UNIVERSIDADE FEDERAL DE SERGIPE
CENTRO DE CIÊNCIAS EXATAS E TECNOLOGIA
DEPARTAMENTO DE MATEMÁTICA
MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL

Aritmética Modular, Códigos Elementares e Criptografia

Regene Chaves Pimentel Pereira Barreto

Agosto de 2014
São Cristóvão-SE

UNIVERSIDADE FEDERAL DE SERGIPE
CENTRO DE CIÊNCIAS EXATAS E TECNOLOGIA
DEPARTAMENTO DE MATEMÁTICA
MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL

Regene Chaves Pimentel Pereira Barreto

Aritmética Modular, Códigos Elementares e Criptografia

Trabalho apresentado ao Departamento de Matemática da Universidade Federal de Sergipe como requisito parcial para a conclusão do Mestrado Profissional em Matemática (PROFMAT).

ORIENTADOR: Prof. Dr. J. Anderson Valença Cardoso

Este exemplar corresponde à versão final da dissertação defendida pela aluna **Regene Chaves Pimentel Pereira Barreto**, orientada pelo Prof. Dr. José Anderson Valença Cardoso.

Agosto de 2014
São Cristóvão-SE

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA CENTRAL
UNIVERSIDADE FEDERAL DE SERGIPE

Barreto, Regene Chaves Pimentel Pereira
B273a Aritmética modular, códigos elementares e criptografia / Regene Chaves Pimentel Pereira Barreto; orientador José Anderson Valença Cardoso – São Cristóvão, 2014.
111 f. : il.

Dissertação (Mestrado Profissional em Matemática) – Universidade Federal de Sergipe, 2014.

O

1. Matemática - Estudo e ensino. 2. Aritmética. 3. Criptografia. 4. Código de barras. I. Cardoso, José Anderson Valença, orient. II. Título.

CDU: 511.1

Dissertação submetida à aprovação pelo Programa de Pós-Graduação em Matemática da Universidade Federal de Sergipe, como parte dos requisitos para obtenção do grau de Mestre em Matemática.

Aritmética Modular, Códigos Elementares e Criptografia

por

Regene Chaves Pimentel Pereira

Aprovada pela Banca Examinadora:

José Anderson Valença Cardoso
Prof. Dr. José Anderson Valença Cardoso - UFS
Orientador

Elisandra F. Gloss de Moraes
Profa. Dra. Elisandra De Fátima Gloss de Moraes - UFPB
Primeiro Examinador

Allyson dos Santos Oliveira
Prof. Dr. Allyson dos Santos Oliveira- UFS
Segundo Examinador

São Cristóvão, 29 de agosto de 2014

Dedico este trabalho à Deus e a minha família pelo apoio, incentivo, força, compreensão, amizade, paciência e amor. Esse sonho só foi possível porque tinha vocês ao meu lado.

Agradecimentos

Inicio meus agradecimentos primeiramente a Deus, pelo dom da vida e por me presentear com pessoas especiais, sem os incentivos e o apoio destas não teria conseguido.

A minha mãe, Edna, a mais generosa de todas as mães. A senhora é meu exemplo de vida. Obrigada por sempre acreditar em mim. Te amo muito!

Ao meu pai, Ferdinando, o mais bandoso e sábio de todos os pais. Obrigada por se fazer sempre presente em minha vida, me incentivando e acreditando no meu potencial. O senhor é o meu herói. Te amo muito!

Ao meu querido esposo, Aézio, por fazer do meu sonho, nosso sonho. Por sempre está ao meu lado me apoiando e me fazendo acreditar que sou capaz de ir além do que imagino. Obrigada por ser paciente, compreensivo, amoroso e amigo. Você me torna completa. Te amo demais!!!

A Alexandre, meu maior presente. A razão por quem vivo. Mamãe te ama muito.

Aos meus irmãos, Reginaldo e Rafaela, pelos incentivos e confiança. Vocês são fundamentais na minha vida. Amo vocês!

Aos meus avós, tios, sobrinhos, cunhados, sogros e primos por todo apoio e por vibrarem sempre comigo.

Ao meu orientador, Anderson, por acreditar na minha capacidade e por estar sempre disponível a ajudar. Você foi fundamental na conclusão desse trabalho. Meu muito obrigada!

Enfim, a todos que de alguma forma contribuiram com mais essa etapa concluida na minha vida.

Resumo

O presente trabalho tem como principal objetivo tratar de aritmética modular dos inteiros e evidenciar alguns tipos de códigos elementares, a exemplo dos Códigos de César, Afim, de Vigenère, de Hill, RSA, de Rabin, MH e ElGamal, existentes na criptografia, ressaltando a matemática que existe por trás do funcionamento de cada um deles. Estudamos conceitos de aritmética modular e os aplicamos ao estudo de matrizes e determinantes que se fazem necessários para o funcionamento desses códigos e para a evolução da criptografia. Apresentamos ainda alguns códigos encontrados no nosso dia a dia, buscando estimular a curiosidade do leitor pelo conhecimento dos códigos. Por fim, a título de informação complementar, expomos um breve apanhado histórico da criptografia.

Palavras Chaves: Criptografia, Aritmética Modular, Código de César, Código Afim, Código de Vigenère, Código Hill, Código RSA, Código de Rabin, Código MH, Código ElGamal.

Abstract

The main objective of this work is to treat the modular arithmetic of whole numbers, and show evidence of some types of elementary code such as Cesar's, Afim, of Vigenere's, Hill's, RSA, Rabin's, MH and ElGamal, those found in cryptography, highlighting the mathematics which exists behind the function of each of them. We have studied the concepts of modular arithmetic and applied them to the study of matrices and determinants that are necessary for the function of these codes and for the evolution of cryptography. We also present some codes found in our day-to-day life, aiming to stimulate the curiosity of the reader into discovering these codes. Finally, for complementary information purposes, we reveal a brief collected history of cryptography.

Key words: cryptography, modular arithmetic, Caesar's code, Afim code, Vigenére's code, Hill's code, RSA code, Radin's code, MH code, ElGamal code.

Sumário

Introdução

Como surgiram os códigos? Para que servem? Qual a matemática que existe por trás desses códigos? Essas perguntas parecem não ser tão comuns assim no nosso dia a dia. No entanto, quando olhamos ao nosso redor percebemos que os códigos estão em todos os lugares. Hoje em dia muitas coisas são identificadas a partir de códigos. Ao começar estudar sobre eles, percebemos o quão antigos são. Com o avanço tecnológico e o surgimento de feixes de luz e scanners tornou-se possível transmitir dados direto e rapidamente aos computadores, criando assim condições para a utilização da codificação. Em 1952, surgiu a primeira patente de um código de barra e então com o passar do tempo esses códigos foram se modernizando até surgir o código de barras que temos hoje.

Aguçando ainda mais nossa curiosidade nos deperamos com o seguinte questionamento: Na sociedade brasileira, o que difere uma pessoa da outra? Uma provável resposta seria o nome com o qual a pessoa foi registrada, o problema é que existem várias pessoas cujo os nomes são iguais. Então como diferenciá-los diante da sociedade? Em 1968, surge o CPF (Cadastro de Pessoas Físicas) um outro tipo de código. Inicialmente criado para ser um documento de arrecadação de imposto de renda, porém hoje, é muito mais do que isso, ele é um documento formado por 11 dígitos, único e intransferível, que identifica cada pessoa e as diferem mesmo quando elas possuem o mesmo nome de registro. No entanto, não existe apenas esses dois códigos citados, com esse avanço tecnológico, outros códigos foram aparecendo, como: CNPJ, ISBN e outros.

Fazendo uma análise mais profunda desses códigos, percebemos que a preocupação que existe em todos eles é a segurança nas informações. Entretanto, avançando mais nos estudos, ficamos diante da seguinte situação (o conto a seguir foi retirado de [4]):

> *Um casal, Alice e Bob, que vivem isolados e apenas podem se comunicar através do correio. Eles sabem que o carteiro é um tremendo "fofoqueiro" e que lê todas as suas cartas. Alice tem uma mensagem para Bob e não quer que ela seja lida. Que é que pode fazer? Ela pensou em lhe enviar um cofre com a mensagem, fechado a cadeado. Mas como lhe fará chegar a chave? Não pode enviar dentro do cofre, pois assim Bob não o poderá abrir. Se enviar a chave em separado, o carteiro pode fazer uma cópia. Depois de muito pensar, ela tem uma idéia. Enviar-lhe o cofre fechado com um cadeado. Sabe que Bob é esperto e acabará por perceber a sua ideia. Com mais uma ida e uma volta do correio, e sem nunca terem trocado chaves, a mensagem chega até Bob, que abre o cofre e a lê. Como é que você acha que resolveram o problema? Pense*

bem no assunto, tente responder a questão. É simples... depois que você descobrir, é claro. O "truque" usado foi o seguinte: Bob colocou um outro cadeado no cofre e ele tinha a chave desse segundo cadeado. Devolve o cofre a Alice por correio, desta vez fechado com os dois cadeados. Alice remove o seu cadeado, com a chave que possui e reenvia o cofre pelo correio só com o cadeado colocado por Bob. É claro que Bob tem apenas que abrir o cofre, com a sua própria chave e ler a mensagem enviada pela sua amada. O carteiro não tem como saber o conteúdo do cofre.

A questão principal relatada acima é como transmitir uma mensagem da fonte A para a fonte B, de modo que as fontes não autorizadas não tenham acesso aos conteúdos da mensagem. Para existir uma comunicação segura é importante o estudo de técnicas matemáticas relacionadas com a confidencialidade, integridade e autenticação, que permita uma transformação da mensagem original em um código secreto. A partir dessa situação, percebemos que todos os outros códigos citados anteriormente tinham como única e exclusiva preocupação fazer com que a informação chegue com segurança.

Notamos que os primeiros códigos citados diferem dessa última situação. Eles fazem partes de ramos diferentes da matemática, os primeiros códigos (código de barra, CPF, CNPJ, entres outros) pertencem a teoria dos códigos enquanto essa última situação, o conto, trata-se de código secreto e pertence a criptografia.

Teoria dos códigos e Criptografia são ramos distintos e servem para propósitos diferentes. Na teoria dos códigos, como já citamos, a única preocupação é que a mensagem chegue com segurança ao seu destino. Enquanto na criptografia, a questão principal é como transmitir uma mensagem de uma fonte para outra, de modo que as fontes não autorizadas não tenham acesso a conteúdos da mensagem, utilizando diversas estratégias, regras e fórmulas que permitem a codificação e decodificação da mensagem oferecendo uma comunicação segura. Baseando-se nas pesquisas realizadas no campo dos códigos é que enfatizamos este trabalho no estudo da aritmética modular essencial no desenvolvimento dos diversos códigos de criptografia.

Dividimos este trabalho em 3 capítulos, sendo o primeiro deles tratando da matemática elementar de alguns códigos, onde trabalhamos a aritmética modular juntamente com matrizes, determinante, vetores, combinação linear, tudo de forma sucinta para entendermos as diversas maneiras de codificar e decodificar as mensagens. No segundo capítulo apresentamos vários códigos criptográficos usados nas diversas comunicações de mensagens secretas. No terceiro e último capítulo, temos alguns códigos, referentes à Teoria dos Códigos, para aguçar a curiosidade do leitor, mostrando toda matemática que existe por trás desses. Finalmente, a título de informação complementar, expomos um breve apanhado histórico da criptografia (Apêndice A).

Capítulo 1

A Matemática Elementar de Alguns Códigos

Este capítulo foi baseado nos textos [3, 5, 8, 9, 10, 11, 14] e tem por objetivo subsidiar o estudo dos códigos que serão tratados neste trabalho. Faremos, portanto, uma breve exposição dos principais conceitos matenáticos necessários. Teremos como ponto de partida a aritmética elementar, já estudada desde Euclides[1] que foi importante e norteou os criadores dos diversos códigos existentes hoje.

1.1 Divisibilidade

Definição 1.1. *Se a e b são inteiros, dizemos que a divide b, e denotamos por $a|b$, quando existir um inteiro c tal que $b = ac$. Se a não divide b escrevemos $a \nmid b$.*

Exemplo 1.2. *Pela definição, $2|6$ pois $6 = 2\times 3$; $5|10$ pois $10 = 5\times 2$ e $1|a$ $(\forall a \in \mathbb{Z})$ pois $a = 1 \times a$. No entanto, $0 \nmid b$, com $b \neq 0$, pois $0 \times c = 0 \neq b$.*

Proposição 1.3. *Considere a, b e c números inteiros. Se $a|b$ e $b|c$, então $a|c$.*

Demonstração. Como $a|b$ e $b|c$, existem inteiros k_1 e k_2 com

$$b = k_1 a \qquad \text{e} \qquad c = k_2 b.$$

Substituindo o valor de b na equação $c = k_2 b$ teremos

$$c = k_2 k_1 a,$$

o que implica existir $k = k_1 k_2$ inteiro tal que $c = ka$. Logo, $a|c$. □

Exemplo 1.4. *Como $3|12$ e $12|48$, então $3|48$.*

[1] Pouco se conhece sobre a vida e a personalidade de Euclides. Provavelmente sua formação matemática tenha se dado na escola platônica de Atenas. Ele foi professor do Museu em Alexandria. Euclides escreveu cerca de uma dúzia de tratados e um livro sobre seções cônicas; porém, mais da metade do que ele escreveu se perdeu. Os Elementos de Euclides não tratam apenas de geometria, mas também de teoria dos números e álgebra elementar. O livro é composto de quatrocentos e sessenta e cinco proposições distribuídas em treze livros ou capítulos, dos quais os seis primeiros são sobre geometria plana elementar, os três seguintes sobre teoria dos números, o livro X sobre incomensuráveis e os três últimos tratam sobre geometria no espaço. Além disso, encontramos também uma exposição da teoria das proporções numérica ou pitagórica.

Proposição 1.5. *Considere a, b, c, m e n números inteiros. Se $c|a$ e $c|b$ então $c|(ma+nb)$.*

Demonstração. Se $c|a$ e $c|b$ então

$$a = k_1 c \qquad \text{e} \qquad b = k_2 c.$$

Multiplicando-se estas duas equações respectivamente por m e n teremos

$$ma = mk_1 c \qquad \text{e} \qquad nb = nk_2 c.$$

Somando-se membro a membro obtemos

$$ma + nb = (mk_1 + nk_2)c,$$

o que nos diz que $c|(ma+nb)$. □

Exemplo 1.6. *Como $3|15$ e $3|42$, então*

$$3|(8 \times 15 - 7 \times 42).$$

Teorema 1.7. *Considere a, d e n números inteiros. A divisibilidade tem as seguintes propriedades:*

(i) $n|n$;

(ii) $d|n \Rightarrow ad|an$;

(iii) $a \neq 0$ *e* $ad|an \Rightarrow d|n$;

(iv) $1|n$;

(v) $n|0$;

(vi) $d|n$ *e* $n \neq 0 \Rightarrow |d| \leq |n|$;

(vii) $d|n$ *e* $n|d \Rightarrow |d| = |n|$;

(viii) $d|n$ *e* $d \neq 0 \Rightarrow (n/d)|n$.

Demonstração. *(i)*: Como $n = 1n$ segue da definiçaõ que $n|n$.

(ii): Se $d|n$ então $n = cd$ para algum inteiro c. Logo $an = cad$, o que conclui a demonstração.

(viii): Se $d|n$ então $n = k_1 d$ e portanto n/d é um inteiro. Como $(n/d)d = n$ segue da definição que $(n/d)|n$.

Os demais itens também são consequências imediatas da definição de divisibilidade. □

1.2 Algoritmo da Divisão de Euclides

O Algoritmo da Divisão de Euclides, que veremos a seguir, foi usado por Euclides no seu livro Elementos e estabelece uma divisão com resto. O estudo do algoritmo nesta seção se baseia no que é conhecido como Princípio da Boa Ordenação.

Princípio da Boa Ordenação

> *"Todo subconjunto não vazio dos números naturais possui um menor elemento".*

Para ilustrar o princípio, observe por exemplo que os subconjuntos

$$A = \{4, 5, 8, 9\} \quad \text{e} \quad B = \{2, 4, 6, 8, 10, \cdots\}$$

possuem como menores elementos 4 e 2, respectivamente.

Teorema 1.8. *Dados dois inteiros a e d, $d > 0$, existe um único par de inteiros q e r tais que*

$$a = qd + r, \ \textit{com}\ 0 \leq r < d \ \ (r = 0 \ \Leftrightarrow \ d|a) \tag{1.1}$$

(q é chamado de quociente e r de resto da divisão de a por d).

Demonstração.

Existência: Seja S o conjunto de todos os inteiros não-negativos que são da forma $a - dx$, com $x \in \mathbb{Z}$, isto é:

$$S = \{a - dx : x \in \mathbb{Z} \text{ e } a - dx \geq 0\}.$$

O conjunto S é não vazio. De fato, sendo $d > 0$, temos $d \geq 1$ e, portanto, considerando $x = -|a|$ obtemos

$$a - dx = a + d|a| \geq a + |a| \geq 0.$$

Logo, $a - d(-|a|) \in S$. Agora, sendo S não vazio, pelo Princípio da Boa Ordenação, existe o elemento mínimo r de S e um número inteiro q tal que

$$r \geq 0 \quad \text{e} \quad r = a - dq,$$

ou seja, $a = dq + r$ com algum $q \in \mathbb{Z}$. Além disso, temos $r < d$. De fato, se fosse $r \geq d$ teríamos

$$0 \leq r - d = a - dq - d = a - d(q + 1) < r.$$

Dessa forma, obteríamos $r - d \in S$ de modo que r não seria o elemento mínimo de S. Portanto, temos garantida a parte da existência de (1.1).

Unicidade: Para demonstrar a unicidade de q e r, suponhamos que existem dois outros inteiros q_1 e r_1 tais que

$$a = dq_1 + r_1 \quad \text{e} \quad 0 \leq r_1 < d.$$

Então, teremos:

$$dq_1 + r_1 = dq + r \quad \Rightarrow \quad r_1 - r = d(q - q_1) \quad \Rightarrow \quad d|(r_1 - r).$$

Por outro lado, temos

$$-d < -r \leq 0 \quad \text{e} \quad 0 \leq r_1 < d,$$

que implica

$$-d < r_1 - r < d,$$

ou seja,

$$|r_1 - r| < d.$$

Assim, $d|(r_1 - r)$ e $|r_1 - r| < d$. Logo, $r_1 - r = 0$. Além disso, como $d \neq 0$ e agora $q_1 d = qd$, segue que $q = q_1$. Logo, $r_1 = r$ e $q_1 = q$. □

Corolário 1.9 (**Algoritmo da Divisão de Euclides**). *Se a e d são dois inteiros com $d \neq 0$, então existem números inteiros q e r, e são únicos, tais que*

$$a = dq + r, \quad 0 \leq r < |d|.$$

Demonstração. Se $d > 0$, a conclusão é obtida do Teorema 1.8. Agora, se $d < 0$ então $|d| > 0$, novamente pelo Teorema 1.8, existem únicos inteiros q_1 e r tais que

$$a = |d|q_1 + r, \quad 0 \leq r < |d|.$$

Neste caso, note que $|d| = -d$, de modo que

$$a = d(-q_1) + r, \ 0 \leq r < |d|.$$

Portanto, existem únicos inteiros $q = -q_1$ e r tais que

$$a = dq + r, \ 0 \leq r < |d|.$$

□

Os inteiros a, d, q e r são chamados respectivamente de dividendo, divisor, quociente e resto da divisão de a por d.

Exemplo 1.10. *Achar o quociente q e o resto r na divisão de $a = -83$ por $b = 12$ que satisfazem as condições do algoritmo da divisão.*

Efetuando a divisão usual dos valores absolutos de a e b, obtemos

$$83 = 12 \times 6 + 11,$$

ou ainda,

$$-83 = 12 \times (-6) - 11.$$

Como o termo $r = -11 < 0$ não satisfaz a condição $0 \leq r < 12$, então somando e subtraindo o valor $b = 12$ ao segundo menbro da igualdade anterior, obtemos

$$-83 = 12 \times (-6) - 12 + 12 - 11 = 12 \times (-7) + 1.$$

Logo, como $0 \leq r = 1 < 12$, o quociente é $q = -7$ e o resto é $r = 1$.

1.3 O Máximo Divisor Comum

O livro VII da obra "Os Elementos" de Euclides começa com o processo para achar o máximo divisor comum de dois ou mais números inteiros, hoje conhecido como algoritmo euclidiano, e o usa para verificar se dois inteiros são *primos entre si*.

Definição 1.11. *Sejam a e b dois inteiros não conjuntamente nulos ($a \neq 0$ ou $b \neq 0$). Chama-se Máximo Divisor Comum de a e b um número inteiro positivo d ($d > 0$) que satisfizer às seguintes condições:*

(1) $d|a$ e $d|b$;

(2) se $c|a$ e $c|b$, então $c|d$.

Observe-se que, pela condição (1), d é um divisor comum de a e b e, pela condição (2), d é o maior dentre todos os divisores comuns de a e b. O Máximo Divisor Comum de a e b é denotado pela notação $mdc(a, b)$[2].

Por exemplo, sejam $a = 6$ e $b = 8$. Indicando por D_x o conjunto dos divisores de $x \in \mathbb{Z}$, temos

$$D_6 = \{-6, -3, -2, -1, 1, 2, 3, 6\} \quad \text{e} \quad D_8 = \{-8, -4, -2, -1, 1, 2, 4, 8\},$$

de modo que

$$D_6 \cap D_8 = \{-1, -2, 1, 2\}.$$

Agora observamos que:

1) $2|6, 2|8$;

2) se $c|6$ e $c|8$, então c pode ser $-1, -2, 1, 2$. No entanto, 2 é máximo divisor comum de 6 e 8.

Logo, o $mdc(6, 8) = 2$.

É imediato observar que:

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

Em particular, convencionamos:

- $mdc(0, 0) = 0$.

Note que nesse último caso o máximo divisor comum não é o maior dos divisores comuns: como $1|0, 2|0, 3|0, ...$ não há um maior divisor comum para 0 e 0; isso é apenas uma convenção adequada. Além disso, temos:

- $mdc(a, 1) = 1$;
- se $a \neq 0$, então o $mdc(a, 0) = |a|$;

[2]Na literatura é comum usa-se a notação para $mdc(a, b)$ simplesmente como (a, b)

- $mdc(a, b)$.

Exemplo 1.12.

a) $mdc(8, 1) = 1$

b) $mdc(-3, 0) = |-3| = 3$

c) $mdc(-6, 12) = |-6| = 6$

Proposição 1.13. *Se $a|b$, então $mdc(a, b) = |a|$.*

Demonstração. De fato, $|a||a$ e $|a||b$ (segue da definição de divisibiladade e da hipótese). Além disso, para $c > 0$, se $c|a$ e $c|b$, é óbvio que $c||a|$. □

Proposição 1.14. *Se $a = bq + r$ e $d = mdc(a, b)$, então $d = mdc(b, r)$. Além disso, se $d = mdc(b, r)$, então $d = mdc(a, b)$.*

Demonstração. Como $d = mdc(a, b)$, então $d|a$ e $d|b$. Dessa última relação resulta que $d|bq$. Logo

$$d|(a - bq),$$

ou seja, $d|r$. Por outro lado, se $c|b$ e $c|r$, então

$$c|(bq + r).$$

Como $bq + r = a$, então $c|a$ e $c|b$, o que implica $c|d$, pois $d = mdc(a, b)$.

A segunda afirmação se prova de maneira análoga. □

Retornaremos agora a questão da existência de máximo divisor comum. Para provar a existência aplicaremos, sucessivamente, a partir de a e b, o algoritmo da divisão da seguinte maneira:

$$\begin{aligned} a &= bq_1 + r_1 \qquad (0 \leq r_1 < |b|) \\ b &= r_1q_2 + r_2 \qquad (0 \leq r_2 < r_1) \\ r_1 &= r_2q_3 + r_3 \qquad (0 \leq r_3 < r_2) \\ &\vdots \end{aligned} \tag{1.2}$$

É claro que, se acontecer de r_1 ser nulo, então a Proposição 1.13 nos garante que $|b| = mdc(a, b)$ e o processo termina na primeira etapa. Mas, de qualquer maneira, na sequência

$$|b| > r_1 > r_2 > r_3 > ...$$

deverá ocorrer $r_{n+1} = 0$, para algum índice n. De fato, se todos os r_i fossem não nulos, então

$$\{|b|, r_1, r_2, ...\}$$

não possuiria um menor elemento, o que contraria o Princípio da Boa Ordenação. Assim, para algum n;

$$r_{n-2} = r_{n-1}q + r_n$$

$$r_{n-1} = r_n q_{n+1}.$$

Como consequência das Proposições 1.13 e 1.14, obtém-se então o seguinte:

$$r_n = mdc(r_{n-1}, r_n) = mdc(r_{n-2}, r_{n-1}) = ... = mdc(b, r_1) = mdc(a, b),$$

ou seja,

$$r_n = mdc(a, b).$$

Observe que a demonstração da existência de mdc é construtiva. O dispositivo prático que costuma ser empregado para aplicá-lo na prática é conhecido como **processo das divisões sucessivas** ou **algoritmo de Euclides**. É usual a seguinte organização em forma de tabela desse dispositivo de cálculo de $mdc(a, b)$:

	q_1	q_2	q_3		q_n	q_{n+1}
a	b	r_1	r_2	$\ldots$	r_{n-1}	r_n
r_1	r_2	r_3	r_4		0	

A tabela se traduz na seguinte regra: para se "achar" o $mdc(a, b)$, dividi-se a por b e encontra-se o "primeiro" resto r_1. O "segundo" resto r_2 é obtido pela divisão de b por r_1. O terceiro resto r_3 é obtido pela divisão de r_1 por r_2, e assim sucessivamente até encontrar um resto nulo. O último resto não nulo é o máximo divisor comum procurado.

Exemplo 1.15. *Achar o* $mdc(630, 22)$ *pelo algoritmo de Euclides. Temos, sucessivamente:*

$$630 = 22 \times 28 + 14$$

$$22 = 14 \times 1 + 8$$

$$14 = 8 \times 1 + 6$$

$$8 = 6 \times 1 + \boxed{2}$$

$$6 = 2 \times 3 + 0$$

Logo, $2 = mdc(630, 22)$. *Usualmente procede-se assim:*

	28	1	1	1	3
630	22	14	8	6	2
14	8	6	$\boxed{2}$	0	

Portanto, o $mdc(630, 22) = 2$.

O algoritmo de Euclides também pode ser usado para achar expressão do $mdc(a, b) = r_n$ como combinação linear de a e b, ou seja, é possível encontrar números inteiros x e y tais que

$$mdc(a, b) = ax + by. \tag{1.3}$$

Para encontrar os números x e y basta eliminar sucessivamente os restos

$$r_{n-1}, r_{n-2}, \ldots, r_3, r_2, r_1$$

entre as n primeiras igualdades de (1.2).

Exemplo 1.16. *Achar expressão do* $mdc(630, 22)$ *como combinação linear de* 630 *e* 22. *Como no Exemplo 1.15:*

$$\begin{aligned} 630 &= 22 \times 28 + 14 \\ 22 &= 14 \times 1 + 8 \\ 14 &= 8 \times 1 + 6 \\ 8 &= 6 \times 1 + 2 \\ 6 &= 2 \times 3. \end{aligned} \tag{1.4}$$

Logo, $2 = mdc(630, 22)$. *Agora, para obter* $2 = mdc(630, 22)$ *como combinação linear de* 630 *e* 22 *basta eliminar os restos* 6, 8 *e* 14 *entre as quatro primeiras igualdades de* (1.4), *do seguinte modo:*

$$\begin{aligned} 2 &= 8 - 6 \times 1 \\ &= 8 - (14 - 8 \times 1) \\ &= -14 + 8 \times 2 \\ &= -14 + 2(22 - 14 \times 1) \\ &= 2 \times 22 - 3 \times 14 \\ &= 2 \times 22 - 3 \times (630 - 28 \times 22) \\ &= 630(-3) + 22(86), \end{aligned}$$

isto é,

$$2 = mdc(630, 22) = 630x + 22y$$

onde $x = -3$ *e* $y = 86$.

A representação do inteiro $2 = mdc(630, 22)$ *como combinação linear de* 630 *e* 22 *não é única. Observe, por exemplo, que somando e subtraindo o produto* 630×22 *ao segundo membro da igualdade:*

$$2 = 630(-3) + 22(86);$$

obtemos:

$$2 = 630(-3 + 22) + 22(86 - 630) = 630 \times 19 + 22 \times (-544),$$

que é uma outra representação do inteiro $2 = mdc(630, 22)$ *como combinação linear de* 630 *e* 22.

Definição 1.17. *Dois números inteiros* a *e* b *se dizem primos entre si se* $mdc(a, b) = 1$. *Neste caso diz-se também que* a *é primo com* b *ou vice-versa.*

Exemplo 1.18. *Dois números consecutivos* a *e* $a + 1$ *são sempre primos entre si. De fato, é claro que* $1|a$ *e* $1|(a + 1)$. *Agora, se* $c|a$ *e* $c|(a + 1)$, *então*

$$c|[(a + 1) - a],$$

ou seja, $c|1$.

Proposição 1.19. *Se $d = mdc(a, b)$, então $mdc(sa, sb) = |s|d$, para todo $s \in \mathbb{Z}$.*

Demonstração. Multipliquemos por $|s|$ cada uma das igualdades obtidas pelo algoritmo da divisão no processo das divisões sucessivas que leva a d, a partir de $|a|$ e $|b|$:

$$\begin{aligned}
|s||a| &= (|s||b|)q_1 + |s|r_1 \\
|s||b| &= (|s|r_1)q_2 + |s|r_2 \\
&\vdots \\
|s|r_{n-2} &= (|s|r_{n-1})q_n + |s|r_n \\
|s|r_{n-1} &= (|s|r_n)q_{n+1}.
\end{aligned}$$

As Proposições 1.13 e 1.14 nos garantem então que

$$|s|d = |s|r_n = mdc(|s|r_{n-1}, |s|r_n) = ... = mdc(|s||b|, |s|r_1) = mdc(|s||a|, |s||b|).$$

Portanto,

$$|s|d = mdc(|s||a|, |s||b|) = mdc(|sa|, |sb|) = mdc(sa, sb).$$

□

Corolário 1.20. *Se $a, b \in \mathbb{Z} \setminus \{0\}$ e $d = mdc(a, b)$, temos que $mdc\,(a/d, b/d) = 1$. Em outras palavras, a/d e b/d são primos entre si.*

Demonstração. Como

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

e $d \neq 0$, então:

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

□

Corolário 1.21. *Sejam $a, b, c \in \mathbb{Z}$. Se $a|bc$ e $mdc(a, b) = 1$, então $a|c$.*

Demonstração. Por hipótese $mdc(a, b) = 1$. Usando a Proposição 1.19, que

$$mdc(ac, bc) = |c|.$$

Por hipótese $a|bc$, e obviamente $a|ac$. Então, $a|mdc(ac, bc)$. Portanto, $a|c$. □

Corolário 1.22. *Sejam $a, b, c \in \mathbb{Z}$. Se a e b são divisores de c e $mdc(a, b) = 1$, então $ab|c$.*

Demonstração. De $mdc(a, b) = 1$ decorre, em virtude da Proposição 1.19, que $mdc(ac, bc) = |c|$. Por hipótese, $a|c$ e $b|c$. Assim,

$$ab|cb \qquad \text{e} \qquad ab|ac.$$

Logo ab divide $mdc(ac, bc)$. Portanto, $ab|c$. □

Exemplo 1.23. *Para que um número seja divisível por* 6 *é necessário e sufuciente que seja divisível por* 2 *e por* 3 *pois o* $mdc(2,3) = 1$.

