UNIVERSIDADE ESTADUAL DE MARINGÁ
CENTRO DE CIÊNCIAS EXATAS
DEPARTAMENTO DE MATEMÁTICA
MESTRADO PROFISSIONAL EM MATEMÁTICA

Criptografia Clássica, Matrizes e Tecnologia.

Gilberto Aparecido Tenani

Orientador
Prof. Dr. Marcos Roberto Teixeira Primo

2016

UNIVERSIDADE ESTADUAL DE MARINGÁ
CENTRO DE CIÊNCIAS EXATAS
DEPARTAMENTO DE MATEMÁTICA
MESTRADO PROFISSIONAL EM MATEMÁTICA

Criptografia Clássica, Matrizes e Tecnologia.

Gilberto Aparecido Tenani

Dissertação apresentada ao Programa de Pós-Graduação – Mestrado Profissional em Matemática em Rede Nacional como requisito parcial para a obtenção do grau de Mestre.

Orientador
Prof. Dr. Marcos Roberto Teixeira Primo

2016

Dados Internacionais de Catalogação na Publicação (CIP)
(Biblioteca Central - UEM, Maringá, PR, Brasil)

T289c

Tenani, Gilberto Aparecido
Criptografia clássica, matrizes e tecnologia / Gilberto Aparecido Tenani -- Maringá, 2016.
52 f. : il., color., figs., tabs.

Orientador: Prof. Dr. Marcos Roberto Teixeira Primo.
Dissertação (mestrado) - Universidade Estadual de Maringá, Centro de Ciências Exatas, Departamento de Matemática, Mestrado Profissional em Matemática, 2016.

1. Àlgebra matricial. 2. Criptografia. 3. Tecnologia educacional. 4. Aritmética modular. 5. Cifras Hill. I. Primo, Marcos Roberto Teixeira, orient. II. Universidade Estadual de Maringá. Centro de Ciências Exatas. Departamento de Matemática. Mestrado Profissional em Matemática. III. Título.

CDD 21.ed. 512.74
AHS-002835

GILBERTO APARECIDO TENANI

CRIPTOGRAFIA A CLÁSSICA, MATRIZES E TECNOLOGIA

Trabalho de Conclusão de Curso, apresentada ao Programa de Mestrado Profissional em Matemática em Rede Nacional do Departamento de Matemática, Centro de Ciências Exatas da Universidade Estadual de Maringá, como parte dos requisitos necessários para a obtenção do título de Mestre em Matemática tendo a Comissão Julgadora composta pelos membros:

COMISSÃO JULGADORA:

Prof. Dr. Marcos Roberto Teixeira Primo
DMA/Universidade Estadual de Maringá (Presidente)

Prof. Dr. Jair da Silva
Universidade Federal do Paraná – Campus Jandaia do Sul

Prof. Dr. Laerte Bemm
DMA/Universidade Estadual de Maringá

Aprovada em: 13 de janeiro de 2016.
Local de defesa: Sala 202, Bloco F67, campus da Universidade Estadual de Maringá.

Dedico esta Dissertação à Leiliane e Paula, pela ausência que a mesma me fez prescindir da companhia de ambas.

Agradecimentos

À minha querida esposa Leiliane, à minha amada filha Paula e a todos meus amigos por me darem o suporte necessário para esta caminhada.

Aos meus pais, por terem-me dado educação, valores e por terem-me ensinado a andar.

À Universidade Estadual de Maringá, seu corpo docente, direção e administração que oportunizaram a janela por onde vislumbro um horizonte superior.

Ao meu orientador Prof. Dr. Marcos Roberto Teixeira Primo, pelo grande suporte prestado, pelos momentos de reflexão proporcionados, pelas correções e pelo incentivo.

Ao Coordenador do PROFMAT da UEM Prof. Dr. Laerte Bemm pelo incentivo e disponibilidade.

Agradeço a todos os professores do PROFMAT da UEM por me proporcionarem o conhecimento não apenas racional, mas a manifestação do caráter e afetividades da educação no processo de formação.

Aos colegas de curso, pelo companheirismo, pela ajuda nas dúvidas e pela motivação durante todo o mestrado.

E a todos que, direta ou indiretamente, fizeram parte da minha formação, o meu muito obrigado.

Mesmo que a rota da minha vida me conduza a uma estrela, nem por isso fui dispensado de percorrer os caminhos do mundo.

José Saramago

Resumo

Neste trabalho apresentamos métodos criptográficos e de criptoanálise clássicos utilizando álgebra matricial. Após fazermos uma breve introdução à criptografia clássica, introduzimos os métodos conhecidos como cifras de Hill, mostramos como criptografar e descriptografar mensagens usando essas cifras. Ainda, mostramos quando e como é possível quebrar esses métodos e apresentamos uma ferramenta computacional, auxiliar na realização de cálculos baseado na linguagem de programação Julia e no ambiente interativo JuliaBox. Além disso, destacamos os principais resultados matemáticos que justificam o funcionamento desses métodos, tais como: divisibilidade, congruências e congruências lineares.

Palavras-chave: Álgebra Matricial, Criptografia, Tecnologia, Aritmética Modular, Cifras Hill.

Abstract

This work presents classic criptography and cryptanalysis methods based on matrix algebra. After a brief introduction about classic criptography we introduce the methods known as the Hill's ciphers. We also show when and how it is possible to break this method and an additional computing tool for based on Julia programming language and the interaction enviroment JuliaBox. Furthermore, we focus the main mathematical results that justify the operation of these methods, such as: divisibility, congruences and linear congruences.

Keywords: Matrix Algebra, Cryptography, Technology, Modular Arithmetic, Hill Ciphers.

Lista de Figuras

Sumário

Introdução

Pessoas sempre tiveram fascinação em manter informação escondida de outros. Quando crianças, muito de nós tínhamos maneiras secretas de enviar mensagens codificadas para nossos amigos mantendo segredo de irmãos, pais e professores. A história nos mostra muitos exemplos de pessoas e nações que tentaram manter informações longe do alcance de inimigos. Uma das formas de se fazer isso é a codificação da mensagem. Com a evolução da sociedade, novos e mais sofisticados métodos de proteger informação através da codificação surgiram. As técnicas necessárias para codificar informações pertencem ao campo de estudo conhecido como **criptografia**. Naturalmente, junto com a criptografia surgiu também o campo de estudo conhecido como **criptoanálise** que consiste justamente no processo inverso da criptografia, ou seja, as técnicas necessárias para descobrir as informações verdadeiras contidas em mensagens codificadas.
Tecnicamente, a **criptologia** é o termo que engloba todo o estudo sobre comunicação em canais não seguros e seus problemas relacionados. A criptologia moderna é um campo de conhecimento que exige forte domínio de conteúdo matemático e computacional.
Nesse trabalho, trataremos da parte da criptologia conhecida como clássica. Os métodos criptográficos e de criptoanálise chamados clássicos foram desenvolvidos antes da era do computador pessoal (por volta de 1970) e continuam ainda sendo aplicados em inúmeras situações. Em particular, trabalharemos com métodos criptográficos e de criptoanálise conhecidos como **cifras de Hill**, que têm por base transformações matriciais. Apresentaremos vários exemplos que podem ser utilizados no ensino médio e como o uso de ferramentas tecnológicas pode nos auxiliar nessa tarefa.
Um dos requisitos básicos para os métodos criptográficos são as ideias de divisibilidade e congruências. A ideia básica de congruência é bem simples. Dado dois número inteiros a e b, dizemos que a é congruente a b módulo m e escrevemos $a \equiv b(mod\, m)$, se $m|(a-b)$. A congruência módulo m nos permite definir o conjunto $\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$, denominado um conjunto completo de resíduos módulo m (os elementos desse conjunto são os possíveis restos da divisão de um inteiro a por m). No capítulo 1 estudaremos os conceitos básicos de divisibilidade e congruências, suas propriedades e os principais resultados que são importantes para o entendimento dos métodos criptográficos e de

criptoanálise.

Criptografia é o estudo dos métodos de enviar mensagens de maneira disfarçada de tal forma que somente o destinatário original possa remover o disfarce e ler a mensagem. Com a evolução da sociedade, métodos mais sofisticados de proteção de dados foram criados. A maioria dos métodos criptográficos e de criptoanálise envolvem grande quantidade de matemática, simples e complexa. No capítulo 2, introduziremos as noções básicas sobre criptografia e criptoanálise, definindo os principais conceitos e termos utilizados e apresentando alguns métodos simples de criptografia e de criptoanálise.

Um caso particular da criptografia e da criptoanálise clássica, as cifras de Hill, são bastante interessantes ao utilizarem álgebra matricial e congruências para criar métodos de criptografia e criptoanálise de mensagens. O nome é em referência a Lester S. Hill (1891–1961) que introduziu esses métodos em [4] e [5]. No capítulo 3 trataremos de congruências utilizando matrizes, dos métodos de criptografia e criptoanálise usando as cifras de Hill, analisaremos como e quando é possível quebrar o método e mostraremos como ferramentas tecnológicas podem nos auxiliar na realização de cálculos que seriam bastante tediosos se feitos a mão.

Finalmente, o apêndice A fornece mais informações sobre a linguagem de programação Julia a o ambiente JuliaBox.

1 Divisibilidade e Congruências

Teoria dos números, de uma maneira geral, é o estudo do conjunto dos números inteiros, representado por $\mathbb{Z}$, e de suas propriedades. Neste capítulo, faremos uma revisão de alguns tópicos de teoria elementar dos números que usaremos posteriormente em nosso trabalho. Em particular, estaremos interessados na aritmética modular do conjunto dos números naturais $\mathbb{N}$. Os resultados exibidos foram extraídos, quase em sua totalidade, de [3] e [7].

1.1 Divisibilidade

Como a divisão de um número inteiro por outro, quando existir, nem sempre é exata, expressa-se esta possibilidade através da relação de divisibilidade.

Definição 1.1. *Dados a e $b \in \mathbb{Z}$, dizemos que a **divide** b se existir um inteiro d tal que $b = ad$. Neste caso, também é dito que a é **divisor** ou **fator** de b, ou ainda, b é um **múltiplo** de a.*
Se a divide b escrevemos $a \mid b$, caso contrário, escrevemos $a \nmid b$.

Exemplo 1.2. Temos que

$$13 \mid 65, \quad -5 \mid 15, \quad 13 \mid 169, \quad 6 \nmid 35 \text{ e } 0 \nmid 17$$

Exemplo 1.3. Os divisores de 4 são

$$\pm 1, \pm 2 \text{ e } \pm 4$$

Proposição 1.4. *Se $a, b, c \in \mathbb{Z}$ com $a \mid b$ então $a \mid bc$.*

Prova: Como $a \mid b$, existe natural $d_1 \in \mathbb{Z}$ tal que $b = ad_1$. Assim, $bc = (ad_1)c = a(d_1c)$, completando a demonstração. □

Proposição 1.5. *(Transitividade) Se $a, b, c \in \mathbb{Z}$ com $a \mid b$ e $b \mid c$ então $a \mid c$.*

Prova: Como $a \mid b$ e $b \mid c$, existem d_1 e $d_2 in \mathbb{Z}$ tais que $b = ad_1$ e $c = bd_2$. Assim, $c = bd_2 = (ad_1)d_2 = a(d_1d_2)$ e, portanto, $a \mid c$, completando a demonstração.□

Proposição 1.6. *Se $a, b, c, m, n \in \mathbb{Z}$ e $a \mid b$ e $a \mid c$, então $a \mid (mb + nc)$.*

Prova: Como $a \mid b$ e $a \mid c$ existem inteiros d_1 e d_2 tais que $b = ad_1$ e $c = ad_2$. Assim, $mb + nc = m(ad_1) + n(ad_2) = a(md_1 + nd_2)$ e, portanto, $a \mid (mb + nc)$„ completando a demonstração. □

Corolário 1.7. *Se $a, b, c \in \mathbb{N}$ com $a \mid b$ e $a \mid c$ então $a \mid (b + c)$ e $a \mid (b - c)$.*

A definição a seguir é necessária para a demonstração do Teorema 1.11.

Definição 1.8. *Seja $x \in \mathbb{R}$. O maior inteiro menor ou igual a x é indicado por $[x]$.*

Exemplo 1.9.

$$[2, 4] = 2, \qquad [-3, 2] = -4, \qquad [5] = 5, \qquad \left[\frac{3}{2}\right] = 1.$$

Segue diretamente da definição que

Proposição 1.10. *Se $x \in \mathbb{R}$ então $x - 1 < [x] \leq x$.*

Quando não existir a relação de divisibilidade entre dois números inteiros, veremos que, ainda assim, será possível efetuar uma divisão com resto, chamada de *divisão euclidiana.*

Teorema 1.11. *(Algoritmo da Divisão) Se $a, b \in \mathbb{Z}$ com $b > 0$, então existem inteiros únicos q, r tais que $a = bq + r$, com $0 \leq r < b$.*

O número $q \in \mathbb{Z}$ é chamado de **quociente** e o número $r \in \mathbb{Z}$ é chamado de **resto** da divisão.
Prova: Sejam $q = [a/b]$ e $r = a - b[a/b]$. Temos então que $a = bq + r$. Mostraremos que o resto r satisfaz a desigualdade $0 \leq r < b$. Para isso, observe que

$$a/b - 1 < [a/b] \leq a/b.$$

Multiplicando essa desigualdade por b, obtemos

$$a - b < b[a/b] \leq a.$$

Multiplicando por -1,encontramos

$$-a \leq -b[a/b] < b - a$$

Adicionando a a cada membro, chegamos a

$$0 \leq r = a - b[a/b] < b$$

Para mostrar que o quociente $q \in \mathbb{Z}$ e o resto $r \in \mathbb{Z}$ são únicos, suponhamos que $a = bq_1 + r_1$ e $a = bq_2 + r_2$, com $0 \leq r_1 < b$ e $0 \leq r_2 < b$. Logo

$$0 = b(q_1 - q_2) + (r_1 - r_2).$$

Assim, temos que

$$r_2 - r_1 = b(q_1 - q_2)$$

Disto resulta que b divide $r_2 - r_1$. Desde que $0 \leq r_1 < b$ e $0 \leq r_2 < b$, temos $-b < r_2 - r_1 < b$. Isto mostra que b pode dividir $r_2 - r_1$ se, e somente se, $r_2 - r_1 = 0$, ou, em outras palavras, se $r_2 = r_1$. Desde que $bq_1 = r_1 = bq_2 + r_2$ e $r_1 = r_2$, vemos que $q_1 = q_2$, completando a demonstração. □
Obviamente, a é divisível por b se, e somente se, $r = 0$ no algoritmo da divisão.

