada, basta encontrarmos o resto da divisão de 2630 por 30 e de 1431 por 24, conforme anotado na pasta por Valentina. Ou seja,

$$2630 \equiv 20 \bmod 30 \text{ e}$$
$$1431 \equiv 15 \bmod 24,$$

a mensagem foi enviada no dia 20 às 15 horas.

Atividade 3

Valentina interceptou a seguinte mensagem por rádio

$$C(x) = 175 - 134 - 175 - 89 - 175 - 48 - 176 - 134 - 176 - 243 - 228 - 176 - 185 - 101 - 243 - 223 - 241 - 176 - 206 - 228 - 176 - 212 - 115 - 48 - 175 - 228.$$

Como informado na atividade, a chave privada é constituída dos números $(m, a) = (253, 7)$. Procederemos da mesma forma que a atividade anterior.

No sistema PARI/GP registramos $a = 7$, $m = 253$ e $C = Mod(C(x_i), m)$. Em seguida calculamos $x = C(x_i)\hat{}a$, para cada $C(x_i)$ da sequência $C(x)$.

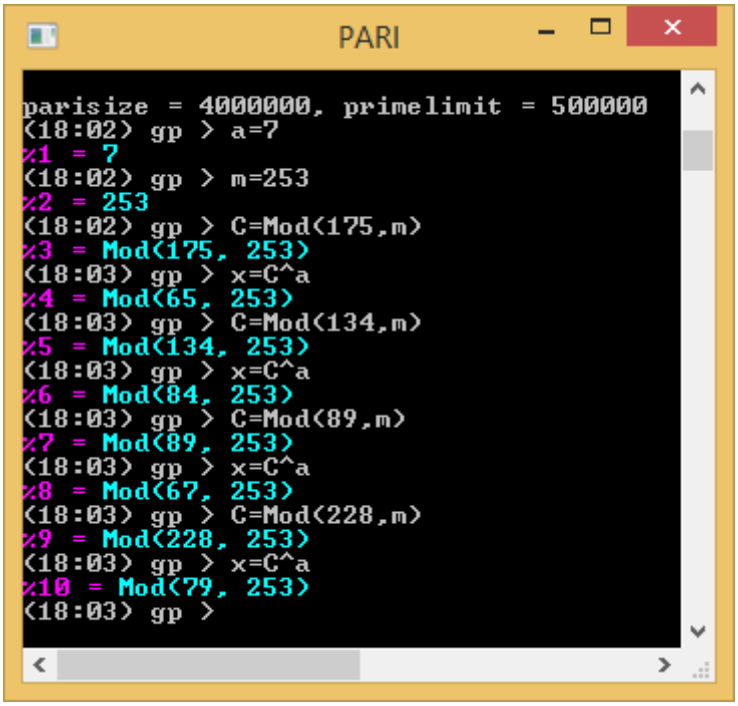

Figura 29: Resolução da Atividade 3

Assim, a decodificação de cada $C(x_i)$ é

$$\begin{aligned} 175^a &\equiv 65 \bmod m, \\ 134^a &\equiv 84 \bmod m, \\ 175^a &\equiv 65 \bmod m, \\ 89^a &\equiv 67 \bmod m, \\ &\vdots \\ 228^a &\equiv 79 \bmod m. \end{aligned}$$

E como também foi descoberto a tabela de conversão, consultamos a mesma e descobrimos que a mensagem interceptada foi "ATACAR T NO FINAL DO VERAO", o que nos leva a crer que Séquia atacaria Tínia no final do verão.

