UNIVERSIDADE DE SÃO PAULO
Instituto de Ciências Matemáticas e de Computação

Criptografia RSA: da teoria à aplicação em sala de aula

Evelyn Gomes da Silva

Dissertação de Mestrado do Programa de Mestrado Profissional em Matemática em Rede Nacional (PROFMAT)

ICMC USP SÃO CARLOS

Evelyn Gomes da Silva

Criptografia RSA: da teoria à aplicação em sala de aula

Dissertação apresentada ao Instituto de Ciências Matemáticas e de Computação – ICMC-USP, como parte dos requisitos para obtenção do título de Mestra em Ciências – Mestrado Profissional em Matemática em Rede Nacional. *VERSÃO REVISADA*

Área de Concentração: Mestrado Profissional em Matemática em Rede Nacional

Orientadora: Profa. Dra. Regilene Delazari dos Santos Oliveira

USP – São Carlos
Junho de 2019

Ficha catalográfica elaborada pela Biblioteca Prof. Achille Bassi
e Seção Técnica de Informática, ICMC/USP,
com os dados inseridos pelo(a) autor(a)

Gc

Gomes da Silva, Evelyn
Criptografia RSA: da teoria à aplicação em sala de aula / Evelyn Gomes da Silva; orientadora Regilene Delazari dos Santos Oliveira. -- São Carlos, 2019.
65 p.

Dissertação (Mestrado - Programa de Pós-Graduação em Mestrado Profissional em Matemática em Rede Nacional) -- Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, 2019.

1. Teoria de números. 2. Números primos. 3. Teorema de Fermat. 4. Criptografia RSA. I. Delazari dos Santos Oliveira, Regilene, orient. II. Título.

Bibliotecários responsáveis pela estrutura de catalogação da publicação de acordo com a AACR2:
Gláucia Maria Saia Cristianini - CRB - 8/4938
Juliana de Souza Moraes - CRB - 8/6176

Evelyn Gomes da Silva

RSA Cryptography: from the theory to a classroom application

Master dissertation submitted to the Institute of Mathematics and Computer Sciences – ICMC-USP, in partial fulfillment of the requirements for the degree of Mathematics Professional Master's Program. *FINAL VERSION*

Concentration Area: Professional Master Degree Program in Mathematics in National Network

Advisor: Profa. Dra. Regilene Delazari dos Santos Oliveira

USP – São Carlos
June 2019

Dedico este trabalho ao meu avô José Gomes que,
com seu exemplo, me mostrou que a honestidade, o amor e a dedicação
nos leva a alcançar nossos sonhos. E que não necessariamente
precisamos fazer algo grande, mas sempre colocar amor em tudo que fazemos.

AGRADECIMENTOS

Aos meus amigos de PROFMAT: Adriana, André, Antonio Carlos, Carlos, Diego, Douglas, Marcelo, Meryelen, Marcos, Marineusa, Hélio e Rosimar, que foram pessoas fantásticas, sempre me ajudando e tornando as sextas-feiras menos cansativas. Obrigado, vocês são incríveis.

Aos professores do PROFMAT, Paulo Dattori, Luiz Ladeira, Sérgio Zani, Michela Tuchapesk, Erica Filletti e em especial aos professores Ires Dias e Hermano Ribeiro, que se dedicaram muito para que todos alcançassem seus objetivos e nunca desistiram de nós.

À minha orientadora Regilene Delazari, pela sua paciência e compreensão. Sempre que me encontrava desanimada, bastava conversar que novamente meu ânimo retornava. Obrigada pelo apoio e por se mais que uma orientadora.

À CAPES, que me apoiou com uma bolsa de estudos durante o desenvolvimento deste projeto.

Aos meus alunos, que sempre se interessam e questionam, me permitindo desenvolver sempre mais. Vocês são essenciais para o crescimento de um professor.

Por fim, a todos que direta ou indiretamente estiveram presentes nessa caminhada. Obrigada à todos.

“Eu acredito que ás vezes são as pessoas que
ninguém espera nada que fazem as coisas que
ninguém consegue imaginar.”
(Alan Turing)

RESUMO

SILVA, E. G. **Criptografia RSA: da teoria à aplicação em sala de aula**. 2019. 65 p. Dissertação (Mestrado em Ciências – Mestrado Profissional em Matemática em Rede Nacional) – Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos – SP, 2019.

Esta dissertação tem por objetivo apresentar a Criptografia RSA, que é o método de criptografia mais utilizado no mundo atualmente. Iniciamos a dissertação com um breve histórico sobre a criptografia e em seguida introduzimos a teoria matemática empregada no método pertencente a teoria dos números. Finalizamos a dissertação com a descrição de uma aplicação simples do método levado para uma sala de aula do ensino médio. Este texto pretende introduzir o tema de maneira simples e por esta razão, fazemos uso de muitos exemplos. Esperamos ainda que o leitor compreenda o que torna este método eficiente e seguro.