A definição de máximo divisor comum pode ser estendida de maneira óbvia para três ou mais números. Para o cálculo do máximo divisor comum de três números, por exemplo, pode-se lançar mão do seguinte resultado:

$$mdc(a,b,c) = mdc(mdc(a,b),c) = mdc(a,mdc(b,c))$$

Provemos a primeira dessas igualdades. Seja $d = mdc(a,b,c)$. Então $d|a$, $d|b$ e $d|c$. Das duas primeiras dessas relações segue que $d|mdc(a,b)$. Assim,

$$d|mdc(a,b) \qquad \text{e} \qquad d|c.$$

Seja, agora, k um divisor de $d_1 = mdc(a,b)$ e de c. Como $d_1|a$ e $d_1|b$, pela transitividade conclui-se que $k|a$, $k|b$ e $k|c$. Logo $k|d$ pois $d = mdc(a,b,c)$. A demonstração fica completa considerando-se a unicidade do máximo divisor comum.

Exemplo 1.24. *Achemos o* $mdc(6,8,20)$. *Usando o Algorítmo de Euclides temos*

	1	3
8	6	2
$\boxed{2}$	0	

Logo, $mdc(2,20) = 2$, *pois* $2|20$. *Então,*

$$mdc(6,8,20) = 2.$$

1.4 Mínimo Múltiplo Comum

No caso de um número inteiro a dividir um inteiro b dizemos também que o número b é *Múltiplo* de a.

Definição 1.25. *Um número natural* m *é dito Mínimo Múltiplo Comum de dois números inteiros* a *e* b *quando:*

(1) $a|m$ *e* $b|m$;

(2) para qualquer $k > 0$, *se* $a|k$ *e* $b|k$, *então* $m|k$.

Observe-se que, em linguagem literal, a condição (1) da definição diz que m é múltiplo tanto de a quanto de b; enquanto que a condição (2) diz que todo múltiplo positivo de a e de b é também múltiplo de m, que caracteriza a nomenclatura "mínimo". Note ainda que se m e n satisfazem a definição, então pela condição (2) da definição temos $m|n$ e $n|m$. Logo, $m = n$ e concluímos que o mínimo múltiplo comum, se existir, deve ser único. Usaremos a notação $m = mmc(a,b)$ para representar o Mínimo Múltiplo Comum. Da definição decorre diretamente que

- $mmc(a,b) = mmc(b,a)$;

- $mmc(|a|, |b|) = mmc(a, b)$;

Por exemplo, sejam $a = -6$ e $b = 8$. Indicando por M_x o conjunto dos multiplos de $x \in \mathbb{Z}$, temos

$$M_{-6} = \{\cdots, -12, -6, 0, 6, 12, 18, 24, \cdots\} \quad \text{e} \quad M_8 = \{\cdots, -16, -8, 0, 8, 16, 24, \cdots\},$$

de modo que

$$M_{-6} \cap M_8 = \{\cdots - 72, -48, -24, 0, 24, 48, \cdots\}.$$

Agora observamos que:

1) $-6|24, 8|24$;

2) se $-6|n$ e $8|c$, então c deve ser $24, 48, 72, ...$ No entanto, 24 é menor múltiplo comum positivo de -6 e 8.

Logo, o $mdc(-6, 8) = 24$.

Quanto à existência de mínimo múltiplo comum, consideremos inicialmente o caso $a = 0$ e b qualquer. Devemos então concluir que $mmc(0, b) = 0$. De fato:

- $0|0$ e $b|0$ (note que $0 = b0$.)
- $0|m'$ e $b|m' \to 0|m'$

Para os demais casos a garantia de existência é dada pela proposição seguinte.

Proposição 1.26. *Sejam $a, b \in \mathbb{Z}$. Então,*

$$mmc(a, b) \cdot mdc(a, b) = |ab|.$$

Demonstração. Vamos primeiro considerar $a, b \in \mathbb{N}$ e $d = mdc(a, b)$. Desde que $d|a$ e $d|b$, tem-se $d|ab$. Então, $m = ab/d \in \mathbb{N}$, além de $a/d, b/d \in \mathbb{N}$. Assim:

- como
$$a\frac{b}{d} = \frac{ab}{d} = m,$$
então $a|m$. Analogamente se mostra que $b|m$.

- Seja m' um múltiplo de a e de b. Logo, existem $r, s \in \mathbb{Z}$ tais que $m' = ar$ e $m' = bs$. Então $ar = bs$ e, portanto,
$$\frac{a}{d}r = \frac{b}{d}s.$$
Daí segue que a/d divide $(b/d)s$. Como $mdc\,(a/d, b/d) = 1$, temos que $(a/d)|s$ (Corolário 1.21 - Proposição 1.19). Assim,
$$s = \frac{a}{d}t$$
para algum $t \in \mathbb{Z}$. Desde que $m' = bs$, obtemos
$$m' = b\frac{a}{d}t = \frac{ab}{d}t = mt,$$
ou seja, $m|m'$.

Portanto, por definição, $m = mmc(a, b)$.

Para o caso $a, b \in \mathbb{Z}$, basta notar que

$$mdc(a, b) = mdc(|a|, |b|) \qquad \text{e} \qquad mmc(a, b) = mmc(|a|, |b|),$$

pois teremos

$$mdc(a, b) \cdot mmc(a, b) = mdc(|a|, |b|) \cdot mmc(|a|, |b|) = |a||b| = |ab|.$$

□

Corolário 1.27. *Se a e b são primos entre si, então $mmc(a, b) = |ab|$.*

Demonstração. De fato, como $d = mdc(a, b) = 1$, então $mmc(a, b) = |ab|$. □

Observação 1.28. *Sejam $a, b \in \mathbb{N} \setminus \{0\}$. Pelo que foi visto, $\dfrac{ab}{d} = m \in M_a \cap M_b$. Mas $0 \in M_a \cap M_b$ e como $m > 0$, então m não é o menor dos múltiplos comuns de a e b. Na verdade, neste caso $m = mmc(a, b)$ é o menor dos múltiplos comuns não nulos de a e b.*

Exemplo 1.29. *Vamos usar a proposição anterior para achar $mmc(20, 8)$. Calculando o mdc, temos*

	2	2
20	8	4
4	0	

.

Então

$$mmc(20, 8) = \frac{20 \times 8}{4} = 40.$$

Proposição 1.30. *Se $m = mmc(a, b)$, então $mmc(sa, sb) = |s|m$ para qualquer $s \in \mathbb{Z}$.*

Demonstração. Quando $a = 0$ ou $b = 0$, então $m = 0$ e $sa = 0$ e $sb = 0$; daí $mmc(sa, sb) = 0 = sm$. Se $s = 0$, ficamos com $mmc(0, 0) = 0$ e o resultado também é verdadeiro.

Suponhamos a, b e s não nulos. Então, pela duas proposições anteriores:

$$mmc(sa, sb) = \frac{|sasb|}{mdc(sa, sb)} = \frac{s^2|ab|}{|s| \cdot mdc(a, b)} = \frac{|sab|}{mdc(a, b)} = |s| \cdot mmc(a, b).$$

□

Generalização: A extensão do conceito de mínimo múltiplo comum em $\mathbb{N}$ para 3 ou mais números se faz naturalmente. No caso de 3 número, por exemplo, o cálculo pode ser feito com base na seguinte propriedade cuja demonstração é imediata:

$$mmc(a, b, c) = mmc(a, mmc(b, c)) = mmc(mmc(a, b), c).$$

Por exemplo:

$$mmc(3, 5, 20) = mmc(mmc(3, 5), 20) = mmc(15, 20) = 60.$$

1.5 Números Primos

A noção de numero primo foi, provavelmente, introduzida por Pitágoras, aproximadamente 530 AC. A escola pitagórica dava grande importância ao número um, que era chamada de unidade (em grego: Monad). Os demais números inteiros naturais - o 2, 3, 4, etc - tinham caráter subalterno, sendo vistos como meras multiplicidades geradas pela unidade e por isso recebiam a denominação de número (em grego: Arithmos). Entretanto, a preocupação com a geração dos números não parava por aí. Pitágoras teria atinado que existem dois tipos de arithmós:

- Os protoi arithmós (números primários ou primos), que são aqueles que não podem ser gerados, através da multiplicação, por outros arithmós, como é o caso de $2, 3, 5, 7....$
- Os deuterói arithmós (números secundários), podem ser gerados por outros arithmós, por exemplo, $4 = 2.2, 6 = 3.2$, etc.

A noção de primo fora, muito provavelmente, introduzida por Pitágoras. É impossível ter completa segurança nessa atribuição, pois Pitágoras não deixou nenhum registro escrito de seus trabalhos e os documentos mais antigos que temos falando de suas ideias resumem-se a pequenos fragmentos de textos escritos várias gerações após ele. Entretanto, esses fragmentos, apesar de conterem informações muito escassas, são unânimes em afirmar que Pitágoras iniciou o estudo de números primos. O mais antigo livro de matemática que chegou completo aos nossos dias e que desenvolve sistematicamente o estudo de números primos e Os Elementos de Euclides. Como se sabe, Euclides seguiu muito de perto as orientações matemáticas dos pitagóricos. Assim, não é surpreendente que, no capítulo de sua obra em que trata da teoria dos números, ele defina número primo de um modo absolutamente compatível com as ideias pitágoricas expostas acima. Em Os Elementos, Vol. VII, Definição 11, há: *"protós arithmós estin monadi mone metroymenos"*, que significa "Número primo é todo aquele que só pode ser medido através da unidade".

Definição 1.31. *Diz-se que um número inteiro p é um Número Primo, ou apenas um primo, quando $|p| > 1$, e 1 e $|p|$ são seus únicos divisores positivos. Um inteiro diferente de 1 e que não é primo diz-se composto.*

Teorema 1.32. *Se um número primo p não divide um inteiro a, então a e p são relativamente primos (primos entre si).*

Demonstração. Seja $d = mdc(a, p)$. Então $d|a$ e $d|p$. Da relação $d|p$, resulta que $d = 1$ ou $d = |p|$, porque p é primo. Como $d = |p|$ é impossível, porque p não divide a, segue-se que $d = 1$, isto é, o $mdc(a, p) = 1$. Logo, a e p são relativamente primos. □

Corolário 1.33. *Se p é um primo tal que $p|ab$, então $p|a$ ou $p|b$ (podendo ser fator de ambos, a e b).*

Demonstração. Se $p|a$, não há o que demonstrar. Suponha que p não divide a. Então, pelo teorema anterior, temos $mdc(p, a) = 1$. Logo, $p|b$, pelo Corolário 1.21. □

Corolário 1.34. *Se p é um primo tal que $p(|a_1a_2a_3\ldots a_n)$, então existe um índice k, com $1 \leq k \leq n$ tal que $p|a_k$.*

Demonstração. Usando Indução, a proposição é verdadeira para $n = 1$ (imediato) e para $n = 2$ (pelo Corolário 1.20). Assim, suponhamos $n > 2$ e que: se p divide um produto com menos de n fatores, então p divide pelo menos um dos fatores (hipótese de indução). Logo, pelo Corolário 1.33, se $p|(a_1a_2\ldots a_{n-1})$, então $p|a_n$ ou $(p|a_1a_2\ldots a_{n-1})$. Se $p|a_n$, a proposição está demonstrada. Porém, se $p|a_1a_2\ldots a_{n-1}$, então a hipótese de indução assegura que $p|a_k$, com algum $1 \leq k \leq n-1$. Em qualquer dos casos, p divide um dos inteiros $a_1, a_2, a_3, \ldots, a_n$. □

Corolário 1.35. *Se os inteiros $p, q_1, q_2, \ldots, q_n$ são todos primos e $p|(q_1q_2\ldots q_n)$, então existe um índice k, com $1 \leq k \leq n$, tal que $p = q_k$.*

Demonstração. De fato, pelo Corolário 1.34, existe um índice k, com $1 \leq k \leq n$, tal que $p|q_k$. Como os únicos divisores positivos de q_k são 1 e $|q_k|$, porque q_k é primo, segue-se que $p = 1$ ou $p = q_k$. Mas, $|p| > 1$, porque p é primo. Logo, $p = q_k$. □

Teorema 1.36. *Todo inteiro composto possui um divisor primo.*

Demonstração. Seja a um inteiro composto. Consideremos o conjunto A de todos os divisores positivos de a, exceto os divisores 1 e a, isto é:

$$A = \{x : x|a \quad \text{e} \quad 1 < x < a\}.$$

Pelo "Princípio da Boa Ordenação" existe o elemento mínimo p de A, que vamos mostrar ser primo. De fato, se p fosse composto admitiria pelo menos um divisor d tal que $1 < d < p$, e então $d|p$ e $p|a$, o que implica $d|a$, isto é, p não seria o elemento mínimo de A, se fosse composto. Logo, p é primo. □

Teorema 1.37 (Teorema Fundamental da Aritmética)**.** *Todo inteiro positivo $n > 1$ é igual a um produto de fatores primos.*

Demonstração. Mostraremos a existência da fatoração por indução. Se n é primo não há o que provar (escrevemos $m = 1, p_1 = n$). Se n é composto podemos escrever $n = ab$, $a, b \in \mathbb{N}, 1 < a < n, 1 < b < n$. Por hipótese de indução, a e b se decompõem como produto de primos. Juntando as fatorações de a e b (e reordenando os fatores) obtemos uma fatoração de n. □

Corolário 1.38. *A decomposição de um inteiro positivo $n > 1$ como produto de fatores primos é única, a menos da ordem dos fatores.*

Demonstração. Suponha que

$$n = p_1 \ldots p_m = q_1 \ldots q_r$$

com, $p_1 \leq \ldots \leq p_m$, $q_1 \leq \ldots \leq q_r$. Como $p_1|q_1 \ldots q_r$ temos $p_1|q_i$ para algum valor de i. Como q_i é primo, $p_1 = q_i$ e $p_1 \geq q_1$. Analogamente temos $q_1 \leq p_1$, donde $p_1 = q_1$. Mas por hipótese de indução

$$\frac{n}{p_1} = p_2 \ldots p_m = q_2 \ldots q_r$$

admite uma única fatoração, donde $m = r$ e $p_i = q_i$ para todo i. □

Corolário 1.39. *Todo inteiro positivo $n > 1$ admite uma única decomposição da forma*

$$n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$$

onde, para $i = 1, 2, \dots, r$ cada k_i é um inteiro positivo e cada p_i é um primo, com

$$p_1 < p_2 < \dots < p_r,$$

denominada decomposição canônica do inteiro positivo $n > 1$.

Demonstração. Pelo Corolário 1.38, n é um produto de fatores primos $q_1 q_2 \dots q_m$, com $q_1 \leq q_2 \leq \dots \leq q_m$ $(m \geq 1)$. Agrupando-se os fatores primos repetidos na forma de potências de primos, temos a representação enunciada e tal representação é única. □

1.6 Congruência

Definição 1.40. *Dados a e b números inteiros, dizemos que a é congruente a b módulo $m (m > 0)$ quando $m|(a - b)$, e denotamos por*

$$a \equiv b (\text{mod } m).$$

Se $m \nmid (a - b)$, dizemos que a é incongruente a b módulo m e denotamos

$$a \not\equiv b (\text{mod } m).$$

Exemplo 1.41. $11 \equiv 3 (\text{mod } 2)$ *pois* $2|(11 - 3)$. *Como* $5 \nmid 6$ *e* $6 = 17 - 11$ *temos que* $17 \not\equiv 11 (\text{mod } 5)$.

Observação 1.42.

1. *Dois inteiros quaisquer são congruentes módulo* 1.
2. *Dois inteiros são congruentes módulo* 2, *se ambos são pares ou ambos são ímpares.*
3. $a \equiv 0 (\text{mod} - m)$ *se, e somente se,* $m|a$.

Proposição 1.43. *Se a e b são inteiros, temos que $a \equiv b (\text{mod } m)$ se, e somente se, existir um inteiro k tal que $a = b + km$.*

Demonstração. Se $a \equiv b (\text{mod } m)$, então $m|(a - b)$ o que implica na existência de um inteiro k tal que $a - b = km$, isto é,

$$a = b + km.$$

A recíproca também é simples pois se existe k satisfazendo $a = b + km$, temos $km = a - b$, então $m|(a - b)$ e, portanto, $a \equiv b (\text{mod } m)$. □

Proposição 1.44. *Se a, b, m e d são inteiros, $m > 0$, as seguintes sentenças são verdadeiras:*

(i) $a \equiv a (\text{mod } m)$ *(Propriedade reflexiva),*

(ii) *se* $a \equiv b (\mathrm{mod}\ m)$ *, então* $b \equiv a (\mathrm{mod}\ m)$ *(Propriedade simétrica),*

(iii) *se* $a \equiv b (\mathrm{mod}\ m)$ *e* $b \equiv d (\mathrm{mod}\ m)$*, então* $a \equiv d (\mathrm{mod}\ m)$ *(Propriedade transitiva).*

Demonstração. **(i)** Como $m|0$, então $m|(a-a)$, o que implica $a \equiv a (\mathrm{mod}\ m)$.

(ii) Se $a \equiv b (\mathrm{mod}\ m)$, então $a = b + k_1 m$ para algum inteiro k_1. Logo $b = a - k_1 m$, o que implica, pela Proposição 1.43, $b \equiv a (\mathrm{mod}\ m)$.

(iii) Se $a \equiv b (\mathrm{mod}\ m)$ e $b \equiv d (\mathrm{mod}\ m)$, então existem inteiros k_1 e k_2 tais que $a - b = k_1 m$ e $b - d = k_2 m$. Somando-se, membro a membro, estas últimas equações, obtemos $a - d = (k_1 + k_2)m$, o que implica $a \equiv d (\mathrm{mod}\ m)$.

□

Esta proposição nos diz que a relação de congruência, definida no conjunto dos inteiros, é uma relação de equivalência, pois acabamos de provar que ela é reflexiva, simétrica e transitiva.

Teorema 1.45. *Se* a, b, c, d *e* m *são inteiros tais que* $a \equiv b (\mathrm{mod}\ m)$ *e* $c \equiv d (\mathrm{mod}\ m)$*, então*

(i) $a + c \equiv b + d (\mathrm{mod}\ m)$.

(ii) $a - c \equiv b - d (\mathrm{mod}\ m)$

(iii) $ac \equiv bd (\mathrm{mod}\ m)$.

Demonstração. **(i)** De $a \equiv b (\mathrm{mod}\ m)$ e $c \equiv d (\mathrm{mod}\ m)$ temos $a - b = km$ e $c - d = k_1 m$. Somando-se membro a membro obtemos

$$(a + c) - (b + d) = (k + k_1)m$$

e isso implica $a + c \equiv b + d (\mathrm{mod}\ m)$.

(ii) Basta subtrair membro a membro $a - b = km$ e $c - d = k_1 m$ obtemos

$$(a - b) - (c - d) = (a - c) - (b - d) = (k - k_1)m$$

o que implica $a - c \equiv b - d (\mathrm{mod}\ m)$.

(iii) Multiplicamos ambos os lados de $a - b = km$ por c e ambos os lados de $c - d = k_1 m$ por b, obtendo

$$ac - bc = ckm \qquad \text{e} \qquad bc - bd = bk_1 m.$$

Basta, agora, somar membro a membro as últimas igualdades obtendo

$$ac - bc + bc - bd = ac - bd = (ck + bk_1)m,$$

o que implica $ac \equiv bd (\mathrm{mod}\ m)$.

□

Teorema 1.46. *Se a, b, c e m são inteiros e $ac \equiv bc \pmod{m}$, então $a \equiv b \pmod{m/d}$ onde $d = mdc(c, m) \neq 0$.*

Demonstração. Da hipótese $ac \equiv bc \pmod{m}$, existe um inteiro k tal que

$$ac - bc = c(a - b) = km.$$

Se dividirmos os dois membros por d, teremos $(c/d)(a - b) = k(m/d)$. Logo

$$(m/d)|(c/d)(a - b).$$

Pelo Corolário 1.20, tem-se $mdc(m/d, c/d) = 1$. Então, pelo Corolário 1.21, $(m/d)|(a - b)$, o que implica

$$a \equiv b \pmod{m/d}.$$

□

Definição 1.47 (Inverso aditivo)**.** *Dados números inteiros a, b e $m > 0$, diz-se que b é um Inverso Aditivo de a módulo m quando $a + b \equiv 0 \bmod m$.*

Definição 1.48 (Inverso multiplicativo)**.** *Dados números inteiros a, b e $m > 0$, diz-se que b é um Inverso Multiplicativo de a módulo m quando $ab \equiv 1 \bmod m$.*

Observação 1.49. *Note que, se $mdc(a, m) = 1$, entao a possui um único inverso multiplicativo módulo m. De fato, suponha*

$$ab \equiv 1 \bmod m \qquad e \qquad ac \equiv 1 \bmod m.$$

Então, exitem números inteiros k_1 e k_2 tais que

$$ab - 1 = k_1 m \qquad e \qquad ac - 1 = k_2 m.$$

Logo

$$ab - ac = (k_1 + k_2)m,$$

de modo que $m|a(b - c)$. Agora, como por hipótese $mdc(a, m) = 1$, aplicando o Corolário 1.21, obtemos que $m|(b - c)$, que significa $b \equiv c \bmod m$ (isto é, b e c são iguais módulo m).

Definição 1.50. *Se h e k são dois inteiros com $h \equiv k \pmod{m}$, dizemos que k é um resíduo de h módulo m.*

Definição 1.51. *Um conjunto de inteiros $\{r_1, r_2, \ldots, r_s\}$ é um sistema completo de resíduos módulo m quando:*

1. *$r_i \not\equiv r_j \pmod{m}$ para $i \neq j$,*
2. *para todo inteiro n, existe um r_i tal que $n \equiv r_i \pmod{m}$.*

Exemplo 1.52. *O conjunto $\{0, 1, 2, \ldots, m - 1\}$ é um sistema completo de resíduos módulo m.*
Solução: *Com efeito:*

1. *Sejam* $i, j \in \{0, 1, 2, \ldots, m-1\}$, *digamos que com* $i < j$. *Temos que* $j \not\equiv i \pmod{m}$ *pois, se* $j \equiv i \pmod{m}$, *então pela definição existiria um número* k *tal que* $j - i = km$ *(note que* $k > 0$*), que implicaria dizer que* $j \geq m$.

2. *Seja* $n \in \mathbb{Z}$. *Pelo Algoritmo da Divisão de Euclides (Corolário 1.9), existem* $q, r \in \mathbb{Z}$, *com* $0 \leq r < m$ *tal que* $n = qm + r$. *Logo,* $n \equiv r \pmod{m}$.

Portanto, $\{0, 1, 2, \ldots, m-1\}$ *é um sistema completo de resíduos módulo* m.

Teorema 1.53. *Se* k *inteiros* $r_1, r_2, \ldots, r_k$ *formam um sistema completo de resíduos módulo* m *então* $k = m$.

Demonstração. Pelo Exemplo 1.52, o conjunto $\{0, 1, 2, \ldots, m-1\}$ é um sistema completo de resíduos módulo m. Dessa forma, concluímos que cada r_i é congruente a exatamente um dos i, o que nos garante $k \leq m$. Como o conjunto $r_1, r_2, \ldots, r_k$ forma, por hipótese, um sistema completo de resíduos módulo m, cada i é congruente a exatamente um dos r_i e portanto $m \leq k$. Assim, $k = m$. □

Teorema 1.54. *Se* $r_1, r_2, \ldots, r_m$ *é um sistema completo de resíduos módulo* m *e* a *e* b *são inteiros com* $mdc(a, m) = 1$, *então*

$$ar_1 + b, \quad ar_2 + b, \quad \ldots, \quad ar_m + b$$

também é um sistema completo de resíduos módulo m.

Demonstração. Considerando-se o resultado do teorema anterior, será suficiente mostrar que quaisquer dois inteiros do conjunto $ar_1 + b, ar_2 + b, \ldots, ar_m + b$, são incongruentes módulo m. Para tanto, suponha que $ar_i + b \equiv ar_j + b \pmod{m}$. Assim, pelo Teorema 1.45, temos $ar_i \equiv ar_j \pmod{m}$. Mas, como $mdc(a, m) = 1$, o Teorema 1.46 nos diz $r_i \equiv r_j \pmod{m}$. O fato de $r_i \equiv r_j \pmod{m}$ implica $i = j$, uma vez que, $r_1, r_2, \ldots, r_m$ formam um sistema completo de resíduos módulo m, o que completa a demonstração. □

Proposição 1.55. *Se* a, b, k *e* m *são inteiros com* $k > 0$ *e* $a \equiv b \pmod{m}$, *então* $a^k \equiv b^k \pmod{m}$.

Demonstração. Se $a \equiv b \pmod{m}$, então $m|(a - b)$. Como

$$a^k - b^k = (a - b)(a^{k-1} + a^{k-2}b + a^{k-3}b^2 + \ldots + ab^{k-2} + b^{k-1}),$$

tem-se que $m|(a^k - b^k)$, e portanto $a^k \equiv b^k \pmod{m}$. □

Proposição 1.56. *Sejam* $a, b \in \mathbb{Z}$, $m, n, m_1, \ldots, m_r \in \mathbb{N} \setminus \{0, 1\}$. *Temos que:*

(i) *se* $a \equiv b \pmod{m}$ *e* $n|m$, *então* $a \equiv b \pmod{n}$;

(ii) $a \equiv b \pmod{m_i}$, $i = 1, \ldots, r \iff a \equiv b \pmod{\text{mmc}(m_1, \ldots, m_r)}$;

(iii) *se* $a \equiv b \pmod{m}$, *então* $mdc(a, m) = mdc(b, m)$.

Demonstração. Suponhamos que $b \geq a$; caso fosse $a \geq b$ argumentamos de modo análogo.

(i) Se $a \equiv\ b \pmod{m}$, então $m|(b-a)$. Como $n|m$, segue-se que $n|(b-a)$. Logo, $a \equiv\ b \pmod{n}$.

(ii) Se $a \equiv\ b \pmod{m_i}$, $i = 1, \ldots, r$, então $m_i|(b-a)$, para todo i. Sendo $b-a$ um múltiplo de cada m_i, segue-se que $\text{mmc}(m_1, \ldots, m_r)|(b-a)$ o que prova que $a \equiv\ b \pmod{\text{mmc}(m_1, \ldots, m_r)}$. A recíproca decorre do ítem (i).

(iii) Se $a \equiv\ b \pmod{m}$, então $m|(b-a)$ e, portanto, $b = a + tm$ com $t \in \mathbb{N}$. Logo, pela Proposição 1.14, temos que[3]

$$mdc(b, m) = mdc(a + tm, m) = mdc(a, m).$$

□

Teorema 1.57 (Pequeno Teorema de Fermat)**.** *Seja p primo. Se $p \nmid a$ então*

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

Demonstração. Sabemos que o conjunto formado pelos p números $0, 1, 2, \ldots, p-1$ constitui um sistema completo de resíduos módulo p. Isto significa que qualquer conjunto contendo no máximo p elementos incongruentes módulo p pode ser colocado em correspondência biunívoca com um subconjunto de $0, 1, 2, \ldots, p-1$. Vamos, agora, considerar os números $a, 2a, 3a, \ldots, (p-1)a$. Como $mdc(a, p) = 1$, nenhum destes números ia, $1 \leq i \leq p-1$ é divisível por p, ou seja, nenhum é congruente a zero módulo p. Quaisquer dois deles são incongruentes módulo p, pois $aj \equiv ak \pmod{p}$ implica $j \equiv k \pmod{p}$ e isto só é possível se $j = k$, uma vez que ambos j e k são positivos e menores do que p. Temos, portanto, um conjunto $\{a, 2a, 3a, \ldots, (p-1)a\}$ de $p-1$ elementos incongruentes módulo p e não-divisíveis por p. Logo, cada um deles é congruente a exatamente um dentre os elementos $1, 2, 3, \ldots, p-1$. Se multiplicarmos estas congruências, membro a membro, teremos pelo Teorema 1.45

$$(1a)(2a)(3a)\cdots(p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) (\text{mod } p),$$

ou seja

$$a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}.$$

Mas, como $mdc((p-1)!, p) = 1$, podemos cancelar o fator $(p-1)!$ em ambos os lados, obtendo

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

o que conclui a demonstração. □

Corolário 1.58. *Se p é um primo e a é um inteiro positivo, então $a^p \equiv a \pmod{p}$.*

Demonstração. Temos que analisar dois casos, se $p|a$ e se $p \nmid a$. Se $p|a$, então $p|(a(a^{p-1}-1))$, portanto $a^p \equiv a (\text{mod } p)$. Se $p \nmid a$, pelo Teorema 1.57 $p|(a^{p-1}-1)$ e, portanto, $p|(a^p - a)$. Logo, em ambos os casos, $a^p \equiv a \pmod{-p}$. □

[3] O resultado também segue direto do **LEMA DE EUCLIDES:** Sejam $a, b, n \in \mathbb{N}$ com $a < na < b$. Se existe $mdc(a, b-na)$, então $mdc(a, b)$ existe e $mdc(a, b) = mdc(a, b-na)$.

Exemplo 1.59. *Usando o Pequeno Teorema de Fermat, encontre o resto da divisão de* 2^{100000} *por* 17.
Solução: *Pelo Teorema de Fermat temos* $a^{p-1} \equiv 1 (\text{mod } p)$ *quando* p *é primo e* $p \nmid a$. *Logo, como* 17 *é primo e* $17 \nmid 2$, *temos* $2^{16} \equiv 1 (\text{mod } 17)$. *Mas* $100000 = 6250 \times 16$ *e, portanto,*

$$2^{100000} = (2^{16})^{6250} \equiv 1^{6250} \equiv 1 \ (\text{mod } 17).$$

Logo, o resto da divisão por 17 de 2^{100000} é 1.

Definição 1.60. *Se* n *é um inteiro positivo, a função* ϕ *de Euler, denotada por* $\phi(n)$, *é definida como sendo o número de inteiros positivos menores do que ou iguais a* n *que são relativamente primos com* n.

Exemplo 1.61. *Pela definição temos, por exemplo,*

$$\phi(8) = 4 \qquad e \qquad \phi(p) = p \qquad (p - primo),$$

pois $1, 3, 5, 7$ *são realativamente primos com* 8 *e* $1, 2, \ldots, p-1$ *são relativamente primos com* p.

Definição 1.62. *Um Sistema Reduzido de Resíduos módulo* m *é um conjunto de* $\phi(m)$ *inteiros* $r_1, r_2, \ldots, r_{\phi(m)}$, *tais que cada elemento do conjunto é relativamente primo com* m, *e se* $i \neq j$, *então* $r_i \not\equiv r_j (\text{mod } m)$.

Exemplo 1.63. *O conjunto* $\{0, 1, 2, 3, 4, 5, 6, 7\}$ *é um sistema completo de resíduos módulo* 8, *portanto* $\{1, 3, 5, 7\}$ *é um sistema reduzido de resíduos módulo* 8. *A fim de se obter um sistema reduzido de resíduos de um sistema completo módulo* m, *basta retirar os elementos do sistema completo que não são relativamente primos com* m.

Teorema 1.64. *Seja* a *um inteiro positivo tal que* $mdc(a, m) = 1$. *Se* $r_1, r_2, \ldots, r_{\phi(m)}$ *é um sistema reduzido de resíduos módulo* m, *então* $ar_1, ar_2, \ldots, ar_{\phi(m)}$ *é, também, um sistema reduzido de resíduos módulo* m.