Exemplo 1.12. Temos:

a) $133 = 21.6 + 7$

b) $-50 = 8.(-7) + 6$

1.2 Números Primos

Nesta seção faremos uma breve revisão sobre números primos, um dos conceitos mais importantes de toda a Matemática.

Definição 1.13. *Um número* ***primo*** $p \in \mathbb{Z}$ *é um número maior que 1 que é divisível apenas por 1 e por ele mesmo.*

Um número que não é primo é chamado **composto**. Assim, se um número inteiro $n > 1$ é composto, existirá um divisor natural n_1 de n tal que $n_1 \neq 1$ e $n_1 \neq n$. Portanto, existirá um número natural n_2 tal que

$$n = n_1 \times n_2, \quad \textbf{com } 1 < n_1 < n \text{ e } 1 < n_1 < n$$

Exemplo 1.14. Temos:

a) Os números 5, 7, 11, 101 e 163 são primos.

b) Os números 4, 33, 111 e 200 são compostos.

Se a e $b \in \mathbb{Z}$, não ambos nulos, então o conjunto dos divisores comuns de a e de b é um conjunto de números inteiros finito, sempre contendo os inteiros $+1$ e -1.

Definição 1.15. *O* ***máximo divisor comum*** *entre dois inteiros a e b, não ambos nulos, é o maior inteiro que divide ambos a e b. O máximo divisor comum entre a e b será indicado por $mdc(a, b)$.*

Exemplo 1.16. Os divisores comuns de 24 e 84 são $\pm 1, \pm 2, \pm 3, \pm 4, \pm 6$ e ± 12. Assim

$$mdc(24, 84) = 12$$

Definição 1.17. *Se o* ***máximo divisor comum*** *entre dois inteiros a e b, não nulos, for igual a 1, diremos que a e b são* ***primos entre si****.*

Exemplo 1.18. Desde que $mdc(25, 42) = 1$ temos que 25 e 42 são primos entre si.

Teorema 1.19. *O máximo divisor comum entre os inteiros a e b, não ambos nulos, é o menor inteiro positivo que é combinação linear de a e b.*

Prova: Seja d o menor inteiro positivo que é uma combinação linear de a e b. (Existem tal menor inteiro positivo desde que pelo menos uma das combinações lineares $1.a+0.b$ e $(-1)a + 0.b$ é positiva). Escrevemos

$$d = ma + nb,$$

onde m e n são inteiros. Mostraremos que $d|a$ e $d|b$. Pelo algoritmo da divisão, nós temos

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

Destas equações nós vemos que

$$r = a - dq = a - q(ma + nb) = (1 - qm)a - qnb.$$

Isto mostra que o inteiro r é uma combinação linear de a e b. Desde que $0 \leq e < d$, e d é o menor inteiro positivo que é combinação linear de a e b, concluímos que $r = 0$, e assim $d|a$. De forma similar, mostra-se que $d|b$.
Mostramos que d, o menor inteiro positivo que é combinação linear de a e b, é um divisor de a e de b. Resta mostrar que d é o maior divisor comum de a e de b. Para isto, devemos mostrar que qualquer divisor comum c de a e de b deve dividir d. Desde que que $d = ma + nb$, se $c|a$ e $c|b$, o Teorema 1.6 garante que $c|d$, então $c \leq d$. Completando a demonstração. □

Proposição 1.20. *Sejam $a, b, p \in \mathbb{Z}$, com p primo. Se $p|ab$, então $p|a$ ou $p|b$.*

Prova: Basta provar que, se $p|ab$ e $p \not| a$ então $p|b$. Mas se $p|ab$, então existe $c \in \mathbb{Z}$ tal que $ab = pc$. Como $mdc(p, a) = 1$ então, temos que existem $m, n \in \mathbb{Z}$ tais que

$$np + ma = 1.$$

Multiplicando por b ambos os lados da igualdade acima, temos que

$$b = npb + mab.$$

Substituindo ab por pc nesta última igualdade , temos que

$$b = npb + mpc = p(nb + mc),$$

e, portanto, $p|b$, completando a demonstração.
□

Teorema 1.21. *(Teorema Fundamental da Aritmética) Todo número inteiro $n > 1$ ou é primo ou se escreve de modo único (a menos da ordem dos fatores) como um produto de números primos.*

A demonstração do Teorema Fundamental da Aritmética pode ser encontrada em [7], página 112.

1.3 Congruência

A linguagem de congruência foi desenvolvida no começo do Século XIX por Gauss e é extremamente útil para a Teoria dos Números. Trata-se da realização de uma aritmética com os restos da divisão euclidiana por um número fixado.

Definição 1.22. *Seja m um número inteiro não nulo. Dizemos que dois números inteiros a e b são congruentes módulo m, se $m \mid (a - b)$.*
Se a é congruente a b módulo m, escrevemos

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

Se $m \nmid (a - b)$, escrevemos $a \not\equiv b(mod\ m)$.

Essa definição é equivalente a dizer que os números inteiros a e b são congruentes módulo m, se os restos de suas divisões euclidianas por m são iguais.

Exemplo 1.23. Temos que:

a)

$$21 \equiv 13(mod\ 2)$$

pois os restos da divisão de 21 e de 13 por 2 são iguais a 1.

b)

$$22 \equiv 4(mod\ 9)$$

pois $9|(22-4) = 18$.

Proposição 1.24. *Se a e b são números inteiros, então $a \equiv b(mod\ m)$ se e, somente se, existe um inteiro k tal que $a = b + km$.*

Prova: Se $a \equiv b(mod\ m)$, então $m \mid (a-b)$. Isto significa que existe um inteiro k tal que $km = a - b$, isto é, $a = b + km$. Por outro lado, se existe um inteiro k tal que $a = b + km$, então $km = a - b$. Assim $m \mid (a-b)$, e portanto, $a \equiv b(mod\ m)$, completando a demonstração. □

Proposição 1.25. *Seja $m \in \mathbb{Z}$. A congruência módulo m satisfaz as seguintes propriedades:*

i) (Reflexiva) Se a é um inteiro, então $a \equiv a(mod\ m)$.

ii) (Simétrica) Se a e b são inteiros tais que $a \equiv b(mod\ m)$, então $b \equiv a(mod\ m)$.

iii) (Transitiva) Se a, b e c são inteiros tais que $a \equiv b(mod\ m)$ e $b \equiv c(mod\ m)$, então $a \equiv c(mod\ m)$.

Prova:

i) $a \equiv a(mod\ m)$, pois $m \mid 0 = (a-a)$.

ii) Se $a \equiv b(mod\ m)$, então $m \mid (a-b)$. Assim, existe um inteiro k tal que $km = a-b$. Isto mostra que $(-k)m = b-a$ e então $m \mid (b-a)$. Consequentemente $b \equiv a(mod\ m)$.

iii) Se $a \equiv b(mod\ m)$ e $b \equiv c(mod\ m)$, então $m \mid (a-b)$ e $m \mid (b-c)$. Assim, existem inteiros k e l com $km = a - b$ e $lm = b - c$. Desta forma,

$$a - c = (a-b) + (b-c) = km + lm = (k+l)m.$$

Consequentemente, $m \mid (a-c)$ e $a \equiv c(mod\ m)$, completando a demonstração. □

A Proposição 1.25 mostra que, fixado $m \in \mathbb{Z}$, a congruência módulo m forma uma relação de equivalência sobre o conjunto $\mathbb{Z}$ dos números inteiros e, assim, o conjunto $\mathbb{Z}$ é particionado em m diferentes conjuntos chamados *classes de congruência módulo* m ou *classes residuais módulo* m, cada qual contendo os inteiros que são congruentes módulo m. O conjunto das classes de congruências módulo m será representado por $\mathbb{Z}_m$.

Exemplo 1.26. As 5 classes de congruências módulo 5 são dadas por

$$\cdots \equiv -10 \equiv -5 \equiv 0 \equiv 5 \equiv 10 \ldots (mod\ 5)$$
$$\cdots \equiv -9 \equiv -4 \equiv 1 \equiv 6 \equiv 11 \ldots (mod\ 5)$$
$$\cdots \equiv -8 \equiv -3 \equiv 2 \equiv 7 \equiv 12 \ldots (mod\ 5)$$
$$\cdots \equiv -7 \equiv -2 \equiv 3 \equiv 8 \equiv 13 \ldots (mod\ 5)$$
$$\cdots \equiv -6 \equiv -1 \equiv 4 \equiv 9 \equiv 14 \ldots (mod\ 5)$$

Seja $a \in \mathbb{Z}$ um inteiro. Dado o inteiro positivo $m > 1$, pelo algoritmo da divisão, temos que $a = bm + r$ com $0 \leq r \leq m-1$. Da equação $a = bm + r$, vemos que $a \equiv r(mod\ m)$. Assim, qualquer inteiro é congruente módulo m a algum dos inteiros $0, 1, \ldots, m-1$, o qual é o resto de sua divisão por m. Como não existem dois inteiros entre 0 e $m-1$ congruentes entre si módulo m, temos que qualquer inteiro é congruente módulo m a exatamente um destes inteiros $0, 1, \ldots, m-1$.

Definição 1.27. *Um* ***sistema completo de resíduos módulo*** m *é um conjunto de* m *inteiros* $\{a_1, a_2, \ldots, a_m\}$ *que se* $a_i \neq a_j$ *então* $a_i \not\equiv a_j (mod\ m)$.

Dado um sistema de resíduos módulo m, qualquer inteiro é congruente módulo m a exatamente um inteiro desse conjunto.

Exemplo 1.28. O algoritmo da divisão mostra que o conjunto dos inteiros $\{0, 1, 2, \ldots, m-1\}$ é um sistema completo de resíduos módulo m.

Faremos agora alguma aritmética com congruências, sendo que estas tem muitas das propriedades que a igualdade possui. Começamos mostrando que adição, subtração e multiplicação em ambos os lados de uma congruência preserva a congruência.

Teorema 1.29. *Se* a, b, c *e* m *são inteiros, com* $m > 0$ *tais que* $a \equiv b(mod\ m)$, *então*

i) $a + c \equiv b + c(mod\ m)$;

ii) $a - c \equiv b - c(mod\ m)$;

iii) $ac \equiv bc(mod\ m)$.

Prova:

i) Como $a \equiv b(mod\ m)$, $m \mid (a-b)$. Agora, de $(a+c)-(b+1) = a-b$, vemos que $m \mid [(a+c)-(b+c)]$. Assim $a+c \equiv b+c(mod\ m)$.

ii) Análogo ao item (i).

iii) Observe que $ac-bc = c(a-b)$. Desde que $m \mid (a-b)$, segue que $m \mid c(a-b)$, e assim, $ac \equiv bc(mod\ m)$
, completando a demonstração. □

Exemplo 1.30. Desde que $18 \equiv 2(mod\ 8)$ segue do Teorema 1.29 que

$$25 = 18+7 \equiv 2+7 = 9(mod\ 8)$$
$$17 = 18-1 \equiv 2-1 = 1(mod\ 8)$$
$$36 = 18 \times 2 \equiv 2 \times 2 = 4(mod\ 8)$$

□

Uma pergunta natural que podemos nos fazer é: O que acontece quando ambos os lados de uma congruência são "divididos" por um inteiro? O exemplo a seguir mostra que a congruência nem sempre é preservada quando ambos o lados da mesma são divididos pelo mesmo número.

Exemplo 1.31. Temos que

$$2 \times 7 \equiv 2 \times 4(mod\ 6)\ \textbf{mas}\ 7 \not\equiv\ 4(mod\ 6).$$

□

Em outras palavras, a lei do cancelamento não vale na congruência, ao contrário da igualdade.

Teorema 1.32. *Se $a, b, c, m \in \mathbb{Z}$ com $c \neq 0$ e $m > 1$ são inteiros tais que $mdc(c, m) = d$, então $ac \equiv bc(mod\ m)$, se, e somente se, $a \equiv b(mod\ m/d)$.*

Prova:
Como m/d e c/d são primos entre si, temos que

$$ac \equiv bc(mod\, m) \iff m \mid (b-a)c \iff m/d \mid (b-a)c/d \iff m/d \mid (b-a) \iff a \equiv b(mod\, m/d),$$

completando a demonstração. □

Exemplo 1.33. Temos $5 \times 10 \equiv 2 \times 10(mod\ 15)$ e $mdc(10, 15) = 5$. Então,

$$\frac{5 \times 10}{10} \equiv \frac{2 \times 10}{10}(mod\ \frac{15}{5}),\ \text{ou seja, } 5 \equiv 2(mod\ 3).$$

Corolário 1.34. *Se $a, b, c, m \in \mathbb{Z}$ com $c \neq 0$ e $m > 1$ são tais que $mdc(c, m) = 1$, então $ac \equiv bc(mod\ m)$, se, e somente se, $a \equiv b(mod\ m)$.*

Exemplo 1.35. Como $6 \times 7 \equiv 1 \times 7(mod\ 5)$ e $mdc(5, 7) = 1$, temos

$$\frac{6 \times 7}{7} \equiv \frac{1 \times 7}{7}(mod\ 5),\ \textbf{ou}\ 6 \equiv 1(mod\ 5).$$

Teorema 1.36. *Se $a, b, c, d, m \in \mathbb{Z}$ são inteiros tais que $m > 0$, $a \equiv b(mod\ m)$ e $c \equiv d(mod\ m)$, então:*

i) $a + c \equiv b + d(mod\ m)$

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

iii) $ac \equiv bd(mod\ m)$

Prova: Desde que $a \equiv b(mod\ m)$ e $c \equiv d(mod\ m)$, temos $m \mid (a - b)$ e $m \mid (c - d)$. Assim, existem inteiros k e l com $km = a - b$ e $lm = c - d$. Disso temos:

i) $(a + c) - (b + d) = (a - b) + (c - d) = km + lm = (k + l)m$.
Assim, $m \mid [(a + c) - (b + d)]$, e, portanto, $a + c \equiv b + d(mod\ m)$

ii) $(a - c) - (b - d) = (a - b) - (c - d) = km - lm = (k - l)m$.
Assim, $m \mid [(a - c) - (b - d)]$,e, portanto, $a - c \equiv b - d(mod\ m)$

iii) $ac - bd = ac - bc + bc - bd = c(a - b) + b(c - d) = ckm + blm = m(ck + bl)$.
Assim $m \mid (ac - bd)$ e, logo $ac \equiv bd(mod\ m)$, completando a demonstração.□

Exemplo 1.37. Temos que $13 \equiv 8(mod\ 5)$ e $7 \equiv 2(mod\ 5)$. Pelo Teorema 1.36 vemos que:

a) $13 + 7 \equiv 8 + 2(mod\ 5)$;

b) $13 - 7 \equiv 8 - 7(mod\ 5)$;

c) $13 \times 7 \equiv 8 \times 2(mod\ 5)$.