Palavras-chave: Teoria dos números, números primos, Teorema de Fermat, Criptografia RSA.

ABSTRACT

SILVA, E. G. **RSA Cryptography: from the theory to a classroom application**. 2019. 65 p. Dissertação (Mestrado em Ciências – Mestrado Profissional em Matemática em Rede Nacional) – Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos – SP, 2019.

The main goal of this work is to introduce the RSA Criptography that is the most used method in Criptography nowadays. We begin the dissertation with a brief introduction about criptography and then we discuss concepts from number theory used in the method. Finally we present a description of a simple application of Criptography made in a High school classroom. This text intend to introduce the subject in a simple way for this reason we present several examples. We hope that the reader have the comprehension of the methods and of its security.

Keywords: Number theory, prime numbers, Theorem of Fermat, RSA Cryptography.

LISTA DE ILUSTRAÇÕES

SUMÁRIO

CAPÍTULO

1

INTRODUÇÃO

Esta dissertação traz o estudo do método de Criptografia conhecido como Criptografia RSA. Segundo consta na literatura, a criptografia é uma técnica tão antiga quanto a própria escrita, uma vez que existem indícios que ela já estava presente no sistema de escrita hieroglífica dos egípcios. Há evidências de que os romanos utilizavam códigos secretos para comunicar seus planos de batalhas. Além disso, a tecnologia de Criptografia se manteve por um longo período. Depois da Segunda Guerra Mundial, com a invenção do computador, a técnica incorporou algoritmos matemáticos. Durante a guerra, os ingleses ficaram conhecidos por seus esforços para decifração de mensagens, estes deram origem a área atualmente conhecida como ciência da computação.

A criptografia pode ser entendida como um conjunto de técnicas que permitem tornar incompreensível uma mensagem originalmente escrita com clareza, de forma a permitir que apenas o destinário a decifre e a compreenda, e isso só é possivel, a partir do conhecimento das convenções e mecanismos de codificação e decodificação adotados, ou seja, ter acesso à chave que codifica e decodifica a mensagem. A chave é o procedimento do algoritmo utilizado em um dado método. Para exemplificar imagine uma festa em que os convidados tenham que usar máscaras. A necessidade das máscaras é para que não se identifique a pessoa que a está usando, portanto a chave é a máscara.

A Criptografia RSA é o método mais difundido nos dias de hoje e é bastante simples. Ele é empregado em sistemas bancários e eletrônicos de modo geral. O método da Criptografia RSA faz uso de conceitos básicos e fundamentais da teoria dos números.

Nos dias de hoje todos nós estamos em contato com esta técnica sem tomar conhecimento dos conceitos matemáticos envolvidos em seu funcionamento. Assim, nos sentimos empenhados em investigar alternativa(s) para levar o tema para sala de aula, esperando assim, motivar os alunos para o ensino de matemática.

Nesta dissertação nosso material de apoio para o estudo de conceitos relacionados a

teoria dos números e a compreensão do método da Criptografia foi formado principalmente pelas referências (COUTINHO, 1997; COUTINHO, 2015).

Iniciamos este trabalho apresentando um breve histórico sobre a Criptografia RSA e em seguida, apresentamos os conceitos matemáticos necessários para a compreensão do método e de sua eficiência. Nesta primeira etapa nosso objetivo é entender como e por que o método funciona, além de compreender as razões pelas quais ele é seguro.

Em seguida apresentamos uma atividade realizada em sala de aula relacionada a Criptografia. O objetivo da atividade foi despertar no aluno o interesse pela matemática, mostrar como funciona a criptografia e como a matemática está presente em nosso dia a dia. Vale ressaltar que a atividade realizada em sala de aula não teve por objetivo apresentar os conceitos matemáticos envolvidos no método e nesse caso não foi utilizada a Criptografia RSA.

Encerramos a dissertação com algumas considerações finais sobre a dissertação e o impacto do Mestrado profissionalizante em minha postura em sala de aula.

CAPÍTULO

2

CRIPTOGRAFIA

A palavra Criptografia é originária do grego e é formada por duas partes: *kryptós*, que significa "segredo"e *logia*, "estudo". Podemos afirmar que é o método e o estudo da técnica empregada para comunicação segura na presença de terceiros (também chamados adversários).

A criptografia nos dias de hoje existe como um tema na intersecção de disciplinas como matemática, ciência da computação, engenharia elétrica, ciência da comunicação e física.

Neste capítulo fazemos um breve histórico sobre a criptografia, especialmente a Criptografia RSA.

2.1 A criptografia ao longo do tempo

A criptografia surgiu da necessidade de enviar mensagens codificadas. Codificar uma mensagem para que se interceptada não seja compreendida pelo adversário.