Demonstração. Considere $ar_1, ar_2, \ldots, ar_{\phi(m)}$, $\phi(m)$ elementos. Devemos mostrar que todos eles são relativamente primos com m e, dois a dois, incongruentes módulo m. Por hipótese $mdc(a, m) = 1$ e $mdc(r_i, m) = 1$. Seja $d = mdc(ar_i, m)$. Assim, $d|ar_i$ e $d|m$. Como $mdc(a, m) = 1$, pelo Corolário 1.21, tem-se que $d|r_i$. Mas assim, $d|m$ e $d|r_i$, o que implica que $d = 1$, isto é, $mdc(ar_i, m) = 1$. Logo, nos resta mostrar que $ar_i \not\equiv ar_j (\text{mod } m)$ se $i \neq j$. Mas, como $mdc(a, m) = 1$, se $ar_i \equiv ar_j (\text{mod } m)$, pelo Teorema 1.46, temos $r_i \equiv r_j (\text{mod } m)$, o que implica $i = j$, uma vez que $r_1, r_2, \ldots, r_{\phi(m)}$, é um sistema reduzido de resíduos módulo m. Portanto, concluímos a demonstração. □

Teorema 1.65 (Teorema de Euler)**.** *Se* m *é um inteiro positivo e* a *um inteiro com* $mdc(a, m) = 1$, *então*

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

Demonstração. A demonstração deste teorema requer argumentos mais elaboradas e preferimos não apresentá-la aqui. Uma demonstração pode ser encontrada por exemplo em [14, página 43]. □

Observe que o Teorema de Fermat é uma consequência do Teorema de Euler, basta supor que $m = p$. Por outro lado, temos que $\varphi(p) = p - 1$. Portanto, o Teorema de Euler nos fornece a mesma afirmação do Teorema de Fermat, nesse caso.

Exemplo 1.66. *Mostrar que* 2, 3, 45, 7 *e* 13 *são divisores de* $n^{13} - n$ *para todo* n. ***Solução:*** *Como* $n^{13} - n = n(n^{12} - 1)$,

$$n^{12} - 1 = (n-1)(n^{11} + n^{10} + \ldots + n + 1),$$
$$n^{12} - 1 = (n^2 - 1)(n^{10} + n^8 + \ldots + n^2 + 1),$$
$$n^{12} - 1 = (n^4 - 1)(n^8 + n^4 + 1)$$

e

$$n^{12} - 1 = (n^6 - 1)(n^6 + 1),$$

temos que $n, (n-1), (n^2-1), (n^4-1), (n^6-1)$ *e* $(n^{12}-1)$ *são divisores de* $n^{13} - n$. *Logo,* $2|(n^{13} - n)$ *pois* $n(n-1)$ *é par. Agora, caso* n *não seja divisível por* $3, 5, 7$ *e* 13 *teremos que:*

$$3|(n^{13} - n) \quad pois \quad n^2 \equiv 1(\text{mod } 3) \text{ } (Euler),$$
$$5|(n^{13} - n) \quad pois \quad n^4 \equiv 1(\text{mod } 5) \text{ } (Euler),$$
$$7|(n^{13} - n) \quad pois \quad n^6 \equiv 1(\text{mod } 7) \text{ } (Euler)$$

e

$$13|(n^{13} - n) \quad pois \quad n^{12} \equiv 1(\text{mod } 13) \text{ } (Euler).$$

1.7 Congruências lineares

Definição 1.67. *Uma congruência algébrica do tipo*

$$ax \equiv b(\text{mod } m)$$

onde a, b, $m \in \mathbb{Z}$, $a \neq 0$ *e* $m > 0$, *e* x *é uma variável em* $\mathbb{Z}$, *recebe o nome de congruência linear ou congruência de primeiro grau.*

Uma ***solução*** de $ax \equiv b(\text{mod } m)$ é um u inteiro tal que

$$au \equiv b(\text{mod } m).$$

Aplicando o algoritmo da divisão para u e m, temos que existem inteiros q e x_0 $(0 \leq x_0 < m)$ tais que

$$u = mq + x_0.$$

Assim, $au = amq + ax_0$ ou $au - ax_0 = amq$. Desde que $amq \equiv 0(\text{mod } m)$, segue que $(au - ax_0) \equiv 0(\text{mod } m)$, então $ax_0 \equiv au(\text{mod } m)$. Logo, pela Proposição 1.44, tem-se

$$ax_0 \equiv b(\text{mod } m),$$

o que mostra que x_0 também é solução da congruência considerada. Convencionaremos que todos os $x \in \mathbb{Z}$ tais que $x \equiv x_0(\text{mod } m)$ constituem uma única solução de $ax \equiv b(\text{mod } m)$.

Exemplo 1.68. *Por exemplo, como* 4 *é solução de* $2x \equiv 3(\text{mod } 5)$*, então todos os elementos de*

$$\{4 + 5t : t \in \mathbb{Z}\} = \{\ldots -6, -1, 4, 9, \ldots\}$$

são apenas representações da mesma solução.

Proposição 1.69. *Uma congruência linear* $ax \equiv b(\text{mod } m)$*, onde* $a \neq 0$*, admite soluções em* $\mathbb{Z}$ *se, e somente se,* b *é divisível por* $d = mdc(a, m)$*. Neste caso, se* x_0 *é uma solução particular, então o conjunto de todas as soluções tem* d *elementos, a saber:*

$$x_0,\ x_0 + \frac{m}{d},\ x_0 + 2\frac{m}{d},\ \ldots,\ x_0 + (d-1)\frac{m}{d}.$$

Demonstração. ($\Rightarrow$) Suponha que x_0 seja uma solução de $ax \equiv b(\text{mod } m)$. Então $ax_0 - my_0 = b$, para algum $y_0 \in \mathbb{Z}$. Desde que $d|ax_0$ e $d|my_0$, logo $d|b$.

($\Leftarrow$) Agora vamos $d|b$. Então, existe $t \in \mathbb{Z}$ tal que $b = tb$. Por outro lado, de (1.3), sabemos que é possível encontrar x_1 e y_1 tais que $d = ax_1 + my_1$. Assim,

$$b = td = a(tx_1) + m(ty_1).$$

Então, $m|(a(tx_1) - b)$, ou seja, tx_1 é solução de $ax \equiv b(\text{mod } m)$.

Considerando garantida a existência da solução particular x_0 de $ax \equiv b(\text{mod } m)$, vamos supor que x seja uma outra solução qualquer. Então,

$$ax_0 \equiv b(\text{mod } m) \qquad \text{e} \qquad ax \equiv b(\text{mod } m).$$

Logo, $a(x - x_0) \equiv 0(\text{mod } m)$. Então, exite $l \in \mathbb{Z}$ tal que $a(x - x_0) = lm$. Considerando agora $r = a/d$ e $s = m/d$, pelo Corolário 1.20, temos $mdc(r, s) = 1$. Logo,

$$a(x - x_0) = lm \qquad \Rightarrow \qquad rd(x - x_0) = lsd \qquad \Rightarrow \qquad r(x - x_0) = ls.$$

Como $mdc(r, s) = 1$, pelo Corolário 1.21, concluímos que $s|(x - x_0)$, que por definição, existe $t \in \mathbb{Z}$ tal que $x - x_0 = ts$, ou seja,

$$x = x_0 + t\frac{m}{d}.$$

Aplicando o algoritmo da divisão para t e d, tem-se $t = dq + r \quad (0 \leq r < d)$. Assim,

$$x_0 + \frac{m}{d}t_1 \equiv x_0 + \frac{m}{d}t_2(\text{mod } m)$$

onde $0 \leq t_1 < t_2 < d$, então

$$\frac{m}{d}t_1 \equiv \frac{m}{d}t_2(\text{mod } m)$$

e como $mdc(m/d, m) = m/d$, leva a concluir que

$$t_1 \equiv t_2(\text{mod } m)$$

o que é impossível. Portanto, as soluções do enunciado, sendo incongruentes módulo m, são todas as soluções de $ax \equiv b(\text{mod } m)$, conforme convenções feita após a Definição 1.67. □

Exemplo 1.70. *Se em* $ax \equiv b(\text{mod } m)$ *se tem* $mdc(a,m) = 1$*, então essa congruência linear só admite uma solução. É o caso de*

$$3x \equiv 1(\text{mod } 5)$$

cujo conjunto solução é $\{2\}$*.*

Exemplo 1.71. *A congruência* $6x \equiv 15(\text{mod } 21)$ *admite* 6 *como solução particular. Como* $mdc(6,21) = 3$*, o conjunto de soluções é* $\{6, 6+\frac{21}{3}, 6+2\frac{21}{3}\} = \{6, 13, 20\}$*.*

1.8 Sistemas de congruências

Uma vez estudadas as congruências lineares, podemos pensar agora em resolver sistemas de congruências lineares simultâneas. Tais sistemas se apresentam genericamente assim:

$$\begin{cases} a_1x \equiv b_1(\text{mod } m_1) \\ a_2x \equiv b_2(\text{mod } m_2) \\ \quad\vdots \\ a_rx \equiv b_r(\text{mod } m_r) \end{cases}$$

onde os a_i $(i = 1, 2, \ldots, r)$ são supostos não nulos. Uma ***Solução*** do sistema é um inteiro x_0 que é solução de cada uma das congruências que dele fazem parte. Assim, se uma de suas congruências não admite solução, o mesmo ocorre com o sistema. Para introduzir as idéias, consideremos o seguinte exemplo:

$$\begin{cases} 3x \equiv 1(\text{mod } 5) \\ 2x \equiv 3(\text{mod } 9 \end{cases}$$

Uma das soluções da primeira congruência é 2 e uma solução particular da segunda é 6. Logo, as soluções gerais são dadas por

$$x = 2 + 5t,\ t \in \mathbb{Z} \text{ (para a primeira equação)}$$

e

$$x = 6 + 9s,\ s \in \mathbb{Z} \text{ (para a segunda equação)}$$

que podem ser traduzidas, em termos de congruências, por:

$$x \equiv 2(\text{mod } 5) \qquad \text{e} \qquad x \equiv 6(\text{mod } 9).$$

Como a multiplicação da primeira dessas congruências por 3 leva a $3x \equiv 1(\text{mod } 5)$ e a multiplicação da segunda por 2 leva a $2x \equiv 3(\text{mod } 9)$, então o sistema dado equivale a:

$$\begin{cases} x \equiv 2(\text{mod } 5) \\ x \equiv 6(\text{mod } 9). \end{cases}$$

Daí porque, doravante, nos ateremos apenas a este tipo de sistema (coeficientes de x iguais a 1). Aliás a resolução deste último, em se tratando de achar a intersecção dos conjuntos soluções de cada congruência do sistema, pode ser encaminhado da maneira habitual neste tipo de problema. Vejamos como: substituindo-se a solução geral $x = 2 + 5t$ da primeira congruência na segunda obtém-se

$$2 + 5t \equiv 6(\text{mod } 9)$$

que equivale a

$$5t \equiv 4(\text{mod } 9)$$

Sendo $t_0 = 8$ uma solução particular desta última, então $t = 8 + 9k$ é sua solução geral. Assim,

$$x = 2 + 5t = 2 + 5(8 + 9k) = 42 + 45k \ (k \in \mathbb{Z})$$

ou

$$x \equiv 42(\text{mod } 45)$$

é a solução do sistema.

Proposição 1.72. *Um sistema*

$$\begin{cases} x \equiv a_1(\text{mod } m_1) \\ x \equiv a_2(\text{mod } m_2) \end{cases}$$

admite solução, se, e somente se, $a_1 - a_2$ é divisível por $d = mdc(m_1, m_2)$. Neste caso, se x_0 é uma solução particular do sistema e se $m = mmc(m_1, m_2)$, então $x \equiv x_0(\text{mod } m)$ é sua solução geral.

Demonstração. ($\Rightarrow$) Se x_0 é solução particular do sistema, então $t \in \mathbb{Z}$ tal que

$$x_0 = a_1 + m_1 t \qquad \text{e} \qquad a_1 + m_1 t \equiv a_2(\text{mod } m_2).$$

Daí,

$$m_1 t \equiv a_2 - a_1(\text{mod } m_2)$$

e, pela Proposição 1.69, $d|(a_2 - a_1)$.

($\Leftarrow$) Como $d|(a_2 - a_1)$, por hipótese, então

$$m_1 y \equiv a_2 - a_1(\text{mod } m_2)$$

admite uma solução y_0. Logo,

$$a_1 + m_1 y_0 \equiv a_2(\text{mod } m_2).$$

Como, obviamente,

$$a_1 + m_1 y_0 \equiv a_1(\text{mod } m_1),$$

então $a_1 + m_1 y + 0$ é solução do sistema.

Se x_0 indica uma solução particular do sistema e x indica genericamente suas soluções, então $x_0 \equiv a_1(\text{mod } m_1)$ e $x \equiv a_1(\text{mod } m_1)$, e segue que

$$x \equiv x_0(\text{mod } m_1),$$

ou seja, $m_1|(x - x_0)$. Analogamente se chega que $m_2|(x - x_0)$. Então, $m|(x - x_0)$, o que tem o seguinte significado:

$$x \equiv x_0(\text{mod } m).$$

□

Corolário 1.73. *Um sistema de congruências*

$$\begin{cases} x \equiv a_1 (\text{mod } m_1) \\ x \equiv a_2 (\text{mod } m_2) \\ \quad \vdots \\ x \equiv a_r (\text{mod } m_r) \end{cases}$$

admite soluções se, e somente se, $a_i - a_j$ é divisível por $d_{ij} = mdc(m_i, m_j)$, para qualquer par de índices i, j $(i \neq j)$. Neste caso, se x_0 é uma solução particular, então a solução geral do sistema é dada por:

$$x \equiv x_0 (\text{mod } m)$$

onde $m = mmc(m_1, m_2, \ldots, m_r)$.

Exemplo 1.74. *Consideremos o sistema*

$$\begin{cases} x \equiv 2 (\text{mod } 5) \\ x \equiv 3 (\text{mod } 4) \\ x \equiv 9 (\text{mod } 6) \end{cases}$$

Verifica-se que ele satisfaz as condições do corolário e portanto admite soluções. Uma delas é o número 27. Como

$$mmc(5, 4, 6) = mmc(mmc(5, 4), 6) = mmc(20, 6) = 60$$

então

$$x \equiv 27 (\text{mod } 60)$$

é a solução geral.

Proposição 1.75 (**Teorema do Resto Chinês**). *Sejam $m_1, m_2 \ldots, m_r$ números inteiros maiores que zero e tais que $mdc(m_i, m_j) = 1$, sempre que $i \neq j$. Façamos $m = m_1 m_2 \ldots m_r$ e sejam $b_1, b_2, \ldots, b_r$, respectivamente, soluções das congruências lineares*

$$\frac{m}{m_j} y \equiv 1 (\text{mod } m_j) \quad (j = 1, 2, \ldots, r)$$

Então o sistema

$$\begin{cases} x \equiv a_1 (\text{mod } m_1) \\ x \equiv a_2 (\text{mod } m_2) \\ \quad \vdots \\ x \equiv a_r (\text{mod } m_r) \end{cases}$$

é possível (admite soluções) para quaisquer $a_1, a_2, \ldots, a_r \in \mathbb{Z}$ se sua solução geral é dada por:

$$x \equiv a_1 b_1 \frac{m}{m_1} + \ldots + a_r b_r \tfrac{m}{m_r} (\text{mod } m)$$

Demonstração. Que o sistema é possível decorre do corolário da proposição anterior. Notemos que, como $mdc(m_j, m_i) = 1$, para $i \neq j$, então

$$mdc(m_j, \frac{m}{m_j}) = 1,$$

que implica a existência de soluções para cada congruência linear

$$\frac{m}{m_j} y \equiv 1 (\text{mod } m_j),$$

as quais estamos indicando por b_j $(j = 1, 2, \ldots, r)$. Assim,

$$\frac{m}{m_j} b_j \equiv 1 (\text{mod } m_j)$$

e portanto:

$$a_j b_j \frac{m}{m_j} \equiv a_j (\text{mod } m_j) \quad (j = 1, 2, \ldots, r).$$

Por outro lado, se $i \neq j$,

$$\frac{m}{m_i} \equiv 0 (\text{mod } m_j)$$

e então

$$a_i b_i \frac{m}{m_i} \equiv 0 (\text{mod } m_j).$$

Logo,

$$a_1 b_1 \frac{m}{m_1} + \ldots + a_j b_j \frac{m}{m_j} + \ldots + a_r b_r \frac{m}{m_r} \equiv a_j (\text{mod } m_j),$$

para todo j, $1 \leq j \leq r$. Assim, de fato

$$x_0 \sum_{i=1}^{r} a_i b_i \frac{m}{m_i}$$

é uma solução particular do sistema. O corolário da proposição anterior garante então que

$$x \equiv x_0 (\text{mod } m)$$

é a solução geral posto que, como $mdc(m_i, m_j) = 1$, sempre que $i \neq j$, então $mmc(m_1, m_2, \ldots, m_r) = m_1 m_2 \ldots m_r = m$. □

Exemplo 1.76. *Vamos resolver o sistema*

$$\begin{cases} x \equiv 1 (\text{mod } 2) \\ x \equiv 2 (\text{mod } 3) \\ x \equiv 3 (\text{mod } 5) \end{cases}$$

usando o Toerema do Resto Chinês. Neste caso $m = 30$ e as congruências a resolver são:

$$15y \equiv 1 (\text{mod } 2), \quad 10y \equiv 1 (\text{mod } 3) \quad e \quad 6y \equiv 1 (\text{mod } 5),$$

das quais $b_1 = 1, b_2 = 1$ e $b_3 = 1$ são soluções particulares. Assim, a solução geral do sistema é dada por

$$x \equiv 1.1.15 + 2.1.10 + 3.1.6 \equiv 23 (\text{mod } 30).$$

1.9 Método dos Quadrados Repetidos

O objetivo desse método é calcular a congruência de b^r módulo n, sendo b, r e n números naturais grandes. Para fazer esse cálculo, é necessário convertermos r em número binário. Para tanto, suponhamos

$$r = \sum_{j=0}^{k} a_j 2^j,$$

sendo $a_j = 0$ ou 1. Por exemplo, se $r = 106$, passamos-o para a base binária fazendo a conta simples

$$106 = 0 \cdot 2^0 + 1 \cdot 2^1 + 0 \cdot 2^2 + 1 \cdot 2^3 + 0 \cdot 2^4 + 1 \cdot 2^5 + 1 \cdot 2^6,$$

de forma que $k = 6$, e $a_0 = 0$, $a_1 = 1$, $a_2 = 0$, $a_3 = 1$, $a_4 = 0$, $a_5 = 1$ e $a_6 = 1$.

Algoritmo:

Sejam c, d e b_j; $j = 0, \ldots, k$ números naturais (auxiliares).
Passo 1) Se $a_0 = 1$, então faça $c = b$. Senão, faça $c = 1$.
Passo 2) Seja $b_0 = b$.
Passo 3) Para cada $j = 1, \ldots, k$ faça: calcule

$$b_j \equiv b_{j-1}^2 (\text{mod } n).$$

Se $a_j = 1$, calcule

$$d \equiv c b_j (\text{mod } n)$$

e faça $c = d$. Senão deixe c inalterado.
Passo 4) O número c é congruente a b^r módulo n, ou seja,

$$c \equiv b^r (\text{mod } n).$$

Percebemos que na etapa i do Passo 3, temos

$$c \equiv b_0^{\sum_{j=0}^{i} a_j 2^j} (\text{mod } n).$$

Assim, ao término do algoritmo, temos $c \equiv b^r (\text{mod } n)$.

Exemplo 1.77. *Encontremos a tal que* $a \equiv b^r (\text{mod } n)$, *sendo* $b = 227$, $r = 106$ *e* $n = 451$.
Solução: *Conforme destacamos antes, passando* $r = 106$ *para a base binária, temos:*

$$106 = 0 \cdot 2^0 + 1 \cdot 2^1 + 0 \cdot 2^2 + 1 \cdot 2^3 + 0 \cdot 2^4 + 1 \cdot 2^5 + 1 \cdot 2^6 = 1101010_2,$$

onde $k = 6$ *e* $a_0 = 0$, $a_1 = 1$, $a_2 = 0$, $a_3 = 1$, $a_4 = 0$, $a_5 = 1$ *e* $a_6 = 1$. *Seguindo o algoritmo:*
Passo 1) *Como* $a_0 \neq 1$, *então* $c = 1$.
Passo 2) $b_0 = 227$.
Passo 3)

- *Para* $j = 1$
  $b_1 \equiv 227^2 (\text{mod } 451) \Rightarrow b_1 = 115$
  $a_1 = 1$, *então* $d \equiv 1.115 (\text{mod } 451) \Rightarrow d = 115 \Rightarrow c = 115$.

- *Para* $j = 2$
  $b_2 \equiv 115^2 (\text{mod } 451) \Rightarrow b_2 = 146$
  $a_2 = 0 \Rightarrow c = 115$.

- *Para* $j = 3$
  $b_3 \equiv 146^2 (\text{mod } 451) \Rightarrow b_3 = 119$
  $a_3 = 1$, *então* $d \equiv 115.119 (\text{mod } 451) \Rightarrow d = 20 \Rightarrow c = 20$.

- *Para* $j = 4$
  $b_4 \equiv 119^2 (\text{mod } 451) \Rightarrow b_4 = 180$
  $a_4 = 0 \Rightarrow c = 20$.

- *Para* $j = 5$
  $b_5 \equiv 180^2 (\text{mod } 451) \Rightarrow b_5 = 379$
  $a_5 = 1$, *então* $d \equiv 20.379 (\text{mod } 451) \Rightarrow d = 364 \Rightarrow c = 364$.

- *Para* $j = 6$
  $b_6 \equiv 379^2 (\text{mod } 451) \Rightarrow b_6 = 223$
  $a_6 = 1$, *então* $d \equiv 364.223 (\text{mod } 451) \Rightarrow d = 443 \Rightarrow c = 443$.

Passo 4) *Logo,*

$$a \equiv b^r (\text{mod } n) \Rightarrow 443 \equiv 227^{106} (\text{mod } 451).$$

1.10 Matrizes

Um técnico de basquetebol, querendo analisar o desempenho dos titulares de sua equipe, colocou em uma tabela o número de pontos marcados por cada titular em sete jogos:

Titulares (i)Jogos (j)	1	2	3	4	5	6	7
1	18	17	18	17	21	18	20
2	15	16	18	18	22	21	18
3	20	19	20	21	14	14	22
4	18	22	20	20	18	22	23
5	19	18	12	14	20	17	18

na qual cada elemento da linha i e coluna j é o número de pontos marcados por cada titular i em cada jogo j. Note a simplicidade dessa tabela. Se quisermos, por exemplo, saber qual o número de pontos marcado pelo titular de número 2 no 5º jogo, basta olharmos para o cruzamento da linha 2 com a coluna 5 e encontar 22. Tabelas como essa são denominada **matrizes**. Vamos formalizar o que é uma matriz, ou seja, definiremos uma matriz e suas operações.

Definição 1.78. *Dados dois números m e n naturais, não nulos, chama-se matriz m por n (indica-se $m \times n$) toda tabela M formada por números reais distribuídos em m linhas e n colunas. Uma matriz pode ser representada entre parênteses ( ) ou entre colchetes [ ].*

Exemplo 1.79.

1. $\begin{pmatrix} 3 & 5 & -1 \\ 0 & \frac{4}{5} & \sqrt{2} \end{pmatrix}$ *é uma matriz* 2×3.
2. $\begin{bmatrix} 0 & 9 & -1 & 7 \end{bmatrix}$ *é uma matriz* 1×4.

Em uma matriz qualquer M, cada elemento é indicado por a_{ij}, e é *chamado de entrada da matriz* M. O índice i indica a linha e o índice j a coluna às quais o elemento pertence. Como as linhas são enumeradas de cima para baixo (de 1 até m) e as colunas da esquerda para a direita (de 1 até n), então uma matriz $m \times n$ é representada por:

$$M = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}.$$

Matrizes especiais

Há matrizes que, por apresentarem uma utilidade maior na teoria das matrizes, recebem nomes especiais.

1. **Matriz linha:** É uma matriz do tipo $1 \times n$, isto é, é uma matriz que tem uma única linha.

   Exemplo.
   $$\begin{pmatrix} 0 & 9 & -1 & 7 \end{pmatrix}$$

2. **Matriz coluna:** É uma matriz do tipo $m \times 1$, isto é, é uma matriz que tem uma única coluna.

   Exemplo.
   $$\begin{pmatrix} 5 \\ 1 \\ -3 \end{pmatrix}$$

3. **Matriz nula:** É uma matriz que tem todos os elementos iguais a zero. Indicamos por $0_{m \times n}$. Isto significa que, se $0_{m \times n} = (a_{ij})_{m \times n}$, deve-se ter $a_{ij} = 0,\ \forall i, j, 1 \leq i \leq m$ e $1 \leq j \leq n$.

   Exemplo.
   $$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

4. **Matriz quadrada de ordem n:** É uma matriz do tipo $n \times n$, ou seja, é uma matriz que tem igual número de linhas e colunas.

   Exemplo.

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \ddots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}$$

   Chama-se diagonal principal de uma matriz quadrada de ordem n o conjunto dos elementos que têm os índices iguais, isto é:

$$\{a_{ij} | i = j\} = \{a_{11}, a_{22}, a_{33}, \dots, a_{nn}\}.$$

   Chama-se diagonal secundária de uma matriz quadrada de ordem n o conjunto dos elementos que tem soma dois índices igual a $n + 1$, isto é:

$$\{a_{ij} | i + j = n + 1\} = \{a_{1n}, a_{2,n-1}, a_{3,n-2}, \dots, a_{n1}\}.$$

   Exemplo 1.80. *A matriz*

$$M = \begin{pmatrix} 8 & 9 & -7 \\ 6 & 4 & -5 \\ -1 & 2 & 3 \end{pmatrix}$$

   é quadrada de ordem 3. Sua diagonal principal é $\{8, 4, 3\}$ *e sua diagonal secundária é* $\{-7, 4, -1\}$.

5. **Matriz diagonal:** É uma matriz quadrada cujos elementos que não pertencem à diagonal principal são iguais a zero.

   Exemplo.

$$\begin{pmatrix} 3 & 0 \\ 0 & -2 \end{pmatrix}$$

6. **Matriz unidade (ou matriz identidade) de ordem n (indica-se I_n):** É uma matriz diagonal em que os elementos da diagonal principal são iguais a 1, ou seja, $I_n = (a_{ij})_{n \times n}$ tal que

$$a_{ij} = \begin{cases} 1, & \text{se} \quad i = j \\ 0, & \text{se} \quad i \neq j \end{cases}.$$

   Exemplo.

$$I_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

7. **Matriz Triangular Superior:** É uma matriz quadrada onde todos os elementos abaixo da diagonal principal são nulos, isto é, $m = n$ e $a_{ij} = 0$, para $i > j$.

   Exemplo.
   $$\begin{pmatrix} 2 & -1 & 0 \\ 0 & -1 & 4 \\ 0 & 0 & 3 \end{pmatrix}.$$

8. **Matriz Triangular Inferior:** É uma matriz quadrada em que $m = n$ e $a_{ij} = 0$, para $i < j$.

   Exemplo.
   $$\begin{pmatrix} 2 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 1 & 2 & 2 & 0 \\ 1 & 0 & 5 & 4 \end{pmatrix}.$$

9. **Matriz Simétrica:** É uma matriz onde $m = n$ e $a_{ij} = a_{ji},\ \forall i, j, 1 \leq i, j \leq n$.

   Exemplo.
   $$\begin{pmatrix} 4 & 3 & -1 \\ 3 & 2 & 0 \\ -1 & 0 & 5 \end{pmatrix}.$$

   Observe que, no caso de uma matriz simétrica, a parte superior é uma "reflexão" da parte inferior, em relação à diagonal principal.

Operações com Matrizes

Igualdade de Matrizes

Definição 1.81. *Duas matrizes são ditas iguais quando possuem a mesma ordem e as entradas correspondentes são iguais.*

Exemplo 1.82. *Considere as matrizes*
$$A = \begin{pmatrix} 1 & -1 \\ 4 & 0 \\ 2 & 5 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 4 \\ -2 & 5 \\ 1 & 0 \end{pmatrix} \quad e \quad C = \begin{pmatrix} 1 & -1 \\ 4 & 0 \\ 2 & 5 \end{pmatrix}.$$
Temos $A = C$ e A não igual (diferente) a C (notação usual: $A \neq B$).

Adição

Definição 1.83. *A soma de duas matrizes de mesma ordem, $A_{m\times n} = [a_{ij}]$ e $B_{m\times n} = [b_{ij}]$, é definida por $[a_{ij} + b_{ij}]$ e denotada por $A + B$. Simbolicamente,*
$$A + B = [a_{ij} + b_{ij}]_{m\times n}.$$

Exemplo 1.84.
$$\begin{pmatrix} 1 & -1 \\ 4 & 0 \\ 2 & 5 \end{pmatrix} + \begin{pmatrix} 0 & 4 \\ -2 & 5 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 3 \\ 2 & 5 \\ 3 & 5 \end{pmatrix}$$

Propriedades:

Dadas as matrizes A, B e C de mesma ordem $m \times n$, temos:

i) $A + B = B + A$ (comutatividade)

ii) $A + (B + C) = (A + B) + C$ (associatividade)

iii) $A + 0 = A$, onde 0 denota a matriz nula $m \times n$.

A verificação dessas propriedades é simples. O leitor pode encontrá-las em [2, 3].

Multiplicação de um número por matriz

Definição 1.85. *O produto de um número k por uma matriz $A = (a_{ij})_{m\times n}$, é definido por $kA = [ka_{ij}]$.*

Na multiplicação, cada elemento da matriz kA é igual ao produto da entrada correspondente em A, pelo número k.

Exemplo 1.86.

$$4\begin{pmatrix} 2 & -5 \\ 3 & 0 \\ 1 & 6 \end{pmatrix} = \begin{pmatrix} 8 & -20 \\ 12 & 0 \\ 4 & 24 \end{pmatrix}$$

Propriedades:

Sendo A e B matrizes do mesmo tipo e sendo r e s números, tem-se que:

i) $r(sA) = s(rA) = (rs)A$;

ii) $r(A + B) = rA + rB$;

iii) $(r + s)A = rA + sA$;

iv) $1A = A$.

A verificação dessas propriedades é simples. O leitor pode encontrá-las em [2, 3].

Transposição

Definição 1.87. *Dada uma matriz $A = [a_{ij}]_{m\times n}$, podemos obter uma outra matriz $A^t = [b_{ij}]_{n\times m}$, cujas linhas são as colunas de A, isto é, $b_{ij} = a_{ji}$. A^t é chamada transposta de A.*

Exemplo 1.88.

$$A = \begin{pmatrix} 2 & 1 \\ 0 & 3 \\ -1 & 4 \end{pmatrix}_{3\times 2} \Rightarrow \quad A^t = \begin{pmatrix} 2 & 0 & -1 \\ 1 & 3 & 4 \end{pmatrix}_{2\times 3}.$$

Propriedades:

i) Uma matriz é simétrica se, e somente se, ela é igual à sua transposta, isto é, se, e somente se, $A = A^t$.

Exemplo.

$$B = \begin{pmatrix} 1 & 3 \\ 3 & 2 \end{pmatrix} \quad \Rightarrow \quad B^t = \begin{pmatrix} 1 & 3 \\ 3 & 2 \end{pmatrix}_{2\times 3}.$$

ii) $(A^t)^t = A$. Isto é, a transposta da transposta de uma matriz é ela mesma.

iii) $(A + B)^t = A^t + B^t$. Em palavras, a transposta de uma soma é igual à soma das transpostas.

iv) $(kA)^t = kA^t$, onde k é qualquer escalar.

A verificação dessas propriedades é simples. O leitor pode encontrá-las em [2, 3].

Multiplicação de Matrizes

Antes de definirmos a multiplicação de matrizes, vamos definir produto de linha por coluna.

Definição 1.89. *Sejam as matrizes $A = (a_{ij})_{m\times k}$ e $B = (b_{ij})_{k\times n}$. Consideremos a linha i de A e a coluna j de B, isto é:*

$$\begin{pmatrix} a_{i1} & a_{i2} & a_{i3} & \cdots & a_{ik} \end{pmatrix} \quad e \quad \begin{pmatrix} b_{1j} \\ b_{2j} \\ b_{3j} \\ \vdots \\ b_{kj} \end{pmatrix}.$$

O produto da linha pela coluna é:

$$a_{i1}b_{1j} + a_{i2}b_{2j} + a_{i3}b_{3j} + \ldots + a_{ik}b_{1k}.$$

Ou seja, multiplicamos, ordenadamente, os elementos da linha i pelos elementos da coluna j e somamos os resultados obtidos.