Teorema 1.38. *Se $\{r_1, r_2, \ldots, r_m\}$ é um sistema completo de resíduos módulo m e se a é um inteiro positivo com $mdc(a, m) = 1$, então*

$$\{ar_1 + b, ar_2 + b, \ldots, ar_m + b\}$$

é um sistema completo de resíduos módulo m.

Prova: Inicialmente, mostraremos que não existem inteiros

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

que sejam congruentes módulo m. Para isto, observe que se

$$ar_j + b \equiv ar_k + b(mod\ m),$$

então pelo item (ii) do Teorema 1.29, temos

$$ar_j \equiv ar_k(mod\ m).$$

Desde que $mdc(a, m) = 1$, o Corolário 1.34 garante

$$r_j \equiv r_k(mod\ m).$$

Com, por definição, $r_j \not\equiv r_k(mod\ m)$ se $j \neq k$, concluímos que $j = k$.
Desde que o conjunto dos inteiros em questão consiste de m inteiros não congruentes entre si módulo m, estes inteiros devem formar um sistema completo de resíduos módulo m, completando a demonstração. □

Teorema 1.39. *Se a, b, n e m são inteiros tais que $n > 0, m > 0$ e $a \equiv b(mod\ m)$ então $a^n \equiv b^n(mod\ m)$.*

Prova: Vamos fazer a demonstração por indução sobre $n \in \mathbb{N}$. Se $n = 1$, o resultado é imediato.
Suponhamos, então que o resultado seja verdadeiro para $n \in \mathbb{N}$ e mostremos que o resultado é válido também para $n + 1 \in \mathbb{N}$. De fato, pela hipótese de indução, $a^n \equiv b^n(mod\ m)$. Como $a \equiv b(mod\ m)$ segue do Teorema 1.36 que $a^n a \equiv b^n b(mod\ m)$. Logo, $a^{n+1} \equiv b^{n+1}(mod\ m)$, o que demonstra nosso resultado.□

Exemplo 1.40. Temos que $7 \equiv 2(mod\ 5)$. Então o Teorema 1.39 nos diz que

$$7^3 \equiv 2^3(mod\ 5) \textbf{ ou } 343 \equiv 8(mod\ 5).$$

Definição 1.41. *Dizemos que um número natural m é o **mínimo múltiplo comum (mmc)** dos números inteiros $m_1, m_2, \ldots, m_k$, não nulos simultaneamente, se*

i) m é um múltiplo comum de $m_1, m_2, \ldots, m_k$, e

ii) se c é um múltiplo comum de $m_1, m_2, \ldots, m_k$, então $m|c$.

Indicaremos o mínimo múltiplo comum dos números $m_1, m_2, \ldots, m_k$ por

$$mmc(m_1, m_2, \ldots, m_k).$$

Teorema 1.42. *Se $m_1, m_2, \ldots, m_k$ são números naturais primos entre si, então*

$$mmc(m_1, m_2, \ldots, m_k) = m_1 \times m_e \times \cdots \times m_k.$$

A demonstração deste Teorema é uma consequência imediata da proposição 5.3.1, pagina 63 de [3].

Teorema 1.43. *Se $a \equiv b(mod\, m_1), a \equiv b(mod\, m_2), \ldots, a \equiv b(mod\, m_k)$ com $a, b, m_1, m_2, \ldots m_k$ inteiros e $m_1, m_2, \ldots, m_k$ positivos, então*

$$a \equiv b(mod\ mmc(m_1, m_2, \ldots, m_k)).$$

Prova: Desde que $a \equiv b(mod\ m_1), a \equiv b(mod\ m_2), \ldots, a \equiv b(mod\ m_k)$, nós temos que $m_1 \mid (a-b), m_2 \mid (a-b), \ldots, m_k \mid (a-b)$. Assim

$$mmc(m_1, m_2, \ldots, m_k) \mid (a-b)$$

e consequentemente

$$a \equiv b(mod\ mmc(m_1, m_2, \ldots, m_k))$$

, completando a demonstração. □

Corolário 1.44. *Se $a \equiv b(mod\ m_1), a \equiv b(mod\ m_2), \ldots, a \equiv b(mod\ m_k)$ onde a e b são inteiros e $m_1, m_2, \ldots m_k$ inteiros positivos e primos entre si, então*

$$a \equiv b(mod\ m_1 \times m_2 \times \cdots \times m_k),$$

completando a demonstração.

Prova: Desde que $m_1, m_2, \ldots, m_k$ são primos entre si, temos, pelo Teorema 1.42, que

$$mmc(m_1, m_2, \ldots, m_k) = m_1 \times m_2 \times \cdots \times m_k$$

Assim, do Teorema (1.43), segue que

$$a \equiv b(mod\ m_1 \times m_2 \times \cdots \times m_k),$$

completando a demonstração. □

1.4 Congruências Lineares

Nesta seção, estudaremos congruências lineares. O conhecimento deste tópico pode vir a facilitar a resolução de questões de Teoria dos Números.

Definição 1.45. *Uma congruência da forma*

$$ax \equiv b(mod\ m),$$

onde $x \in \mathbb{Z}$ é um número inteiro desconhecido, é chamada uma ***congruência linear em uma variável.***

Observe que se $x = x_0$ é uma solução da congruência $ax \equiv b(mod\ m)$, e se $x_1 \equiv x_0(mod\ m)$, então $ax_1 \equiv ax_0 \equiv b(mod\ m)$, o que implica que x_1 também é solução. Assim, se um membro da classe de congruência módulo m é solução de uma congruência linear, então todos os elementos desta classe também são soluções.

Teorema 1.46. *Sejam $a, b, m \in \mathbb{Z}$ inteiros com $m > 0$ e $mdc(a, m) = d$. Se $d \nmid b$, então $ax \equiv b(mod\ m)$ não tem soluções. Se $d|b$, então $ax \equiv b(mod\ m)$ tem exatamente d soluções módulo m não congruentes entre si.*

Prova: A congruência linear $ax \equiv b(mod\ m)$ é equivalente a uma equação em duas variáveis na forma $ax - my = b$. O inteiro x é uma solução de $ax \equiv b(mod\ m)$ se, e somente se, existe $y \in \mathbb{Z}$ com $ax - my = b$. Sabemos da proposição 6.6.1, página 66 de [3] que se $d \nmid |b$, não existem soluções para a equação $ax \equiv b(mod\ m)$, enquanto que se $d|b$, a equação $ax - my = b$ tem infinitas soluções dadas por

$$x = x_0 + (m/d)t, \quad y = y_0 + (a/d)t,$$

onde $x = x_0$ e $y = y_0$ são soluções particulares da equação. Os valores de x,

$$x = x_0 + (m/d)t,$$

são soluções da congruência linear. Para determinar quantas soluções não congruentes entre si existem, vejamos as condições que descrevem quando duas das soluções $x_1 = x_0 + (md)t_1$ e $x_2 = x_0 + (m/d)t_2$ são congruentes módulo m. Se estas duas soluções são congruentes então

$$x_0 + (m/d)t_1 \equiv x_0 + (m/d)t_2(mod\ m).$$

Subtraindo x_0 de ambos os lados desta congruência, encontramos que

$$(m/d)t_1 \equiv (m/d)t_2(mod\ m).$$

Como $m/d|m$ temos $mdc(m, m/d) = m/d$ e, portanto, pelo Teorema 1.32 vemos que

$$t_1 \equiv t_2 (mod\ d).$$

Isto mostra que um conjunto completo de soluções não congruentes entre si é obtido tomando-se $x = x_0 + (m/d)t$, onde t varia através de um sistema completo de resíduos módulo d. Esse conjunto é dado por $x = x_0 + (m/d)t$ onde $t \in \{0, 1, 2, \ldots, d-1\}$, completando a demonstração. □

Exemplo 1.47. Vamos encontrar todas as soluções não congruentes entre si de $9x \equiv 12(mod\ 15)$,
Solução: Como $mdc(9, 15) = 3$ e $3 \mid 12$, existem exatamente três soluções não congruentes entre si. Podemos encontrar essas soluções primeiro encontrando uma solução particular e, então, somando os múltiplos corretos de $15/3 = 5$.
Para encontrar uma solução particular, observe que resolver a congruência linear $9x \equiv 12(mod\ 15)$ é mesmo que resolver a equação

$$9x - 15y = 12.$$

Pelo algoritmo de Euclides, temos

$$\begin{aligned} 15 &= 9.1 + 6, \\ 9 &= 6.1 + 3, \\ 6 &= 3.2. \end{aligned}$$

Assim,

$$3 = 9 - 6.1 = 9 - (15 - 9.1) = 9.2 - 15.$$

O que resulta

$$9.8 - 15.4 = 12,$$

e uma solução particular de $9x - 15y$ é dada por

$$x_0 = 8 \text{ e } y_0 = 4.$$

Do Teorema 1.46 vemos que um conjunto completo de 3 soluções não congruentes entre si é dado por

$$\begin{aligned} x &= 8 + 5 \times 0 \equiv 8(mod\ 15), \\ x &= 8 + 5 \times 1 \equiv 13(mod\ 15), \\ x &= 8 + 5 \times 2 \equiv 3(mod\ 15). \end{aligned}$$

Vamos considerar congruências lineares na forma

$$ax \equiv 1(mod\ m).$$

Sabemos do teorema 1.46 que existe uma solução para esta congruência se, e somente se, $mdc(a, m) = 1$ e que, neste caso, todas as soluções são congruentes módulo m.

Definição 1.48. *Dados inteiros a e m com $m > 0$ e $mdc(a, m) = 1$, uma solução de $ax \equiv 1(mod\ m)$ é chamado um* ***inverso de*** *a* ***módulo*** *m.*

Exemplo 1.49. Vamos encontrar todas as soluções de $7x \equiv 1(mod\ 31)$.
Temos

$$mdc(7, 31) = 1.$$

Logo, essa congruência linear possui solução. Para encontrar uma solução, consideramos a equação

$$7x - 31y = 1,$$

cuja solução particular é dada por $x = 9$. Assim, desde que as soluções de $7x \equiv 1(mod\ 31)$ satisfazem

$$x \equiv 9(mod\ 31),$$

temos que 9 e todos os inteiros congruentes a 9 módulo 31, são inversos de 7 módulo 31.

Quando conhecermos um inverso de a módulo m, podemos usá-lo para resolver qualquer congruência na forma

$$ax \equiv b(mod\ m).$$

Para isto, seja $\bar{a}$ o inverso de a módulo m, i.é, $a\bar{a} \equiv 1(mod\ m)$. Então, se

$$ax \equiv b(mod\ m),$$

multiplicando ambos os lados desta congruência por $\bar{a}$, temos

$$\bar{a}(ax) \equiv \bar{a}b(mod\ m),$$

e, desta forma,

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

Exemplo 1.50. Vamos resolver a congruência linear $7x \equiv 22(mod\ 31)$.
Solução: Como $mdc(7, 31) = 1$, a congruência

$$7x \equiv 22(mod\ 31),$$

tem uma única solução. Resolvendo a congruência, encontramos $\bar{7} = 9$ e assim, multiplicando ambos os lados da congruência por 9, obtemos

$$x \equiv 63x \equiv 9 \times 7x \equiv 9 \times 22 (mod\ 31),$$

u seja,

$$x \equiv 198 \equiv 12 (mod\ 31).$$

Logo, $7x \equiv 22 (mod\ 31)$ tem uma única solução, a saber, $x = 12$.

Proposição 1.51. *Seja p um primo. Um inteiro positivo a é seu próprio inverso módulo p se, e somente se, $a \equiv 1 (mod\ p)$ ou $a \equiv -1 (mod\ p)$.*

Prova: Se $a \equiv 1 (mod\ p)$ ou $a \equiv -1 (mod\ p)$, então $a^2 \equiv 1 (mod\ p)$ e a é seu próprio inverso módulo p. Por outro lado, se a é seu próprio inverso módulo p, segue que $a^2 = a.a \equiv 1 (mod\ p)$. Assim, $p|(a^2 - 1)$. Desde que $a^2 - 1 = (a-1)(a+1)$, ou $p|(a-1)$ ou $p|(a+1)$. Logo, $a \equiv 1 (mod\ p)$ ou $a \equiv -1 (mod\ p)$. □

1.5 Sistemas de Congruências Lineares 2×2

Consideraremos agora sistemas com duas congruências lineares e duas incógnitas, todas com o mesmo módulo. Nosso objetivo é estudar quando sistemas desta forma tem solução e determiná-las.