Ao longo da história o método de enviar mensagens criptografadas foi muito utilizado, especialmente em guerras, neste caso a criptografia permitiu a comunicação evitando a interpretação de mensagens, exceto pelo legítimo destinatário, o detentor do código de decodificação. O primeiro exemplo desse tipo de código secreto que se tem notícia foi utilizado pelo ditador Júlio César para comunicar-se com legiões romanas em combate pela Europa.

As primeiras formas de codificar uma mensagem eram bem simples, consistiam muitas vezes em substituir uma letra por outra, e dessa forma era bem simples quebrar o código e decodificar a mensagem.

Com o tempo esses métodos foram se aperfeiçoando cada vez mais, por exemplo o processo conhecido como *código de blocos*, que consiste em dividir a mensagem em blocos de várias letras e embaralhar estas letras. Observamos que esse método contém várias falhas que o tornam frágil, principalmente nos dias atuais com o avanço dos computadores e da internet.

Nos dias de hoje, a criptografia consiste num processo onde a mensagem é facilmente codificada porém dificilmente decodificada. Trata-se de um método onde duas chaves (códigos) são empregados. Uma delas é conhecida como *chave pública*, a de encriptação, e no processo de codificação ela pode ser conhecida por qualquer pessoa, sem que isso comprometa a segurança do código. O método ficou conhecido como Criptografia RSA.

2.2 Criptografia RSA

O acrônimo RSA é composto das letras iniciais dos sobresnomes de Ron Rivest, Adi Shamir e Leonard Adleman, fundadores da atual empresa *RSA Data Security, Inc.*, os quais foram os primeiros a descrever o algoritmo em 1978. Atualmente sabe-se que Cliffor Cocks, um matemático Inglês que trabalhava para a agência de inteligência britânica *Government Communications Headquarters* (GCHQ), desenvolveu um sistema equivalente em 1973, mas ele não foi revelado até 1997 (ANDRADE, 2014).

A Criptografia RSA é considerada das mais seguras. Um usuário do RSA cria e então publica uma chave pública baseada em dois números primos grandes, junto com um valor auxiliar. Os números primos devem ser mantidos secretos. Qualquer um pode usar a chave pública para encriptar a mensagem, mas com métodos atualmente publicados, e se a chave pública for muito grande, apenas alguém com o conhecimento dos números primos pode decodificar a mensagem de forma viável. Quebrar a encriptação RSA é tão difícil quanto o problema de fatoração em números primos, que permanece como uma questão em aberto.

A Criptografia RSA envolve um par de chaves, uma chave pública que pode ser conhecida por todos e uma chave privada que deve ser mantida em sigilo. Toda mensagem cifrada usando uma chave pública só pode ser decifrada usando a respectiva chave privada.

A Criptografia RSA atua diretamente na internet, por exemplo, em mensagens de emails, em compras on-line e o que você imaginar; tudo isso é codificado e recodificado pela criptografia RSA.

Com o objetivo de compreender este método vamos estudar a teoria envolvida em sua construção, tema do próximo capítulo desta dissertação. Mais adiante retornamos a Criptografia RSA.

CAPÍTULO

3

INTRODUÇÃO À ARITMÉTICA

O conceito primordial para a Criptografia RSA é o de número primos, dessa forma iniciaremos esse capítulo com a definição e alguns teoremas importantes referente à isso.

3.1 Números Primos

Definição 1. Dizemos que um número inteiro positivo maior que 1 é primo se ele é divisível apenas por 1 e por ele mesmo. Caso contrário, dizemos que o número inteiro é composto.

Dado um número inteiro qualquer não existe um critério para decidir se este número é primo ou composto. Ao longo da história alguns algoritmos foram propostos, porém esse é um problema em aberto na Matemática. Vejamos alguns desses algoritmos..

1. Crivo de Eratóstenes

   O Crivo de Erastótenes é um método bem conhecido empregado para determinar números primos. Ele consiste em eliminar os números compostos e assim aqueles que não possuem números divisores serão os números primos. Esse método não é eficiente quando o primo for um número grande. Por se tratar de um método mais simples de encontrar primos, esse é um dos primeiros introduzidos na educação básica.

2. Números de Fermat: $F(n) = 2^{2^n} + 1, n \in \mathbb{N}$.

   Fermat acreditava que todos os números da forma acima eram primos. Realmente os números F(1), F(2), F(3) e F(4) são primos, porém Euler provou que F(5) é composto, e dessa forma a teoria formulada por Fermat foi quebrada. Os números de Fermat primos são chamados de primos de Fermat.