Definição 1.90. *O produto da matriz $A = (a_{ij})_{m\times k}$ pela matriz $B = (b_{ij})_{k\times n}$ que se indica por AB ou por $A \times B$, é a matriz $C = (c_{ij})_{m\times n}$ tal que cada elemento c_{ij} é igual ao produto da linha i de A pela coluna j de B.*

Exemplo 1.91.

$$\begin{pmatrix} 2 & 5 & 8 \\ 1 & 4 & 3 \end{pmatrix} \begin{pmatrix} 4 & 3 & 4 \\ 3 & 6 & 1 \\ 1 & 2 & 0 \end{pmatrix} =$$

$$= \begin{pmatrix} 2\times 4 + 5\times 3 + 8\times 1 & 2\times 3 + 5\times 6 + 8\times 2 & 2\times 4 + 5\times 1 + 8\times 0 \\ 1\times 4 + 4\times 3 + 3\times 1 & 1\times 3 + 4\times 6 + 3\times 2 & 1\times 4 + 4\times 1 + 3\times 0 \end{pmatrix} =$$

$$= \begin{pmatrix} 31 & 52 & 13 \\ 13 & 21 & 8 \end{pmatrix}.$$

Observação 1.92. *Se A e B são matrizes, então:*

1. *o produto AB é definido apenas quando o número de colunas de A for igual ao número de linhas de B.*

   Exemplo.
   $$\begin{pmatrix} 2 & 1 \\ 4 & 2 \\ 5 & 3 \end{pmatrix}_{3\times 2} \begin{pmatrix} 1 & -1 \\ 0 & 4 \end{pmatrix}_{2\times 2} = \begin{pmatrix} 2 & 2 \\ 4 & 4 \\ 5 & 7 \end{pmatrix}_{3\times 2}.$$
   Como o número de colunas da primeira matriz é igual ao número de linhas da segunda matriz foi possível fazer a multiplicação.

   Exemplo.
   $$\begin{pmatrix} 1 & -1 \\ 0 & 4 \end{pmatrix}_{2\times 2} \begin{pmatrix} 2 & 1 \\ 4 & 2 \\ 5 & 3 \end{pmatrix}_{3\times 2}.$$
   Não é possível efetuar esta multiplicação, porque o número de colunas da primeira matriz é diferente ao número de linhas da segunda matriz.

2. *a matriz C tal que $C = AB$ possui o mesmo número de linhas de A e o mesmo número de colunas de B, isto é: $A_{m\times k}B_{k\times n} = C_{m\times n}$.*

3. *Em geral $AB \neq BA$.*

   Exemplo. *Sejam* $A = \begin{pmatrix} 1 & -1 & 1 \\ -3 & 2 & -1 \\ -2 & 1 & 0 \end{pmatrix}$ *e* $B = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 4 & 6 \\ 1 & 2 & 3 \end{pmatrix}$. *Então*
   $$AB = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad e \quad BA = \begin{pmatrix} -11 & 6 & -1 \\ -22 & 12 & -2 \\ -11 & 6 & -1 \end{pmatrix}.$$
   Note ainda que $AB = 0$, sem que $A = 0$ ou $B = 0$.

Propriedades:

Desde que sejam possíveis as operações, as seguintes propriedades são válidas:

1. $AI = IA = A$ (Isto justifica o nome da matriz identidade.)
2. $A(B + C) = AB + AC$ (distributividade à esquerda da multiplicação, em relação à soma)
3. $(A+B)C = AC+BC$ (distributividade à direita da multiplicação, em relação à soma)
4. $(AB)C = A(BC)$ (associatividade)
5. $(AB)^t = B^tA^t$
6. $0A = 0$ e $A0 = 0$

A verificação dessas propriedades é simples. O leitor pode encontrá-las em [2, 3].

1.11 Determinante

Determinante de uma matriz (quadrada)

De forma heurística, o Determinante de uma matriz quadrada $A = [a_{ij}]$ de ordem n é um número real a ela associado. Para apresentar o conceito de determinante de modo minimamente fundamentado, definiremos determinante indutivamente através da ordem da matriz. Cada matriz tem um único determinante. Indicaremos o determinante dessa matriz por: $\det(A)$ ou

$$\begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \ddots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix}.$$

Determinante de uma matriz de 1ª ordem

O determinante de uma matriz $A = (a_{11})$, de 1ª ordem, é o valor do seu único elemento a_{11}, ou seja:

$$\det(A) = |a_{11}| = a_{11}.$$

Exemplo 1.93. *Se* $M = (4)$, *então* $\det(M) = 4$.

Determinante de uma matriz de 2ª ordem

Dada uma matriz quadrada de 2ª ordem $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$, o determinante de A é definido como o número real

$$a_{11}a_{22} - a_{12}a_{21}.$$

Note que

$$\det(A) = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}\det([a_{22}]) - a_{12}\det([a_{21}]).$$

Exemplo 1.94. *Calcule o determinante da matriz* $M = \begin{pmatrix} 2 & -3 \\ 1 & 5 \end{pmatrix}$.

Solução:

$$\det(M) = \begin{vmatrix} 2 & -3 \\ 1 & 5 \end{vmatrix} = 2 \cdot 5 - (-3) \cdot 1 = 10 + 3 = 13.$$

O determinante da matriz M *é 13.*

Determinante de uma matriz de 3ª ordem

Com certa analogia ao caso de 2ª ordem, dada uma matriz de ordem $n = 3$

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix},$$

definimos

$$\det(A) = a_{11} \det \begin{pmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{pmatrix} - a_{12} \det \begin{pmatrix} a_{21} & a_{23} \\ a_{31} & a_{33} \end{pmatrix} + a_{13} \det \begin{pmatrix} a_{21} & a_{22} \\ a_{31} & a_{32} \end{pmatrix}.$$

Observe que as matrizes

$$A_{11} = \begin{pmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{pmatrix}, \quad A_{12} = \begin{pmatrix} a_{21} & a_{23} \\ a_{31} & a_{33} \end{pmatrix} \quad \text{e} \quad A_{13} = \begin{pmatrix} a_{21} & a_{22} \\ a_{31} & a_{32} \end{pmatrix},$$

são obtidas da matriz A ao se retirar a 1ª linha e a 1ª coluna, a 1ª linha e a 2ª coluna e a 1ª linha e a 3ª coluna, respectivamente. Assim, podemos escrever

$$\det(A) = a_{11} \det(A_{11}) - a_{12} \det(A_{12}) + a_{13} \det(A_{13}).$$

A partir da submatriz A_{ij} obtida da matriz A quando se retira a $i-$ésima linha e a $j-$ésima coluna, temos os chamados Cofatores

$$\Delta_{ij} = (-1)^{i+j} \det(A_{ij}).$$

Logo,

$$\det(A) = a_{11}\Delta_{11} + a_{12}\Delta_{11} + a_{13}\Delta_{11}. \tag{1.5}$$

Desenvolvendo todas as contas, também se tem

$$|A| = a_{11}.a_{22}.a_{33} + a_{12}.a_{23}.a_{31} + a_{13}.a_{21}.a_{32} - a_{13}.a_{22}.a_{31} - a_{11}.a_{23}.a_{32} - a_{12}.a_{21}.a_{33},$$

conhecida com Regra de Sarrus.

Exemplo 1.95. *Calcule o determinante da matriz* $A = \begin{pmatrix} 1 & 3 & 4 \\ 5 & 2 & -3 \\ 1 & 4 & 2 \end{pmatrix}$.

Solução: *Temos:*

$\det(A) = 1.2.2+1.(-3).3+4.4.5-1.2.4-2.3.5-1.4.(-3) = 4-9+80-8-30+12 = 49.$

O determinante da matriz A *é* 49.

Determinante de uma matriz de ordem maior que 3

O método de cálculo de determinante apresentado aqui é chamado de Desenvolvimento de Laplace e nos permite calcular determinantes de matrizes com ordem n, para $n \geq 4$. Para tanto, inspirado na fórmula (1.5), dada uma matriz

$$A_{n\times n} = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \ddots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix},$$

definimos

$$\det(A_{n\times n}) = a_{11}\Delta_{11} + a_{12}\Delta_{12} + \ldots + a_{1n}\Delta_{1n} \tag{1.6}$$

Deve-se destacar fortemente que na fórmula (1.6) dada, o determinante foi "desenvolvido" através da 1ª linha. O mesmo raciocínio pode ser aplicado através da $i-$ésima linha, ou até mesmo através da $j-$ésima coluna, que o resultado do determinante será o mesmo.

Exemplo 1.96. *Consideremos o cálculo pela 2ª coluna. Temos*

$$|B| = \begin{vmatrix} 1 & -2 & 3 \\ 2 & 1 & -1 \\ -2 & -1 & 2 \end{vmatrix} = (-2)\Delta_{12} + 1\Delta_{22} + (-1)\Delta_{32},$$

onde

$$\begin{aligned}
\Delta_{12} &= (-1)^{1+2}\begin{vmatrix} 2 & -1 \\ -2 & 2 \end{vmatrix} = -\begin{vmatrix} 2 & -1 \\ -2 & 2 \end{vmatrix} = -2 \\
\Delta_{12} &= (-1)^{1+2}\begin{vmatrix} 2 & -1 \\ -2 & 2 \end{vmatrix} = -\begin{vmatrix} 2 & -1 \\ -2 & 2 \end{vmatrix} = -2 \\
\Delta_{22} &= (-1)^{2+2}\begin{vmatrix} 1 & 3 \\ -2 & 2 \end{vmatrix} = 8 \\
\Delta_{32} &= (-1)^{3+2}\begin{vmatrix} 1 & 3 \\ 2 & -1 \end{vmatrix} = 7.
\end{aligned}$$

Portanto

$$|B| = (-2)\cdot(-2) + 1\cdot 8 + (-1)\cdot 7 = 5.$$

O desenvolvimento de Laplace é uma fórmula de recorrência que permite calcular o determinante de uma matriz de ordem n, a partir dos determinantes das submatrizes quadradas de ordem $n-1$. Em grande parte dos casos ele simplifica muito o cálculo de determinantes, principalmente se for utilizado em conjunto com outras propriedades do determinante.

Propriedades:

1. Se todos os elementos de uma linha (ou coluna) de uma matriz A são nulos, então $\det(A) = 0$;

2. $\det(A) = \det(A^t)$;

3. Se multiplicarmos uma linha (ou coluna) da matriz por uma constante, o determinante fica multiplicado por esta constante;

4. Uma vez trocada a posição de duas linhas (ou colunas), o determinante troca de sinal;

5. O determinante de uma matriz que tem duas linhas (ou colunas) iguais é zero;

6. $$\begin{vmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ b_{i1}+c_{i1} & \dots & b_{in}+c_{in} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{vmatrix} = \begin{vmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ b_{i1} & \dots & b_{in} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{vmatrix} + \begin{vmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ c_{i1} & \dots & c_{in} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{vmatrix}.$$

   Cuidado! Observe que aqui temos a soma numa linha, e não uma soma de matrizes. De modo geral, o determinante de uma soma de duas matrizes não é igual à soma dos determinantes das matrizes. Ou seja, pode acontecer de $\det(A+B) \neq \det(A) + \det(B)$;

7. O determinante não se altera se somarmos a uma linha (ou coluna) outra linha (ou coluna) multiplicada por uma constante;

   Exemplo. $\begin{vmatrix} 3 & -2 & 1 \\ 2 & 5 & 0 \\ 2 & 4 & -2 \end{vmatrix} = \begin{vmatrix} 3 & -2 & 1 \\ 2 & 5 & 0 \\ 8 & 0 & 0 \end{vmatrix}$.
   Aqui, à terceira linha, somamos a primeira linha multiplicada por 2.

8. $\det(AB) = \det(A)\det(B)$.

Mais detalhes sobre essas propriedades podem ser encontrados, por exemplo, em [2, 3].

1.12 Matriz Adjunta - Matriz Inversa

Consideremos a seguinte matriz quadrada:

$$\left(\begin{array}{ccc|c|cc} a_{11} & a_{12} & \dots & a_{1j} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2j} & \dots & a_{2n} \\ a_{31} & a_{32} & \dots & a_{3j} & \dots & a_{3n} \\ \vdots & \vdots & \ddots & \vdots & \dots & \vdots \\ \hline a_{i1} & a_{i2} & \dots & a_{ij} & \dots & a_{in} \\ \hline \vdots & \vdots & \dots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nj} & \dots & a_{nn} \end{array}\right).$$

Como destacado na seção anterior, a partir de cada entrada a_{ij} da matriz temos o "cofator do elemento a_{ij}", que é o número que indicamos por Δ_{ij} ("lê-se cofator do elemento a_{ij}"), definido por:

$$\Delta_{ij} = (-1)^{i+j} \det(A_{ij}),$$

onde A_{ij} é a matriz que se obtém eleminando a linha i e a coluna j da matriz A. Com esses cofatores podemos formar uma nova matriz $\overline{A}$, denominada matriz dos cofatores de A, ou seja,

$$\overline{A} = [\Delta_{ij}].$$

Exemplo 1.97. *Dada a matriz*

$$A = \begin{pmatrix} 2 & 1 & 0 \\ -3 & 1 & 4 \\ 1 & 6 & 5 \end{pmatrix}.$$

Determine a matriz dos cofatores de A.
Solução: *Usando a definição e desenvolvendo os cálculos obtemos*

$$\Delta_{11} = (-1)^{1+1} \det \begin{pmatrix} 1 & 4 \\ 6 & 5 \end{pmatrix} = -19;$$

$$\Delta_{12} = (-1)^{1+2} \det \begin{pmatrix} -3 & 4 \\ 1 & 5 \end{pmatrix} = 19;$$

$$\Delta_{13} = (-1)^{1+3} \det \begin{pmatrix} -3 & 1 \\ 1 & 6 \end{pmatrix} = -19;$$

e analogamente os demais cofatores. Então,

$$\overline{A} = \begin{pmatrix} -19 & 19 & -19 \\ -5 & 10 & -11 \\ 4 & -8 & 5 \end{pmatrix}.$$

Definição 1.98. *Dada uma matriz quadrada A, chamaremos de matriz adjunta de A à transposta da matriz dos cofatores de A. Simbolicamente:*

$$adj(A) = \overline{A}^t.$$

Exemplo 1.99. *Usando as informações do exemplo anterior, temos*

$$adj(A) = \overline{A}^t = \begin{pmatrix} -19 & -5 & 4 \\ 19 & 10 & -8 \\ -19 & -11 & 5 \end{pmatrix}.$$

Devemos notar que usando as matrizes dos dois exemplos anteriores, temos

$$A \cdot adj(A) = \begin{pmatrix} 2 & 1 & 0 \\ -3 & 1 & 4 \\ 1 & 6 & 5 \end{pmatrix} \begin{pmatrix} -19 & -5 & 4 \\ 19 & 10 & -8 \\ -19 & -11 & 5 \end{pmatrix} = \begin{pmatrix} -19 & 0 & 0 \\ 0 & -19 & 0 \\ 0 & 0 & -19 \end{pmatrix}$$

$$= -19 \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = -19 I_3.$$

Esse caso particular não é uma mera coincidência, pois na verdade temos em geral o seguinte teorema.

Teorema 1.100. *Se A é matriz quadrada de ordem n e I_n é a matriz identidade de ordem n, então*

$$A \cdot adj(A) = adj(A) \cdot A = \det(A) I_n.$$

A demonstração desse teorema, apesar de simples, não a apresentaremos aqui. O leitor pode encontrá-la [3, página 73].

Definição 1.101. *Dada uma matriz quadrada A de ordem n, diz-se que A é inversível quando existe uma matriz B de ordem n tal que $AB = BA = I_n$, onde I_n é a matriz identidade de ordem n. Quando a matriz B existe, diz-se que ela é a inversa de A e denotamos $B = A^{-1}$ e dizemos A^{-1} é a inversa de A.*

Exemplo 1.102. *Seja*

$$A = \begin{pmatrix} 6 & 2 \\ 11 & 4 \end{pmatrix}.$$

Assumindo a princípio que a inversa existe, podemos procurar

$$B = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

tal que $AB = I_2$ e $BA = I_2$. Impondo a primeira condição,

$$\begin{pmatrix} 6 & 2 \\ 11 & 4 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

temos

$$\begin{pmatrix} 6a+2c & 6b+2d \\ 11a+4c & 11b+4d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Portanto,

$$\begin{cases} 6a + 2c = 1 \\ 11a + 4c = 0 \end{cases} \quad e \quad \begin{cases} 6b + 2d = 0 \\ 11b + 4d = 1 \end{cases}.$$

Resolvendo os sistemas, temos $a = 2, b = -1, c = -\frac{11}{2}$ e $d = 3$. Então,

$$\begin{pmatrix} 6 & 2 \\ 11 & 4 \end{pmatrix}\begin{pmatrix} 2 & -1 \\ -\frac{11}{2} & 3 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

ou seja, $AB = I$. Também

$$\begin{pmatrix} 2 & -1 \\ -\frac{11}{2} & 3 \end{pmatrix}\begin{pmatrix} 6 & 2 \\ 11 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

ou seja, $BA = I$ e, portanto,

$$A^{-1} = B = \begin{pmatrix} 2 & -1 \\ -\frac{11}{2} & 3 \end{pmatrix}$$

é a inversa da matriz A e denotamos.

Observação 1.103. *1. Se A e B são matrizes quadradas de mesma ordem, ambas inversíveis (isto é, existem A^{-1} e B^{-1}), então AB é inversível e $(AB)^{-1} = B^{-1}A^{-1}$.*

De fato, basta observar que

$$(AB)(B^{-1}A^{-1}) = A(BB^{-1})A^{-1} = AIA^{-1} = AA^{-1} = I$$

e que, analogamente, $(B^{-1}A^{-1})(AB) = I$.

2. *Se A é uma matriz quadrada e existe uma matriz B tal que $BA = I$, então A é inversível, ou seja, A^{-1} existe e, além disso, $B = A^{-1}$.*

Teorema 1.104. *Uma matriz quadrada A de ordem n é inversível se, e somente se,* $\det(A) \neq 0$.

Demonstração. ($\Rightarrow$) Se A é inversível, então existe matriz quadrada A^{-1} tal que $AA^{-1} = A^{-1}A = I_n$. Logo, temos

$$\det(AA^{-1}) = \det(A^{-1}A) = \det(I_n).$$

Pela Propriedade 8 de determinante, juntamente com o fato que $\det(I_n) = 1$, temos que

$$\det(A)\det(A^{-1}) = \det(A^{-1})\det(A) = 1.$$

Concluímos então que $\det(A) \neq 0$ (pois caso contrário, isto é, se $\det(A) = 0$, teríamos $\det(A)\det(A^{-1}) = 0$).
($\Leftarrow$) Suponha agora que $\det(A) \neq 0$. Sendo A uma matriz quadrada de ordem n, pelo Teorema 1.100, temos que $A \cdot adj(A) = adj(A) \cdot A = \det(A)I_n$. Assim, sendo $\det(A) \neq 0$, podemos concluir que

$$A\left(\frac{1}{\det(A)}adj(A)\right) = \left(\frac{1}{\det(A)}adj(A)\right)A = I_n.$$

Logo, A é inversível e sua inversa é

$$A^{-1} = \frac{1}{\det(A)}adj(A) \tag{1.7}$$

. □

Observação 1.105. *Com o teorema anterior é possível dar exemplos de matrizes quadradas que não são inversíveis. Por exemplo,*

$$A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

não é inversível pois $\det(A) = 0$.

Exemplo 1.106. *Considere a matriz*

$$A = \begin{pmatrix} 6 & 2 \\ 11 & 4 \end{pmatrix}.$$

$\det(A) = 24 - 22 = 2 \neq 0$ *e, portanto, existe a inversa de A. Calculemos a inversa pela fórmula* (1.7). *Desenvolvendo os cálculos, obtemos*

$$\overline{A} = \begin{pmatrix} 4 & -11 \\ -2 & 6 \end{pmatrix} \quad e \quad adj(A) = \begin{pmatrix} 4 & -2 \\ -11 & 6 \end{pmatrix}.$$

Então,

$$A^{-1} = \frac{1}{\det(A)}adj(A) = \frac{1}{2}\begin{pmatrix} 4 & -2 \\ -11 & 6 \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -\frac{11}{2} & 3 \end{pmatrix}.$$

1.13 Matrizes Elementares

Definição 1.107. *Dada uma matriz A, entende-se por Operações Elementares sobre as Linhas de A, qualquer uma das seguintes operações:*

1. *permutar duas linhas de A;*
2. *multiplicar todos os elementos de uma linha por uma número não nulo;*
3. *substituir uma linha pela soma dela mesma com um múltiplo de outra.*

Observação 1.108. *Note que todas as 3 operações elementares sobre linhas são reversíveis, ou seja, ao aplicar uma operação e obter outra matriz, pode-se voltar para a matriz original com a aplicação da mesma operação adequandamente.*

Exemplo 1.109. *Temos por exemplo:*

$$A = \begin{pmatrix} 1 & 2 \\ 1 & 0 \end{pmatrix} : \quad \textit{Operação 1} \longmapsto \quad \begin{pmatrix} 1 & 0 \\ 1 & 2 \end{pmatrix} : \quad \textit{Operação 1} \longmapsto \quad \begin{pmatrix} 1 & 2 \\ 1 & 0 \end{pmatrix},$$

$$B = \begin{pmatrix} 2 & 2 & 3 \\ 0 & 1 & 0 \end{pmatrix} : \textit{ Operação 2} \longmapsto \begin{pmatrix} 2 & 2 & 3 \\ 0 & 5 & 0 \end{pmatrix} : \textit{ Operação 2} \longmapsto \begin{pmatrix} 2 & 2 & 3 \\ 0 & 1 & 0 \end{pmatrix}$$

e

$$C = \begin{pmatrix} 2 & 1 \\ 0 & 1 \\ 3 & 1 \end{pmatrix} : \quad \textit{Operação 3} \longmapsto \quad \begin{pmatrix} 2 & 1 \\ 0 & 1 \\ 7 & 3 \end{pmatrix} : \quad \textit{Operação 3} \longmapsto \quad \begin{pmatrix} 2 & 1 \\ 0 & 1 \\ 3 & 1 \end{pmatrix}.$$

Definição 1.110. *Uma Matriz Elementar é uma matriz obtida a partir da matriz identidade I_n, através da execusão de uma única operação elementar sobre as linhas de I_n.*

Exemplo 1.111. *Temos por exemplo:*

$$I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} : \quad \textit{Operação 1} \longmapsto \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

$$I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} : \quad \textit{Operação 2} \longmapsto \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 3 \end{pmatrix}$$

e

$$I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} : \quad \textit{Operação 3} \longmapsto \quad \begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Observação 1.112. *Uma matriz elementar E_1 é inversível e sua inversa é a matriz elementar E_2, que corresponde à matriz obtida por efetuar a operação inversa com linhas da operação efetuada para obter E_1.*

Teorema 1.113. *Seja E uma matriz elementar obtida de I_n. Se A é uma matriz $m \times n$, então EA é igual a matriz obtida de A efetuando-se a mesma operação elementer para se obter E.*

Demonstração. Faremos a prova de um caso particular que pode ser falcilmente adaptado para qualquer outro caso. Considere I_3,

$$E = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ k & 0 & 1 \end{bmatrix} \qquad \text{e} \qquad A = \begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \end{bmatrix},$$

onde E é obtida de I_3 pela operação elementar 3, com k um número real. Efetuando a multiplicação das matrizes, obtemos

$$EA = \begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ ka_{11} + a_{31} & ka_{12} + a_{32} & ka_{13} + a_{33} & ka_{14} + a_{34} \end{bmatrix},$$

que é exatamente a matriz obtida quando efetua-se a operação 3 na matriz A. □

Teorema 1.114. *Seja A uma matriz $n \times n$. A é inversível se, e somente se,*

$$A = E_k^{-1} \cdots E_2^{-1} E_1^{-1},$$

onde $E_1, E_2, \ldots, E_k$ são matrizes elementares.

A demonstração desse teorema, apesar de simples, não a apresentaremos aqui. O leitor pode encontrá-la [2, página 58].

Na prática, operamos simultaneamente com as matrizes A e I, através de operações elementares, até chegarmos à matriz I na posição correspondete à matriz A. A matriz obtida no lugar correspondente à matriz I será a inversa de A:

$$(A|I) \longrightarrow (I|A^{-1}).$$

Exemplo 1.115. *Seja*

$$A = \begin{pmatrix} 1 & 2 & 7 \\ 0 & 3 & 1 \\ 0 & 5 & 2 \end{pmatrix}.$$

Coloquemos a matriz junto com a matriz identidade e apliquemos as operações elementares sobre linhas, para reduzir a parte esquerda (que corresponde a A) à forma da identidade. Cada operação deve ser efetuada simultaneamente na parte direita da matriz:

$$\left(\begin{array}{ccc|ccc} 1 & 2 & 7 & 1 & 0 & 0 \\ 0 & 3 & 1 & 0 & 1 & 0 \\ 0 & 5 & 2 & 0 & 0 & 1 \end{array}\right).$$

Trocando a segunda e terceira linhas, obtemos:

$$\left(\begin{array}{ccc|ccc} 1 & 2 & 7 & 1 & 0 & 0 \\ 0 & 5 & 2 & 0 & 0 & 1 \\ 0 & 3 & 1 & 0 & 1 & 0 \end{array}\right).$$

Somamos à segunda a terceira linha multiplicada por -2:

$$\left(\begin{array}{ccc|ccc} 1 & 2 & 7 & 1 & 0 & 0 \\ 0 & -1 & 0 & 0 & -2 & 1 \\ 0 & 3 & 1 & 0 & 1 & 0 \end{array}\right).$$

Multiplicamos a segunda linha por -1*:*

$$\left(\begin{array}{ccc|ccc} 1 & 2 & 7 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 2 & -1 \\ 0 & 3 & 1 & 0 & 1 & 0 \end{array}\right).$$

Somamos à primeira a segunda linha multiplicads por -2*:*

$$\left(\begin{array}{ccc|ccc} 1 & 0 & 7 & 1 & -4 & 2 \\ 0 & 1 & 0 & 0 & 2 & -1 \\ 0 & 3 & 1 & 0 & 1 & 0 \end{array}\right).$$

Somamos à terceira a segunda linha multiplicada por -3*:*

$$\left(\begin{array}{ccc|ccc} 1 & 0 & 7 & 1 & -4 & 2 \\ 0 & 1 & 0 & 0 & 2 & -1 \\ 0 & 0 & 1 & 0 & -5 & 3 \end{array}\right).$$

Somamos à primeira a terceira linha multiplicada por -7*:*

$$\left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 31 & -19 \\ 0 & 1 & 0 & 0 & 2 & -1 \\ 0 & 0 & 1 & 0 & -5 & 3 \end{array}\right).$$

Finalmente, obtemos a identidade à esquerda e a inversa de A *à direita. Portanto,*

$$A^{-1}\left(\begin{array}{ccc} 1 & 31 & -19 \\ 0 & 2 & -1 \\ 0 & -5 & 3 \end{array}\right).$$

1.14 Matrizes e aritmética modular

Unindo os estudos que já desenvolvemos, vamos agora apresentar alguns breves resultados que relacionam propriedades de matrizes consideradas com artimética modular.

Definição 1.116. *Dados* $m \in \mathbb{Z}, m > 0$*, e as matrizes*

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1l} \\ a_{21} & a_{22} & \dots & a_{2l} \\ \vdots & \vdots & \ddots & \vdots \\ a_{k1} & a_{k2} & \dots & a_{kl} \end{pmatrix} \quad e \quad B = \begin{pmatrix} b_{11} & b_{12} & \dots & b_{1l} \\ b_{21} & b_{22} & \dots & b_{2l} \\ \vdots & \vdots & \ddots & \vdots \\ b_{k1} & b_{k2} & \dots & b_{kl} \end{pmatrix},$$

com $a_{ij}, b_{ij} \in \mathbb{Z}, 1 \leq i \leq k$ *e* $1 \leq j \leq l$*, dizemos que a matriz* A *é Congruente a matriz* B *quando* $a_{ij} \equiv b_{ij} \pmod{m}$*, para* $1 \leq i \leq k$ *e* $1 \leq j \leq l$*, e denotamos por*

$$A \equiv B \pmod{m}.$$

De modo análogo, temos a Propriedade 8 e o Teorema 1.100 para matrizes com aritmética modular.

Teorema 1.117. *Se A e B são matrizes quadrada com entradas de $\mathbb{Z}$ e ordens n, então*

$$\det(AB) \equiv \det(A)\det(B) \pmod{m}.$$

Demonstração. Por simplicidade, vamos demonstrar o caso $n = 2$. Considere

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \qquad \text{e} \qquad B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix},$$

com $a_{ij}, b_{ij} \in \mathbb{Z}, 1 \leq i \leq 2$ e $1 \leq j \leq 2$, de modo que

$$AB = \begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}a_{21} & a_{21}b_{12} + a_{22}b_{22} \end{pmatrix}.$$

Então,

$$\begin{aligned} \det(AB) &\equiv (a_{11}b_{11} + a_{12}b_{21})(a_{21}b_{12} + a_{22}b_{22}) - (a_{11}b_{12} + a_{12}b_{22})(a_{21}b_{11} + a_{22}a_{21}) \\ &\equiv (a_{11}a_{22} - a_{12}a_{21})(b_{11}b_{22} - b_{12}b_{21}) \\ &\equiv \det(A)\det(B) \pmod{m}. \end{aligned}$$

□

Teorema 1.118. *Se A é matriz quadrada com entradas de $\mathbb{Z}$ e ordem n e I_n é a matriz identidade de ordem n, então*

$$A \cdot adj(A) \equiv adj(A) \cdot A \equiv \det(A) I_n \pmod{m}.$$

Demonstração. Por simplicidade, vamos demonstrar o caso $n = 2$. Considere

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

com $a_{ij} \in \mathbb{Z}, 1 \leq i \leq 2$ e $1 \leq j \leq 2$, de modo que

$$adj(A) = \begin{pmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{pmatrix}.$$

Então,

$$A \cdot adj(A) = \begin{pmatrix} a_{11}a_{22} - a_{12}a_{21} & 0 \\ 0 & a_{11}a_{22} - a_{12}a_{21} \end{pmatrix} \equiv \det(A) I_2 \pmod{m}.$$

De forma análoga, obtemos

$$adj(A) \cdot A \equiv \det(A) I_2 \pmod{m}.$$

□

Com os dois resultados anteiores podemos demonstrar o análogo em aritimética modular do Teorema 1.104.

Definição 1.119. *Dada uma matriz quadrada A com entradas em $\mathbb{Z}$ e de ordem n, diz-se que A é inversível* (mod m) *quando existe uma matriz B de ordem n tal que $AB \equiv BA \equiv I_n \pmod{m}$. Quando a matriz B existe, diz-se que ela é a inversa de A* (mod m) *e denotamos $B = A^{-1}$ e dizemos A^{-1} é a inversa de A* (mod m).

Teorema 1.120. *Uma matriz quadrada A com entradas em $\mathbb{Z}$ é inversível módulo m se, e somente se, o resíduo de* $\det(A)$ *módulo m tem um inverso multiplicativo módulo m.*

Demonstração. A demonstração é análoga ao caso real.
($\Rightarrow$) Se A é inversível módulo m, então existe matriz quadrada A^{-1} tal que $AA^{-1} \equiv A^{-1}A \equiv I_n \pmod{m}$. Logo, temos

$$\det(AA^{-1}) \equiv \det(A^{-1}A) \equiv \det(I_n) \pmod{m}.$$

Pelo Teorema 1.117„ juntamente com o fato que $\det(I_n) \equiv 1 \pmod{m}$, temos que

$$\det(A)\det(A^{-1}) \equiv \det(A^{-1})\det(A) \equiv 1 \pmod{m}.$$

Concluímos então que $\det(A)$ tem um inverso multiplicativo (mod m).
($\Leftarrow$) Suponha agora que $\det(A)$ tem um inverso multiplicativo (mod m). Sendo A uma matriz quadrada de ordem n, pelo Teorema 1.118, temos que

$$A \cdot adj(A) \equiv adj(A) \cdot A \equiv \det(A) I_n \pmod{m}.$$

Assim, tendo $\det(A)$ um inverso multiplicativo (mod m), podemos concluir que

$$A\left(\frac{1}{\det(A)} adj(A)\right) \equiv \left(\frac{1}{\det(A)} adj(A)\right) A \equiv I_n \pmod{m}.$$

Logo, A é inversível e sua inversa é

$$A^{-1} = \frac{1}{\det(A)} adj(A) \pmod{m}. \tag{1.8}$$

. □

Sabemos que o resíduo do $\det(A)$ módulo m só terá um inverso multiplicativo módulo m se, e somente se, este resíduo e m não tiverem fator primo comum. Temos o seguinte corolário.