Atividade 4

A última mensagem enviada por Valentina ao D.E.T. foi

$$C(x) = 147 - 29 - 147 - 225 - 23 - 147 - 73 - 147 - 214 - 73 - 3033.$$

Utilizando o PARI/GP encontramos

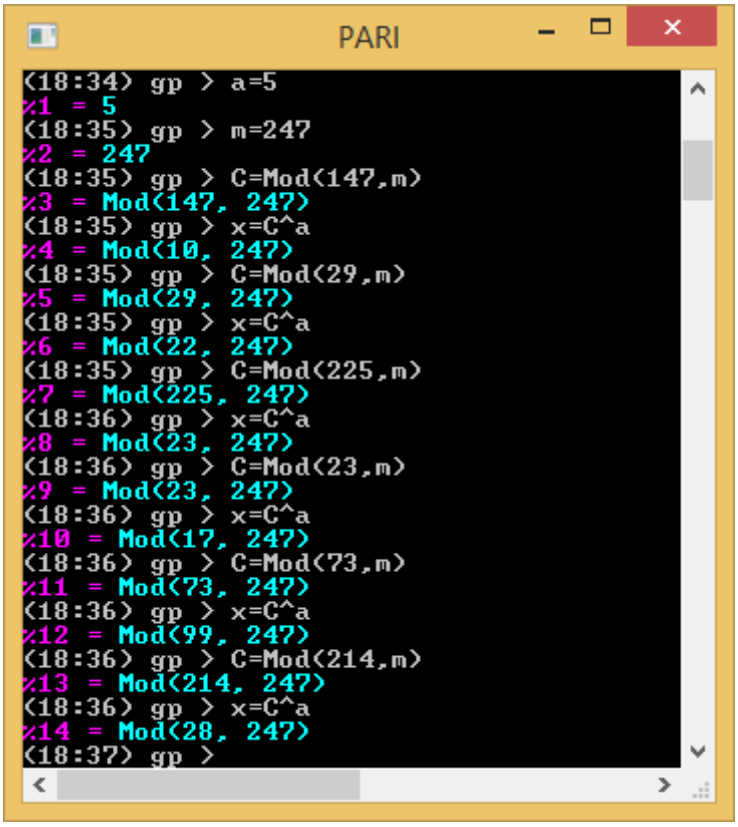

Figura 30: Resolução da Atividade 4

Logo, obtemos os números da decodificação e consultando a tabela de conversão determinamos

$$\begin{aligned}
147^a \equiv 10 \bmod m &\to \text{A},\\
29^a \equiv 22 \bmod m &\to \text{M},\\
147^a \equiv 10 \bmod m &\to \text{A},\\
225^a \equiv 23 \bmod m &\to \text{N},\\
23^a \equiv 17 \bmod m &\to \text{H},\\
147^a \equiv 10 \bmod m &\to \text{A},\\
73^a \equiv 99 \bmod m &\to \text{“espaço”},\\
147^a \equiv 10 \bmod m &\to \text{A},\\
214^a \equiv 28 \bmod m &\to \text{S},\\
73^a \equiv 99 \bmod m &\to \text{“espaço”},
\end{aligned}$$

sendo $(m, a) = (247, 5)$.

De acordo com as instruções, o próximo número da sequência $C(x)$ representa o horário que a equipe atacaria o prédio em Séquia. Então, como $3033 \equiv 9 \bmod 24$, o horário planejado para o ataque foi às 9 horas. Portando, o D.E.T. recebeu a mensagem *“AMANHA AS (9 HORAS)”* de Valentina.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] S. C. Coutinho, *Criptografia*, Programa de Iniciação Científica da OBMEP, Rio de Janeiro, IMPA, 2015, disponível em `http://www.obmep.org.br/docs/apostila7.pdf`.

[2] S. C. Coutinho, *Números Inteiros e Criptografia RSA*, Coleção Matemática e Aplicações, IMPA, 2014.

[3] F. Dutenhefner, L. Cadar, *Encontros de Aritmética*, Programa de Iniciação Científica da OBMEP, Rio de Janeiro, IMPA, 2015, disponível em `http://www.obmep.org.br/docs/aritmetica.pdf`.

[4] A. C. Faleiros, *Criptografia*, Notas em Matemática Aplicada, SBMAC, 2011, disponível em `http://www.sbmac.org.br/arquivos/notas/livro_52.pdf`.

[5] L. M. Figueiredo, *Introdução à Criptografia*, v. 2, Fundação CECIERJ, Rio de Janeiro, 2010.

[6] D. Fomim, S. Genkin, I. Itenberg, *Círculos Matemáticos - A Experiência Russa*, Rio de Janeiro, IMPA, 2015.

[7] A. Hefez, *Iniciação à Aritmética*, Programa de Iniciação Científica da OBMEP, Rio de Janeiro, IMPA, 2016, disponível em `http://www.obmep.org.br/docs/apostila1.pdf`.

[8] A. Hefez, *Aritmética*, Coleção PROFMAT, SBM, 2014.

[9] J. P. O. Santos, *Introdução à Teoria dos Números*, Coleção Matemática Universitária, Rio de Janeiro, IMPA, 2015.