3. Números de Mersenne : $M(n) = 2^n - 1$, onde n é primo.

No intervalo entre 2 e 5000 os números de Mersenne que são primos, chamados de primos de Mersenne, correspondem aos seguintes valores de p: 2, 3, 5, 7, 13, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253 e 4423.

Porém esses métodos não são suficientes ou eficientes para encontrar primos em geral.

Atualmemte existe um projeto chamado GIMPS (Grande Busca na Internet pelo Primo Mersenne, tradução literal do inglês), cujo principal objetivo é descobrir números primos, a procura é por primos de Mersenne. Desde 1996 milhares de voluntários em todo o mundo emprestam seus computadores para realização de cálculos automáticos enviados por um servidor central e desde então 17 números primos de Mersenne foram descobertos. O maior número primo conhecido foi descoberto no final de 2018. Ele possui 24.862.048 dígitos, 1,5 milhão a mais do que o número primo recorde descoberto em 2017. Este pode ser expresso como $2^{282589933} - 1$ e foi descoberto por Patrick Laroche, 35 anos. Patrick é um profissional de TI que usava o software GIMPS como um "teste de estresse" gratuito para suas compilações de computador.(IMPA, 2019)

Este processo nos leva a questionar se esta busca terá fim. Adiante veremos um Teorema que nos responderá essa questão..

Iniciamos essa seção com o algoritmo da divisão, um teorema importante para a teoria que vamos estudar em seguida.

3.2 Algoritmo da Divisão

Basicamente, o teorema a seguir nos diz que dados dois inteiros, o quociente e o resto da divisão entre eles existem e são únicos. Vamos enunciá-lo.

Teorema 1. Sejam a e b números inteiros positivos. Existem únicos números inteiros q e r tais que

$$a = b \cdot q + r \quad \text{com} \quad 0 \leqslant r < b.$$

Demonstração. (Unicidade) Se existem q', r', q e r satisfazendo as condições do teorema e $r \geq r'$, ou seja,

$$a = b \cdot q' + r' \quad \text{e} \quad 0 \leqslant r' < b.$$

e,

$$a = b \cdot q + r \quad \text{e} \quad 0 \leqslant r < b, \tag{3.1}$$

mostramos que $q = q'$ e $r = r'$. Note que de (3.1) temos

$$r - r' = (a - b \cdot q) - (a - b \cdot q') = b \cdot (q' - q). \tag{3.2}$$

Como por hipótese, r e r' são menores que b e $r \geq r'$, segue que

$$0 \leq r - r' < b.$$

Então de (3.2) temos

$$0 \leq b \cdot (q' - q) < b,$$

ou equivalentemente

$$0 \leq q' - q < 1.$$

Como $q - q' \in \mathbb{Z}$, temos $q' - q = 0$, isto é $q' = q$ e consequentemente $r = r'$.

(Existência) Suponha que $a > b$ e considere, enquanto fizer sentido, os números

$$a, a-b, a-2b, \ldots, a-nb, \ldots$$

Pelo Princípio da Boa Ordenação [1] o conjunto S formado pelos elementos acima tem um menor elemento $r = a - b \cdot q$. Vamos provar que r tem a propriedade requerida, ou seja, que $r < b$.

Se $b|a$, ou seja, se b divide a, então $r = 0$ e nada mais temos a provar. Se, por outro lado $b \nmid a$, então $r \neq b$ e, portanto, basta mostrar que não pode ocorrer $r > b$. De fato, se $r > b$, então existe um número natural $c < r$ tal que $r = c + b$. Consequentemente, $r = c + b = a - b \cdot q$, teríamos,

$$c = a - (q+1)b \in S, \quad \text{com} \quad b < r,$$

contradizendo o fato de r ser o menor elemento de S. Portanto, temos que $a = b \cdot q + r$ com $r < b$, o que prova a existência de q e r. □

3.2.1 Algoritmo de Euclides

O algoritmo de Euclides é uma ferramenta que nos permite encontrar o máximo divisor comum de dois números, denotado daqui em diante por *mdc* entre dois números, antes de enunciá-lo vejamos algumas definições importantes.

Dados dois números $a, b \neq 0$, dizemos que o número inteiro d é um divisor comum de a e b se $d|a$ e $d|b$.

Definição 2 (mdc)**.** O máximo divisor comum de a e b (dois inteiros), é denotado por $d = (a,b) = mdc(a,b)$, e é o número inteiro d estritamente positivo tal que

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

(ii) Se $c|a$ e $c|b \Rightarrow c|d$.

Exemplo 1. Por exemplo $mdc(12,18) = 6$

[1] (LIMA, 2006) Todo subconjunto S $\subset \mathbb{N}$ possui um menor elemento, isto é, um elemento $n_0 \in S$ tal que $n_0 < n$ para todo $n \in S$.

Observação 1. Se $mdc(a,b) = 1$, dizemos que a e b são primos entre si.