Corolário 1.121. *Uma matriz quadrada A com entradas em $\mathbb{Z}$ é invertível módulo m se, e somente se, m e o resíduo de* $\det(A)$ *módulo m não têm fatores primos em comuns.*

Como os únicos fatores primos de $m = 26$ são 2 e 13, temos o seguinte corolário.

Corolário 1.122. *Uma matriz quadrada A com entradas em $\mathbb{Z}_{26}$ é invertível módulo* 26 *se, e somente se, o resíduo de* $\det(A)$ *módulo* 26 *não é divisível por* 2 *ou* 13.

Caso particular:

Se

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

tem entradas em $\mathbb{Z}$ e o $\det(A) = ad - bc \pmod{m}$ é relativamente primo com m, então a inversa de $\det(A) \pmod{m}$ é dada por:

$$A^{-1} = (ad - bc)^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \pmod{m} \tag{1.9}$$

onde $(ad - bc)^{-1}$ é o inverso de $ad - bc \pmod{m}$.

Exemplo 1.123. *Encontre a inversa de*

$$A = \begin{pmatrix} 5 & 3 \\ 8 & 5 \end{pmatrix}$$

módulo 26.
Solução: *O* $\det(A) = ad - bc = 5 \cdot 5 - 3 \cdot 8 = 25 - 24 = 1$. *Logo,* $(ad - bc)^{-1} = 1^{-1} \equiv 1 \pmod{26}$ *(inverso multiplicativo). Assim por* (1.9)*, temos:*

$$A^{-1} = 1 \begin{pmatrix} 5 & -3 \\ -8 & 5 \end{pmatrix} \equiv \begin{pmatrix} 5 & 23 \\ 18 & 5 \end{pmatrix} \pmod{26}.$$

Capítulo 2

Códigos Elementares e Criptografia

A criptografia representa a transformação de textos comuns em mensagens codificadas, que tem como objetivo ocultar a informação para que pessoas não autorizadas não tenham acesso, garantindo privacidade. A palavra criptografia tem origem grega (kriptos = escondido, oculto e grifo = grafia) e representa a ciência dos códigos, na qual se utiliza um conjunto de técnicas que transformam uma mensagem em códigos através de um processo chamado codificação, permitindo que apenas o destinatário desejado consiga decodificar e ler a mensagem, a partir do processo inverso, a decodificação.

Mas afinal, o que é um código? Segundo o minidicionário (ver [6]), código é um conjunto de sinais convencionais ou secretos utilizados em correspondências e comunicações, ou seja, código é um conjunto de substitutos para uma determinada informação.

Do ponto de vista matemático, baseado em [1], podemos definir um código da seguinte forma:

Definição 2.1. *Um Código é um sistema formado por um quíntuplo* (T, C, K, S, D), *onde*

- T *é o conjunto formado pelos caracteres do texto comum (mensagem original).*
- C *é o conjunto formado pelos caracteres da mensagem codificada.*
- K *é um conjunto de chaves que obedecem determinadas regras.*
- S *é o conjunto de regras de codificação.*
- D *é o conjunto de regras de decodificação.*

que satisfaz a seguinte condição:

> *para cada* $k \in K$ *existe uma regra para codificar,* $s_k \in S$, *e uma regra correspondente para decodificar,* $d_k \in D$, *tais que* $s_k : T \longrightarrow C$, $d_k : C \longrightarrow T$ *e* $d_k(s_k(t)) = t$, *para qualquer* $t \in T$.

A Figura 2.1 ilustra a Definição 2.1. Existem duas maneiras simples de transformar uma mensagens em códigos, ou seja, de criptografar mensagens. A primeira delas procura esconder o conteúdo da mensagem através de códigos

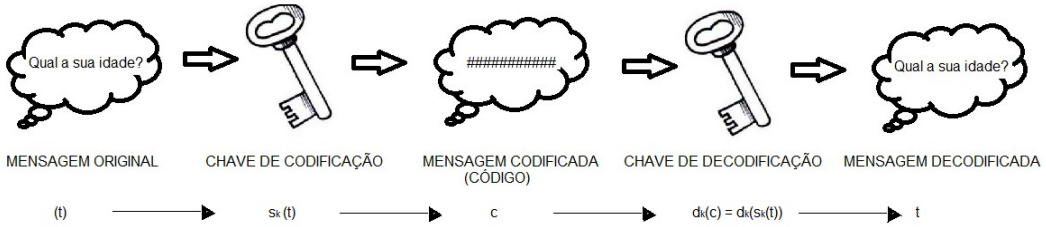


Figura 2.1: Ilustração

predefinidos entre as partes envolvidas na troca de mensagens. Imagine a seguinte situação: uma rebelião em um presídio e o comandante da operação juntamente com os policiais devem decidir se vão invadir ou não o presídio. Para isso, o comandante diz que vai analisar a situação e, de acordo com a análise, decidir o que fazer. Se ele gritar a palavra "TRANQUE" é para invadir o presídio, mas se ele gritar "PREMA", não deve invadir. Dessa maneira, se a mensagem cair em mãos erradas nada acontecerá já que não terá significado. No entanto, ao tomar uma decisão que não seja nenhuma dessas duas, ele não terá como avisar aos policiais, uma vez que esse tipo de troca de mensagens só dá certo se essas forem predefinidas anteriormente, o que faz com que essa maneira de trocar mensagens se torne frágil. A outra maneira de codificar mensagem é usando as técnicas de criptografia. Neste caso, podemos destacar os seguintes tipos de codificações:

- Código de Júlio César: Consiste em trocar cada letra pela terceira letra subsequente do alfabeto.
- Código Afim: É uma generalização do código de Júlio César, baseado na substituição cíclica do alfabeto.
- Código de Vigenère: É um método de codificação que usa uma série de diferentes códigos de Júlio César generalizado com diferentes valores de deslocamento baseado em letras de uma chave.
- Código de Hill: Nesse tipo de código, a mensagem é dividida em blocos e codificada através de operações com matrizes.
- Sistema RSA: Baseia-se na dificuldade para descobrir os fatores primos existentes em números muito grandes.
- O código de Rabin: Baseia-se na dificuldade de fatorar inteiros, assim como o Sistema RSA.
- O Método MH (Merkle e Hellman): Este método foi criado por Merkle e Hellman, em 1978, baseando-se na dificuldade do chamado **Problema da Mochila**.
- Código ElGamal: É um sistema com o uso de chaves assimétricas, criado pelo estudioso de criptografia egípcio Taher Elgamal, em 1984. Sua segurança se baseia na dificuldade de solução que o problema do logaritmo discreto pode apresentar.

A principal vantagem na utilização desses códigos é a não limitação das possíveis mensagens a serem enviadas, além de se tornarem mais difíceis de serem decodificadas. Todo o conhecimento adquirido e exposto neste capítulo é com base em [1], [2] e [15].

2.1 Código de César

O código de César, conhecido também como código de substituição, é uma das mais simples e conhecidas técnicas de criptografia, além de ser um caso particular do código Afim, como veremos na próxima seção. O nome desse código é em homenagem a Júlio César, o imperador romano, que o usava para enviar ordens secretas aos seus generais.

Considerando-se o alfabeto, o código de César consiste em trocar cada letra pela terceira letra subsequente. Observe na Tabela 2.1 que as letras da primeira e terceira linhas representam o alfabeto comum e as letras da segunda e quarta linhas representam o **código**.

A	B	C	D	E	F	G	H	I	J	K	L	M
D	E	F	G	H	I	J	K	L	M	N	O	P
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Tabela 2.1: Codificação de César

Nesse tipo de codificação, a fonte A escreve uma mensagem em código e envia para a fonte B. Após receber a mensagem, a fonte B utiliza a Tabela 2.1 e transforma a mensagem codificada em alfabeto comum, decifrando a mensagem. Portanto, a chave dessa comunicação é a Tabela 2.1.

Exemplo 2.2. *Considere a mensagem:*

DGRUR FULSXRJUDILD.

Se a fonte A envia esta mensagem para a fonte B então, utilizando a Tabela 2.1, a fonte B decifra a mensagem e ver o que o texto diz:

ADORO CRIPTOGRAFIA.

Como veremos na próxima seção, o código de César é um caso particular do código Afim. Para tornar isto claro, representaremos cada letra do alfabeto por um número de dois dígitos, ou seja, a letra A é representada por 00, a letra B por 01, e sucessivamente até a letra Z por 25, conforme mostrado na Tabela 2.2.

De acordo com o que consiste o código de César e feita a representação das letras do alfabeto por números de dois dígitos, o código passa a ser constituído pela troca de cada número pelo terceiro número subsequente, veja a Tabela 2.3.

Podemos notar que o código de Júlio César baseia-se na seguinte fórmula de congruência (Veja Tabela 2.3):

$$\alpha \equiv (\beta + 03) \bmod 26 \tag{2.1}$$

A	B	C	D	E	F	G	H	I	J	K	L	M
00	01	02	03	04	05	06	07	08	09	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Tabela 2.2: Representação do Alfabeto por Dígitos

00	01	02	03	04	05	06	07	08	09	10	11	12
03	04	05	06	07	08	09	10	11	12	13	14	15
13	14	15	16	17	18	19	20	21	22	23	24	25
16	17	18	19	20	21	22	23	24	25	01	02	03

Tabela 2.3: Codificação de César em Números de Dois Dígitos

onde α representa os números codificados (veja Tabela 2.3) e β os números que representam cada letra do alfabeto (veja Tabela 2.2). Podemos também fazer o processo inverso, isto é, decifrar a mensagem. Para isso é necessário calcular β em termos de α, podendo ser calculado através de:

$$\beta \equiv (\alpha - 03) \bmod 26. \tag{2.2}$$

Exemplo 2.3. *Observe a mensagem:*

1114172407011723

Usando a Tabela 2.3, o texto decifrado é I LOVE YOU.

Exemplo 2.4. *Codifique a mensagem "O COPO QUEBROU". Usando* (2.1) *e a Tabela 2.2, temos:*

$$\begin{aligned}
O &\longrightarrow 14+03 \equiv 17 \bmod 26 \longrightarrow R\\
C &\longrightarrow 02+03 \equiv 05 \bmod 26 \longrightarrow F\\
O &\longrightarrow 14+03 \equiv 17 \bmod 26 \longrightarrow R\\
P &\longrightarrow 15+03 \equiv 18 \bmod 26 \longrightarrow S\\
O &\longrightarrow 14+03 \equiv 17 \bmod 26 \longrightarrow R\\
Q &\longrightarrow 16+03 \equiv 19 \bmod 26 \longrightarrow T\\
U &\longrightarrow 20+03 \equiv 23 \bmod 26 \longrightarrow X\\
E &\longrightarrow 04+03 \equiv 07 \bmod 26 \longrightarrow H\\
B &\longrightarrow 01+03 \equiv 04 \bmod 26 \longrightarrow E\\
R &\longrightarrow 17+03 \equiv 20 \bmod 26 \longrightarrow U\\
O &\longrightarrow 14+03 \equiv 17 \bmod 26 \longrightarrow R\\
U &\longrightarrow 20+03 \equiv 23 \bmod 26 \longrightarrow X.
\end{aligned}$$

Logo, a mensagem codificada é "RFRSRTXHEURX".

2.2 Códigos Afins

Como já mencionado na seção anterior, o código afim é uma generalização do código de Júlio César - JC. Relembrando que no código de JC a posição das letras

do texto e os códigos obedecem a congruência $\alpha \equiv (\beta + 3) \text{mod } 26$. Agora, seja k (chamado chave) um inteiro satisfazendo $0 \leq k \leq 25$. Em vez de utilizarmos o número 3 no código JC, iremos usar k e definir um novo código que chamaremos de código JC generalizado. Poderíamos imaginar esse código como um código baseado na substituição cíclica do alfabeto, através do uso de dois discos concêntricos contendo todas as letras, tornando dessa forma a substituição mais simples (veja a Figura 2.2, retirada de [25]).

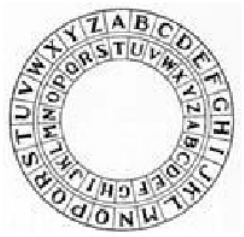


Figura 2.2: Discos Concêntricos Contendo Todas as Letras do Alfabeto

Podemos representar o código JC generalizado baseado na seguinte fórmula:

$$\alpha \equiv (\beta + k) \text{ mod } 26,$$

onde k, um inteiro satisfazendo $0 \leq k \leq 25$, é a chave de codificação, β é a posição da letra (veja a Tabela 2.2) e α representa a posição da nova letra. Dessa forma, obtemos a mensagem codificada. Observe que quando $k = 0$ o código obtido é exatamento o texto da mensagem sem alterações e quando $k = 3$ temos o código JC. No entanto, para decodificar a mensagem, é necessário encontrar a chave de decodificação. Para tanto, basta encontrar j tal que $(j + k) \equiv 0 \text{ mod } 26$ (Ver Defiição 1.47, simétrico aditivo), trocar k por j e proceder da mesma maneira.

Exemplo 2.5. *Observe como codificar a frase "ESTOU COM FRIO", usando como chave* $k = 15$*, ou seja,* $\alpha \equiv (\beta + 15) \text{ mod } 26$.

$$\begin{aligned}
E &\longrightarrow 04 + 15 \equiv 19\text{mod } 26 \longrightarrow T \\
S &\longrightarrow 18 + 15 \equiv 07\text{mod } 26 \longrightarrow H \\
T &\longrightarrow 19 + 15 \equiv 08\text{mod } 26 \longrightarrow I \\
O &\longrightarrow 14 + 15 \equiv 03\text{mod } 26 \longrightarrow D \\
U &\longrightarrow 20 + 15 \equiv 09\text{mod } 26 \longrightarrow J \\
C &\longrightarrow 02 + 15 \equiv 17\text{mod } 26 \longrightarrow R \\
O &\longrightarrow 14 + 15 \equiv 03\text{mod } 26 \longrightarrow D \\
M &\longrightarrow 12 + 15 \equiv 01\text{mod } 26 \longrightarrow B \\
F &\longrightarrow 05 + 15 \equiv 20\text{mod } 26 \longrightarrow U \\
R &\longrightarrow 17 + 15 \equiv 06\text{mod } 26 \longrightarrow G \\
I &\longrightarrow 08 + 15 \equiv 23\text{mod } 26 \longrightarrow X \\
O &\longrightarrow 14 + 15 \equiv 03\text{mod } 26 \longrightarrow D.
\end{aligned}$$

Portanto, a mensagem codificada é

"THIDJRDBUGXD".

Para decodificar a mensagem, considerando que $15 + 11 \equiv 0 \bmod 26$ *(Definição 1.47, inverso aditivo), temos que a chave decodificadora é* 11*. Logo, procede-se assim:*

$$
\begin{aligned}
T &\longrightarrow 19 + 11 \equiv 04 \bmod 26 \longrightarrow E \\
H &\longrightarrow 07 + 11 \equiv 18 \bmod 26 \longrightarrow S \\
I &\longrightarrow 08 + 11 \equiv 19 \bmod 26 \longrightarrow T \\
D &\longrightarrow 03 + 11 \equiv 14 \bmod 26 \longrightarrow O \\
J &\longrightarrow 09 + 11 \equiv 20 \bmod 26 \longrightarrow U \\
R &\longrightarrow 17 + 11 \equiv 02 \bmod 26 \longrightarrow C \\
D &\longrightarrow 03 + 11 \equiv 14 \bmod 26 \longrightarrow O \\
B &\longrightarrow 01 + 11 \equiv 12 \bmod 26 \longrightarrow M \\
U &\longrightarrow 20 + 11 \equiv 05 \bmod 26 \longrightarrow F \\
G &\longrightarrow 06 + 11 \equiv 17 \bmod 26 \longrightarrow R \\
X &\longrightarrow 23 + 11 \equiv 08 \bmod 26 \longrightarrow I \\
D &\longrightarrow 03 + 11 \equiv 14 \bmod 26 \longrightarrow O.
\end{aligned}
$$

Definição 2.6. *Chamaremos de código afim a codificação baseada na troca de letras do alfabeto através da regra de congruência*

$$\alpha \equiv (a \cdot \beta + b) \bmod 26, \tag{2.3}$$

onde a *e* b *são números inteiros com* $0 \leq a \leq 25$ *e* $0 \leq b \leq 25$ *e o* $mdc(a, 26) = 1$*. Os números* a *e* b *são chamados chaves do código afim.*

Para decodificar uma mensagem no código afim, a congruência pode ser escrita assim:

$$a.\beta \equiv (\alpha - b) \bmod 26.$$

Como o $mdc(a, 26) = 1$, isso garante que existe i tal que $a.i \equiv 1 \bmod 26$ (Definição 1.48, inverso multiplicativo). Assim, multiplicando ambos os membros por i teremos:

$$i.a.\beta \equiv i.(\alpha - b) \bmod 26.$$

Logo,

$$\beta \equiv i.(\alpha - b) \bmod 26. \tag{2.4}$$

Portanto, com essa congruência podemos determinar o texto e o conteúdo dessa mensagem.

Observe que, a partir da congruência (2.3), obtemos o código JC generalizado fazendo $a = 1$. Com isto surge o seguinte questionamento: quantos códigos de JC generalizados e quantos códigos afins existem?

Teorema 2.7. i) *Existem* 26 *códigos de JC generalizados;*

ii) *Existem* 312 *códigos afins.*

Demonstração. **i)** Os códigos de JC dependem unicamente do valor de k, onde $0 \leq k \leq 25$. Logo existem 26 possibilidades para a escolha de k.
ii) Nos códigos afins, a condição $mdc(a, 26) = 1$ mostra que há 12 possibilidades $(1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25)$ para escolher a. Uma vez que o valor de a foi escolhido, temos 26 opções para b e, portanto, no total $12 \times 26 = 312$ maneiras de escolher a e b. □

Exemplo 2.8. *Utilizando a Tabela 2.2 e sabendo que $a = 5$ e $b = 11$ são as chaves da codificação, codifique a palavra "UNIVERSO".*
Solução: *Vamos representar em uma tabela a mensagem que será codificada com seus respectivos valores de β. De acordo com a Tabela 2.4 e aplicando a fórmula*

	U	N	I	V	E	R	S	O
β	20	13	08	21	04	17	18	14

Tabela 2.4:

(2.3), *temos:*

$$\alpha \equiv (5 \cdot 20 + 11) \bmod 26 \Rightarrow \alpha = 7 = H;$$
$$\alpha \equiv (5 \cdot 13 + 11) \bmod 26 \Rightarrow \alpha = 24 = Y;$$
$$\alpha \equiv (5 \cdot 8 + 11) \bmod 26 \Rightarrow \alpha = 25 = Z;$$
$$\alpha \equiv (5 \cdot 21 + 11) \bmod 26 \Rightarrow \alpha = 12 = M;$$
$$\alpha \equiv (5 \cdot 4 + 11) \bmod 26 \Rightarrow \alpha = 5 = F;$$
$$\alpha \equiv (5 \cdot 17 + 11) \bmod 26 \Rightarrow \alpha = 18 = S;$$
$$\alpha \equiv (5 \cdot 18 + 11) \bmod 26 \Rightarrow \alpha = 23 = X;$$
$$\alpha \equiv (5 \cdot 14 + 11) \bmod 26 \Rightarrow \alpha = 3 = D;$$

Portanto, a mensagem codificada é "HYZMFSXD".

Exemplo 2.9. *Utilizando a Tabela 2.2 e sabendo que $a = 7$ e $b = 12$ são as chaves da codificação, decodifique a palavra "TBMIQL".*
Solução: *Vamos representar em uma tabela a mensagem que será decodificada com seus respectivos valores de α. Como o $mdc(7, 26) = 1$, isso garante que existe i*

	T	B	M	I	Q	L
α	19	01	12	08	16	11

Tabela 2.5:

tal que $7.i \equiv 1 \bmod 26$ (Definição 1.48, inverso multiplicativo) e portanto $i = 15$. Conhecendo i, α (veja Tabela 2.5) e b, e aplicando essas informações em (2.4), *conseguimos decodificar a mensagem. Observe que:*

$$\beta \equiv 15 \cdot (19 - 12) \bmod 26 \Rightarrow \beta = 1 = B;$$
$$\beta \equiv 15 \cdot (1 - 12) \bmod 26 \Rightarrow \beta = 17 = R;$$
$$\beta \equiv 15 \cdot (12 - 12) \bmod 26 \Rightarrow \beta = 0 = A;$$
$$\beta \equiv 15 \cdot (8 - 12) \bmod 26 \Rightarrow \beta = 18 = S;$$
$$\beta \equiv 15 \cdot (16 - 12) \bmod 26 \Rightarrow \beta = 8 = I;$$
$$\beta \equiv 15 \cdot (11 - 12) \bmod 26 \Rightarrow \beta = 11 = L.$$

Portanto, a mensagem decodificada é "BRASIL".

2.3 Código de Vigenère

O Código de Vigenère[1] é um método de codificação que usa uma série de diferentes códigos de Júlio César generalizado com diferentes valores de deslocamento baseado em letras de uma chave. A codificação pode ser escrita algebricamente como:

$$C_i \equiv (P_i + a_i)(\text{mod } m), \tag{2.5}$$

e a decodificação como

$$P_i \equiv (C_i - a_i)(\text{mod } m) \tag{2.6}$$

e a chave como

$$a_i \equiv (C_i - P_i)(\text{mod } m) \tag{2.7}$$

onde P_i corresponde aos valores das letras a serem codificadas, a_i aos valores das letras da chave, C_i aos valores das letras codificadas e m representa a congruência envolvida ($\mathbb{Z}_m$).

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Q	R	S	T	U	V	W	X	Y	Z	?	Á	Ã	É	[ ]	
17	18	19	20	21	22	23	24	25	26	27	28	29	30	0	

Tabela 2.6:

Exemplo 2.10. *De acordo com a Tabela 2.6, codifique a mensagem "FRONTEIRAS DO BRASIL" utilizando a chave TIGRE.*
***Solução**: Vamos representar em uma tabela a mensagem que será codificada com sua respectiva chave. De acordo com a Tabela 2.7 e aplicando* (2.5)*, temos:*

F	R	O	N	T	E	I	R	A	S		D	O		B	R	A	S	I	L
6	18	15	14	20	5	9	18	1	19	0	4	15	0	2	18	1	19	9	12
T	I	G	R	E	T	I	G	R	E	T	I	G	R	E	T	I	G	R	E
20	9	7	18	5	20	9	7	18	5	20	9	7	18	5	20	9	7	18	5

Tabela 2.7:

$C_1 \equiv (6 + 20)(\text{mod } 31) \Rightarrow C_1 = 26 = Z;$
$C_2 \equiv (18 + 9)(\text{mod } 31) \Rightarrow C_2 = 27 = ?;$
$C_3 \equiv (15 + 7)(\text{mod } 31) \Rightarrow C_3 = 22 = V;$
$C_4 \equiv (14 + 18)(\text{mod } 31) \Rightarrow C_4 = 1 = A;$
$C_5 \equiv (20 + 5)(\text{mod } 31) \Rightarrow C_5 = 25 = Y;$
$C_6 \equiv (5 + 20)(\text{mod } 31) \Rightarrow C_6 = 25 = Y;$
$C_7 \equiv (9 + 9)(\text{mod } 31) \Rightarrow C_7 = 18 = R;$
$C_8 \equiv (18 + 7)(\text{mod } 31) \Rightarrow C_8 = 25 = Y;$
$C_9 \equiv (1 + 18)(\text{mod } 31) \Rightarrow C_9 = 19 = S;$

[1]Este nome é uma homenagem erradamente atribuída a Blaise de Vigenère, uma vez que o código foi inventado e originalmente descrito por Giovan Batista Belaso em seu livro datado de 1553 com o título Lacifra del. Sig. Giovan Batista Belaso.

$C_{10} \equiv (19+5)(\text{mod } 31) \Rightarrow C_{10} = 24 = X$;
$C_{11} \equiv (0+20)(\text{mod } 31) \Rightarrow C_{11} = 20 = T$;
$C_{12} \equiv (4+9)(\text{mod } 31) \Rightarrow C_{12} = 13 = M$;
$C_{13} \equiv (15+7)(\text{mod } 31) \Rightarrow C_{13} = 22 = V$;
$C_{14} \equiv (0+18)(\text{mod } 31) \Rightarrow C_{14} = 18 = R$;
$C_{15} \equiv (2+5)(\text{mod } 31) \Rightarrow C_{15} = 7 = G$;
$C_{16} \equiv (18+20)(\text{mod } 31) \Rightarrow C_{16} = 7 = G$;
$C_{17} \equiv (1+9)(\text{mod } 31) \Rightarrow C_{17} = 10 = J$;
$C_{18} \equiv (19+7)(\text{mod } 31) \Rightarrow C_{18} = 26 = Z$;
$C_{19} \equiv (9+18)(\text{mod } 31) \Rightarrow C_{19} = 27 = ?$;
$C_{20} \equiv (12+5)(\text{mod } 31) \Rightarrow C_{20} = 17 = Q$;

Portanto, a mensagem codificada é "Z?VAYYRYSXTMVRGGJZ?Q".

Exemplo 2.11. *Utilizando a Tabela 2.6 e* (2.6)*, decodifique a mensagem abaixo, usando a palavra-chave CASA:*

$$FPDBCECAPVBER.$$

Solução: *Vamos representar em uma tabela a mensagem codificada com sua respectiva chave. De acordo com a Tabela 2.8 e aplicando a* (2.6)*, temos:*

F	P	D	B	C	E	C	A	P	V	B	E	R
6	16	4	2	3	5	3	1	16	22	2	5	18
C	A	S	A	C	A	S	A	C	A	S	A	C
3	1	19	1	3	1	19	1	3	1	19	1	3

Tabela 2.8:

$P_1 \equiv (6-3)(\text{mod } 31) \Rightarrow P_1 = 3 = C$;
$P_2 \equiv (16-1)(\text{mod } 31) \Rightarrow P_2 = 15 = O$;
$P_3 \equiv (4-19)(\text{mod } 31) \Rightarrow P_3 = 16 = P$;
$P_4 \equiv (2-1)(\text{mod } 31) \Rightarrow P_4 = 1 = A$;
$P_5 \equiv (3-3)(\text{mod } 31) \Rightarrow P_5 = 0 = [\ ]$;
$P_6 \equiv (5-1)(\text{mod } 31) \Rightarrow P_6 = 4 = D$;
$P_7 \equiv (3-19)(\text{mod } 31) \Rightarrow P_7 = 15 = O$;
$P_8 \equiv (1-1)(\text{mod } 31) \Rightarrow P_8 = 0 = [\ ]$;
$P_9 \equiv (16-3)(\text{mod } 31) \Rightarrow P_9 = 13 = M$;
$P_{10} \equiv (22-1)(\text{mod } 31) \Rightarrow P_{10} = 21 = U$;
$P_{11} \equiv (2-19)(\text{mod } 31) \Rightarrow P_{11} = 14 = N$;
$P_{12} \equiv (5-1)(\text{mod } 31) \Rightarrow P_{12} = 4 = D$;
$P_{13} \equiv (18-3)(\text{mod } 31) \Rightarrow P_{13} = 15 = O$;

Portanto, a mensagem decodificada é "COPA DO MUNDO".

Exemplo 2.12. *Dada a palavra em texto simples "TECNOLOGIA", e o seu respectivo texto codificado "ETUCPÁÉYÃB", encontre a chave que foi utilizada na codificação.*

Solução: *Vamos representar em uma tabela a mensagem e sua respectiva codificação. De acordo com a Tabela 2.17 e aplicando a fórmula* (2.7)*, temos:*

T	E	C	N	O	L	O	G	I	A
20	5	3	14	15	12	15	7	9	1
E	T	U	C	P	Á	É	Y	Ã	B
5	20	21	3	16	28	30	25	29	2

Tabela 2.9:

$a_1 \equiv (5-20)(\text{mod } 31) \Rightarrow a_1 = 16 = P;$
$a_2 \equiv (20-5)(\text{mod } 31) \Rightarrow a_2 = 15 = O;$
$a_3 \equiv (21-3)(\text{mod } 31) \Rightarrow a_3 = 18 = R;$
$a_4 \equiv (3-14)(\text{mod } 31) \Rightarrow a_4 = 20 = T;$
$a_5 \equiv (16-15)(\text{mod } 31) \Rightarrow a_5 = 1 = A;$
$a_6 \equiv (28-12)(\text{mod } 31) \Rightarrow a_6 = 16 = P;$
$a_7 \equiv (30-15)(\text{mod } 31) \Rightarrow a_7 = 15 = O;$
$a_8 \equiv (25-7)(\text{mod } 31) \Rightarrow a_8 = 18 = R;$
$a_9 \equiv (29-9)(\text{mod } 31) \Rightarrow a_9 = 20 = T;$
$a_{10} \equiv (2-1)(\text{mod } 31) \Rightarrow a_{10} = 1 = A;$

Portanto, a chave de codificação é "PORTA".

2.4 Código de Hill

Os códigos de substituição possuem uma desvantagem por serem relativamente fáceis de serem decodificados. No entanto, existem códigos que, ao invés de criptografar letra por letra, dividem o texto em grupos de letras. Esse tipo de código faz parte de um sistema poligráfico no qual um texto comum é dividido em conjuntos de n letras, cada um dos quais é substutuído por um conjunto de n letras codificadas. O código de Hill[2] representa uma classe de sistemas poligráficos. Neste tipo de código, vamos estabelecer para cada letra do texto comum e do texto codificado um valor numérico que especifica sua posição no alfabeto padrão (ver Tabela 2.10). Os espaços em branco entre letras ou palavras serão representados pelo símbolo [ ].

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	0

Tabela 2.10:

Nos casos mais simples do código de Hill, transformamos pares sucessivos de texto comum em texto codificado, por exemplo, utilizando a Tabela 2.10 e a estrutura do $\mathbb{Z}_{26}$, usando o seguinte procedimento:

1. Escolha uma matriz 2×2

[2]Em 1929 Lester S. Hill publicou seu livro Cryptography in an Algebraic Alphabet, no qual um bloco de texto comum é codificado através de operações com matrizes

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

com entradas inteiras para efetuar a codificação.

2. Agrupe letras sucessivas de texto comum em pares e substitua cada letra de texto comum por seu valor numérico. Se o texto comum tem um número ímpar de letras, adicione uma letra fictícia para completar o último par e proceda como antes.

3. Converta cada par sucessivo p_1, p_2 de letras de texto comum em um vetor-coluna
$$p = \begin{pmatrix} p_1 \\ p_2 \end{pmatrix}$$
e forme o produto Ap, onde p é o vetor comum e Ap o correspondente vetor codificado.