Teorema 1.52. *Sejam $a, b, c, d, e, f, m \in \mathbb{Z}$ tais que $m > 0$ e $mdc(\Delta, m) = 1$, onde $\Delta = ad - bc$. Então, o sistema de congruências*

$$\begin{cases} ax + by \equiv e (mod\ m) \\ cx + dy \equiv f (mod\ m) \end{cases}$$

tem soluções módulo m dadas por

$$\begin{cases} x \equiv \bar{\Delta}(de - bf) (mod\ m) \\ y \equiv \bar{\Delta}(af - ce) (mod\ m), \end{cases}$$

onde $\bar{\Delta}$ é o inverso de Δ módulo m.

Prova: Multiplicando a primeira congruência do sistema por d e a segunda por b obtemos

$$\begin{cases} adx + bdy \equiv de (mod\ m) \\ bcx + bdy \equiv bf (mod\ m), \end{cases}$$

Então, subtraímos a segunda congruência da primeira, para encontrar que

$$(ad - bc)x \equiv de - bf (mod\ m),$$

ou

$$\Delta x \equiv de - bf (mod\ m).$$

Agora, multiplicamos ambos os lados desta congruência por $\bar{\Delta}$, um inverso de Δ módulo m, para concluir que

$$x \equiv \bar{\Delta}(de - bf)(mod\ m).$$

De maneira similar, multiplicamos a primeira congruência por c e a segunda por a para obter

$$\begin{cases} acx + bcy \equiv ce (mod\ m) \\ acx + ady \equiv af (mod\ m). \end{cases}$$

Subtraindo a primeira congruência da segunda, encontramos

$$(ad - bc)y \equiv af - ce (mod\ m),$$

ou

$$\Delta y \equiv af - ce (mod\ m).$$

Finalmente, multiplicamos ambos os lados dessa congruência por $\bar{\Delta}$ para concluir que

$$y \equiv \bar{\Delta}(af - ce)(mod\ m).$$

Por outro lado, se tivermos um par (x, y) na forma

$$\begin{cases} x \equiv \bar{\Delta}(de - bf)(mod\ m) \\ y \equiv \bar{\Delta}(af - ce)(mod\ m), \end{cases}$$

então

$$\begin{aligned} ax + by &\equiv a\bar{\Delta}(de - bf) + b\bar{\Delta}(af - ce) \\ &\equiv \bar{\Delta}(ade - abf - abf - bce) \\ &\equiv \bar{\Delta}(ad - bc)e \\ &\equiv e (mod\ m) \end{aligned}$$

e

$$\begin{aligned} cx + dy &\equiv c\bar{\Delta}(de - bf) + d\bar{\Delta}(af - ce) \\ &\equiv \bar{\Delta}(cde - bcf - adf - cde) \\ &\equiv \bar{\Delta}(ad - bc)f \\ &\equiv f (mod\ m). \end{aligned}$$

□

Exemplo 1.53. Vamos resolver o sistema de congruências lineares

$$\begin{cases} 3x + 4y \equiv 5 (mod\ 13) \\ 2x + 5y \equiv 7 (mod\ 13) \end{cases}.$$

Temos $\Delta = ad - bc = 3 \times 5 - 4 \times 2 = 7$ e $mdc(\Delta, m) = mdc(7, 13) = 1$. Um inverso de 7 módulo 13 é 2 e, então

$$x \equiv \bar{\Delta} \times (de - bf) = 2 \times (5.5 - 4.7) = -6 \equiv 7 (mod\ 13)$$

e

$$y \equiv \bar{\Delta} \times (af - ce) = 2 \times (3.7 - 2.5) = 22 \equiv 9 (mod\ 13).$$

2 Introdução à Criptografia Clássica

Cifras são formas de transformar uma mensagem de *texto plano* em uma mensagem de texto alterada chamada de *texto cifrado* de forma que esta seja indecifrável para qualquer um que não conheça a regra de transformação - *chave* [1]. O processo de converter um texto plano para um texto cifrado é chamado *criptografar*, e o processo contrário é chamado *descriptografar*. Neste capítulo faremos uma breve introdução aos métodos clássicos (pré-1970).

2.1 Visão Geral

Em um cenário simples de troca de informações como o mostrado na figura 2.1 , existem dois lados, que nós chamaremos de Alice e Bob [2], que desejam comunicar-se de maneira segura. E, entre eles, está Eva, que deseja interceptar essa comunicação.

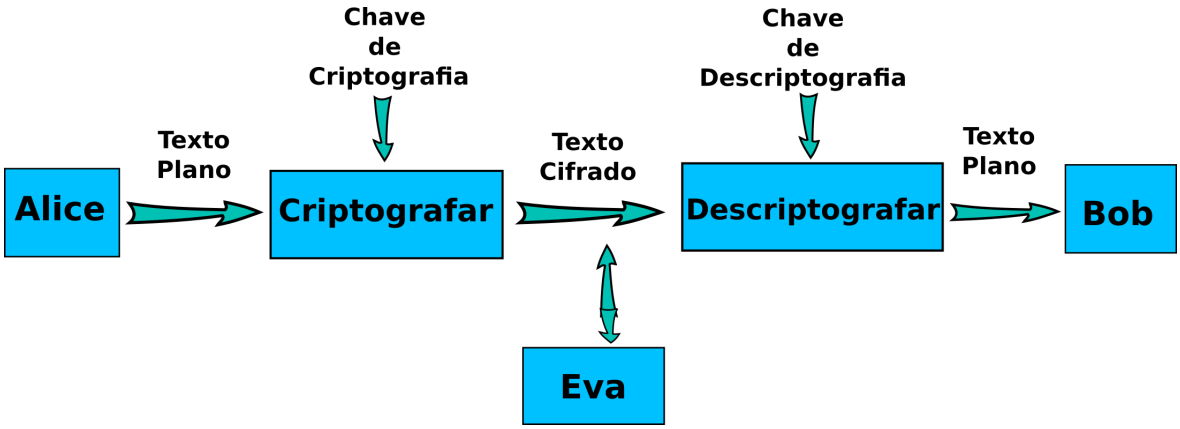

Figura 2.1: Cenário básico de comunicação.

Quando Alice deseja enviar uma mensagem secreta para Bob, ela encripta o texto

[1] Em sistemas modernos de criptografia, a chave não precisa ser secreta. Em um sistema como o RSA, por exemplo, a chave pode ser conhecida publicamente desde que a obtenção da chave inversa através dessa seja extremamente difícil.

[2] Vamos manter os personagens usados na referência [8], visto que é usual nos mais diversos textos sobre o assunto.

usando um método combinado anteriormente com Bob. Normalmente, o método de criptografar a mensagem é conhecido por Eva. O que ela não conhece é a chave de descriptografar e, é isso, que mantém a mensagem em segredo. Quando Bob recebe a mensagem com o texto cifrado, ele recupera o texto plano usando a chave de descriptografar.
Eva pode ter qualquer um dos objetivos a seguir:

- Ler uma mensagem.
- Encontrar a chave e ler todas as mensagens criptografadas com aquela chave.
- Adulterar mensagens de Alice de forma que Bob receba uma mensagem falsa.
- Passar por Alice, de tal forma que Bob acredite que esteja se comunicando com Alice.

Eva pode agir de várias maneiras para tentar atingir seus objetivos. A diferença entre elas depende da quantidade de informação que ela possui quando estiver tentando determinar a chave. Por exemplo:

- Eva pode ter acesso somente ao texto criptografado.
- Eva tem cópia de um texto criptografado e o texto plano correspondente.

Exemplo 2.1. Durante a segunda guerra mundial, no deserto do Saara, um posto Alemão enviava todos os dias a mesma mensagem criptografada dizendo que não havia nada de novo para informar. Então, a cada dia, os aliados tinham acesso a uma cópia de texto criptografado e o texto plano correspondente.

De qualquer maneira, o principal objetivo de Eva é descobrir a chave para criptografar e descriptografar mensagens visto que um dos mais importantes princípios de segurança usados na criptografia é o **princípio de Kerckhoffs** [3]: devemos sempre assumir que o inimigo conhece o método sendo usado.

2.1.1 Métodos de Chave Simétrica e de Chave Pública

Os métodos para criptografar e descriptografar mensagens podem ser classificados em métodos de **chave simétrica** e métodos de **chave pública**.

Chaves Simétricas: As chaves para criptografar e descriptografar mensagens são conhecidas pelo emissário e receptor. Em muitos casos, sendo a mesma.

[3] Esse princípio foi enunciado por Auguste Kerckhoffs em 1883 no tratado *La Cryptographie Militaire*

Chaves Públicas: A chave de encriptação é pública, mas é computacionalmente impossível encontrar a chave de desencriptação sem informações conhecidas apenas pelo receptor.

Enquanto todos os métodos clássicos de criptografia e alguns métodos modernos são simétricos, métodos de chave pública introduzidos após 1970 revolucionaram a criptografia e representam o passo final em uma sequência histórica interessante. Nos métodos mais antigos de criptografia, a segurança dependia de manter em segredo o método de criptografar mensagens. Posteriormente, assumiu-se conhecido esse método e a segurança passou a depender da manutenção da chave (simétrica) em segredo. Finalmente, com os algoritmos de chave pública, o método e a chave de criptografar mensagens são públicas e qualquer um sabe o que deve ser feito para obter a chave de descriptografar mensagens. A segurança depende do fato de que obter a mesma é computacionalmente impossível com os computadores atuais.
Em uma cifra simétrica, o emissor e o receptor deverão compartilhar entre si uma chave. Eles obviamente não podem enviar essa chave via texto pois um intermediário pode facilmente interceptar a mensagem e então descobrir a chave. Isso significa que o emissor e o receptor devem se encontrar pessoalmente e de uma forma segura para poder trocar a chave.
A afirmação acima pode sugerir que os algoritmos de chave pública fizeram os métodos simétricos obsoletos. Entretanto, essa flexibilidade não é de graça e tem um custo computacional muito grande. Devido a esse fato, métodos de chave pública não são interessantes quando se deseja criptografar grandes quantidades de informações. Por esta razão, métodos de chave pública são utilizados somente em aplicações onde apenas pequenas quantidades de informações são processadas

2.1.2 Cifras

As mensagens criptografadas usando métodos de chave simétrica podem ser enviadas de forma contínua ou em blocos.

Cifras Contínuas: As informações são enviadas para o processo de criptografia em pequenas partes, normalmente bits ou caracteres, e a saída também é produzida em pequenas partes.

Cifras em Bloco: As informações são agrupadas para serem enviadas para o processo de encriptação e, da mesma forma, a saída também é produzida em blocos.

2.1.3 Comprimento da chave

É difícil mensurar a segurança dos métodos criptográficos. A segurança do método, obviamente, está relacionada com a dificuldade em se determinar a chave. O método mais simples de ataque é tentar toda e qualquer combinação de chave possível. Tal método é conhecido como **ataque de força bruta**. Em um ataque de força bruta o tempo necessário para descobrir a chave é diretamente proporcional ao seu comprimento. Por exemplo, se a chave tem um comprimento de 16 bits, então existem $2^{16} = 65536$ chaves possíveis. Chaves longas são vantajosas, mas não garantem a segurança. O método também tem um papel bastante importante na segurança.

2.2 Alguns Sistemas Criptográficos Clássicos

O texto plano e o texto cifrado são, usualmente, escritos em um mesmo *alfabeto* consistindo de um certo número m de *letras*. O termo "letra" não necessariamente se refere aos caracteres alfabéticos A-Z, mas também números, espaços em branco, marcas de pontuação e outros símbolos.

O texto plano e o texto cifrado são quebrados em **unidades de mensagem**. Uma unidade de mensagem pode ser uma letra simples, um par de letras (**dígrafo**), ou um bloco de 30 letras. Uma **Transformação de Criptografia** é uma função que leva cada unidade de mensagem de um texto plano em uma unidade de mensagem de texto criptografado. Isto é, uma transformação de encriptação é uma função f do conjunto P de todas as mensagens planas no conjunto C de todas as mensagens criptografadas. Sempre consideraremos que f é uma função bijetora. A **Transformação de Descriptografia** é a função inversa f^{-1} de f.

$$P \xrightarrow{f} C \xrightarrow{f^{-1}} P$$

O primeiro passo ao criar um método de criptografia é converter todas as unidades de mensagem de texto plano e todas as mensagens de texto cifrado usando números naturais em algum intervalo [4].

Exemplo 2.2. Se nossas unidades de mensagens de texto plano e texto cifrado são simplesmente as 26 letras do alfabeto A-Z, então nós podemos rotular as letras usando os números $0, 1, \ldots, 25$, chamados de *equivalentes numéricos*. Então, no lugar do A escrevemos 0, no lugar do B escrevemos 1, e assim, sucessivamente.

Exemplo 2.3. Se nossas unidades de mensagens forem pares de letras, que chamaremos de *dígrafos*, em um alfabeto de 27 letras consistindo das letras A-Z e do espaço

[4] Pode-se converter unidades de mensagem para outros objetos matemáticos como pontos ou vetores, porém, neste texto, nos restringiremos a usar números naturais.

em branco, nós podemos primeiro associar o equivalente numérico 26 para o espaço em branco e então converter cada dígrafo, cujas letras x e y pertencem ao conjunto $\{0, 1, 2, \ldots, 26\}$ no número

$$27x + y \in \{0, 1, 2, \ldots, 728\}\,.$$

Assim, por exemplo, o dígrafo EU corresponde a

$$27 \times 4 + 20 = 128.$$

Analogamente, se usarmos sequências três letras, que chamaremos *trígrafos*, como unidade de mensagem, podemos rotulá-las por naturais da formas $729x + 27y + z \in \{0, 1, 2, \ldots, 19682\}$. E, ainda, mais geralmente podemos rotular blocos de k letras em um alfabeto de m letras por naturais de 0 a $m^k - 1$.
Começaremos exemplificando o caso em que uma unidade de mensagem é uma letra de um alfabeto de m letras rotuladas pelos naturais $0, 1, 2, \ldots, m-1$. Então, por definição, uma transformação de criptografia, neste caso, é uma permutação destes m inteiros.
Para facilitar o processo de criptografar e descriptografar de maneira rápida é conveniente ter um método relativamente simples para realizar tal permutação. Um caminho para isso, é pensar o conjunto $\{0, 1, 2, \ldots m-1\}$ como o conjunto da classes de congruência módulo m, e fazer uso das propriedades de adição e multiplicação da congruência módulo m .