A observação acima é de extrema importância nessa dissertação.

Exemplo 2. $mdc(20,33) = 1$; logo, 20 e 33 são ditos números primos entre si, ou apenas primos entre si.

O lema a seguir mostra a relação entre o algoritmo da divisão e o mdc.

Lema 1. Se $a = b \cdot q + r$ então $mdc(a,b) = mdc(b,r)$.

Demonstração. Se $d = mdc(a,b)$ então $d|a$ e $d|b$, em particular $d|a - b \cdot q = r$, pois é uma combinação inteira de a e b. Portanto, $d|b$ e $d|r$.

Por outro lado, se $c|b$ e $c|r$, então $c|b \cdot q + r = a$, o que implica $c|d = mdc(a,b)$. Logo, $d = mdc(b,r)$. □

Chegamos então ao algoritmo que nomeia a nossa seção, o Algoritmo de Euclides. Vamos entender aqui seu procedimento.

Algoritmo de Euclides: Sejam a e $b \in \mathbb{Z}$. Procedemos da seguinte forma, utilizando o algoritmo da divisão, diversas vezes:(DIAS; GODOY, 2006)

$$a = b \cdot q_1 + r, \ \ 0 \leqslant r < b$$

$$b = r \cdot q_2 + r_1, \ \ 0 \leqslant r_1 < r$$

$$r = r_1 \cdot q_3 + r_2, \ \ 0 \leqslant r_2 < r_1$$

$$r_1 = r_2 \cdot q_4 + r_3, \ \ 0 \leqslant r_3 < r_2$$

$$\vdots$$

$$r_{n-2} = r_{n-1} \cdot q_{n+1} + r_n, \ \ 0 \leqslant r_n < r_{n-1}$$

$$r_{n-1} = r_n \cdot q_{n+2}.$$

Então r_n (o último resto não nulo) é o $mdc(a,b)$.

Demonstração. De fato, segue do lema anterior que

$$mdc(a,b) = mdc(b,r_1) = mdc(r_1,r_2) = \ldots = mdc(r_{n-1},r_n).$$

Como $r_n|r_{n-1}$, segue que $mdc(r_{n-1},r_n) = r_n$ e, portanto, $mdc(a,b)$ existe e é igual a r_n, que é o ultimo resto diferente de zero. □

Exemplo 3. (FIARRESGA, 2010) Para determinar $mdc(245,135)$, procedemos da seguinte forma:

$$245 = 1 \cdot 135 + 110,$$

$$135 = 1 \cdot 110 + 25,$$

$$110 = 4 \cdot 25 + 10,$$

$$25 = 2 \cdot 10 + 5,$$

$$10 = 2 \cdot 5 + 0.$$

Pelo Algoritmo de Euclides, concluímos que o $mdc(245,135) = 5$.

Proposição 1. Sejam a e $b \in \mathbb{Z}$. Se $d = mdc(a,b)$ então existem x_0 e $y_0 \in \mathbb{Z}$ tais que $d = a \cdot x_0 + b \cdot y_0$.

Demonstração. Se $a \neq 0$ ou $b \neq 0$, considere

$$S = \{m \cdot a + n \cdot b,\ m,n \in \mathbb{Z}\}.$$

Como$a \cdot a + b \cdot b = a^2 + b^2 > 0$ e $a^2 + b^2 \in S$, temos que em S existem elementos estritamente positivos. Logo, pelo Princípio da Boa Ordenação, existe o menor deles. Seja d este mínimo. Agora é suficiente mostrar que $d = mdc(a;b)$.

Temos que $d \geq 0$ pela maneira como foi escolhido. Como $d \in S$, temos que existem $x_0 e y_0 \in \mathbb{Z}$ tais que $d = ax_0 + by_0$. Do algoritmo da divisão temos que $a = dq + r$, com $0 \leqslant r < d$. Substituindo d nesta igualdade obtemos

$$a = (a_x 0 + by_0)q + r,$$

de onde segue que

$$r = a(1 - qx_0) + bq([-y_0]).$$

Assim, $r \in S$ e, como $r \geq 0$, pela minimalidade de d, temos que $r = 0$. Portanto $a = dq$, o que mostra que $d|a$. De maneira análoga mostra-se que $d|b$.

Além disso, se $c \in Z$ é tal que $c|a$ e $c|b$, temos que $c|d = ax_0 + by_0$, como queríamos.

□

Observe que podemos estender essa Proposição para a definição de números primos entre si, como mostra o Corolário abaixo.

Corolário 1. Dois números a e b inteiros são primos entre si se, e somente se, existem x_0 e y_0 $\in \mathbb{Z}$ tais que $a \cdot x_0 + b \cdot y_0 = 1$.

Demonstração. ($\Rightarrow$) Segue imediatamente da Proposição anterior.