4. Converta cada vetor codificado em seu equivalente alfabético.

Exemplo 2.13. *Use a matriz*

$$A = \begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix}$$

para obter o código de Hill da mensagem de texto comum

$$CADEIRA.$$

Solução: *Primeiramente, devemos agrupar o texto comum em pares de letras e adicionar a letra fictícia A para completar o último par, já que o quantidade de letras que forma a palavra é ímpar, daí temos:*

$$CA \quad DE \quad IR \quad AA$$

ou ainda, usando a Tabela 2.10,

$$3\ 1 \quad 4\ 5 \quad 9\ 18 \quad 1\ 1.$$

Agora, devemos efetuar o produto matricial referente a cada par de letras. Para isso, observe que a tabela vai até o número 25*, logo, sempre que ocorrer um inteiro maior do que* 26*, ele será substituído pelo resto da divisão deste inteiro por* 26*, ou seja, devemos encontrar um novo número b que seja congruente a a módulo* 26*,* ($a \equiv\ b \bmod 26$)*. Começaremos, então, a codificação pelo par CA, assim temos:*

$$\begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix} \begin{pmatrix} 3 \\ 1 \end{pmatrix} = \begin{pmatrix} 3+2 \\ 0+3 \end{pmatrix} = \begin{pmatrix} 5 \\ 3 \end{pmatrix} \bmod 26,$$

que fornece o texto codificado EC pela Tabela 2.10. Dando sequência, iremos codificar o par DE,

$$\begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix} \begin{pmatrix} 4 \\ 5 \end{pmatrix} = \begin{pmatrix} 14 \\ 15 \end{pmatrix} \bmod 26,$$

que de acordo com a Tabela 2.10, fornece o texto codificado NO. Continuando, temos o codificação do par IR,

$$\begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix} \begin{pmatrix} 9 \\ 18 \end{pmatrix} = \begin{pmatrix} 45 \\ 54 \end{pmatrix} \equiv \begin{pmatrix} 19 \\ 2 \end{pmatrix} \bmod 26.$$

Dessa forma, obtemos o texto codificado SB pela Tabela 2.10 para o par IR.

Já o par AA, temos:

$$\begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 3 \\ 3 \end{pmatrix} \bmod 26,$$

de modo que o texto codificado é CC.

Juntando os pares codificados, obtemos a mensagem codificada completa que, normalmente, seria transmitida como um único texto sem espaços:

$$ECNOSBCC.$$

Observe que no Exemplo 2.13 o texto comum foi agrupado em pares e criptografado por uma matriz 2×2. Neste caso, dizemos que o código de Hill do exemplo é um **2 - código de Hill**. No entanto, podemos agrupar o texto comum em conjuntos de n letras e codificarmos com uma matriz codificadora $n \times n$ de entradas inteiras, neste caso, dizemos que o código de Hill é um **n- código de Hill**.

Exemplo 2.14. *Utilizando a matriz*

$$A = \begin{pmatrix} 7 & 8 & 1 \\ 12 & 23 & 14 \\ 22 & 4 & 21 \end{pmatrix}$$

como chave, codifique a mensagem "MATEMÁTICA É LEGAL" em $\mathbb{Z}_{32}$ tendo como referência a Tabela 2.11.

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26
Ê	?	Á	Ã	É	[ ]							
27	28	29	30	31	0							

Tabela 2.11:

Solução: *Convertendo a mensagem conforme Tabela 2.11, temos:*

$$MAT = \begin{pmatrix} 13 \\ 1 \\ 20 \end{pmatrix}, \; EMÁ = \begin{pmatrix} 5 \\ 13 \\ 29 \end{pmatrix}, \; TIC = \begin{pmatrix} 20 \\ 9 \\ 3 \end{pmatrix}, \; A\_É = \begin{pmatrix} 1 \\ 0 \\ 31 \end{pmatrix},$$

$$\_LE = \begin{pmatrix} 0 \\ 12 \\ 5 \end{pmatrix} \quad e \quad GAL = \begin{pmatrix} 7 \\ 1 \\ 12 \end{pmatrix}.$$

Para codificarmos a mensagem, basta multiplicar cada matriz 3×1 *obtida pela matriz codificadora A.*

$$\begin{pmatrix} 7 & 8 & 1 \\ 12 & 23 & 14 \\ 22 & 4 & 21 \end{pmatrix} \begin{pmatrix} 13 \\ 1 \\ 20 \end{pmatrix} = \begin{pmatrix} 23 \\ 11 \\ 6 \end{pmatrix} \bmod 32$$

$$\begin{pmatrix} 7 & 8 & 1 \\ 12 & 23 & 14 \\ 22 & 4 & 21 \end{pmatrix} \begin{pmatrix} 5 \\ 13 \\ 29 \end{pmatrix} = \begin{pmatrix} 8 \\ 29 \\ 3 \end{pmatrix} \bmod 32$$

$$\begin{pmatrix} 7 & 8 & 1 \\ 12 & 23 & 14 \\ 22 & 4 & 21 \end{pmatrix} \begin{pmatrix} 20 \\ 9 \\ 3 \end{pmatrix} = \begin{pmatrix} 23 \\ 9 \\ 27 \end{pmatrix} \bmod 32$$

$$\begin{pmatrix} 7 & 8 & 1 \\ 12 & 23 & 14 \\ 22 & 4 & 21 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 31 \end{pmatrix} = \begin{pmatrix} 6 \\ 30 \\ 1 \end{pmatrix} \bmod 32$$

$$\begin{pmatrix} 7 & 8 & 1 \\ 12 & 23 & 14 \\ 22 & 4 & 21 \end{pmatrix} \begin{pmatrix} 0 \\ 12 \\ 5 \end{pmatrix} = \begin{pmatrix} 5 \\ 26 \\ 25 \end{pmatrix} \bmod 32$$

$$\begin{pmatrix} 7 & 8 & 1 \\ 12 & 23 & 14 \\ 22 & 4 & 21 \end{pmatrix} \begin{pmatrix} 7 \\ 1 \\ 12 \end{pmatrix} = \begin{pmatrix} 5 \\ 19 \\ 26 \end{pmatrix} \bmod 32$$

Assim, a mensagem codificada é WKFHÁCWIÊFÃAEZYESZ.

2.4.1 Decodificando

Para decodificar os códigos de Hill, usamos a inversa (mod m) da matriz codificadora. Suponha que

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \ddots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}$$

é invertível módulo m e que esta matriz é usada para um $n-$código de Hill. Se

$$p = \begin{pmatrix} p_1 \\ p_2 \\ \vdots \\ p_n \end{pmatrix} \tag{2.8}$$

é um vetor comum, então

$$c = Ap \tag{2.9}$$

é o correspondente vetor codificado e

$$p = A^{-1}c.$$

Assim, cada vetor comum pode ser recuparado do correspondente vetor codificado pela multiplicação à esquerda por $A^{-1}(\text{mod } m)$.

O importante aqui, é saber quais as matrizes são invertíveis módulo m e como obter suas inversas, e para isso fazemos uso do Teorema 1.120, Corolário 1.121 e Corolário 1.122.

Exemplo 2.15. *Decodifique a mensagem*

$$SAKNOXAOJX$$

sabendo que é um código de Hill com matriz codificadora

$$A = \begin{pmatrix} 4 & 1 \\ 3 & 2 \end{pmatrix}.$$

Solução: *Primeiramente devemos encontrar a matriz inversa da matriz codificadora*

$$A = \begin{pmatrix} 4 & 1 \\ 3 & 2 \end{pmatrix}$$

módulo 26. *Assim por* (1.9), *temos que*

$$\det(A) = ad - bc = 4 \cdot 2 - 1 \cdot 3 = 8 - 3 = 5$$

de modo que

$$(ad - bc)^{-1} = 5^{-1} = 21(\text{mod } 26)$$

(inverso multiplicativo, veja Definição 1.48). Logo, por (1.9), *tem-se*

$$A^{-1} = 21 \begin{pmatrix} 2 & -1 \\ -3 & 4 \end{pmatrix} = \begin{pmatrix} 42 & -21 \\ -63 & 84 \end{pmatrix} = \begin{pmatrix} 16 & 5 \\ 15 & 6 \end{pmatrix} (\text{mod } 26).$$

Agora, encontrada a matriz inversa, daremos início à decodificação. Pela Tabela 2.10, o equivalente numérico do texto codificado é a Tabela 2.12, de modo que os correspondentes vetores codificados são:

$$p_1 = \begin{pmatrix} 19 \\ 1 \end{pmatrix}, \quad p_2 = \begin{pmatrix} 11 \\ 14 \end{pmatrix}, \quad p_3 = \begin{pmatrix} 15 \\ 24 \end{pmatrix}, \quad p_4 = \begin{pmatrix} 1 \\ 15 \end{pmatrix} \quad e \quad p_5 = \begin{pmatrix} 10 \\ 24 \end{pmatrix}.$$

S	A	K	N	O	X	A	O	J	X
19	1	11	14	15	24	1	15	10	24

Tabela 2.12:

Então, para obter os pares de texto comum, multiplicamos cada vetor codificado por A^{-1} *e pela Tabela 2.10 encontramos os equivalentes alfabéticos destes vetores:*

$$\begin{pmatrix} 16 & 5 \\ 15 & 6 \end{pmatrix}\begin{pmatrix} 19 \\ 1 \end{pmatrix} = \begin{pmatrix} 23 \\ 5 \end{pmatrix} (\text{mod } 26) : \begin{matrix} W \\ E \end{matrix}$$

$$\begin{pmatrix} 16 & 5 \\ 15 & 6 \end{pmatrix}\begin{pmatrix} 11 \\ 14 \end{pmatrix} = \begin{pmatrix} 12 \\ 15 \end{pmatrix} (\text{mod } 26) : \begin{matrix} L \\ O \end{matrix}$$

$$\begin{pmatrix} 16 & 5 \\ 15 & 6 \end{pmatrix}\begin{pmatrix} 15 \\ 24 \end{pmatrix} = \begin{pmatrix} 22 \\ 5 \end{pmatrix} (\text{mod } 26) : \begin{matrix} V \\ E \end{matrix}$$

$$\begin{pmatrix} 16 & 5 \\ 15 & 6 \end{pmatrix}\begin{pmatrix} 1 \\ 15 \end{pmatrix} = \begin{pmatrix} 13 \\ 1 \end{pmatrix} (\text{mod } 26) : \begin{matrix} M \\ A \end{matrix}$$

$$\begin{pmatrix} 16 & 5 \\ 15 & 6 \end{pmatrix}\begin{pmatrix} 10 \\ 24 \end{pmatrix} = \begin{pmatrix} 20 \\ 8 \end{pmatrix} (\text{mod } 26) : \begin{matrix} T \\ H \end{matrix} .$$

Logo, decodificando o código temos a seguinte mensagem

"WE LOVE MATH".

2.4.2 Quebrando um Código de Hill

O objetivo ao criptografar uma mensagem é fazer com que essa chegue com segurança ao seu destino. No entanto, agora será discutido uma técnica de quebrar o Código de Hill. Para isso, é necessário primeiro que seja feito uma análise do texto codificado. A partir dessa análise é possível que você descubra alguma informação e então seja possível determinar a matriz decodificadora e consequentemente obtenha acesso ao resto da mensagem. Como exemplo, suponha que você, ao analisar um texto codificado, descubra que esse texto representa uma carta e que começa por DEAR SIR. Esse pequeno dado é suficiente para decodificar o resto do texto. O teorema a seguir fornece uma maneira de fazer isto.

Teorema 2.16 (Determinando a Matriz Decodificadora)**.** *Sejam*

$$p_i = \begin{pmatrix} p_{1i} \\ p_{2i} \\ \vdots \\ p_{ni} \end{pmatrix}, \qquad c_i = \begin{pmatrix} c_{1i} \\ c_{2i} \\ \vdots \\ c_{ni} \end{pmatrix},$$

onde $p_1, p_2, \ldots, p_n$ *são vetores comuns e* $c_1, c_2, \ldots, c_n$ *os correspondentes vetores codificados de um n-código de Hill,*

$$P = \begin{pmatrix} p_1^t \\ p_2^t \\ \vdots \\ p_n^t \end{pmatrix} = \begin{pmatrix} p_{11} & p_{21} & \ldots & p_{n1} \\ p_{12} & p_{22} & \ldots & p_{n2} \\ \vdots & \vdots & & \vdots \\ p_{1n} & p_{2n} & \ldots & p_{nn} \end{pmatrix} \; e \; C = \begin{pmatrix} c_1^t \\ c_2^t \\ \vdots \\ c_n^t \end{pmatrix} = \begin{pmatrix} c_{11} & c_{21} & \ldots & c_{n1} \\ c_{12} & c_{22} & \ldots & c_{n2} \\ \vdots & \vdots & & \vdots \\ c_{1n} & c_{2n} & \ldots & c_{nn} \end{pmatrix},$$

onde p_i^t e c_i^t representam a transpostas de p_i e c_i respectivamente. Se P é inversível, então a sequência de operações elementares sobre linhas que reduz C a I transforma P em $(A^{-1})^t$.

Demonstração. Por (2.9) e pela definição de P e C, efetuando a multiplicação das matrizes, temos $C^t = AP^t$. Assim, podemos escrever $C = P \cdot A^t$. Sendo A e P inversíveis, resulta das propriedades de determinante e do Teorema 1.104 que C é uma matriz inversível. Sejam $E_1, \ldots, E_k$ as matrizes elementares que correspondem às operações elementares com as linhas que reduzem C a I, ou seja, $E_k \ldots E_1 C = I$. Substituindo em $C = P \cdot A^T$, encontramos $E_k \ldots E_1 P A^T = I$. Multiplicando ambos os membros por $(A^{-1})^t$, temos $E_k \ldots E_1 P = (A^{-1})^t$, ou seja, a mesma sequência de operações com as linhas que reduz C a I converte P a $(A^{-1})^t$. □

A partir desse teorema, chegamos a conclusão que para encontrar a transposta da matriz decodificadora A^{-1} devemos efetuar operações elementares sobre linhas que reduz C a I e essas mesmas operações aplicar sobre linhas de P.

Exemplo 2.17. *Decodifique o 2-código de Hill*

$$LNGIHGYBVRENJYQO$$

sabendo que as quatro últimas letras do texto comum são ATOM.
Solução: *Pela Tabela 2.10, o equivalente numérico do texto comum conhecido é:*

A	T	O	M
1	20	15	13

;

Tabela 2.13:

e o equivalente numérico do texto codificado correspondente é:

J	Y	Q	O
10	25	17	15

Tabela 2.14:

de modo que os vetores comuns e correspondentes vetores codificados são:

$$p_1 = \begin{pmatrix} 1 \\ 20 \end{pmatrix} \longleftrightarrow c_1 = \begin{pmatrix} 10 \\ 25 \end{pmatrix}$$

e

$$p_2 = \begin{pmatrix} 15 \\ 13 \end{pmatrix} \longleftrightarrow c_2 = \begin{pmatrix} 17 \\ 15 \end{pmatrix}.$$

Queremos reduzir

$$C = \begin{pmatrix} c_1^t \\ c_2^t \end{pmatrix} = \begin{pmatrix} 10 & 25 \\ 17 & 15 \end{pmatrix}$$

a I (matriz identidade) por operações elementares sobre linhas e simultaneamente aplicar estas operações a

$$P = \begin{pmatrix} p_1^t \\ p_2^t \end{pmatrix} = \begin{pmatrix} 1 & 20 \\ 15 & 13 \end{pmatrix}$$

para obter $(A^{-1})^t$ (a transposta da matriz decodificadora). Para isso, colocamos P à direita de C, $[C|P]$, e aplicamos nesta as operações sobre linhas até que o lado esquerdo esteja reduzido a I. A matriz final então terá o formato $[I|(A^{-1})^T]$. Assim, temos:

$$[C|P] = \left(\begin{array}{cc|cc} 10 & 25 & 1 & 20 \\ 17 & 15 & 15 & 13 \end{array}\right).$$

Observe que $7 \cdot 15 \equiv 1 \mod 26$. Assim, multiplicamos a linha 2 por 7 e obtemos

$$\left(\begin{array}{cc|cc} 10 & 25 & 1 & 20 \\ 119 & 105 & 105 & 91 \end{array}\right).$$

Substituindo $119, 105$ e 91 pelos seus resíduos módulo 26, tem-se

$$\left(\begin{array}{cc|cc} 10 & 25 & 1 & 20 \\ 15 & 1 & 1 & 13 \end{array}\right).$$

Multiplicando a segunda linha por -25 e somando à primeira linha, obtemos

$$\left(\begin{array}{cc|cc} -365 & 0 & -24 & -305 \\ 15 & 1 & 1 & 13 \end{array}\right).$$

Substituímos -365, -24 e -305 pelos seus resíduos módulo 26

$$\left(\begin{array}{cc|cc} 25 & 0 & 2 & 7 \\ 15 & 1 & 1 & 13 \end{array}\right).$$

Multiplicamos a primeira linha por $25^{-1} = 25$, temos

$$\left(\begin{array}{cc|cc} 1 & 0 & 50 & 175 \\ 15 & 1 & 1 & 13 \end{array}\right).$$

Substituímos 50 e 175 pelos seus resíduos módulo 26

$$\left(\begin{array}{cc|cc} 1 & 0 & 24 & 19 \\ 15 & 1 & 1 & 13 \end{array}\right).$$

Multiplicando a primeira linha por -15 e somando à segunda, obtém-se

$$\left(\begin{array}{cc|cc} 1 & 0 & 24 & 19 \\ 0 & 1 & -359 & -272 \end{array}\right).$$

Substituímos -359 e -272 pelos seus resíduos módulo 26, concluímos que

$$\left(\begin{array}{cc|cc} 1 & 0 & 24 & 19 \\ 0 & 1 & 5 & 14 \end{array}\right).$$

Logo,

$$(A^{-1})^T = \begin{pmatrix} 24 & 19 \\ 5 & 14 \end{pmatrix}$$

e portanto a matriz decodificadora é

$$A^{-1} = \begin{pmatrix} 24 & 5 \\ 19 & 14 \end{pmatrix}.$$

Para decodificar a mensagem, primeiro agrupamos o texto codificado em pares e encontramos os equivalentes numéricos de cada letra (veja a Tabela 2.15). Em

L	N	G	I	H	G	Y	B	V	R	E	N	J	Y	Q	O
12	14	7	9	8	7	25	2	22	18	5	14	10	25	17	15

Tabela 2.15:

seguida, multiplicamos os vetores codificados sucessivamente pela esquerda por A^{-1} *e encontramos os equivalentes alfabéticos dos pares de texto comum resultantes:*

$$\begin{pmatrix} 24 & 5 \\ 19 & 14 \end{pmatrix}\begin{pmatrix} 12 \\ 14 \end{pmatrix} = \begin{pmatrix} 20 \\ 8 \end{pmatrix} \pmod{26} \Longrightarrow \begin{matrix} T \\ H \end{matrix}$$

$$\begin{pmatrix} 24 & 5 \\ 19 & 14 \end{pmatrix}\begin{pmatrix} 7 \\ 9 \end{pmatrix} = \begin{pmatrix} 5 \\ 25 \end{pmatrix} \pmod{26} \Longrightarrow \begin{matrix} E \\ Y \end{matrix}$$

$$\begin{pmatrix} 24 & 5 \\ 19 & 14 \end{pmatrix}\begin{pmatrix} 8 \\ 7 \end{pmatrix} = \begin{pmatrix} 19 \\ 16 \end{pmatrix} \pmod{26} \Longrightarrow \begin{matrix} S \\ P \end{matrix}$$

$$\begin{pmatrix} 24 & 5 \\ 19 & 14 \end{pmatrix}\begin{pmatrix} 25 \\ 2 \end{pmatrix} = \begin{pmatrix} 12 \\ 9 \end{pmatrix} \pmod{26} \Longrightarrow \begin{matrix} L \\ I \end{matrix}$$

$$\begin{pmatrix} 24 & 5 \\ 19 & 14 \end{pmatrix}\begin{pmatrix} 22 \\ 18 \end{pmatrix} = \begin{pmatrix} 20 \\ 20 \end{pmatrix} \pmod{26} \Longrightarrow \begin{matrix} T \\ T \end{matrix}$$

$$\begin{pmatrix} 24 & 5 \\ 19 & 14 \end{pmatrix}\begin{pmatrix} 5 \\ 14 \end{pmatrix} = \begin{pmatrix} 8 \\ 5 \end{pmatrix} \pmod{26} \Longrightarrow \begin{matrix} H \\ E \end{matrix}$$

$$\begin{pmatrix} 24 & 5 \\ 19 & 14 \end{pmatrix}\begin{pmatrix} 10 \\ 25 \end{pmatrix} = \begin{pmatrix} 1 \\ 20 \end{pmatrix} \pmod{26} \Longrightarrow \begin{matrix} A \\ T \end{matrix}$$

$$\begin{pmatrix} 24 & 5 \\ 19 & 14 \end{pmatrix}\begin{pmatrix} 17 \\ 15 \end{pmatrix} = \begin{pmatrix} 15 \\ 13 \end{pmatrix} \pmod{26} \Longrightarrow \begin{matrix} O \\ M \end{matrix}$$

Finalmente, construímos a mensagem a partir dos pares de texto comum:

"THEY SPLIT THE ATOM".

2.5 Sistema RSA

O sistema RSA[3] é simples e baseia-se na dificuldade para descobrir os fatores primos existentes em números muito grandes. O seguinte teorema mostra como funciona o sistema RSA, como estão definidos os códigos e como podemos decodificá-los.

Teorema 2.18. *Suponhamos que:*

1. $n = pq$, *onde* p *e* q *são números primos distintos;*

2. e *é um número inteiro positivo invertível módulo* $\phi(n)$. *Em outras palavras* $mdc(e, \phi(n)) = mdc(e, (p-1)(q-1)) = 1$;

3. b *é um inteiro positvo tal que* $b \not\equiv 0(\text{mod } p)$ *e* $b \not\equiv 0(\text{mod } q)$, *representa cada bloco numérico e* $b < n$;

4. $C(b)$ *é um inteiro positivo que representa cada bloco codificado definido por*

$$C(b) \equiv b^e(\text{mod } n),$$

   onde $0 \leq C(b) < n$;

5. d *é um inteiro positivo e é o inverso de* e *módulo* $\phi(n)$, *ou seja,* $ed \equiv 1(\text{mod}\phi(n))$, $1 \leq d < (p-1)(q-1)$.

6. $D(c)$ *é um inteiro positivo que representa o bloco decodificado definifo por*

$$D(c) \equiv c^d(\text{mod } n),$$

   onde $0 \leq D(c) < n$.
   Em outras palavras, $D(C(b)) = b$, *ou seja, decodificando um bloco de mensagem codificada, encontramos um bloco da mensagem original.*

Demonstração. Consideremos então $n = pq$. Vamos provar que

$$D(C(b)) \equiv b(\text{mod } n).$$

Observe que $D(C(b))$ e b são menores que $n-1$. Por isso escolhemos b menor que n e mantivemos os blocos separados depois da codificação. Por definição, temos que

$$D(C(b)) \equiv (b^e)^d \equiv b^{ed}(\text{mod } n).$$

Mas d é o inverso de e módulo $\phi(n)$. Logo existe inteiro K tal que $ed = 1 + k\phi(n)$. Logo,

$$b^{ed} \equiv b^{1+k\phi(n)} \equiv (b^{\phi(n)})^k b(\text{mod } n).$$

Se $mdc(b, n) = 1$, então podemos usar o Teorema 1.65:

$$b^{ed} \equiv (b^{\phi(n)})^k b \equiv b(\text{mod } n).$$

[3] O sistema RSA recebe esse nome em homenagem a seus inventores Ronald Rivest, Adi Shamir e Leonard Adleman, foi o primeiro criptossistema de chave pública

Se b e n não são primos entre si, observe que $n = pq$, p e q primos distintos. Logo,

$$b^{ed} \equiv b^{1+k\phi(n)} \equiv (b^{(p-1)})^{k(q-1)} b (\text{mod } p).$$

Se $mdc(b, p) = 1$, então podemos usar o Teorema 1.57 ($b^{p-1} \equiv 1 (\text{mod } p)$). Se não, temos que $p|b$ e portanto,

$$b^{ed} \equiv b \equiv o (\text{mod } p).$$

Logo,

$$b^{ed} \equiv b (\text{mod } p)$$

qualquer que seja b. Fazendo o mesmo para o primo q, obtendo:

$$b^{ed} \equiv b (\text{mod } q).$$

Portanto,

$$b^{ed} \equiv b (\text{mod } pq)$$

como queríamos. □

Definição 2.19. *Chamaremos o número $n = pq$ de módulo, o número e de potência de codificação, d de potência de decodificação e a tripla (n, e, d) de a chave do sistema RSA.*

Os números n, d e e são todos escolhidos por usuários do sistema RSA desde que sejam satisfeita as condições de 1 a 5 do Teorema 2.18.

Definição 2.20. *O par (n, e) é a chave pública do sistema RSA e o par (n, d) é a chave privada do sistema RSA.*

Para que haja comunicação entre duas fontes é necessário o uso das chaves pública e privada. A chave pública da fonte A deve ser conhecida pela fonte B e vice-versa. Dessa forma B e A podem trocar mensagens secretas. No entanto, para isso acontecer algumas etapas são importantes:

1. B deve saber da chave pública (n, e) de A.

2. B converte a mensagem para números através de uma tabela onde cada letra do alfabeto está representado por um número formado por 2 algarismos para evitar ambiguidade (essa tabela deve ser conhecido por ambas as fontes).

3. B escreve b em blocos numéricos $b_1, b_2, \cdots, b_r$, esses blocos não devem ultrapassar $n = pq$.

Observação 2.21. *A maneira de escolher os blocos não é única, mas é importante evitar que algum bloco comece com o número 0 (por problemas na decodificação).*

4. B encripta os blocos $b_1, b_2, \cdots, b_r$ usando a condição 4 do Teorema 2.18 e assim estabelece os códigos $C(b_1), C(b_2), \cdots, C(b_r)$.

5. B transmite os códigos $C(b_1), C(b_2), \cdots, C(b_r)$ para A.

6. Ao receber o código, a fonte A decodifica os códigos $C(b_1), C(b_2), \cdots, C(b_r)$ usando o item 6 do Teorema 2.18.

7. Uma vez que $D(c_1), D(c_2), \cdots, D(c_r)$ são conhecidos por A, basta usar a tabela e transformar esses blocos numéricos na mensagem original.

Dessa forma o processo fica concluído.

Exemplo 2.22. *Usando a chaves pública* $(n, e) = (1037, 7)$ *e a Tabela 2.16, codifique e decodifique a seguinte palavra: SONHO.*

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
[ ]												
99												

Tabela 2.16:

Solução: *Inicilmente, de acordo com a Tabela 2.16, devemos trocar cada letra pelo seu respectivo valor numérico:*

$$S\ O\ N\ H\ O$$
$$28\ 24\ 23\ 17\ 24$$

Em seguida, devemos trocar a mensagem acima em blocos, que devem ter valor menor que 1037 e maior que zero:

$$282,\ 423,\ 172,\ 4$$

A partir do Teorema 2.18 item 4*, descobriremos seu respectivo valor codificado.*

$C_1(282) = 282^7 \bmod 1037$
$C_1(282) = 282^2 .282^4.282 \bmod 1037$
$C_1(282) = 712.282^4 282 \bmod 1037$
$C_1(282) = 712.712^2.282 \bmod 1037$
$C_1(282) = 712.888.282 \bmod 1037$
$C_1(282) = 723.282 \bmod 1037$
$C_1(282) = 634 \bmod 1037$

Procedendo dessa maneira com todos os blocos, teremos:

$$C_2(423) = 423^7 \bmod 1037 = 934,$$

$$C_3(172) = 172^7 \bmod 1037 = 621$$

e

$$C_4(4) = 4^7 \bmod 1037 = 829.$$

Logo, obtemos a seguinte mensagem codificada:

$$634 - 934 - 621 - 829$$

Para fazer a decodificação, devemos primeiro encontrar o valor de d que determina o par (n, d) *que é a chave de decodificação.*

$$ed = l(p-1)(q-1) + 1$$

Temos que, $n = pq = 1037 = 17.61$*, logo,* $p = 17$ *e* $q = 61$*. Daí, temos:*

$$\begin{aligned}
&7d = l.(61-1).(17-1) + 1\\
&7d = l.60.16 + 1\\
&d = \tfrac{960l}{7} + \tfrac{1}{7}\\
&d = \tfrac{959l}{7} + \tfrac{l}{7} + \tfrac{1}{7}\\
&d = \tfrac{959l}{7} + \tfrac{l+1}{7}\\
&d = 137l + \tfrac{l+1}{7}
\end{aligned}$$

Fazendo $l = 6$*, temos:*

$$d = 823.$$

Sabendo o valor de d, e usando o Teorema 2.18 tópico 5, temos:

$$\begin{aligned}
&T_1(634) = 634^{823} \bmod 1037\\
&T_1(634) = (634^2)^{411}.634 \bmod 1037\\
&T_1(634) = (637)^{411}.634 \bmod 1037\\
&T_1(634) = (637^2)^{205}.637.634 \bmod 1037\\
&T_1(634) = (302^2)^{102}.302.637.634 \bmod 1037\\
&T_1(634) = (985^2)^{51}.302.637.634 \bmod 1037\\
&T_1(634) = (630^2)^{25}.630.302.637.634 \bmod 1037\\
&T_1(634) = (766^2)^{12}.766.630.302.637.634 \bmod 1037\\
&T_1(634) = (851^2)^{6}.766.630.302.637.634 \bmod 1037\\
&T_1(634) = (375^2)^{3}.766.630.302.637.634 \bmod 1037\\
&T_1(634) = 630^2.630^2.766.302.637.634 \bmod 1037\\
&T_1(634) = 766^2.766.302.637.634 \bmod 1037\\
&T_1(634) = 851.766.302.637.634 \bmod 1037\\
&T_1(634) = 630.302.637.634 \bmod 1037\\
&T_1(634) = 489.637.634 \bmod 1037\\
&T_1(634) = 393.634 \bmod 1037\\
&T_1(634) = 282 \bmod 1037
\end{aligned}$$

Procedendo dessa maneira com todos os blocos, teremos:

$$T_2(934) = 934^{823} \bmod 1037 = 423,$$

$$T_3(621) = 621^{823} \bmod 1037 = 172$$

e

$$T_4(829) = 829^{823} \bmod 1037 = 4.$$

Dessa forma, utilizando a Tabela 2.16, teremos a mensagem original "SONHO".

2.6 Código de Rabin

O código de Rabin, assim como o sistema RSA, é baseado na dificuldade de fatorar inteiros, mas em contraste com o RSA, pode ser mostrado que alguém que quebre o código de Rabin, pode também fatorar inteiros de maneira eficiente e portanto, pode também quebrar o RSA.

No código de Rabin, tal como no RSA, precisamos de dois primos grandes p e q, só que neste código costuma-se impor a condição adicional

$$p, q \equiv 3 \bmod 4,$$

para simplificar os cálculos. Nota-se que o código de Rabin funciona mesmo que os primos não verifiquem esta condição. A chave pública é $n = pq$, a chave privada é o par (p, q). O espaço das mensagens originais é $\{0, 1, \ldots, n-1\}$. Para codificar a mensagem $m \in \{0, 1, \ldots, n-1\}$, devemos determinar:

$$c \equiv m^2 \bmod n.$$

Para recuperar a mensagem original m da mensagem codificada c, devemos determinar:

$$m_p \equiv c^{\frac{p+1}{4}} \bmod p \quad \text{e} \quad m_q \equiv c^{\frac{q+1}{4}} \bmod p$$

Assim, $\pm m_p$ são as duas raízes quadradas de $c \bmod p$ e $\pm m_q$ são as duas raízes quadradas de $c \bmod q$. Daí, temos os seguintes pares de congruência.

1. $m \equiv m_p \bmod p \quad \text{e} \quad m \equiv m_q \bmod q$
2. $m \equiv m_p \bmod p \quad \text{e} \quad m \equiv -m_q \bmod q$
3. $m \equiv -m_p \bmod p \quad \text{e} \quad m \equiv m_q \bmod q$
4. $m \equiv -m_p \bmod p \quad \text{e} \quad m \equiv -m_q \bmod q$

Usando o Teorema 1.75 em cada um dos pares de congruência, obtém-se quatro inteiros x_1, x_2, x_3 e x_4 cujo quadrado é congruente a $c \bmod n$ e um deles é a mensagem original m.

Há vários métodos para escolher a mensagem original das quatro raízes quadradas de $c \bmod n$. Por exemplo, podemos escolher aquela que faz sentido após ter sido decodificada. No entanto, este método nem sempre funciona.