Exemplo 2.4. Tomemos um alfabeto de 26 letras $A, B, \ldots Z$ com rótulos $0, 1, \ldots 25$ respectivamente. Seja $x \in \{0, 1, 2, \ldots 25\}$ um rótulo numérico para uma unidade de mensagem em texto plano e a função f do conjunto $\{0, 1, 2, \ldots 25\}$ nele mesmo dada por

$$f(x) = \left\{ \begin{array}{ll} x + 3, & \text{se } x < 23, \\ x - 23, & \text{se } x \geq 23 \end{array} \right\}$$

Em outras palavras, f simplesmente adiciona 3 módulo 26. Deste modo,

$$f(P) \equiv P + 3 (mod\ 26).$$

Então, com esse sistema, para encriptar a palavra

PITAGORAS

primeiro convertemos a palavra para os números:

15 8 19 0 6 14 17 0 18,

então adicionamos 3 módulo 26, obtendo

$$18\ 11\ 22\ 3\ 19\ 17\ 20\ 3\ 21,$$

e então convertemos de volta para letras

SLWDJRUDV.

Para decifrar a mensagem, basta subtrairmos 3 módulo 26.
Para este exemplo, o texto cifrado

WDOHV

equivale ao texto plano

TALES.[5]

Suponhamos que estamos usando um alfabeto de m letras com os equivalentes numéricos $0, 1, \ldots, m-1$. Seja $b \in \mathbb{N}$ fixo. O Exemplo 2.4 pode ser generalizado usando uma transformação de deslocamento.

Definição 2.5. *Dados $b, m \in \mathbb{Z}, m > 0$, uma* ***transformação de deslocamento*** *é uma função f de criptografia definida por*

$$y = f(x) \equiv y + b(mod\ m).$$

onde x e y variam no conjunto dos rótulos numéricos equivalentes as unidades de mensagem plana ou criptografada.

No caso do exemplo 2.4 temos uma transformação de deslocamento com $m = 26$ e $b = 3$. Para decifrar uma unidade de mensagem cifrada $y \in \{0, 1, \ldots, m-1\}$, simplesmente calculamos

$$x = f^{-1}(y) \equiv y - b(mod\ m).$$

Suponhamos que temos acesso a algumas mensagens em texto plano e suas equivalentes em texto cifrado e gostaríamos de ler outras mensagens cifradas. O processo de descobrir os parâmetros usados em certo método criptográfico é conhecido como **quebra** do código, e a ciência de quebrar códigos é conhecida com **criptoanálise**.
Para quebrar um sistema criptográfico, necessitamos de dois tipos de informações. A estrutura do sistema e o conhecimento de certos parâmetros usados pelo sistema. Em nosso Exemplo 2.4 a estrutura do sistema era dada por um alfabeto de 26 letras

[5]Esse método de encriptação foi aparentemente usado em Roma por Júlio César, que, supostamente foi o próprio inventor do método segundo [6] .

$A - Z$ com equivalentes numéricos $0 - 25$ respectivamente e o único parâmetro foi a constante de deslocamento b. Uma vez obtida essa informação podemos criptografar e descriptografar mensagens usando as fórmulas $y \equiv x + b(mod\ m)$ e $x \equiv y - b(mod\ m)$. Como vimos na Seção 2.1, devemos sempre assumir que a estrutura geral do sistema de criptografia e descriptografia é conhecida. Então, para aumentar a segurança do sistema, frequentemente altera-se os valores dos parâmetros utilizados pelo sistema. O parâmetro b (sistemas de criptografia mais complexos têm vários parâmetros) é uma **chave** ou, mais precisamente, uma **chave de criptografia**.

Exemplo 2.6. Suponhamos que interceptamos a mensagem

QHGKYCUTUI.

Sabendo que a mesma foi criptografada usando uma transformação de deslocamento sobre letras simples de uma alfabeto de 26 letras como visto anteriormente, resta-nos descobrir o valor do parâmetro b. Um caminho para isto é a análise de frequência. Sabemos que a letra "E" é uma das que tem maior frequência na língua portuguesa. Como a letra "U" é a letra com maior frequência no texto cifrado, é razoável supor que a letra "U" no texto cifrado corresponde ao "E" no texto plano. Isso significa que o deslocamento leva "E" = 4 em "U" = 20. Isto é,

$$20 \equiv 4 + b(mod\ 26),$$

e logo $b = 16$.
Para decifrar a mensagem basta subtrair 16 (módulo 26) dos equivalentes numéricos de

QHGKYCUTUI.

$$QHGKYCUTUI \mapsto 17\ 08\ 07\ 11\ 25\ 03\ 21\ 20\ 21\ 09$$

$$\mapsto 01\ 18\ 17\ 21\ 09\ 13\ 05\ 04\ 05\ 19 \mapsto ARQUIMEDES$$

A tabela a seguir mostra a frequência de letras na língua portuguesa segundo o site cryptogram.org [6]

[6] visitado em 01/11/2015

letra	%	letra	%	letra	%	letra	%	letra	%
e	14,8438	t	5.00919	b	0.919118	á	0.298713	õ	0.0229779
a	12.1094	n	4.71048	ã	0.873162	nh	0.252757		
o	10.2711	u	3.81434	q	0.827206	é	0.229779		
i	7.14614	c	3.58456	h	0.804228	j	0.183824		
r	5.97426	l	3.10202	f	0.804228	ó	0.160846		
s	5.74449	v	1.86121	ç	0.551471	x	0.137868		
d	5.3079	p	1.83824	z	0.32169	lh	0.0919118		
m	5.00919	g	1.26379	ê	0.298713	â	0.0459559		

No caso da criptografia por deslocamento sobre letras simples de um alfabeto de 26 letras, não é nem mesmo necessário ter um longo texto criptografado para encontrar a letra que ocorre com mais frequência. Existem somente 26 possibilidades para o valor de b, que podem ser testadas uma a uma, sendo que apenas uma delas fará com o texto plano tenha sentido.
Assim, este tipo de sistema, apesar de ser bem simples, é também muito fácil de ser quebrado. Uma melhora pode ser feita usando um tipo mais geral de transformação.

Definição 2.7. *Uma* ***transformação afim*** *é uma função f do conjuntos dos rótulos de unidades de mensagem nele mesmo dada por*

$$y = f(x) \equiv ax + b(mod\ m), \tag{2.1}$$

onde a e b são constantes naturais e m é o comprimento do alfabeto.

Observe que para que uma transformação afim esteja bem definida é necessário que $mdc(a, m) = 1$, pois se $mdc(a, m) > 1$ existiria mais do que um rótulo representando um unidade de texto plano levada no mesmo rótulo no conjunto dos rótulos representando uma unidade de texto cifrado. E, portanto, essa função não seria injetora.

Exemplo 2.8. Usando o alfabeto de 26 letras, vamos criptografar nossa mensagem

ARQUIMEDES

usando a transformação afim com $a = 7$ e $b = 12$.Assim

$$y \equiv 7x + 12(mod\ 26),$$

e temos

$$ARQUIMEDES \mapsto 00\ 17\ 16\ 20\ 08\ 12\ 04\ 03\ 04\ 18$$

$$\mapsto 12\ 01\ 20\ 22\ 16\ 18\ 14\ 07\ 18\ 08 \mapsto MBUWQSOHOI$$

Para decifrar uma mensagem que foi criptografada usando uma transformação afim $y \equiv ax + b(mod\ m)$, devemos escrever x em função de y, obtendo

$$y \equiv \bar{a} - \bar{a}b(mod\ m), \tag{2.2}$$

onde $\bar{a}$ é inverso de a módulo m e b' é igual a $a^{-1}b$. Isto é possível somente se e, por definição, esta não é uma função de criptografia.
Um caso especial da transformação afim é aquele em que $a = 1$, obtendo uma transformação de deslocamento. Outro caso especial se dá quando $b = 0$. Tal função é chamada de **tranformação linear**.
Suponhamos, agora, que interceptamos uma mensagem que foi criptografada usando uma transformação afim em um alfabeto de m letras. Como determinar os parâmetros a e b de tal forma que a mensagem possa ser lida? Necessitamos de duas informações para resolver isto.

Exemplo 2.9. Vamos neste exemplo trabalhar com um alfabeto de 27 ($m = 27$) letras consistindo nas letras A-Z rotulados de 0 a 25 e o espaço em branco rotulado como 26. Suponhamos que a letra com maior ocorrência no texto cifrado seja "M ", e que a segunda letra que ocorre com maior frequência seja "I ". É razoável supor que estas são as letras cifradas correspondentes ao "E "e ao "A "respectivamente, que são as duas letras mais frequentes na língua portuguesa. Então, trocando as letras pelos seus rótulos numéricos e substituindo em P e C na fórmula da transformação afim, obtemos:

$$\begin{cases} 4a + b & \equiv 12(mod\ 27) \\ 0a + b & \equiv 8(mod\ 27) \end{cases}$$

Temos um sistema de duas congruências com duas incógnitas, a e b. Como $\Delta = 4 \times 1 - 1 \times 0 = 4$ tem inverso $\bar{\Delta} = 7$ e $mdc(\Delta, m) = mdc(4, 27) = 1$ a Seção 1.5 mostra que a solução única do sistema anterior é dada por:

$$\begin{cases} a \equiv 7(1 \times 3 - 1 \times 0)(mod\ 27) \\ b \equiv 7(12 \times 0 - 8 \times 3)(mod\ 27) \end{cases} \Longrightarrow \begin{cases} a \equiv 1(mod\ 27) \\ b \equiv 8(mod\ 27) \end{cases}$$

Assim, nossa transformação afim de criptografia é dada por

$$y \equiv x + 8(mod\ 27).$$

Como $mdc(a, m) = mdc(1, 27) = 1$, a transformação acima é invertível e, substituindo

na equação 2.2 nossa transformação afim de descriptografia resulta em

$$x \equiv y - 8(mod\ 27).$$

Exemplo 2.10. Suponhamos que temos uma parte de um texto cifrado que foi criptografado usando uma transformação afim em um alfabeto de 28 letras ($m = 28$) consistindo de A-Z, um branco que será representado aqui por "␣", e o sinal ?, onde A-Z tem equivalentes numéricos 0-25, "␣" tem equivalente numérico = 26 e ? tem equivalente numérico 27. Uma análise de frequência mostra que as letras mais comuns no texto cifrado são "B" e "?", nesta ordem. Desde que, neste caso, saibamos que os símbolos que mais aparecem em língua portuguesa são "␣" e "E", nesta ordem, supomos que "B" é o equivalente cifrado de "␣" e "?" é o equivalente cifrado de "E". Desta forma, temos

$$\begin{cases} 26a + b & \equiv 01(mod\ 28) \\ 4a + b & \equiv 27(mod\ 28) \end{cases}$$

Como $\Delta = 26 \times 1 - 1 \times 4 = 22$ e $mdc(\Delta, m) = mdc(22, 28) \neq 1$ o sistema de congruência módulo 28 não possui solução única. Subtraindo as duas congruências, obtemos

$$22a \equiv 26(mod\ 28),$$

que fornece $a = 5$ e $b = 9$ ou $a = 19$ e $b = 9$. Assim, podemos ter duas transformações afins de criptografia,

$$y \equiv 5x + 9(mod\ 28)\ \textbf{e}\ y \equiv 19x + 9(mod\ 28),$$

e, portanto, duas transformações afins de descriptografia

$$x \equiv 11y + 13(mod\ 28)\ \textbf{e}\ x \equiv 3y + 1(mod\ 28).$$

Neste caso, devemos testar as duas possibilidades e usar aquela em que o texto plano faça sentido, ou continuar nossa análise de frequência como o terceiro caractere com maior frequência na língua portuguesa obtendo uma terceira congruência linear. Essa informação extra pode nos ajudar a determinar quais das transformações afim está correta.

3 Criptografia, Matrizes e Tecnologia

3.1 Introdução

Neste capítulo vamos expandir o conceito de congruências para matrizes, explicar o que são as cifras de Hill, como criptografar e descriptografar mensagens usando essas cifras, como quebrar as mesmas e mostrar alguns exemplos de utilização. Veremos também como uma ferramenta tecnológica pode nos auxiliar nos cálculos.

3.2 Congruências e Matrizes

Para estudarmos sistemas de n congruências lineares envolvendo n incógnitas é bastante útil usar a linguagem de matrizes. Usaremos alguns conceitos básicos de matrizes que são discutidos em muitos textos de Álgebra Linear, tal como [2].

Definição 3.1. *Sejam A e B matrizes $n \times k$ com entradas em $\mathbb{Z}$.Fixado um inteiro positivo m, dizemos que A **é congruente a** B **módulo** m se $a_{ij} \equiv b_{ij}(mod\ m)$ para quaisquer que sejam $1 \leq i \leq n$ e $1 \leq j \leq k$. Se A for congruente a B módulo m escrevemos*

$$A \equiv B(mod\ m),$$

caso contrário, escrevemos $A \not\equiv B(mod\ m)$.

Exemplo 3.2. Temos que

$$\begin{pmatrix} 16 & 3 \\ 8 & 13 \end{pmatrix} \equiv \begin{pmatrix} 5 & 3 \\ -3 & 2 \end{pmatrix} (mod\ 11),$$

pois as respectivas entradas são congruentes módulo 11.

Exemplo 3.3. Temos que

$$\begin{pmatrix} 1 & 4 & 2 \\ 2 & 0 & 3 \\ 3 & 1 & 4 \end{pmatrix} \equiv \begin{pmatrix} 1 & 4 & 7 \\ 2 & 5 & 8 \\ 3 & 6 & 9 \end{pmatrix} (mod\ 5),$$

pois as respectivas entradas são congruentes módulo 5.

Claramente a relação de congruência de matrizes é reflexiva, simétrica e transitiva. Quando A, B e C são matrizes com entradas inteiras tal que $A \equiv B(mod\ m)$ e $B \equiv C(mod\ m)$, escreveremos simplesmente $A \equiv B \equiv C(mod\ m)$.