($\Leftarrow$) Se $a \cdot x_0 + b \cdot y_0 = 1$, então $1|a$ e $1|b$ e, 1 é a menor combinação linear positiva de a e b com coeficientes inteiros, logo segue que $mdc(a,b) = 1$. □

Observação 2. O Algoritmo de Euclides nos fornece, portanto, um meio prático de escrever o mdc de dois números como soma de dois múltiplos dos números em questão. Quando utilizarmos o Algoritmo de Euclides para expressar $mdc(a;b)$ na forma $a \cdot x_0 + b \cdot y_0$, com x_0 e $y_0 \in \mathbb{Z}$, nos referiremos a ele como *Algoritmo de Euclides Estendido.*

3.3 Fatoração Única

Abaixo encontramos algumas propriedades que são importantes para o Teorema Fundamental da Aritmética, o resultado chave dessa seção.

3.3.1 Propriedade Fundamental dos Primos

Lema 2. Sejam a, b e c inteiros positivos, com a e b primos entre si.

1. Se b divide o produto $a \cdot c$ então b divide c.
2. Se a e b dividem c então o produto $a \cdot b$ divide c.
3. Se p é primo e $a, b \in \mathbb{Z}_+$. Se $p|a \cdot b$ então $p|a$ ou $p|b$.

Demonstração. 1. $mdc(a,b) = 1$, então

$$a \cdot x + b \cdot y = 1,$$

$$c \cdot a \cdot x + c \cdot b \cdot y = c.$$

Como $b|a \cdot c$ segue que $c \cdot a \cdot x + c \cdot b \cdot y$ é divisível por b. Portanto, $b|c \cdot a \cdot x + c \cdot b \cdot y = c$.

2. Se $a|c$ e $b|c$ temos que $c = a \cdot x$. Como a e b são primos entre si e $b|c = a \cdot x$ então b tem que dividir x e temos $x = b \cdot t$. Portanto,

$$c = a \cdot x = a \cdot (b \cdot t) = (a \cdot b) \cdot t \quad \Rightarrow \quad a \cdot b|c.$$

3. Se $p|a$ está feito. Suponhamos que $p \nmid a$, então p e a são primos entre si. Segue do item (1) desse lema que se $p|a \cdot b$ então $p|b$.

□

3.3.2 Teorema Fundamental da Aritmética

O Teorema Fundamental da Aritmética nos diz que existe e é única a fatoração de um número inteiro positivo.

Teorema 2. Dado um número inteiro positivo $n \geq 2$ podemos sempre escrevê-lo, de modo único, na forma

$$n = p_1^{e_1} \dots p_k^{e_k},$$

onde $1 < p_1 < p_2 < p_3 < \dots < p_k$ são números primos e $e_1, \dots, e_k$ são inteiros positivos.

Demonstração. (Unicidade) Suponha que n admite mais de uma fatoração, então,

$$n = p_1^{e_1} \dots p_k^{e_k} = q_1^{r_1} \dots q_s^{r_s}.$$

Como $p_1 | p_1^{e_1} \dots p_k^{e_k} = n$, então $p_1 | q_1^{r_1} \dots q_s^{r_s}$, assim como p_1 divide um produto de fatores, ele divide um de seus fatores, ou seja, $p_1 | q_j^{j_1}, j \in 1, 2, \dots, s$. Como ambos são primos, então $p_1 = q_j$, $1 \leqslant j \leqslant s$. Fazendo esse rarciocínio para cada fator, provamos a unicidade da fatoração de n.

(Existência) Prova por indução. Se $n = 2$, o resultado segue pois 2 é primo. Suponha o resultado válido para todo número natural menor do que n e vamos provar que vale para n. Se o número n é primo, nada temos a demonstrar. Suponha, então, que n seja composto. Logo, existem números naturais n_1 e n_2 tais que $n = n_1 \cdot n_2$ com $1 < n_1 < n$ e $1 < n_2 < n$. Pela hipótese de indução, temos que existem números primos $p_1, \dots, p_r$ e $q_1, \dots, q_s$, tais que $n_1 = p_1 \cdots p_r$ e $n_2 = q_1 \cdots q_s$. Portanto, $n = p_1 \cdots p_r \cdot q_1 \cdots q_s$. □

Observe que é importante a hipótese $n \geq 2$ no enunciado do Teorema 2, do contrário teríamos por exemplo $6 = 1 \cdot 2 \cdot 3$ e $6 = 2 \cdot 3$ (fatorações distintas do mesmo número).

Exemplo 4. (SAMPAIO; CAETANO, 2008) Exemplificando o Teorema Fundamental da Aritmética, temos as seguintes fatorações de inteiros.