Exemplo 2.23. ***Observe a seguinte situação:*** *Bob codifica a mensagem* $m = 158$ *calculando* $c \equiv m^2 \bmod n$ *e obtém* $c = 170$. *Alice ao receber a mensagem, para decodificá-la, escolhe dois números primos* $p = 11$ *e* $q = 23$ *e calcula* m_p *e* m_q. *Veja:*

$$\begin{aligned}
&m_p \equiv c^{\frac{p+1}{4}} \bmod p \quad e \quad m_q \equiv c^{\frac{q+1}{4}} \bmod q \\
&m_p \equiv 170^{\frac{11+1}{4}} \bmod 11 \quad e \quad m_q \equiv 170^{\frac{23+1}{4}} \bmod 23 \\
&m_p \equiv 170^3 \bmod 11 \quad e \quad m_q \equiv 170^6 \bmod 23 \\
&m_p \equiv 5^3 \bmod 11 \quad e \quad m_q \equiv 9^6 \bmod 23 \\
&m_p \equiv 125 \bmod 11 \quad e \quad m_q \equiv 531441 \bmod 23 \\
&m_p \equiv 4 \bmod 11 \quad e \quad m_q \equiv 3 \bmod 23
\end{aligned}$$

Logo, $m_p = 4$ *e* $m_q = 3$*. Assim* ± 4 *são as duas raízes quadradas de* $170 \bmod 11$ *e* ± 3 *são as duas raízes quadradas de* $170 \bmod 23$*. Daí, temos os seguintes pares de congruência:*

1. $m \equiv 4 \bmod 11 \quad e \quad m \equiv 3 \bmod 23$
2. $m \equiv 4 \bmod 11 \quad e \quad m \equiv -3 \bmod 23 \Rightarrow m \equiv 20 \bmod 23$
3. $m \equiv -4 \bmod 11 \Rightarrow m \equiv 7 \bmod 11 \quad e \quad m \equiv 3 \bmod 23$
4. $m \equiv -4 \bmod 11 \Rightarrow m \equiv 7 \bmod 11 \quad e \quad m \equiv -3 \bmod 23 \Rightarrow m \equiv 20 \bmod 23$

Usando o Teorema 1.75, em cada um dos pares de congruência, Alice obtém quatro inteiros que são 26, 95, 158 *e* 227 *cujo quadrado é congruente com* $c \bmod n$ *e um deles é a mensagem original* m*, que neste caso,* $m = 158$*.*

Teorema 2.24. *Quebrar o código de Rabin é tão difícil como fatorar inteiros. Por outras palavras, se alguém descobrir um algoritmo que quebre o código de Rabin, ele pode usar este algoritmo para fatorar inteiros de uma maneira eficiente.*

Demonstração. Claramente, qualquer pessoa que consiga fatorar n, consegue também quebrar o código de Rabin. Suponhamos agora que uma pessoa descobriu um algoritmo, R, para quebrar o código de Rabin. Seja n, o módulo público, e sejam p e q, os fatores primos. Dada uma mensagem cifrada $c \bmod n$, a pessoa obtém $m = R(c)$. Portanto, dado um quadrado $c \bmod n$, o algoritmo R, permite determinarmos uma raiz quadrada de $c \bmod n$. Vejamos como podemos usar este algoritmo para fatorar n: uma pessoa escolhe, aleatoriamente, um inteiro $1 \leq x \leq n-1$. Se

$$(n, x) = d \neq 1$$

então d é um fator de n e a fatoração de n está encontrada

$$(n = d \times \frac{n}{d}).$$

Caso contrário, a pessoa determina

$$c = x^2 \bmod n \quad \text{e} \quad m = R(c).$$

Sabemos que m é uma das raízes quadradas, mod n, de c, tal como x, mas não é necessariamente igual a x. No entanto, m satisfaz um dos seguintes pares de congruências:

$m \equiv x \bmod p \quad \text{e} \quad m \equiv x \bmod q$
$m \equiv x \bmod p \quad \text{e} \quad m \equiv -x \bmod q$
$m \equiv -x \bmod p \quad \text{e} \quad m \equiv x \bmod q$
$m \equiv -x \bmod p \quad \text{e} \quad m \equiv -x \bmod q$

No primeiro caso, $m = x$ e $(m - x, n) = n$, no segundo caso, $(m - x, n) = p$, no terceiro caso, $(m-x, n) = q$ e no último caso, $m = n-x$ e, como $(n, x) = 1$, obtemos $(m-x, n) = 1$. Depois de aplicarmos este procedimento k vezes, n é fatorizado com probabilidade

$$1 - (\frac{1}{2})^k$$

. □

Exemplo 2.25. *Seja* $n = 253$. *Suponhamos que Olga consegue determinar raízes quadradas* mod 253 *com o seu algoritmo R. Ela seleciona,* $x = 17$ *e obtém* $(17, 253) = 1$. *Depois calcula*

$$c \equiv 17^2 \equiv 36 \bmod 253.$$

As raízes quadradas de 36 mod253 *são,* 6, 17, 236 *e* 247. *Temos*

$$(6 - 17, 253) = 11 \quad e \quad (247 - 17, 253) = 23,$$

portanto, se o algoritmo R obteve 6 *ou* 247 *então Olga encontrou a fatoração de* 253*, caso contrário, Olga escolhe outro inteiro x e aplica o procedimento outra vez. Depois de poucas aplicações é muito provável que Olga tenha encontrado a fatoração de n sem demorar demasiado tempo.*

2.7 O Método MH (Merkle e Hellman)

Este método foi criado por Merkle e Hellman em 1978 baseando-se na dificuldade do chamado **Problema da Mochila**. É um sistema criptográfico monoalfabético e assimétrico pois o algoritmo de codificação é diferente do algoritmo de decodificação.

2.7.1 O Problema da Mochila

Dado o vetor $a = (a_1, a_2, \ldots, a_n)$ de coordenadas naturais e b também natural, o problema da mochila consiste em saber se existe $X = (x_1, x_2, \ldots, x_n)$ onde cada x_i é 0 ou 1, tal que:

$$\sum_{i=1}^{n} a_i x_i = b.$$

Definimos a chave pública de cada destinatário no Método MH pelo vetor $P = (c_1, c_2, \ldots, c_n)$ de naturais, onde $n \approx 100$.

Para que o problema da mochila seja de fácil resolução, a chave pública não pode ser qualquer. Para isso, o destinatário deve inicialmente, antes de divulgar a sua chave pública, criar uma seqüência de números naturais

$$s = (s_1, s_2, \ldots, s_n) \tag{2.10}$$

e também t e k tais que

$$\sum_{i=1}^{r} s_i < s_{r+1} < t$$

para $1 \leq r < n - 1$ e $mdc(k, t) = 1$.

Assim, a sequência $s = (s_1, s_2, \ldots, s_n)$ é essencial para a solução do problema da mochila.

O destinatário mantém o vetor s e os valores de t e k secretos e publica o vetor c, dado por

$$c_i = k s_i \pmod{t},$$

com $1 \leq i \leq n$. Além disso, o destinatário escolhe e mantém secreto o número l que deve satisfazer a equação:

$$lk \pmod{t} = 1.$$

2.7.2 Codificando

Para codificar uma mensagem e enviar ao destinatário, o emissor deve consultar a chave pública $P = (c_1, c_2, \ldots, c_n)$ do destinatário, converter cada símbolo da mensagem original em números naturais m menores do que 2^n e escrevê-lo na base binária, isto é,

$$m = [m_1 m_2 \ldots m_n]_2,$$

sendo $m_i = 0$ ou 1. Então, calcula-se

$$P(m) = \sum_{i=1}^{n} m_i c_i.$$

Assim, o trabalho do destinatário em decodificar $P(m)$ é determinar a solução do problema da mochila sabendo-se

$$P = (c_1, c_2, \ldots, c_n) \text{ e } P(m).$$

2.7.3 Algoritmo para a Resolução do Problema da Mochila - Decodificando

Algoritmo da Mochila

A decodificação da mensagem se dá letre por letra utilizando para isso o Algaritmo da Mochila. O destinatário deve primeiro determinar os valores de

$$d = l.P(m) (\text{mod } t).$$

Em seguida, faça os seguintes procedimentos:
Entrada: $(n, (s_1, s_2, \ldots, s_n), d)$, onde $s = (s_1, s_2, \ldots, s_n)$ é a seqüência 2.10 e

$$d \equiv l \cdot P(m) \ (\text{mod } t).$$

Saída: m.
Etapa 1: Faça $y = d$.
Etapa 2: Para cada $i = n, n-1, n-2, \ldots, 1$, ou seja, para os valores de i serão atribuídos uma sequência decrescente de n até 1, faça:

1. Se $y < s_i$, então, $m_i = 0$.
2. Se $y \geq s_i$, então faça $y = y - s_i$ e tome $m_i = 1$.

Etapa 3:

1. Se $y = 0$, então retorne o vetor: $m = (m_1, m_2, \ldots, m_n)$.
2. Se $y \neq 0$, então o problema da mochila não tem solução.

Exemplo 2.26. *Seja a mensagem BRASIL_2014. Associando a mensagem aos números correspondentes da Tabela 2.17 e utilizando o método MH, faça a codificação e decodificação.*

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
_	0	1	2	3	4	5	6	7	8	9		
36	37	38	39	40	41	42	43	44	45	46		

Tabela 2.17:

Solução:
Primeiramente, é preciso que o destinatário determine a chave pública que será o vetor $P = (c_1, c_2, \ldots, c_n$. Para isso, ele deverá escolher uma sequência s como 2.10. Além disso, k e t, de modo que $\sum_{i=1}^{n} s_i < t$ e $mdc(k,t) = 1$. Para o exemplo escolhemos a sequência:

$$s = (3, 5, 11, 22, 50, 107),$$

$k = 27$ e $t = 199$, pois o $mdc(27, 199) = 1$ e $t > 3 + 5 + 11 + 22 + 50 + 107 = 198$. Temos então a expressão:

$$27l(\text{mod } 199) = 1 \Longrightarrow 199x + 27l = 1.$$

Calculemos o valor de l a partir do Algoritmo Euclides Estendido 2.14. Colocando os valores em uma tabela:

Restos	Quocientes	x_i	y_i
199	_	1	0
27	_	0	1
10	7	1	-7
7	2	-2	15
3	1	-24	177
1	2	-8	59

Tabela 2.18:

Temos, então: $l = y_i = 59$.

Deste modo, o destinatário pública o vetor $c = (c_1, c_2, \ldots, c_n)$, onde $n = 6$ e cujo $c_i = ks_i(\text{mod } t)$.
$c_1 = 27.s_1(\text{mod } 199) \Longrightarrow c_1 = 27.3(\text{mod } 199) \Longrightarrow c_1 = 81(\text{mod } 199)$
$c_2 = 27.s_2(\text{mod } 199) \Longrightarrow c_2 = 27.5(\text{mod } 199) \Longrightarrow c_2 = 135(\text{mod } 199)$
$c_3 = 27.s_3(\text{mod } 199) \Longrightarrow c_3 = 27.11(\text{mod } 199) \Longrightarrow c_3 = 98(\text{mod } 199)$
$c_4 = 27.s_4(\text{mod } 199) \Longrightarrow c_4 = 27.22(\text{mod } 199) \Longrightarrow c_4 = 196(\text{mod } 199)$
$c_5 = 27.s_5(\text{mod } 199) \Longrightarrow c_5 = 27.50(\text{mod } 199) \Longrightarrow c_5 = 156(\text{mod } 199)$
$c_6 = 27.s_6(\text{mod } 199) \Longrightarrow c_6 = 27.107(\text{mod } 199) \Longrightarrow c_6 = 103(\text{mod } 199)$

Assim, temos que a chave pública é $P = (81, 135, 98, 196, 156, 103)$.

Codificando
Agora que conhecemos a chave pública, podemos codificar a mensagem. Para isso,

associamos a mensagem aos números correspondentes na Tabela 2.17, daí temos a seguinte sequência de números:

$$11, 27, 10, 28, 18, 21, 36, 39, 37, 38, 41$$

Passando a sequência de números acima para a base binária 2.14,temos:

$$11 = [001011]_2, 27 = [011011]_2, 10 = [001010]_2, 28 = [011100]_2$$

$$18 = [010010]_2, 21 = [010101]_2, 36 = [100100]_2, 39 = [100111]_2$$

$$37 = [100101]_2, 38 = [100110]_2, 41 = [101001]_2$$

Logo, a primeira letra da mensagem, que é B, que corresponde a $11 = [001011]_2$ é codificada em:

$$P(11) = \sum_{i=1}^{6} m_i c_i = 0.81 + 0.135 + 1.98 + 0.196 + 1.156 + 1.103 = 357$$

Procedendo de modo análogo com os demais símbolos da mensagem, temos: temos a sequência de números:

$$11 \quad 27 \quad 10 \quad 28 \quad 18 \quad 21 \quad 36 \quad 39 \quad 37 \quad 38 \quad 41.$$

Passando a sequência de números acima para a base binária, temos:

$$357 \quad 492 \quad 254 \quad 429 \quad 291 \quad 434 \quad 277 \quad 536 \quad 380 \quad 433 \quad 282$$

Decodificando

Para decifrar a mensagem o destinatário deve primeiro determinar os valores de

$$d = l.P(m)(\text{mod } t).$$

Logo, temos:

Para $P(11)$ então $d = 168$
Para $P(27)$ então $d = 173$
Para $P(10)$ então $d = 61$
Para $P(28)$ então $d = 38$
Para $P(18)$ então $d = 55$
Para $P(21)$ então $d = 134$
Para $P(36)$ então $d = 25$
Para $P(39)$ então $d = 182$
Para $P(37)$ então $d = 132$
Para $P(38)$ então $d = 75$
Para $P(41)$ então $d = 121$

Continuando a decodificação do Método MH, vamos começar decodificando a primeira letra da nossa mensagem utilizando para isso o Algoritmo da Mochila. Temos: $(n, (s_1, s_2, \ldots, s_n), d)$, que corresponde a $(6, (3, 5, 11, 22, 50, 107), 168)$.
Etapa 1**:** Faça $y = 168$.

Etapa 2
Para $i = 6$
Como $y \geq s_6$, ou seja, $y \geq 107$ então faça $y = 168 - 107 = 61$ e tome $m_6 = 1$.
Para $i = 5$
Como $y \geq s_5$, ou seja, $y \geq 50$ então faça $y = 61 - 50 = 11$ e tome $m_5 = 1$.
Para $i = 4$
Como $y < s_4$, ou seja, $y < 22$ então tome $m_4 = 0$.
Para $i = 3$
Como $y \geq s_3$, ou seja, $y \geq 11$ então faça $y = 11 - 11 = 0$ e tome $m_3 = 1$.
Para $i = 2$
Como $y < s_2$, ou seja, $y < 5$ então tome $m_2 = 0$.
Para $i = 1$
Como $y < s_1$, ou seja, $y < 3$ então tome $m_1 = 0$.
Etapa 3**:** Como $y = 0$, então

$$m = [001011]_2 = 11$$

que corresponde à letra B.

De modo análogo, utilizando o Algoritmo da Mochila para os demais símbolos da mensagem, encontramos os respectivos resultados:

$$[001011]_2, [011011]_2, [001010]_2, [011100]_2$$

$$[010010]_2, [010101]_2, [100100]_2, [100111]_2$$

$$[100101]_2, [100110]_2, [101001]_2$$

que correspondem a $m = 11, m = 27, m = 10, m = 28, m = 18, m = 21, m = 36, m = 39, m = 37, m = 38, m = 41$.
Formando a mensagem inicial $BRASIL\_2014$.

2.8 Código ElGamal

Código ElGamal é um sistema com o uso de chaves assimétricas [4] criado pelo estudioso de criptografia egípcio Taher Elgamal em 1984. Sua segurança se baseia na dificuldade de solução que o problema do logaritmo discreto pode apresentar.

Na geração das chaves da Criptografia ElGamal, temos que:

1. Escolher um número primo grande p e um gerador α do grupo multiplicativo $\mathbb{Z}_p^*$.

2. Selecionar ao acaso um número natural $a < p - 1$ e calcular $f = \alpha^a \pmod{p}$.

3. A chave pública é (p, α, f) e a chave privada é a.

[4] Chaves assimétricas é um par de chaves formado por uma chave pública e uma chave privada. A chave pública é distribuída livremente para todos os correspondentes, enquanto a chave privada deve ser conhecida apenas pelo seu dono. Nesse tipo de sistema que utiliza esse par de chaves assimétrica, uma mensagem codificada com a chave pública pode somente ser decodificada pela sua chave privada correspondente.

2.8.1 Etapa de Codificação

Nesta etapa o emissor A deverá:

1. Obter a chave pública (p, α, f) de B.
2. Converter as letras, números e símbolos da mensagem em números (m) entre 0 e $p-1$.
3. Escolher ao acaso um número natural b, tal que $b < p-1$.
4. Para cada m obtido acima, calcular:

$$\beta \equiv \alpha^b \pmod{p} \text{ e } \gamma \equiv m(\alpha^a)^b \pmod{p}.$$

5. Enviar a codificação $c = (\beta, \gamma)$ de m para B.

2.8.2 Etapa de Decodificação

Uma vez que o receptor B recebe a mensagem codificada c, então deverá:

1. Usar a chave privada para calcular $\beta^{p-1-a} (\text{mod } p)$.
2. Decodificar m calculando $\beta^{-a}\gamma (\text{mod } p)$.
3. Temos
$$\beta^{-a}\gamma \equiv \alpha^{-ab} m \alpha^{ab} \equiv m (\text{mod } p)$$
devido ao Teorema de Fermat 1.57.

Exemplo 2.27. *Seja a frase PROFMAT_2014. Tome $p = 1999$ e um gerador $\alpha = 7$ de $\mathbb{Z}_p^*$. O destinatário B escolhe a chave privada $a = 117$. Usando a Criptografia ElGamal faça a codificação e decodificação da letra M da mensagem, que corresponde a $m = 22$ na Tabela 2.17.*
Solução: *Suponha que o emissor A escolha $b = 503$. Para codificar o emissor A, deve calcular*

$$f = \alpha^a \pmod{p} = 7^{117} \pmod{1999}.$$

Usando o Método dos Quadrados Repetidos 1.9, encontramos $f = 54$.
Depois calculamos

$$\beta \equiv \alpha^b \pmod{p} = 7^{503} \pmod{1999}.$$

Usando o Método dos Quadrados Repetidos 1.9, encontramos $\beta = 300$.
Em seguida calculamos

$$\gamma \equiv m(\alpha^a)^b \pmod{p} = 22(54)^{503} \pmod{1999}.$$

Usando também o Método dos Quadrados Repetidos 1.9, encontramos $\gamma = 77$.
Logo, A envia $(\beta, \gamma) = (300, 77)$ para B.
Para decodificar, B deve calcular:

$$\beta^{p-1-a} = 300^{1999-1-117} \pmod{1999} = 300^{1881} \pmod{1999}.$$

Usando o Método dos Quadrados Repetidos 1.9, encontramos $\beta^{p-1-a} = 857$. *Finalmente, B calcula m, de modo que:*

$$m = \beta^{-a}\gamma \equiv 857 \times 77 \pmod{1999}.$$

Ao resolver a congruência acima, encontramos $m = 22$, *o que corresponde à letra M da mensagem inicial enviada.*

Capítulo 3

O estudo de alguns códigos com ênfase na matemática modular

Estudaremos agora códigos voltados a Teoria dos Códigos onde o que importa aqui é a segurança contra danificação da informação, ou seja, é importante proteger o conteúdo da mensagem contra destruição entre outros aspectos naturais que podem causar erros durante a transmissão, assim a fonte B recebe a mensagem corretamente.

3.1 Códigos de barras

3.1.1 História

Esta seção foi elaborada baseada nos artigos [12], [23] e [13]. O primeiro código de barras "nasceu" em 1949, formado por quatro linhas brancas sobre um fundo preto, porém como não havia um sistema de leitura de baixo custo, esta idéia ficou nos arquivos, sem ser implementada no mercado.

Em 1952, foi atribuída a Joseph Woodland e Bernard Silver a primeira patente de um código de barras. Seu código consistia num padrão de circunferências concêntricas de espessura variável. Em torno de 1970, uma firma de assessoria, a McKinsey & Co., junto com a Uniform Grocery Product Code Council 1 definiu um formato numérico para identificar produtos e pediu a diversas companhias que elaborassem um código adequado. A companhia vencedora foi a IBM e o código foi criado por George J. Laurer.

O código proposto, formalmente aceito em maio de 1973, passou a ser conhecido como código UPC (Universal Product Code) e foi adotado nos Estados Unidos e Canadá. Ele consistia de uma sequência de 12 dígitos, traduzidos para barras.

Em dezembro de 1976, Laurer criou um novo código o EAN (European Article Numbering system) com 13 dígitos, baseado no UPC−A. Esse código permitiu identificar o país de origem de cada produto classificado.

Outros países também adotam este mesmo sistema, entretanto utilizando outro nome. Por exemplo, no Japão o sistema é conhecido como JAN (Japanese Article Numbering system). No entanto, neste trabalho trataremos apenas do código $EAN-13$ que é o padrão utilizado no Brasil.

3.1.2 O significado dos 13 dígitos

A maioria dos produtos vendidos nos supermercados e lojas são identificados a partir de um código de barra. Nesse sistema, a largura das barras e os espaços em branco entre elas codificam números, que por sua vez representam informações sobre o produto. O código segue padrões internacionais. O padrão $EAN-13$, é o padrão utilizado no Brasil e em outros países. Esse padrão é composto por 13 dígitos e existe um significado pra todos eles.

1. Os 3 primeiros dígitos identificam a entidade que gerencia e controla os códigos utilizados por empresas e seus produtos. No Brasil, a entidade responsável é a $GS1$ Brasil. A $GS1$ trabalha com diversos códigos, exemplos:

   - EAN/UPC Código desenvolvido especificamente para leitura no PDV

Figura 3.1:

     (ponto de venda), devido à agilidade propiciada na captura da informação. Permite codificar os GTIN-8, GTIN-12 e GTIN-13 [1].

   - $GS1$ DataBar

Figura 3.2:

     Compreende uma família de códigos que podem ser escanedos no ponto de venda, podem ser muito menores do que o os códigos EAN/UPC e podem ainda codificar informações adicionais como número serial, número de lote e/ou data de validade.

   - $GS1-128$

[1] GTIN (Global Trade Item Number - Número Global de Item Comercial) é um identificador para itens comerciais desenvolvido e controlado pela GS1. Os GTINs podem ter o tamanho de 8 (GTIN-8), 12 (GTIN-12), 13 (GTIN-13) ou 14 (GTIN-14) dígitos e podem ser construídos utilizando qualquer uma das quatro estruturas de numeração dependendo da aplicação.

Figura 3.3:

Código de barras que permite codificar todas as Chaves $GS1$. Utilizado na gestão logística e de rastreabilidade por meio da codificação de informações adicionais como número serial, número de lote, data de validade, quantidades, número do pedido do cliente etc. Não pode ser utilizado para identificar itens que passarão pelo ponto de venda (PDV)

- $ITF-14$

Figura 3.4:

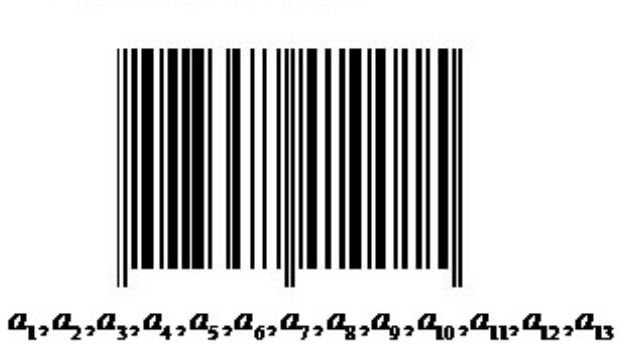
Código de barras desenvolvido para codificar apenas GTINs, pode ser impresso diretamente em substrato corrugado (caixa de papelão) oferecendo um bom desempenho de leitura. Não pode ser utilizado para identificar itens comerciais que passarão pelo ponto de venda.

- $GS1$ DataMatrix

Figura 3.5:

Símbolo bidimensional para aplicações especiais, que permite codificar informações em espaços muito menores que os códigos lineares e agregar informações adicionais como código do produto, lote e validade. O $GS1$ DataMatrix exige um leitor de código de barras bidimensional por isso não deve ser utilizado para identificação de itens que precisam passar pelo ponto de venda que possui apenas leitores lineares.

2. A identificação da empresa responsável pelo produto ocupa de quatro a seis dígitos, podendo ser do 4º ao 7º ou do 4º ao 9º dígito.



3. A identificação do produto ocupa de três a cinco dígitos, podendo ser do 8º ao 12º ou do 10º ao 12º dígito.

4. O 13º dígito é de segurança.

Assim, as informações estão nos números; o código de barras codifica esses números para serem lidos pelas máquinas com leitores ópticos. Esses leitores medem a largura das barras pretas e os espaços em brancos e decodificam os dados para obter os números e em seguida efetuam a verificação de segurança, que consiste em operações matemáticas realizados com os 12 primeiros dígitos (da esquerda para a direita), obtendo como resultado 13° dígito, chamado dígito de segurança. Esse dígíto juntamente com o resultado das operações envolvendo os 12 primeiros dígitos deve ser $\equiv\ 0 \bmod 10$. Se o resultado for diferente desse dígito significa que houve erro na leitura.

3.1.3 Como são gerados os códigos de barras?

Sejam $a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}, a_{11}$ e a_{12}, os primeiros 12 dígitos (da esquerda para a direita) do código de barras. Para determinar o 13º dígito, dígito de segurança, devemos:

1. Adicionar os dígitos localizados nas posições ímpares. Representaremos por:

$$S_1 = a_1 + a_3 + a_5 + a_7 + a_9 + a_{11}.$$

2. Adicionar os dígitos localizados nas posições pares. Representaremos por:

$$S_2 = a_2 + a_4 + a_6 + a_8 + a_{10} + a_{12}.$$

3. Multiplicar a soma dos dígitos localizados nas posições pares por 3, ou seja, $S_3 = 3 \times\ S_2$.

4. Adicionar os resultados anteriores, ou seja, $S_4 = S_1 + S_3$.

5. Encontrar o resto da divisão do resultado por 10: $S_4 \div 10$.

6. Se o resto for zero, o dígito de segurança a_{13} é o próprio zero; caso contrário, o dígito de segurança a_{13} é o resultado de (10− resto). Esse dígito é o menor valor possível, tal que ao ser acrescentado à soma obtida, deve gerar um múltiplo de 10, isto é, se a soma obtida é S_4, o número $S_4 + a_{13}$ deve ser múltiplo de 10, ou seja, $S_4 + a_{13} \equiv 0 \bmod 10$.

Para exemplificar, vamos efetuar a verificação de segurança de um código de barra de uma barra de ceral, que consiste em realizar as operações matemáticas abaixo para conferir o resultado delas como o dígito de segurança.

Figura 3.6:

Sejam 789432161362, os primeiros 12 dígitos (da esquerda para a direita) do código de barras. Para determinar o 13° dígito, dígito de segurança, devemos:

1. Adicionar os dígitos localizados nas posições ímpares:

$$S_1 = 7 + 9 + 3 + 1 + 1 + 6 \Longrightarrow S_1 = 27.$$

2. Adicionar os dígitos localizados nas posições pares:

$$S_2 = 8 + 4 + 2 + 6 + 3 + 2 \Longrightarrow S_2 = 25.$$

3. Multiplicar a soma dos dígitos localizados nas posições pares por 3, ou seja,

$$S_3 = 3 \times 25 \Longrightarrow S_3 = 75.$$

4. Adicionar os resultados anteriores, ou seja,

$$S_4 = 27 + 75 \Longrightarrow S_4 = 102.$$

5. Encontrar o resto da divisão de S_4 por 10: $102 \div 10 = 10$ e deixa resto 2.

6. Logo, o dígito de segurança é o resultado de $(10 - 2 = 8)$ e $102 + 8 \equiv 0$ m 10.

3.2 CPF - Cadastro de Pessoas Físicas

Esta seção foi elaborada baseada nos artigos [13], [17], [18], [19], e [22].

3.2.1 História

Desde a época que o Brasil era colônia que são cobrados impostos da população. De 1534 a 1700, no Brasil, eram cobradas a população 10% dos seus ganhos e interesses e parte desses impostos eram repassados a Coroa Portuguesa. Em 1808, com a chegada da família real no Brasil, foi criado o Conselho da Fazenda, que tinha como objetivo administrar e fiscalizar a arrecadação dos impostos. A primeira tentativa de implantar o imposto de renda no Brasil foi em 1843. Mas só em 1922 é que efetivamente foi implantado seguindo o modelo que era aplicado na França. Com a implantação do Estado Novo de Getúlio Vargas, em 1934, o imposto de renda ganhou status constitucional e passou a ser de competência da União. Em 1968, foi criada a Secretaria da Receita Federal, na qual se uniu os papeis de arrecadação, tributação e fiscalização de impostos. Neste mesmo ano, quem declarasse o imposto de renda, receberia um documento chamado de Identificação do Contribuinte (CIC) emitido eletronicamente e que tinha prazo de validade e deveria ser sempre renovado. Esse documento era de papel e era usado basicamente para as declarações de imposto de renda. Em meados dos anos 80, o CIC foi substituído pelo CPF (Cadastro de Pessoas Físicas), também de papel e com a mesma finalidade como na Figura 3.7. Com o passar dos anos, o CPF foi tornando-se cada vez mais importante passando a ser obrigatório sua apresentação até em aberturas de contas em banco, por exemplo. Com a importância do CPF aumentando, ele deixou de ser de papel e passou a ser de plástico como na Figura 3.8. Mas isso mudou e em setembro de 2010, a Receita efetuou uma mudança no CPF, que agora passa a ser online. Isto é, não será mais emitido o cartão CPF que a maioria tem hoje. O documento passa a ser impresso pela internet.