Proposição 3.4. *Se A e B são matrizes $n \times k$ com $A \equiv B(mod\ m)$, C é uma matriz $k \times p$ e D é uma matriz $p \times n$, todas com entradas em $\mathbb{Z}$, então*

$$AC \equiv BC(mod\ m) \ \textbf{\textit{e}}\ DA \equiv DB(mod\ m).$$

Prova: Sejam a_{ij} e b_{ij} as entradas de A e B respectivamente, para $1 \leq i \leq n$ e $1 \leq j \leq k$, e c_{ij} as entradas de C para $1 \leq i \leq k$ e $1 \leq j \leq p$. Os elementos da linha i e coluna j das matrizes AC e BC são $\sum_{t=1}^{n}(a_{it}c_{tj})$ e $\sum_{t=1}^{n}(b_{it}c_{tj})$, respectivamente. Desde que $A \equiv B(mod\ m)$, temos que $a_{it} \equiv b_{it}(mod\ m)$ para todo i e todo k. Assim, o Teorema 1.36 garante que

$$\sum_{t=1}^{n}(a_{it}c_{tj}) \equiv \sum_{t=1}^{n}(b_{it}c_{tj})(mod\ m).$$

Consequentemente, $AC \equiv BC(mod\ m)$, o que completa a demonstração.
Analogamente $DA \equiv DB(mod\ m)$.□
Vamos considerar o sistema de congruências

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n \equiv b_1(mod\ m) \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n \equiv b_2(mod\ m) \\ \vdots \qquad\quad \vdots \qquad \ddots \qquad \vdots \qquad\quad \vdots \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n \equiv b_n(mod\ m) \end{cases}$$

Usando notação matricial, vemos que este sistema de n congruências é equivalente a congruência matricial

$$AX \equiv B(mod\ m),$$

onde

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}, X = \begin{pmatrix} x_1 \\ X_2 \\ \vdots \\ x_n \end{pmatrix} \text{ e } B = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}.$$

Exemplo 3.5. O sistema

$$\begin{cases} 6x + 8y \equiv 5 (mod\ 11) \\ 4x + 10y \equiv 7 (mod\ 11) \end{cases}$$

é equivalente a

$$\begin{pmatrix} 6 & 8 \\ 4 & 10 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \equiv \begin{pmatrix} 5 \\ 7 \end{pmatrix} (mod\ 11)$$

Definição 3.6. *Se A e $\bar{A}$ são matrizes $n \times n$ com entradas em $\mathbb{Z}$ e se*

$$A\bar{A} \equiv \bar{A}A \equiv I (mod\ m),$$

onde $I = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$ *é a matriz identidade de ordem n, então dizemos que $\bar{A}$ é uma matriz inversa de A módulo m.*

A Proposição 3.4 e a transitividade da congruência nos garante que se $\bar{A}$ é uma inversa de A módulo m e $B \equiv \bar{A} (mod\ m)$, então B também é uma inversa de A módulo m. Por outro lado, se B_1 e B_2 são inversas de A, então $B_1 \equiv B_2 (mod\ m)$. Para ver isto, usamos a Proposição 3.4 e as congruências $B_1A \equiv B_2A \equiv I (mod\ m)$. De fato, temos que $B_1AB_1 \equiv B_2AB_1 (mod\ m)$. Desde que $AB_1 \equiv I (mod\ m)$, concluímos que $B_1 \equiv B_2 (mod\ m)$.

Exemplo 3.7. Desde que

$$\begin{pmatrix} 1 & 3 \\ 2 & 4 \end{pmatrix} \begin{pmatrix} 3 & 4 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 6 & 10 \\ 10 & 16 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} (mod\ 5)$$

e

$$\begin{pmatrix} 3 & 4 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 3 \\ 2 & 4 \end{pmatrix} = \begin{pmatrix} 11 & 25 \\ 5 & 11 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} (mod\ 5)$$

vemos que a matriz $\begin{pmatrix} 3 & 4 \\ 1 & 2 \end{pmatrix}$ é uma inversa de $\begin{pmatrix} 1 & 3 \\ 2 & 4 \end{pmatrix}$ módulo 5.

A proposição a seguir mostra um método para encontrar inversas de matrizes 2×2 módulo m.

Proposição 3.8. *Sejam* $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *uma matriz de números inteiros e* $m > 0$, *tais que* $\Delta = detA = ad - bc$ *e* m *são primos entre si. Então, a matriz* $\bar{A} = \bar{\Delta} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ *é uma inversa de* A *módulo* m, *onde* $\bar{\Delta}$ *é um inverso de* Δ *módulo* m.

Prova: Para verificar que a matriz $\bar{A}$ é a inversa de A módulo m, devemos verificar que $A\bar{A} \equiv \bar{A}A \equiv I(mod\ m)$.
Para ver isto, observe que

$$A\bar{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \bar{\Delta} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \bar{\Delta} \begin{pmatrix} ad - bc & 0 \\ 0 & -bc + ad \end{pmatrix}$$
$$= \bar{\Delta} \begin{pmatrix} \Delta & 0 \\ 0 & \Delta \end{pmatrix} = \begin{pmatrix} \bar{\Delta}\Delta & 0 \\ 0 & \Delta\bar{\Delta} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \equiv I(mod\ m)$$

e

$$\bar{A}A = \bar{\Delta} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \bar{\Delta} \begin{pmatrix} ad - bc & 0 \\ 0 & -bc + ad \end{pmatrix}$$
$$= \bar{\Delta} \begin{pmatrix} \Delta & 0 \\ 0 & \Delta \end{pmatrix} = \begin{pmatrix} \bar{\Delta}\Delta & 0 \\ 0 & \bar{\Delta}\Delta \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \equiv I(mod\ m).$$

□

Exemplo 3.9. Seja $\begin{pmatrix} 3 & 4 \\ 4 & 6 \end{pmatrix}$. Desde que 7 é um inverso de $detA = 2$ módulo 13, e como $mdc(7, 13) = 1$ temos que

$$\bar{A} = 7 \begin{pmatrix} 6 & -4 \\ -4 & 3 \end{pmatrix} = \begin{pmatrix} 42 & -28 \\ -28 & 21 \end{pmatrix} \equiv \begin{pmatrix} 3 & 11 \\ 11 & 8 \end{pmatrix} (mod\ 13).$$

Podemos checar que

$$\begin{pmatrix} 3 & 11 \\ 11 & 8 \end{pmatrix} \begin{pmatrix} 3 & 4 \\ 4 & 6 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} (mod\ 13).$$

Exemplo 3.10. Vamos encontrar a inversa de $\begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix}$ módulo 26.

Desde que 5 é um inverso de $detA = -5 \equiv 21(mod\ 26)$, e como $mdc(5, 16) = 1$ temos que

$$\bar{A} = 5 \begin{pmatrix} 8 & -3 \\ -7 & 2 \end{pmatrix} = \begin{pmatrix} 40 & -15 \\ -35 & 10 \end{pmatrix} \equiv \begin{pmatrix} 14 & 11 \\ 17 & 10 \end{pmatrix} (mod\ 26).$$

Definição 3.11. *A adjunta de uma matriz A de ordem $n \times n$ é uma matriz $n \times n$ com a entrada(i, j) dada por C_{ji}, onde C_{ij} é $(-1)^{i+j}$ vezes o determinante da matriz obtida eliminando-se a i-ésima linha e a j-ésima coluna da matriz A. A adjunta de A será indicada por $adj(A)$*

É claro que se A tem entradas em $\mathbb{Z}$, a adjunta de A também terá entradas em $\mathbb{Z}$.
Para obtermos uma fórmula para a inversa de uma matriz $n \times n$, precisamos do resultado a seguir, cuja demonstração pode ser encontrada em [2], página 73, Teorema 3.5.2.

Teorema 3.12. *Se A é uma matriz $n \times n$ com entradas reais e $det(A) \neq 0$, então* $A^{-1} = \dfrac{1}{det(A)} adj(A)$.

Usaremos esse Teorema para demonstrar a proposição a seguir.

Teorema 3.13. *Se A é uma matriz $n \times n$ com entradas em $\mathbb{Z}$ e $m \in \mathbb{Z}$ é um inteiro positivo tal que $mdc(\Delta, m) = 1$, onde Δ é o determinante de A, então a matriz*

$$\bar{A} = \bar{\Delta} Adj(A)$$

é uma inversa de A módulo m, onde $\bar{\Delta}$ é um inverso de Δ módulo m.

Prova: Se $mdc(\Delta, m) = 1$, então sabemos que $\Delta = det(A) \neq 0$. Assim, do Teorema 3.12, temos

$$\frac{1}{\Delta} adj(A) = A^{-1}.$$

Multiplicando ambos os lados da igualdade por A obtemos

$$\frac{1}{\Delta} A adj(A) = I.$$

De onde obtemos

$$A adj(A) = \Delta I.$$

Desde que $mdc(\Delta, m) = 1$, existe um inverso $\bar{\Delta}$ de Δ módulo m. Assim, para cada $\bar{\Delta}$,

$$A\bar{\Delta} Adj(A) \equiv A Adj(A)\bar{\Delta} \equiv \Delta\bar{\Delta} I \equiv I(mod\ m)$$

e

$$\bar{\Delta} A \equiv \bar{\Delta} Adj(A) A \equiv \bar{\Delta}\Delta I \equiv I(mod\ m).$$

Isto mostra que $\bar{A} = \bar{\Delta} Adj(A)$ é uma inversa de A módulo m, completando nossa demonstração. □

Exemplo 3.14. Seja $A = \begin{pmatrix} 2 & 5 & 6 \\ 2 & 0 & 2 \\ 1 & 2 & 3 \end{pmatrix}$. Vamos determinar uma inversa de A módulo 7.

Temos $\Delta = -5$. Desde que $mdc(\Delta, 7) = 1$, e um inverso de $\Delta = -5$ é $\bar{\Delta} = 4$, encontramos que

$$\bar{A} = 4(adj(A)) = 4 \begin{pmatrix} -2 & -3 & 5 \\ -5 & 0 & 10 \\ 4 & 1 & -10 \end{pmatrix} = \begin{pmatrix} -8 & -12 & 20 \\ -20 & 0 & 40 \\ 0 & 4 & -40 \end{pmatrix} \equiv \begin{pmatrix} 6 & 2 & 6 \\ 1 & 0 & 5 \\ 2 & 4 & 2 \end{pmatrix} (mod\, 7).$$

Podemos agora usar uma inversa de A módulo m para resolver um sistema

$$AX \equiv B(mod\ m), \tag{3.1}$$

sempre que $mdc(det(A), m) = 1$. Pela proposição 3.4, quando multiplicamos ambos os lados desta congruência pela inversa $\bar{A}$ de A, obtemos

$$\begin{aligned} \bar{A}(AX) &\equiv \bar{A}B(mod\ m) \\ (\bar{A}A)X &\equiv \bar{A}B(mod\ m) \\ X &\equiv \bar{A}B(mod\ m) \end{aligned}$$

Assim, encontramos a solução X calculando $\bar{A}B(mod\ m)$.

Exemplo 3.15. Resolver o sistema de congruências

$$\begin{cases} 2x + 3y \equiv 1(mod\ 26) \\ 7x + 8y \equiv 2(mod\ 26) \end{cases}$$

Como

$$A = \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix},$$

é a matriz do Exemplo 3.10, temos

$$\bar{A} = \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix},$$

e

$$X \equiv \bar{A}B = \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix} \begin{pmatrix} 1 \\ 2 \end{pmatrix} \equiv \begin{pmatrix} 10 \\ 11 \end{pmatrix} (mod\ 26).$$

3.3 Cifra de Hill de ordem n

Até aqui, nossas mensagens foram criptografadas caractere por caractere. Agora, vamos criptografar mensagens em que nossa unidade é formada por blocos de 2 ou mais caracteres. Isto significa que o texto plano é dividido em "segmentos" de 2 ou mais caracteres.

Definição 3.16. *Uma **cifra de Hill** é uma cifra em blocos de comprimento n cuja chave de encriptação é uma matriz quadrada E de ordem n e cujas entradas são os números naturais* $0, 1, 2, \ldots m-1$*, onde m representa o comprimento do alfabeto utilizado.*

Observe que, neste caso, para obter um número inteiro de blocos de comprimento n pode ser necessário acrescentar letras extras ao final da mensagem.

3.3.1 O processo de encriptação

A seguir descrevemos um possível processo a ser utilizado para encriptar uma mensagem usando o método de Hill para um bloco de comprimento n e um alfabeto de comprimento m.

1. Considere um matriz quadrada E de ordem n com entradas inteiras que seja invertível módulo m. Essa matriz E será a nossa chave de criptografia e $\bar{E}$ será nossa chave de descriptografia.

2. Remova, se necessário, todos os espaços em branco, símbolos de pontuação e acentos da mensagem de texto plano e converta todas as letras para maiúsculo.

3. Converta cada caractere da mensagem de texto plano para seu equivalente numérico entre 0 e $m-1$.

4. Divida essa sequência de números em t blocos de comprimento n completando, se necessário, o final da mensagem com números aleatórios para que tenhamos todos os blocos de comprimento n.

5. Escreva cada bloco como um vetor coluna p_i de ordem $n \times 1$. Nesta etapa, a mensagem é formada por uma sequência de vetores coluna $p_1, p_2, \ldots, p_t$ de ordem $n \times 1$.

6. Multiplique a matriz E de criptografia por cada um dos vetores $p_1, p_2, \ldots, p_t$ obtendo os vetores colunas $c_1, c_2, \ldots, c_t$ também de ordem $n \times 1$. Mais precisamente,

$$c_1 = Ep_1, \quad c_2 = Ep_2, \quad c_1 = Ep_3, \quad \ldots, \quad c_t = Ep_t.$$

7. Use os vetores $c_1, c_2, \ldots, c_t$ para escrever a mensagem criptografada, seguindo a ordem de entrada e convertendo de volta cada número, em seu caractere relacionado.