- $342 = 2 \cdot 3 \cdot 3 \cdot 19 = 2 \cdot 3^2 \cdot 19$,
- $3888 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 = 2^4 \cdot 3^5$,
- $10100 = 2 \cdot 2 \cdot 5 \cdot 5 \cdot 101 = 2^2 \cdot 5^2 \cdot 101$.

Agora como o Teorema Fundamental da Aritmética, voltamos a falar sobre a infinitude de primos.

Teorema 3. Existem infinitos números primos.

Demonstração. Suponha que existam finitos números primos $p_1, \ldots, p_r$. Considere o número natural

$$n = p_1 p_2 \cdots p_r + 1.$$

Pelo Teorema 2, o número n possui fatoração em primos, isto é, existe um número primo p que, deve ser um dos $p_1, \ldots, p_r$ e, consequentemente, divide o produto $p_1 \cdot p_2 \cdots p_r$. Mas isto implica que p divide 1, o que é absurdo. □

Para compreender e fazer uso da Criptografia RSA, precisamos conhecer também as propriedades de aritmética modular, que é tratada no decorrer dessa seção.

3.4 Aritmética Modular

Definição 3. Dizemos que dois números inteiros a e b são congruentes módulo m se $a - b$ é um múltiplo de m.

Notação: $a \equiv b \bmod m$

Exemplo 5. $21 \equiv 13 \bmod 2$. De fato $21 - 13 = 8 = 2 \cdot 4$, múltiplo de 2.

3.4.1 Conjuntos dos Inteiros Módulo m ($\mathbb{Z}_m$)

Seja $m \in \mathbb{Z}, m > 1$. Defina os conjuntos:

$$\bar{0} = \{x \in \mathbb{Z};\ x \equiv 0 \bmod m\}$$
$$\bar{1} = \{x \in \mathbb{Z};\ x \equiv 1 \bmod m\}$$
$$\vdots$$
$$\overline{m-1} = \{x \in \mathbb{Z};\ x \equiv m-1 \bmod m\},$$

ou seja, para $0 \leq a \leq m-1$,

$$\bar{a} = \{x \in \mathbb{Z};\ x \equiv a \bmod m\}.$$

O conjunto $\bar{a} = \{x \in \mathbb{Z};\ x \equiv a \bmod m\}$ é chamado de classe residual módulo m do elemento a de $\mathbb{Z}$.

Para verificar se dois números são congruentes módulo m, não é necessário efetuar a divisão euclidiana de ambos por m para depois comparar os seus restos. É suficiente aplicar o seguinte resultado:

Proposição 2. Suponha que $a, b \in \mathbb{N}$ são tais que $b \geq a$. Tem-se que $a \equiv b \bmod m$, se, e somente se, $m | b - a$.

Demonstração. Sejam $a = mq + r$, com $r < m$ e $b = mq' + r'$, com $r' < m$, as divisões euclidianas de a e b por m, respectivamente. Logo,

$$b - a = m'(q' - q) + (r' - r).$$

Portanto, $a \equiv b \bmod m$ se, e somente se, $r = r'$, o que é equivalente a dizer que $m|b-a$ já que $|r - r'| < m$. □

Note que todo numero natural é congruente módulo m ao seu resto na divisão euclidiana por m e, portanto, é congruente módulo m a um dos números $0, 1, \ldots, m-1$. Além disso, dois desses números distintos não são congruentes módulo m.

Em geral, se $a \equiv r \bmod m$ e $0 \leqslant r < m$, dizemos que r é o *resíduo* de a módulo m.

Proposição 3. Para cada $a \in \mathbb{Z}$ existe um e somente um $r \in \mathbb{N}$, com $r < m$, tal que $\bar{a} = \bar{r}$.

Demonstração. Seja $a \in \mathbb{Z}$. Pela Divisão Euclidiana, existem dois únicos naturais q e r, com $r < m$, tais que $a = m \cdot q + r$. Portanto é único o número natural r tal que $r < m$ e $a \equiv r \bmod m$. Consequentemente, é único o número inteiro r tal que $r < m$ e $\bar{a} = \bar{r}$. □

Chamamos de *sistema completo de resíduos módulo m* a todo conjunto de números naturais cujos restos pela divisão por m são os números $0, 1, \ldots, m-1$, sem repetições e numa ordem qualquer.

Corolário 2. Existem exatamente m classes residuais módulo m distintas, a saber, $\bar{0}, \bar{1}, \ldots, \overline{m-1}$.

Portanto, um sistema completo de resíduos módulo m possui m elementos.

Proposição 4. Sejam $a, b, c, m \in \mathbb{N}$, com $m > 1$, tem-se que

$$a + c \equiv b + c \bmod m \quad \Leftrightarrow \quad a \equiv b \bmod m$$

Demonstração. ($\Leftarrow$) Suponhamos que $a \equiv b \bmod m$. Podemos, sem perda de generalidade, supor $b \geq a$. Logo temos que $m|b-a$.