Figura 3.7: CPF de papel

Figura 3.8: CPF de plástico

3.2.2 Como é gerado o CPF?

O CPF é o registro de um cidadão na Receita Federal brasileira no qual devem estar todos os contribuintes (pessoas físicas nacionais e estrangeiras com negócios no Brasil). Ele armazena informações fornecidas pelo próprio contribuinte e por outros sistemas da Receita Federal. O CPF é um dos principais documento para cidadãos brasileiros, além de ser único e intransferível. Ele é composto por 11 dígitos, onde o nono dígito (da esquerda para a direita) revela a unidade federativa em que a pessoa registrou-se pela primeira vez, dado que é proibido (em condições normais) trocar de número. Logo, observando esse exemplo, o CPF $XXX.XXX.XX\mathbf{5} - YY$, o

número "5" em destaque indica que a origem deste CPF é Bahia ou Sergipe. Abaixo segue a Tabela 3.1 com todos os estados brasileiros:

Nono dígito	A unidade federativa onde originou o CPF
0	Rio Grande do Sul
1	Distrito Federal, Goiás, Mato Grosso, Mato Grosso do Sul e Tocantins
2	Amazonas, Pará, Roraima, Amapá, Acre e Rondônia
3	Ceará, Maranhão e Piauí
4	Paraíba, Pernambuco, Alagoas e Rio Grande do Norte
5	Bahia e Sergipe
6	Minas Gerais
7	Rio de Janeiro e Espírito Santo
8	São Paulo
9	Paraná e Santa Catarina

Tabela 3.1: Nono dígito Unidade Federativa

No exemplo mencionado, os dois últimos dígitos "YY", chamados de dígitos verificadores, são gerados a partir dos outros dígitos através de uma congruência módulo 11. Logo, para gerar o primeiro dígito verificador devemos então fazer operações envolvendo os noves primeiros dígitos, sendo assim, vamos supor que os nove primeiro dígitos, da esquerda para a direita, sejam $a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8$ e a_9. Distribua esses números numa tabela obedecendo a ordem e multiplique pelos seus respectivos pesos $\{10, 9, 8, 7, 6, 5, 4, 3, 2\}$, como mostra a Tabela 3.2.

a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9
10	9	8	7	6	5	4	3	2
$10a_1$	$9a_2$	$8a_3$	$7a_4$	$6a_5$	$5a_6$	$4a_7$	$3a_8$	$2a_9$

Tabela 3.2: Produto entre os 9 primeiros dígitos e seus respectivos pesos

Em seguida, calcule o somatório de todas as multiplicações, que representaremos assim:

$$S = 10a_1 + 9a_2 + 8a_3 + 7a_4 + 6a_5 + 5a_6 + 4a_7 + 3a_8 + 2a_9.$$

O resultado da soma "S" é então dividido por 11, o quociente deverá ser inteiro e o resto da divisão, se for maior ou igual a 2, será subtraído de 11, o resultado dessa subtração determina o primeiro dígito verificador a_{10}. Caso contrário, se o resto for menor que 2, o dígito verificador será 0. Esse dígito é o menor valor possível, tal que ao ser acrescentado à soma obtida, gera um múltiplo de 11, isto é, se a soma obtida é S, o número $S + a_{10}$ deve ser múltiplo de 11, ou seja,

$$S + a_{10} \equiv 0 \bmod 11.$$

Para o cálculo do segundo dígito verificador faremos de modo semelhante, mas agora o primeiro dígito verificador fará parte do cálculo. Então agora teremos 10 dígitos, $a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9$ e a_{10}. Distribua esses números numa tabela obedecendo a ordem, da esquerda para a direita, e multiplique pelos seus respectivos pesos $\{11, 10, 9, 8, 7, 6, 5, 4, 3, 2\}$, como mostra a Tabela 3.3.

a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	a_{10}
11	10	9	8	7	6	5	4	3	2
$11a_1$	$10a_2$	$9a_3$	$8a_4$	$7a_5$	$6a_6$	$5a_7$	$4a_8$	$3a_9$	$2a_{10}$

Tabela 3.3: Produto entre os 10 primeiros dígitos e seus respectivos pesos

Em seguida, calcule o somatório de todas as multiplicações, que representaremos assim:

$$S = 11a_1 + 10a_2 + 9a_3 + 8a_4 + 7a_5 + 6a_6 + 5a_7 + 4a_8 + 3a_9 + 2a_{10}.$$

O resultado da soma "S" é então dividido por 11, o quociente deverá ser inteiro e o resto da divisão, se for maior ou igual a 2, será subtraído de 11, o resultado dessa subtração determina o segundo dígito verificador a_{11}. Caso contrário, se o resto for menor que 2, o dígito verificador será 0. Esse dígito é o menor valor possível, tal que ao ser acrescentado à soma obtida, gera um múltiplo de 11, isto é, se a soma obtida é S, o número $S + a_{11}$ deve ser múltiplo de 11, ou seja,

$$S + a_{11} \equiv \ 0 \bmod 11.$$

Dessa maneira, fica demonstrado como o CPF é gerado.

Para exemplificar, vamos gerar um CPF válido calculando o dígito verificador de um CPF hipotétito, $543.736.128 - YY$. Já sabemos que a origem desse CPF, de acordo com a Tabela 3.1, é São Paulo.

Agora vamos gerar o primeiro dígito verificador

1. Distribua os 9 primeiros dígitos em um quadro e multiplique pelos seus respectivos pesos $10, 9, 8, 7, 6, 5, 4, 3, 2$ abaixo da esquerda para a direita, conforme a Tabela 3.4.

5	4	3	7	3	6	1	2	8
10	9	8	7	6	5	4	3	2
50	36	24	49	18	30	4	6	16

Tabela 3.4:

2. Calcule o somatório dos resultados (50+36+24+49+18+30+4+6+16) = 233

3. O resultado obtido (233) será divido por 11. Considere como quociente apenas o valor inteiro, o resto da divisão será responsável pelo cálculo do primeiro dígito verificador. Logo, 233 dividido por 11 obtemos 21 como quociente e 2 como resto da divisão. Subtrai-se o valor obtido de 11, sendo assim nosso dígito verificador é $11 - 2$, ou seja, 9. Observe também que

$$233 + 9 \equiv \ 0 \bmod 11.$$

Já temos portanto parte do CPF, confira: $543.736.128 - \ 9Y$.

Calculando o Segundo Dígito Verificador

Para o cálculo do segundo dígito será usado o primeiro dígito verificador já calculado. Montaremos uma tabela semelhante a anterior só que desta vez usaremos na segunda linha os valores $11, 10, 9, 8, 7, 6, 5, 4, 3$ e 2.

1. Distribua os 10 primeiros dígitos em um quadro e multiplique pelos seus respectivos pesos $11, 10, 9, 8, 7, 6, 5, 4, 3, 2$ abaixo da esquerda para a direita, conforme a Tabela 3.5.

5	4	3	7	3	6	1	2	8	9
11	10	9	8	7	6	5	4	3	2
55	40	27	56	21	36	5	8	24	18

Tabela 3.5:

2. Calcule o somatório dos resultados (55+40+27+56+21+36+5+8+24+18) = 290

3. O resultado obtido (290) será divido por 11. Considere como quociente apenas o valor inteiro, o resto da divisão será responsável pelo cálculo do primeiro dígito verificador. Logo, 290 dividido por 11 obtemos 26 como quociente e 4 como resto da divisão. Subtrai-se o valor obtido de 11, sendo assim nosso segundo dígito verificador é $11 - 4$, ou seja, 7. Uma vez que

$$290 + 7 \equiv 0 \bmod 11.$$

Neste caso chegamos ao final dos cálculos e descobrimos que os dígitos verificadores do nosso CPF hipotético são os números 9 e 7, portanto o CPF ficaria assim: $543.736.128 - 97$.

3.3 CNPJ - Cadastro Nacional da Pessoa Jurídica

Esta seção foi elaborada baseada nos artigos [13], [16]e [24].

3.3.1 História

O Cadastro Nacional da Pessoa Jurídica (CNPJ) foi instituído em 1998 em substituição ao antigo Cadastro Geral de Contribuintes (CGC) criado em 1964 e extinto em 1999. O CNPJ administrado pela Receita Federal que registra as informações cadastrais das pessoas jurídicas e de algumas entidades não caracterizadas como tais. No entanto, a partir de 01/11/2002, os cartões CNPJ perderam sua validade e, portanto, não estão sendo mais emitidos. Com a extinção do Cartão CNPJ, a comprovação da condição de inscrito passou a ser feita mediante consulta no site da Receita Federal. Neste site é possível fazer a emissão do comprovante de inscrição e da situação cadastrada via on-line sem necessidade do antigo cartão.

3.3.2 Como é gerado o CNPJ?

O CNPJ é um número único que identifica uma pessoa jurídica junto à Receita Federal Brasileira (órgão do Ministério da Fazenda), necessário para que a pessoa jurídica tenha capacidade de fazer contratos e processar ou ser processada. Ele é composto por 14 algarismos, divididos em 3 partes:

- Os 8 primeiros números localizados antes da barra representam o número de inscrição propriamente dito;
- Os 4 primeiros números localizados após a barra representam um código único para a matrix ou filial;
- e os 2 últimos números são chamados de dígitos verificadores (DV);

Logo, observando esse exemplo, o CNPJ XX.XXX.XXX/YYYY-ZZ, os dois últimos dígitos "Z" chamados de dígitos verificadores, são gerados a partir dos outros dígitos através de uma congruência módulo 11. Logo, para gerar o primeiro dígito verificador devemos então fazer operações envolvendo os dozes primeiros dígitos, sendo assim, vamos supor que os dozes primeiro dígitos, da esquerda para a direita, sejam $a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}, a_{11}$ e a_{12}. Distribua esses números numa tabela obedecendo a ordem e multiplique pelos seus respectivos pesos $\{5, 4, 3, 2, 9, 8, 7, 6, 5, 4, 3, 2\}$, como mostra a Tabela 3.6.

a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	a_{10}	a_{11}	a_{12}
5	4	3	2	9	8	7	6	5	4	3	2
$5a_1$	$4a_2$	$3a_3$	$2a_4$	$9a_5$	$8a_6$	$7a_7$	$6a_8$	$5a_9$	$4a_{10}$	$3a_{11}$	$2a_{12}$

Tabela 3.6: Produto entre os 12 primeiros dígitos e seus respectivos pesos

Em seguida, calcule o somatório de todas as multiplicações, que representaremos assim:

$$S = 5a_1 + 4a_2 + 3a_3 + 2a_4 + 9a_5 + 8a_6 + 7a_7 + 6a_8 + 5a_9 + 4a_{10} + 3a_{11} + 2a_{12}.$$

O resultado da soma S é então dividido por 11, o quociente deverá ser inteiro e o resto da divisão, se for maior ou igual a 2, será subtraído de 11, o resultado dessa subtração determina o primeiro dígito verificador a_{13}. Caso contrário, se o resto for menor que 2, o dígito verificador será 0. Esse dígito é o menor valor possível, tal que ao ser acrescentado à soma obtida, gera um múltiplo de 11, isto é, se a soma obtida é S, o número $S + a_{13}$ deve ser múltiplo de 11, ou seja, $S + a_{13} \equiv 0 \bmod 11$.

Para o cálculo do segundo dígito verificador faremos de modo semelhante, mas agora o primeiro dígito verificador fará parte do cálculo. Então agora teremos 13 dígitos, a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}, a_{11}, a_{12} e a_{13}. Distribua esses números numa tabela obedecendo a ordem, da esquerda para a direita, e multiplique pelos seus respectivos pesos $\{6, 5, 4, 3, 2, 9, 8, 7, 6, 5, 4, 3, 2\}$, como mostra a Tabela 3.7.

Em seguida, calcule o somatório de todas as multiplicações, que representaremos assim:

$$S = 6a_1 + 5a_2 + 4a_3 + 3a_4 + 2a_5 + 9a_6 + 8a_7 + 7a_8 + 6a_9 + 5a_{10} + 4a_{11} + 3a_{12} + 2a_{13}.$$

a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	a_{10}	a_{11}	a_{12}	a_{13}
6	5	4	3	2	9	8	7	6	5	4	3	2
$6a_1$	$5a_2$	$4a_3$	$3a_4$	$2a_5$	$9a_6$	$8a_7$	$7a_8$	$6a_9$	$5a_{10}$	$4a_{11}$	$3a_{12}$	$2a_{13}$

Tabela 3.7: Produto entre os 13 primeiros dígitos e seus respectivos pesos

O resultado da soma "S" é então dividido por 11, o quociente deverá ser inteiro e o resto da divisão, se for maior ou igual a 2, será subtraído de 11, o resultado dessa subtração determina o segundo dígito verificador a_{14}. Caso contrário, se o resto for menor que 2, o dígito verificador será 0. Esse dígito é o menor valor possível, tal que ao ser acrescentado à soma obtida, gera um múltiplo de 11, isto é, se a soma obtida é S, o número $S + a_{14}$ deve ser múltiplo de 11, ou seja, $S + a_{14} \equiv 0 \bmod 11$. Dessa maneira, fica demonstrado como o CNPJ é gerado.

Para exemplificar o processo e tornar mais fácil a explicação vamos calcular os dígitos verificadores de um CNPJ hipotético, por exemplo, $11.444.777/0001 - ZZ$. Para gerar o primeiro dígito verificador, distribua esses números numa tabela obedecendo a ordem e multiplique pelos seus respectivos pesos $\{5, 4, 3, 2, 9, 8, 7, 6, 5, 4, 3, 2\}$, como mostra a Tabela 3.8.

Em seguida, calcule o somatório dos resultados:

1	1	4	4	4	7	7	7	0	0	0	1
5	4	3	2	9	8	7	6	5	4	3	2
5	4	12	8	36	56	49	42	0	0	0	2

Tabela 3.8:

$$S = 5 + 4 + 12 + 8 + 36 + 56 + 49 + 42 + 0 + 0 + 0 + 2 = 214.$$

O resultado obtido (214) será divido por 11. Considere como quociente apenas o valor inteiro, o resto da divisão será responsável pelo cálculo do primeiro dígito verificador.

Vamos acompanhar: 214 dividido por 11 obtemos 19 como quociente e 5 como resto da divisão. Caso o resto da divisão seja menor que 2, o nosso primeiro dígito verificador se torna 0 (zero), caso contrário subtrai-se o valor obtido de 11, que é nosso caso. Sendo assim nosso dígito verificador é $11 - 5$, ou seja, 6. Uma vez que

$$214 + 6 \equiv 0 \bmod 11.$$

Já temos portanto, parte do CNPJ, confira: $11.444.777/0001 - 6Z$.

Para o cálculo do segundo dígito verificador faremos de modo semelhante, mas agora o primeiro dígito verificador fará parte do cálculo. Então agora teremos 13 dígitos. Distribua esses números numa tabela obedecendo a ordem, da esquerda para a direita, e multiplique pelos seus respectivos pesos $\{6, 5, 4, 3, 2, 9, 8, 7, 6, 5, 4, 3, 2\}$, como mostra a Tabela 3.9. Em seguida, calcule o somatório dos resultados:

$$S = 6 + 5 + 16 + 12 + 8 + 63 + 56 + 49 + 0 + 0 + 0 + 3 + 12 = 230.$$

1	1	4	4	4	7	7	7	0	0	0	1	6
6	5	4	3	2	9	8	7	6	5	4	3	2
6	5	16	12	8	63	56	49	0	0	0	3	12

Tabela 3.9:

O resultado obtido (230) será divido por 11. Considere como quociente apenas o valor inteiro, o resto da divisão será responsável pelo cálculo do primeiro dígito verificador.
Vamos acompanhar: 230 dividido por 11 obtemos 20 como quociente e 10 como resto da divisão. Caso o resto da divisão seja menor que 2, o nosso primeiro dígito verificador se torna 0 (zero), caso contrário subtrai-se o valor obtido de 11, que é nosso caso. Sendo assim nosso dígito verificador é $11 - 10$, ou seja, 1. Uma vez que

$$230 + 1 \equiv\ 0 \bmod 11.$$

Já temos portanto, o CNPJ, confira: $11.444.777/0001 - 61$.

3.4 ISBN - International Standard Book Number em português Número Padrão Internacional de Livro

Esta seção foi elaborada baseada no artigo [13].

3.4.1 História

Em 1966 realizou-se em Berlim a terceira Conferência Internacional de Investigação e Racionalização do mercado do livro cujo objetivo era criar um sistema internacional de numeração para identificar livros. Desse modo, iniciou-se a busca de um sistema que pudesse identificar cada livro, ou seja, cada livro deveria possuir um número único e universal. Logo, era necessário o controle de todo o estoque e isso seria feito pelo uso de computadores que processassem todas as informações. Em 1970 foi criado e aprovado o ISBN que é regulamentado pela ISO (International Organization for Standardization). Até o fim de 2006 o ISBN era composto por 10 dígitos ficando conhecido como $ISBN - 10$. A partir de 01 de Janeiro de 2007, passou a conter 13 dígitos, para aumentar a capacidade do sistema devido ao aumento no número de publicações, ficando conhecido como $ISBN - 13$. E agora quase todos os países do mundo utilizam o sistema ISBN para identificação de publicações, atribuindo um número único para cada edição.

3.4.2 Como é gerado o $ISBN - 10$?

O $ISBN - 10$ é sempre precedido das letras ISBN e é dividido em quatro partes de comprimento variável, que devem ser separadas por hífen. Cada uma dessas

partes representa respectivamente: país de origem do produto, empresa fabricante (editora), título e digito verificador. Por exemplo, vamos considerar de forma generalizada o seguinte código barras de um livro ISBN $XX-YYY-ZZZZ-W$. Os códigos de barra ISBN servem para identificar os livros de uma forma claramente organizada, então dentro do código, temos:

- Identificador de Grupo, País ou Área Idiomática representado pelos 2 primeiros dígitos, que no nosso exemplo é "XX". Todos os identificadores de grupo são atribuídos pela Agência Internacional do ISBN, em Berlim.
- Identificador de Editor representado pelos 3 seguintes dígitos "YYY", geralmente é indicada a exata identificação da editora e seu endereço. Os prefixos de editoras são atribuídos pela Agência ISBN do grupo responsável pela gestão do sistema ISBN no país, região ou grupo idiomático onde o editor é baseado oficialmente.
- Identificador de Título representado pelos próximos 4 dígitos "$ZZZZ$".
- Dígito verificador representado pelo último dígito do código "W" e que pode ser de 0 a 9 e no caso do número 10 é representado por X, nesse caso teremos o código ISBN 13, que trataremos na sequência.

Como é gerado esse dígito verificador? Considere o dígito verificador citado anteriormente. Distribua os nove primeiros dígitos a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8 e a_9 numa tabela obedecendo a ordem, da esquerda para a direita, e multiplique pelos seus respectivos pesos $\{10, 9, 8, 7, 6, 5, 4, 3, 2\}$, como mostra a Tabela 3.10.

a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9
10	9	8	7	6	5	4	3	2
$10a_1$	$9a_2$	$8a_3$	$7a_4$	$6a_5$	$5a_6$	$4a_7$	$3a_8$	$2a_9$

Tabela 3.10: Produto entre os 9 primeiros dígitos e seus respectivos pesos

Em seguida, calcule o somatório de todas as multiplicações, que representaremos assim: $S = 10a_1+9a_2+8a_3+7a_4+6a_5+5a_6+4a_7+3a_8+2a_9$. O resultado da soma "S" é então dividido por 11, o quociente deverá ser inteiro e o resto da divisão será subtraído de 11, o resultado dessa subtração determina o dígito verificador a_{10}. Esse dígito é o menor valor possível, tal que ao ser acrescentado à soma obtida, gera um múltiplo de 11, isto é, se a soma obtida é "S", o número $S + a_{10}$ deve ser múltiplo de 11, ou seja, $S + a_{10} \equiv 0 \bmod 11$. O resto pode ser o número 0 no entanto, o dígito verificador será o próprio zero. Caso, o resto seja o número 1 (como $11 - 1 = 10$) o dígito verificador será o número 10 em algarismo romano, ou seja, o caractere X será inserido no lugar do número 10, já que o dígito verificador é formado por um único dígito.

Para exemplificar, vamos efetuar a verificação de segurança de um código de um livro de matemática da 3ª série do Ensino Médio , que consiste em realizar as operações matemáticas abaixo para conferir o resultado delas com o dígito de

segurança.

Figura 3.9:

Considere o código ISBN $85-16-01340-5$. Distribua os noves primeiros dígitos 8, 5, 1, 6, 0, 1, 3, 4 e 0 numa tabela obedecendo a ordem, da esquerda para a direita, e multiplique pelos seus respectivos pesos $\{10, 9, 8, 7, 6, 5, 4, 3, 2\}$, como mostra a Tabela 3.11.

8	5	1	6	0	1	3	4	0
10	9	8	7	6	5	4	3	2
80	45	8	42	0	5	12	12	0

Tabela 3.11: Produto entre os 9 primeiros dígitos e seus respectivos pesos

Em seguida, calcule o somatório de todas as multiplicações, que representaremos assim:

$$S = 80 + 45 + 8 + 42 + 0 + 5 + 12 + 12 + 0 = 204.$$

Esse resultado é então dividido por 11, o quociente é 18 e o resto é 6. O resto da divisão é então subtraído de 11, ou seja, $11 - 6 = 5$, o resultado dessa subtração determina o dígito verificador $a_{10} = 5$. Dessa maneira, fica verificado que o código realmente está correto.

3.4.3 Como é gerado o $ISBN - 13$?

O $ISBN - 13$ é composto por 13 dígitos e foi gerado devido ao crescente número de publicações, com suas edições e formatos. Nesse código, os três primeiros dígitos representam o país de registro do produto, os quatro dígitos seguintes identificam o fabricante, os próximos cinco dígitos identificam o produto e o último, como já sabemos, é o dígito verificador ou de controle. O cálculo do dígito de verificação é feito de uma forma diferente. Considere o código ISBN $XXX-YY-ZZZ-YYYY-W$. Distribua os doze primeiros dígitos a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}, a_{11} e a_{12} numa tabela obedecendo a ordem, da esquerda para a direita, e multiplique pelos seus respectivos pesos $\{1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3\}$, como mostra a Tabela 3.12.

a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	a_{10}	a_{11}	a_{12}
1	3	1	3	1	3	1	3	1	3	1	3
$1a_1$	$3a_2$	$1a_3$	$3a_4$	$1a_5$	$3a_6$	$1a_7$	$3a_8$	$1a_9$	$3a_{10}$	$1a_{11}$	$3a_{12}$

Tabela 3.12: Produto entre os 12 primeiros dígitos e seus respectivos pesos

Em seguida, calcule o somatório de todas as multiplicações, que representaremos assim:

$$S = 1a_1 + 3a_2 + 1a_3 + 3a_4 + 1a_5 + 3a_6 + 1a_7 + 3a_8 + 1a_9 + 3a_{10} + 1a_{11} + 3a_{12}.$$

O resultado da soma S é então dividido por 10, sendo o quociente e o resto da divisão números inteiros e com $0 \leq resto \leq 9$. O resto será subtraído de 10, o resultado dessa subtração determina o dígito verificador a_{13}. Esse dígito é o menor valor inteiro positivo possível, tal que ao ser acrescentado à soma obtida, gera um múltiplo de 10, isto é, se a soma obtida é S, o número $S + a_{13}$ deve ser múltiplo de 10, ou seja, $S + a_{13} \equiv 0 \bmod 10$. Sendo o resto o número 0, o dígito verificador será próprio zero. Dessa maneira, fica demonstrado como o $ISBN - 13$ é gerado.

Para exemplificar, vamos efetuar a verificação de segurança de um código de um livro de matemática da 1ª série do Ensino Médio, que consiste em realizar as operações matemáticas abaixo para conferir o resultado delas com o dígito de segurança.

Figura 3.10:

Considere o código ISBN $978-85-262-7731-1$. Distribua os doze primeiros dígitos 9, 7, 8, 8, 5, 3, 9, 9, 0, 2, 7 e 5 numa tabela obedecendo a ordem, da esquerda para a direita, e multiplique pelos seus respectivos pesos $\{1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3\}$, como mostra a Tabela 3.13.

Em seguida, calcule o somatório de todas as multiplicações, que representaremos assim:

$$S = 9 + 21 + 8 + 24 + 5 + 6 + 6 + 6 + 7 + 21 + 3 + 3 = 119.$$

Esse resultado é então dividido por 10, o quociente é 11 e o resto é 9. O resto da divisão é então subtraído de 10, ou seja, $10 - 9 = 1$, o resultado dessa subtração

9	7	8	8	5	2	6	2	7	7	3	1
1	3	1	3	1	3	1	3	1	3	1	3
9	21	8	24	5	6	6	6	7	21	3	3

Tabela 3.13: Produto entre os 12 primeiros dígitos e seus respectivos pesos

determina o dígito verificador $a_{13} = 1$. Dessa maneira, fica verificado que o código realmente está correto.

Apêndice A

Breve Histórico da Criptografia

Neste apêndice, relateremos uma breve história da criptografia, baseado em alguns artigos como [1] e [7].

Segundo estudos, a criptografia teve início cerca de $1900a.C.$, no antigo Egito, pelo arquiteto Khnumhotep II, que substituiu trechos e palavras de documentos importantes por símbolos de modo a dificultar que ladrões chegassem aos tesouros descritos nesses documentos.

Em $600a.C.$, os hebreus criaram alguns sistemas criptográficos, nomeado por Atbash, que consiste de uma troca simples entre as letras do hebraico, por ordem inversa.

Em $480a.C.$, Heródoto, no livro "As Histórias", relata mensagens tatuadas nas cabeças raspadas de escravos para serem escondidas pelos cabelos, mensagens escritas em tabuletas, ocultas sob camadas de cera, ou mesmo a utilização de tintas invisíveis na escrita sobre a casca de ovos cozidos, mensagem colocada dentro do estômago de animais de caça. Esses tipos de trasmissão de mensagens recebem o nome de esteganografia, que diferentemente da criptografia, a mensagem mantém sua forma e baseia-se no fato de um interceptor não saber da existência da mensagem.

Em $475a.C.$, surgiu o primeiro sistema criptográfico de uso militar, o Scytale ou Bastião de Licurgo, que é um tipo de código de transposição, utilizado pelo general espartano Pasanius, que consiste em escrever a mensagem numa tira estreita de couro ou pergaminho quando esta está enrolada em torno de um bastão de madeira. A mensagem original é escrita no sentido do comprimento do bastão e, portanto, quando a tira é desenrolada obtém-se a mensagem codificada. Para voltar a obter a mensagem original, deve-se enrolar outra vez a tira num bastão com o mesmo perímetro e forma.

Aproximadamente $300a.C.$, surgiu, na Índia, um livro intitulado Arthasastra atribuído a Kautilya onde são referidos os primeiros métodos de criptoanálise.

Algum tempo depois, surgiu o código de deslocamento criado por Júlio César que consistia em substituir cada letra pela letra que se encontra três posições depois no alfabeto.

Em 1466, Leon Battista Alberti, escreveu um ensaio, no qual menciona um código em disco, criando a noção de código polialfabético.

Em 1553, Giovan Batista Belaso inventou um sistema criptográfico polialfabético chamado de código de Vigenère, por ter sido erroneamente atribuído a Blaise de

Vigenère durante o século XIX. Esse sistema é baseado não apenas em um, mas sim em 26 alfabetos codificados. Utiliza o código de César de forma diferente para cada alfabeto, formando assim uma tabela, chamada de Quadrado de Vigenère. Esse código foi considerado indecifrável durante muito tempo, sendo quebrado somente em 1854.

Durante os séculos XVIII e XIX, assistiu-se à proliferação de Câmeras Escuras, gabinetes de espionagem, onde se utilizava a criptologia para fins militares e fins civis, nomeadamente para decodificar mensagens diplomáticas.

Durante a Primeira Guerra Mundial assiste-se a uma proliferação de sistemas criptográficos para usos militares. Como exemplos, temos o Playfair e o ADFGVX. Após esta guerra começam a aparecer as primeiras máquinas cifrantes que usam rotores mecânicos.

Em 1923, Arthur Scherbius desenvolve o ENIGMA, máquina cifrante utilizada pelos alemães durante a Segunda Guerra Mundial para comunicações com os submarinos e para deslocar as suas tropas.

Em 1976, Whitfield Diffie e Martin Hellman publicam o artigo "New Directionsin Cryptograph", onde introduzem a ideia de criptografia de chave pública, neste caso baseada no problema do logaritmo discreto, e avançam com a ideia de autenticação utilizando funções de um só sentido (one way functions). Inspirados por aquele artigo, Ronald L. Rivest, Adi Shamir e Leonard M. Adleman, desenvolvem um código de chave pública, conhecido como RSA, que também pode ser usado para assinaturas digitais, baseado no contraste entre a dificuldade de fatorizar números grandes e a relativa facilidade de identificar números primos grandes.

Em 1984, Taher Elgamal desenvolve o sistema ElGamal também utilizando o problema do logaritmo discreto.

Nos anos 90 aparecem diversos sistemas criptográficos em particular o IDEA (International Data Encryption Algorithm) de Xuejia Lai e James Massey, que pretende ser um substituto do DES. A criptografia quântica é introduzida em 1990. O PGP (Pretty Good Privacy) de Phil Zimmermann, desenvolvido em 1991, ainda é um dos programas mais utilizados para proteger a privacidade do e-mail e dos arquivos guardados no computador do utilizador.

Em 1997, o NIST solicitou propostas para a substituição do DES. Em 2000, o NIST escolheu o Rijndael (de entre os finalistas estava MARS da IBM, RC6 de RSA Laboratories, Rijndael de Joan Daemen e Vincent Rijmen, Serpent de Anderson, Biham e Knudsen, e o twofish de Bruce Schneier e sua equipe), para ser o novo AES (Advanced Encryption Standard). Só em 2005 é que o NIST (National Institute of Standards and Technology), que substituiu o NBS, publica um plano de transição com a duração de dois anos, para que as 10 agências governamentais deixassem de utilizar o DES e passassem a utilizar o AES.

Referências Bibliográficas

[1] Almeida, P. J., *Criptografia e Segurança*, Departamento de Matemática da Universidade de Aveiro (2012).

[2] Anton, H. e Rorres, C. *Álgebra Linear com aplicações*. Editora Bookman, 8ª Ed., Porto Alegre, (2001).

[3] Boldrini, J. L., *Álgebra Linear*. Editora Harbra ltda., 3ª Ed., São Paulo, (1980).

[4] CRATO, N,. *Alice e Bob*. Expresso / Revista, 22 de Setembro, pp. 118 − 120, (2001).

[5] Domingues, Hygino H, *Fundamentos de aritmética*, Editora Atual, São Paulo, (1991).

[6] Ferreira, A. B. de H., *Miniaurélio Século XXI*. Editora Nova Fronteira., Edição especial para o FNDE/PNLD, Rio de Janeiro, (2004).

[7] Freire, P. B. e Castilho, J. E., *A matemática dos códigos criptográficos*, Universidade Católica de Brasília (2005).

[8] Fonseca, Rubens Vilhena., *Teoria dos números*, UEPA / Centro de Ciências Sociais e Educação, Belém, (2011).

[9] Hefez, A., *Elementos de aritmética*, Coleção do Professor de Matemática. Editora SBM, 2ª Ed., Rio de Janeiro, (2006).

[10] Iezzi, G e Hazzan, S, *Sequências, matrizes, determinantes e sistemas*, Coleção Fundamentos da Matemática Elementar - Volume 4. Editora Atual, 6ª Ed., São Paulo, (2001).

[11] Paiva, M., *Matemática* - Volume 2. Editora Moderna, 1ª Ed., São Paulo, (2004).

[12] Milies, C. P., *A Matemática dos Códigos de Barras*, Artigo, UFG(2006).

[13] Sá, I. P. de, *O que é aritmética modular? (A noção de congruência módulo k e suas diversas aplicações no cotidiano)* , Artigo.

[14] Santos, J. P. de O., *Introdução à Teoria dos Números,* Coleção Matemática Universitária. Associação Instituto Nacional de Matemática Pura e Aplicada, Rio de Janeiro,(2003).

[15] Shokranian, S., *Criptografia para iniciantes*. Editora Ciência Moderna, 2ª Ed., Rio de Janeiro, (2012).

[16] Nascimento, D. C. do, Santos, L. D. dos, Pires, L. V., Oliveira, R. de, e Santos, W. R., *CNPJ ? Cadastro Nacional De Pessoa Jurídica*, Trabalho científico apresentado à disciplina de Administração de sistema de informação gerencial. CURITIBA (2007).

[17] *http://www.impostoderenda.net/historia/historia-do-imposto-de-renda-no-brasil/*, página consultada em 14/01/2014. Organizada por Sandra (2011).

[18] *http://www.gerardocumentos.com.br/?pg=entenda-a-formula-do-cpf*, página consultada em 06/01/2014.

[19] *http://www.geradorcpf.com/*, página consultada em 06/01/2014.

[20] *http://www.portal.famat.ufu.br/sites/famat.ufu.br/files/Anexos/Bookpage/famat-revista-13-artigo-3-0.pdf*, página consultada em 14/01/2014.

[21] *http://www.portal.famat.ufu.br/sites/famat.ufu.br/files/Anexos/Bookpage/famat-revista-13-artigo-4-0.pdf*, página consultada em 14/01/2014.

[22] *http://www.acessa.com/tecnologia/arquivo/suporte/2011/02/16-cpf/*, página consultada em 14/01/2014.

[23] *http* : *//www.gs1br.org/main.jsp?lumChannelId* = 40288176383*AC*689013847*EF*03635302, , página consultada em 12/10/2014. Organizada por Associação Brasileira de Automação.

[24] *http* : *//www.geradorcnpj.com/algoritmo* − *do* − *cnpj.htm*, página consultada em 24/02/2014.

[25] *http://www.numaboa.com.br/criptografia/cifras/substituicoes/monoalfabeticas/simples/165-Codigo-de-Cesar*, página consultada em 29/07/2014.