Observação 3.17. No passo (6) podemos usar uma única multiplicação matricial se produzirmos uma matriz $V_{n\times t}$ usando os vetores $p_1, p_2, \ldots, p_t$ como colunas, isto é:

$$P = [p_1, p_2, \ldots, p_t] \Rightarrow C = EP = [c_1, c_2, \ldots, c_t]$$

Exemplo 3.18. Vamos criptografar a mensagem "Pascal" em blocos de comprimento 2, usando um alfabeto de 26 letras e a chave de de criptografia

$$E = \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix}.$$

Temos:

1. A matriz é invertível módulo 26 pelo Exemplo 3.10.

2. Convertendo para maiúsculas.

$$PASCAL.$$

3. Convertendo cada caractere para seu equivalente numérico.

$$15\ 0\ 18\ 2\ 0\ 11.$$

4. Dividindo a sequência em blocos de comprimento 2.

$$15\ 0 \quad 18\ 2 \quad 0\ 11.$$

5. Produzir uma matriz $P_{2\times 3}$ usando os blocos como colunas.

$$P = \begin{pmatrix} 15 & 18 & 0 \\ 0 & 2 & 11 \end{pmatrix}.$$

6. Multiplicar a matriz E de criptografia por P.

$$C = EP \equiv \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix} . \begin{pmatrix} 15 & 18 & 0 \\ 0 & 2 & 11 \end{pmatrix} = \begin{pmatrix} 30 & 42 & 33 \\ 105 & 142 & 88 \end{pmatrix} = \begin{pmatrix} 4 & 16 & 7 \\ 1 & 12 & 10 \end{pmatrix} (mod\, 26).$$

7. Escrever a mensagem criptografada.

$$4\ 1\ 16\ 12\ 7\ 10 \longrightarrow EBQMHK.$$

Exemplo 3.19. Vamos criptografar a mensagem "Matemática legal!" usando blocos de comprimento $n = 3$, com nosso alfabeto de 26 letras e usando a chave de criptografia

$$E = \begin{pmatrix} 2 & 3 & 15 \\ 5 & 8 & 12 \\ 1 & 13 & 4 \end{pmatrix}.$$

1. Desde que $det(E)(mod\ 26) = 11$, e 11 é invertível módulo 26, a matriz E é também invertível módulo 26.

2. A mensagem que está sendo enviada é "Matemática legal!". Removendo espaços, acentos, símbolos de pontuação e convertendo a letra para maiúsculas.

$$MATEMATICALEGAL.$$

3. Convertendo cada letra para seu equivalente numérico.

$$12\ 0\ 19\ 4\ 12\ 0\ 19\ 8\ 2\ 0\ 11\ 4\ 6\ 0\ 11.$$

4. Dividindo o texto em blocos de três unidades.

$$12\ 0\ 19 \quad 4\ 12\ 0 \quad 19\ 8\ 2 \quad 0\ 11\ 4 \quad 6\ 0\ 11.$$

5. Convertendo esses blocos em uma matriz P.

$$P = \begin{pmatrix} 12 & 4 & 19 & 0 & 6 \\ 0 & 12 & 8 & 11 & 0 \\ 19 & 0 & 2 & 4 & 11 \end{pmatrix}.$$

6. Multiplicando pela matriz de encriptação E.

$$C = E.P = \begin{pmatrix} 2 & 3 & 15 \\ 5 & 8 & 12 \\ 1 & 13 & 4 \end{pmatrix} \begin{pmatrix} 12 & 4 & 19 & 0 & 6 \\ 0 & 12 & 8 & 11 & 0 \\ 19 & 0 & 2 & 4 & 11 \end{pmatrix} \equiv \begin{pmatrix} 23 & 18 & 14 & 15 & 21 \\ 2 & 12 & 1 & 6 & 6 \\ 10 & 4 & 1 & 3 & 24 \end{pmatrix}$$

7. Convertendo C em um texto cifrado

$$23\ 2\ 10\ 18\ 12\ 4\ 14\ 1\ 1\ 15\ 6\ 3\ 21\ 6\ 24 \longrightarrow XCKSMEOBBPGDVGY.$$

3.3.2 O processo de Descriptografia

Para a cifra de Hill, o processo de descriptografia do texto cifrado para o texto plano é o inverso da transformação original do texto plano em texto cifrado. Em outras palavras, se uma cifra de Hill tem uma matriz chave E, então a transformação inversa é a cifra de Hill cuja matriz chave é $\bar{E}$.
Se já conhecemos a matriz E, nós podemos usá-la para decifrar o texto.

O processo de desencriptação para m=26

1. Encontre uma matriz $D = \bar{E}(mod\ m)$. Essa é a chave de descriptografia.
2. Converta o texto cifrado em uma matriz C conforme feito na seção anterior.
3. Calcule $P = DC$.
4. Converta a matriz P na mensagem de texto plano. Será necessário inserir os espaços e pontuações se eles tiverem sido removidos.

Exemplo 3.20. Vamos descriptografar a mensagem

AJXGTRJXDGKKIXL,

sabendo que ela foi criptografada usando como chave a matriz

$$E = \begin{pmatrix} 2 & 3 & 15 \\ 5 & 8 & 12 \\ 1 & 13 & 4 \end{pmatrix},$$

em um alfabeto de 26 letras.

1. Calculamos
$$C = \bar{E} = \begin{pmatrix} 10 & 19 & 16 \\ 4 & 23 & 7 \\ 17 & 5 & 19 \end{pmatrix}$$

2. Convertemos o texto cifrado para uma matriz C.

$$AJXGTRJXDGKKIXL \mapsto 0\ 9\ 23\ 6\ 19\ 17\ 9\ 23\ 3\ 6\ 10\ 10\ 8\ 23\ 11$$

E assim,
$$C = \begin{pmatrix} 0 & 6 & 9 & 3 & 8 \\ 9 & 19 & 23 & 6 & 23 \\ 23 & 17 & 3 & 10 & 11 \end{pmatrix}$$

3. Finalmente, calculamos $P = DC$

$$P = DC = \begin{pmatrix} 10 & 19 & 16 \\ 4 & 23 & 7 \\ 17 & 5 & 19 \end{pmatrix} \begin{pmatrix} 0 & 6 & 9 & 3 & 8 \\ 9 & 19 & 23 & 6 & 23 \\ 23 & 17 & 3 & 10 & 11 \end{pmatrix} = \begin{pmatrix} 19 & 17 & 3 & 18 & 17 \\ 4 & 8 & 14 & 12 & 14 \\ 14 & 0 & 13 & 11 & 18 \end{pmatrix}$$

4. Convertendo a matriz P para a mensagem de texto plano.

$$19\ 4\ 14\ 17\ 8\ 0\ 3\ 14\ 13\ 18\ 12\ 11\ 17\ 14\ 18 \mapsto TEORIADOSNUMEROS.$$

Podemos adicionar os espaços e acentos para obter

TEORIA DOS NÚMEROS.

3.3.3 Quebrando a Cifra de Hill

É possível descobrir qual é a chave para a cifra de Hill? Observando o algoritmo de criptografia sabemos que $C = EP$. Se conhecermos um pequeno texto plano e seu correspondente texto cifrado então teremos conhecimento sobre uma pequena parte de P e de C. Se tivermos sorte, a porção de P que possuirmos formará uma matriz $n \times n$ invertível (módulo m). Então $C = EP$ pode ser reescrita como $E = C\bar{P}$, resultando em sua matriz de criptografia. A partir disso, pode-se simplesmente inverter E módulo m para obter D e então descriptografar a mensagem completa.
Na realidade, também é necessário saber o comprimento n do bloco utilizado para obtermos as dimensões da matrizes E, P e C. Isto é um problema. Mas existe um

caminho para testar os possíveis valores de n se o trecho conhecido for uma mensagem completa e não for muito longa, e desde que saibamos que o número de letras na mensagem é um múltiplo do comprimento do bloco.

Exemplo 3.21. Vamos supor que interceptamos a mensagem

TIVLFGLKTILFXAHVGY

e sabemos por algum meio que a mesma significa

CRIPTOGRAFIAELEGAL.

Vemos que a mensagem tem 18 caracteres. Então, o bloco poderá possivelmente ser 2, 3, 6, 9 ou 18. Desde que, queremos formar matrizes quadradas de ordem igual ao comprimento do bloco, se o tamanho do bloco for 6, 9 ou 18 não teremos caracteres suficientes para criar P e C e não será possível encontrar E e portanto D. Resta-nos trabalhar com as possibilidades em que o tamanho do bloco seja 2 ou 3. Se ambos falharem em produzir uma chave, então, não estaremos aptos a quebrar o código.

Vamos mostrar o processo a ser seguido para encontrar a matriz E.

Exemplo 3.22. Supondo novamente que interceptamos a mensagem

TIVLFGLKTILFXAHVGY

cujo significado é

CRIPTOGRAFIAELEGAL.

Como vimos, a mensagem tem 18 caracteres e, assim, o bloco poderá ter comprimento 2, 3, 6, 9 ou 18. Esperamos, entretanto, que $n = 2$ ou $n = 3$. Vamos começar com um bloco de comprimento 2. Temos que o texto plano

CRIPTOGRAFIAELEGAL

é rotulado como

2 17 8 15 19 14 6 17 0 5 8 0 4 11 4 6 0 11.

e encriptado como

TIVLFGLKTILFXAHVGY

que é rotulado

19 8 21 11 5 6 11 10 19 8 11 5 23 0 7 21 6 25

Sabemos que

$$\begin{pmatrix} 2 \\ 17 \end{pmatrix} \textbf{ é levada em } \begin{pmatrix} 19 \\ 8 \end{pmatrix},$$

$$\begin{pmatrix} 8 \\ 15 \end{pmatrix} \textbf{ é levada em } \begin{pmatrix} 21 \\ 11 \end{pmatrix},$$

$$\begin{pmatrix} 19 \\ 14 \end{pmatrix} \textbf{ é levada em } \begin{pmatrix} 5 \\ 6 \end{pmatrix}, \ldots$$

Queremos construir uma matriz 2×2 que é invertível módulo 26. Se usarmos os dois primeiros blocos para construir a matriz

$$P = \begin{pmatrix} 2 & 8 \\ 17 & 15 \end{pmatrix},$$

temos

$$det(P) = -106$$

o qual não é primo relativo com 26 e, portanto, P não é invertível. Se considerarmos o próximo bloco, 19 e 14, mantendo o primeiro, nossa matriz P torna-se,

$$P = \begin{pmatrix} 2 & 19 \\ 17 & 14 \end{pmatrix}$$

cujo determinante é $det(P) = -295$ que é congruente a 17 o módulo 26. Como $mdc(17, 26) = 1$, 17 tem um inverso módulo 26. A matriz C correspondente é

$$\begin{pmatrix} 19 & 5 \\ 8 & 6 \end{pmatrix}$$

, obtida do primeiro e terceiro blocos do rótulo da mensagem criptografada. Assim, nossa equação transforma-se em

$$\begin{pmatrix} 19 & 5 \\ 8 & 6 \end{pmatrix} = E \begin{pmatrix} 2 & 19 \\ 17 & 14 \end{pmatrix}.$$

Então

$$E = \begin{pmatrix} 19 & 5 \\ 8 & 6 \end{pmatrix} \overline{\begin{pmatrix} 2 & 19 \\ 17 & 14 \end{pmatrix}} (mod\ 26) \equiv \begin{pmatrix} 3 & 13 \\ 22 & 4 \end{pmatrix}$$

Para verificar se isto funciona, podemos testar em nossa mensagem

$$CRIPTOGRAFIAELEGAL,$$

que é rotulada como

$$2\ 17\ 8\ 15\ 19\ 14\ 6\ 17\ 0\ 5\ 8\ 0\ 4\ 11\ 4\ 6\ 0\ 11.$$

Assim,

$$P = \begin{pmatrix} 2 & 8 & 19 & 6 & 0 & 8 & 4 & 4 & 0 \\ 17 & 15 & 14 & 17 & 5 & 0 & 11 & 6 & 11 \end{pmatrix},$$

e

$$C = EP = \begin{pmatrix} 3 & 13 \\ 22 & 4 \end{pmatrix} \begin{pmatrix} 2 & 8 & 19 & 6 & 0 & 8 & 4 & 4 & 0 \\ 17 & 15 & 14 & 17 & 5 & 0 & 11 & 6 & 11 \end{pmatrix}$$

$$C = \begin{pmatrix} 19 & 11 & 5 & 5 & 13 & 24 & 25 & 12 & 13 \\ 8 & 2 & 6 & 18 & 20 & 20 & 2 & 8 & 18 \end{pmatrix}.$$

Como os elementos dessa matriz não coincidem com os rótulos da mensagem criptografada, concluímos que o comprimento do bloco não é 2. Então faremos uma tentativa para blocos de comprimento 3. Então, verifiquemos se existe uma matriz quadrada E de ordem 3 com $C = EP$, isto é

$$\begin{pmatrix} 19 & 11 & 11 & 8 & 23 & 21 \\ 8 & 5 & 10 & 11 & 0 & 6 \\ 21 & 6 & 19 & 5 & 7 & 25 \end{pmatrix} = E \begin{pmatrix} 2 & 15 & 6 & 5 & 4 & 6 \\ 17 & 19 & 17 & 8 & 11 & 0 \\ 8 & 14 & 0 & 0 & 14 & 11 \end{pmatrix}.$$

Como anteriormente, selecionamos 3 colunas de nossa matriz de texto plano para produzir uma matriz 3×3 invertível módulo 26. Se Tomarmos as 3 primeiras colunas da matriz de texto plano, teremos

$$P = \begin{pmatrix} 2 & 15 & 6 \\ 17 & 19 & 17 \\ 8 & 14 & 0 \end{pmatrix},$$

cujo determinante módulo 26 é 0 e portanto a matriz não é invertível. Tentamos agora a matriz formada pelas colunas 1, 2 e 6 da matriz de texto plano, obtendo

$$P = \begin{pmatrix} 2 & 15 & 6 \\ 17 & 19 & 0 \\ 8 & 14 & 11 \end{pmatrix}.$$

Como $det(P) \equiv 1(mod\ 26)1$, essa matriz é invertível módulo 26 e devemos ter

$$\begin{pmatrix} 19 & 11 & 21 \\ 8 & 5 & 6 \\ 21 & 6 & 25 \end{pmatrix} = E \begin{pmatrix} 2 & 15 & 6 \\ 17 & 19 & 0 \\ 8 & 14 & 11 \end{pmatrix}.$$

Logo,

$$E = \begin{pmatrix} 19 & 11 & 21 \\ 8 & 5 & 6 \\ 21 & 6 & 25 \end{pmatrix} \overline{\begin{pmatrix} 2 & 15 & 6 \\ 17 & 19 & 0 \\ 8 & 14 & 11 \end{pmatrix}} \equiv \begin{pmatrix} 2 & 3 & 15 \\ 5 & 8 & 12 \\ 9 & 1 & 21 \end{pmatrix} (mod\ 26).$$

Para verificar se isto funciona, vamos testar novamente em nossa mensagem. Temos

$$\begin{pmatrix} 19 & 11 & 11 & 8 & 23 & 21 \\ 8 & 5 & 10 & 11 & 0 & 6 \\ 21 & 6 & 19 & 5 & 7 & 25 \end{pmatrix} = \begin{pmatrix} 2 & 3 & 15 \\ 5 & 8 & 12 \\ 9 & 1 & 21 \end{pmatrix} \begin{pmatrix} 2 & 15 & 6 & 5 & 4 & 6 \\ 17 & 19 & 17 & 8 & 11 & 0 \\ 8 & 14 & 0 & 0 & 14 & 11 \end{pmatrix}.$$

Logo, temos a matriz de criptografia correta e, a partir dela, podemos obter a nossa matriz de descriptografia encontrando sua inversa.

3.4 Tecnologia

Conhecendo o funcionamento das cifras de Hill e como quebrá-las, vamos nos ater a uma ferramenta tecnológica que facilita os cálculos. Discutiremos, na forma de exemplos, os processos para realizarmos operações envolvendo congruência e inversos módulo m, ambos com números e matrizes. A ferramenta tecnológica escolhida para isso foi o JuliaBox. O JuliaBox é um ambiente interativo em nuvem para a linguagem de programação Julia. No momento deste trabalho, a versão atual é a 0.4.2 e pode ser encontrado em

www.juliabox.org.

O JuliaBox contém várias funções pré definidas que lida com álgebra matricial e com congruências. Para saber mais sobre o ambiente JuliaBox e sobre a linguagem de programação Julia consulte o apêndice (A).

Exemplo 3.23. Vamos analisar passo a passo, a sequência de comandos mostrados a

seguir. Inicialmente, carregamos a matriz

$$\begin{pmatrix} 2 & 7 \\ 13 & 9 \end{pmatrix}$$

e a nomeamos de E.

```
In [1]: E = [2 7 ; 13 9]

Out[1]: 2x2 Array{Int64,2}:
          2  7
         13  9
```

A seguir calculamos seu determinante e seu determinante módulo 26.

```
In [3]: det(E)

Out[3]: -73.0

In [4]: mod(-73,26)

Out[4]: 5
```

Agora calculamos $mdc(\Delta, m)$ e seu inverso $\bar{\Delta}$ módulo 26.

```
In [5]: gcd(5,26)

Out[5]: 1

In [6]: invmod(5,26)

Out[6]: 21
```

Para obter a adjunta usual da matriz E multiplicamos elemento por elemento seu determinante pela sua matriz inversa.

Agora, calculamos a matriz adjunta módulo 26.

```
In [7]: adjA=det(E).*inv(E)

Out[7]: 2x2 Array{Float64,2}:
           9.0  -7.0
         -13.0   2.0
```

```
In [12]: adjAmod = mod(adjA,26)

Out[12]: 2x2 Array{Float64,2}:
           9.0  19.0
          13.0   2.0
```

E, finalmente, sua inversa, módulo 26.

```
In [13]: Inversa = mod(21*adjAmod, 26)

Out[13]: 2x2 Array{Float64,2}:
           7.0   9.0
          13.0  16.0
```

Vamos usar a matriz E para criptografar a mensagem ZERO .
Temos:

$$\textbf{ZERO} \longrightarrow 25\ 4\ 17\ 14$$

A matriz P correspondente será

$$\begin{pmatrix} 25 & 17 \\ 4 & 14 \end{pmatrix}$$

Usando o JuliaBox para multiplicar E por P e obter C.
Assim, a mensagem criptografada será

$$0\ 23\ 2\ 9 \longrightarrow \text{AXCJ}$$

Agora, vamos usar a matriz inversa, para descriptografar a palavra AJMG . Temos:

$$\textbf{AJMG} \longrightarrow 0\ 9\ 12\ 6$$

Usando o JuliaBox para multiplicar $\bar{E}$ por C e obter P.

```
In [14]: P = [ 25 17; 04 14]

Out[14]: 2x2 Array{Int64,2}:
          25  17
           4  14
```

```
In [16]: C = mod(E*P,26)

Out[16]: 2x2 Array{Int64,2}:
           0  2
          23  9
```

```
In [17]: C = [ 0 12; 9 6]

Out[17]: 2x2 Array{Int64,2}:
          0  12
          9   6
```

```
In [19]: P = mod(Inversa*C,26)

Out[19]: 2x2 Array{Float64,2}:
           3.0   8.0
          14.0  18.0
```

Assim, a mensagem descriptografada será

$$3\ 14\ 8\ 18 \longrightarrow \text{DOIS}$$

4 Considerações Finais

Existem numerosos tópicos para se dissertar nessa área. Entretanto, na maioria deles os pré-requisitos são elevados para um texto que pretende servir como apoio para Professores da Educação Básica. Assim, optamos por trabalhar a parte da criptologia conhecida como clássica. Apresentamos também exemplos como a tecnologia pode auxiliar neste estudo.

Em especial, nesse trabalho, apresentamos métodos de criptografia e descriptografia associados a matrizes. Para isso, fizemos uma introdução ao estudo das congruências e a criptologia. Na parte principal do trabalho mostramos como matrizes podem ser utilizadas para se criar métodos criptográficos usando cifras em bloco e congruências.

Em virtude do que foi mencionado, acreditamos que o trabalho atingiu os objetivos pretendidos. Porém, pretendemos futuramente criar roteiros didáticos sobre o assunto tratado e aplicá-los em turmas do Ensino Médio e início da graduação em Matemática em que o discente atua.

A Linguagem Julia e JuliaBox

A.1 Introdução

Julia é uma linguagem de programação dinâmica e de alto nível projetada para atender os requisitos da computação de alto desempenho numérico e científico que está crescendo rapidamente em popularidade. Ela providencia um compilador sofisticado, execução paralela, acurácia numérica e uma extensa biblioteca de funções matemáticas. Segundo [1], seu criadores Jeff Bezanson, Stefan Karpinski e Viral Shah criaram Julia após ficarem decepcionados com as ferramentas computacionais atuais na área científica. Julia é uma linguagem de código aberto e grátis com uma licença (MIT) bastante aberta.
Um dos principais objetivos da linguagem Julia é a velocidade de execução dos códigos. Neste ponto, Julia rivaliza com C e Fortran, e deixa outras linguagens dinâmicas de programação bem para trás. Julia tem sintaxe bastante parecida com MATLAB, mas Julia é uma linguagem de programação com propósitos mais gerais do que MATLAB e o caminho em que os cálculos computacionais são realizados são bem distintos.
JuliaBox é uma aplicação hospedada em nuvem para a linguagem de programação Julia contendo alguns pacotes da linguagem já instalados e que permite criar e compartilhar documentos que contém código, equações, visualizações e textos explicativos.

A.2 Usando o JuliaBox

Para usar o JuliaBox basta visitar o site

https://juliabox.org ,

e entrar com uma conta do Google. Assim que entrarmos, veremos uma janela parecida com a figura A.1.

Para criar um arquivo interativo que pode rodar no navegador basta clicar no botão

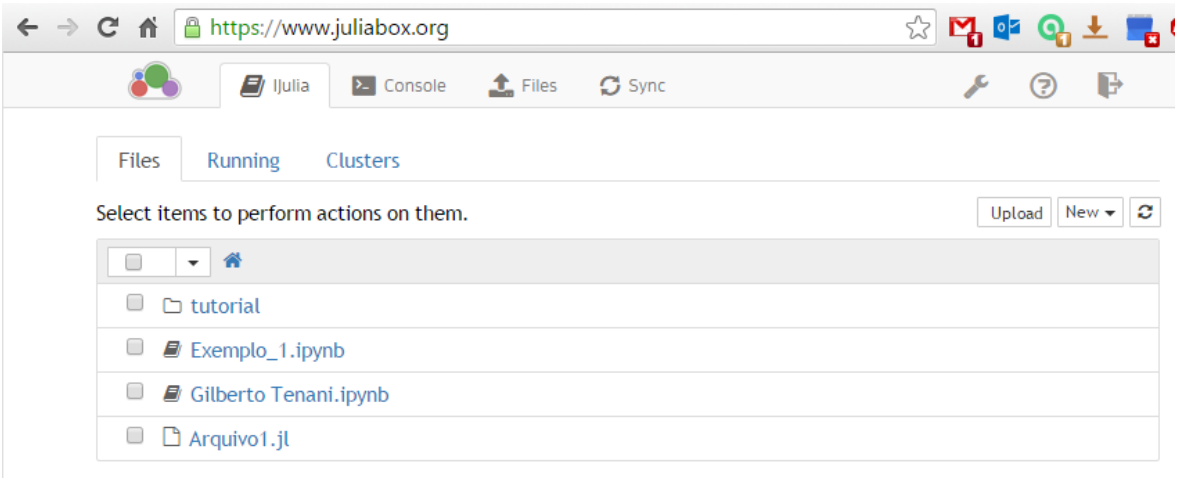

Figura A.1: Tela Principal do JuliaBox

new e selecionar *Julia 0.4.2*. Uma nova página será aberta em seu navegador que se parece com a figura A.2.

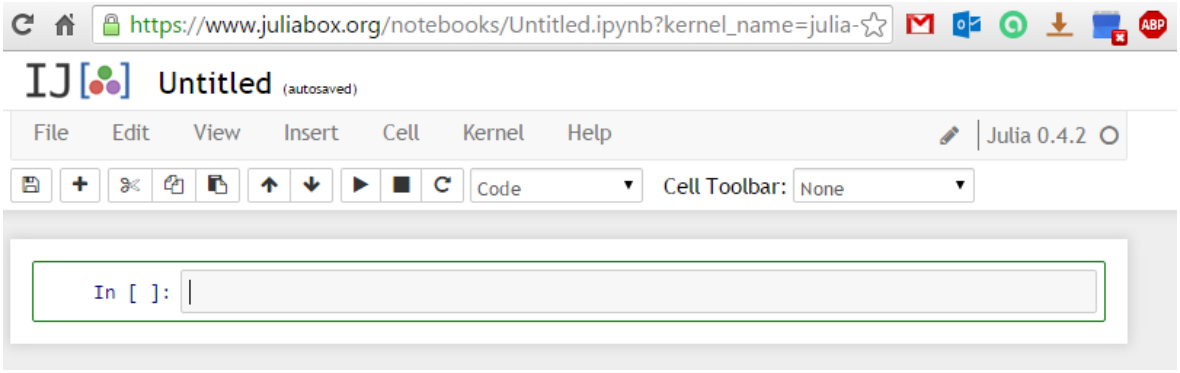

Figura A.2: Tela de um Arquivo Interativo

JulizBox é organizado em células. Podemos digitar diretamente em uma célula. Podemos rodar uma célula selecionando-a e pressionando *Shift + Enter*. A saída da célula é mostrada logo em seguir como podemos observar na figura A.3.

Figura A.3: Execução de um célula

A.2.1 Aritmética Matricial

Para criar uma Matriz no JuliaBox usa-se a seguinte sintaxe:

```
M1 = [1 2 3; 4 5 6; 7 8 9]
```

Isto produzirá a matriz,

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

e atribuirá a ela o nome $M1$. Então em geral, o colchete define a matriz, as linhas são separadas por ponto e vírgula e espaços separam os elementos de um linha. Então, a primeira linha é $\{123\}$. A linguagem Julia diferencia letras maiúsculas e minúsculas. Para os próximos exemplos, considere que as matrizes $A, M, M1$ e $M2$ foram criadas e suas dimensões são compatíveis com as operações.

Adição

```
M3 = M1 + M2
```

Subtração

```
M4 = M1 - M2
```

Multiplicação

```
M5 = M1*M2
```

Multiplicação por Escalar

Se c representa qualquer número real, temos:

```
M6 = cM1
```

Matriz Oposta

```
M7 = -M1
```

Potência de Matriz

Se n representa um número natural, temos:

```
M7 = M1^n
```

Inversa de uma Matriz

Se A representa qualquer matriz invertível, temos:

```
Inversa = inv(A)
```

A.2.2 Aritmética Modular

Cálculo de k Módulo m.

```
mod(k,m)
```

Máximo divisor comum entre dois números inteiros.

```
gcd(m,n)
```

Inverso de um Número módulo m.

```
invmod(k,m)
```

A.2.3 Matrizes e Congruências

Matriz A módulo m.

```
mod(A,m)
```

Referências Bibliográficas

[1] I. Balbaert. *Getting Started with Julia Programming.* Packt Publishing Ltd, 2015.

[2] J.L. Boldrini. *Algebra linear.* HARBRA, 1986.

[3] A. Hefez. *Elementos de Aritmética.* SBM, 2011.

[4] L. S. Hill. Cryptography in an algebric alphabet. *American Mathematical Monthy*, 36:306–312, Junho-Julho 1929.

[5] L. S. Hill. Concerning certain linear transformation apparatus of cryptography. *American Mathematical Monthy*, 38:135–154, Março 1931.

[6] Neal Koblitz. *A Course in Number Theory and Cryptography.* Springer Science + Business Media, LLC, 1998.

[7] K. H. Rosen. *Elementary Number Theory and Its Applications.* Addison-Wesley, 2 edition, 1984.

[8] W. Trappe and L. C. Washington. *Intoduction to Cryptography with coding theory.* Pearson Prentice Hall, 2006.