Observe que $m|(b-a)+(c-c)$ e portanto, $m|(b+c)-(a+c)$ como queríamos demonstrar.

($\Rightarrow$) Suponhamos que $a + c \equiv b + c \bmod m$. Sem perda de generalidade, podemos supor que $b + c \geq a + c$. Logo, $m|b + c - (a + c)$, o que implica que $m|b - a$ e, consequentemente, $a \equiv b \bmod m$. □

A proposição acima nos diz sobre a lei do cancelamento em relação a operação de adição em $\mathbb{Z}_m$. Porém essa mesma relação não é válida, em geral, no caso da operação de multiplicação em $\mathbb{Z}_m$.

Exemplo 6. Como $6 \cdot 9 - 6 \cdot 5 = 24$ e $8|24$, temos que $6 \cdot 9 \equiv 6 \cdot 5 \bmod 8$ e, no entanto, $9 \not\equiv 5 \bmod 8$.

Porém vamos mostrar um caso onde a lei do cancelamento na multiplicação é válida. Denote por $d = mdc(c,m)$.

Proposição 5. Sejam $a,b,c,m \in \mathbb{N}$, com $c \neq 0$ e $m > 1$. Temos que

$$ac \equiv bc \bmod m \quad \Leftrightarrow \quad a \equiv b \bmod \frac{m}{d},$$

onde $d = mdc(c,m)$.

Demonstração. Podemos supor sem perda de generalidade que $bc \geq ac$. Portanto

$$ac \equiv bc \bmod m \quad \Leftrightarrow \quad m|(b-a)c.$$

Como $\frac{m}{d}$ e $\frac{c}{d}$ são primos entre si temos que

$$\frac{m}{d}\Big|(b-a)\frac{c}{d} \quad \Leftrightarrow \quad \frac{m}{d}\Big|b-a.$$

De onde segue que $a \equiv b \bmod \frac{m}{d}$. □

Corolário 3. Sejam $a,b,c,m \in \mathbb{N}$, com $m > 1$ e $(c,m) = 1$. Temos que

$$ac \equiv bc \bmod m \quad \Leftrightarrow \quad a \equiv b \bmod m.$$

Proposição 6. Sejam $a,k,m \in \mathbb{N}$, com $m > 1$ e $(k,m) = 1$. Se $a_1,\ldots,a_m$ é um sistema completo de resíduos módulo m, então

$$a + ka_1, \ldots, a + ka_m,$$

também é um sistema completo de resíduos módulo m.

Demonstração. Segue do corolário acima que para $i, j = 0,\ldots,m-1$, temos

$$a + ka_i \equiv a + ka_j \bmod m.$$

Como por hipótese $(k,m) = 1$, segue que

$$ka_i \equiv ka_j \bmod m \quad \Rightarrow \quad a_i \equiv a_j \bmod m.$$

Portanto, $i = j$. Isto mostra que $a + ka_1, \ldots, a + ka_m$ são dois a dois, não congruentes módulo m e, portanto, formam um sistema completo de resíduos módulo m. □

3.4.2 Operações em $\mathbb{Z}_m$

Definimos as seguintes operações em $\mathbb{Z}_m$:

1. $\bar{a}+\bar{b}=\overline{a+b}$
2. $\bar{a}\cdot\bar{b}=\overline{a\cdot b}$

Observação 3. É fácil verificar que se mudarmos os representantes a e b para as classes residuais $\bar{a}$ e $\bar{b}$, o resultado sempre está na mesma classe, o que mostra que as operações estão bem definidas.

Exemplo 7. (a)

$$51 \equiv 31 \bmod 5 \quad \text{e} \quad 43 \equiv 103 \bmod 5.$$

Assim temos que

$$51+43=94 \quad \text{e} \quad 31+103=134.$$

cuja diferença é -40, assim um múltiplo de 5 e temos

$$51+43 \equiv 31+103 \bmod 5.$$

(b)

$$51 \equiv 31 \bmod 5 \quad \text{e} \quad 43 \equiv 103 \bmod 5.$$

Assim temos que

$$51\cdot 43=2193 \quad \text{e} \quad 31\cdot 103=3193,$$

cuja diferença é -1000 e, portanto, um múltiplo de 5, assim:

$$51\cdot 43 \equiv 31\cdot 103 \bmod 5.$$

Vamos demonstrar então que dados $\bar{a},\bar{a'},\bar{b}$ e $\bar{b'}$, temos que $\overline{a+b}=\overline{a'+b'}$ e $\overline{a\cdot b}=\overline{a'\cdot b'}$.

De fato, considere $\bar{a}=\bar{a'}$ e $\bar{b}=\bar{b'}$.

(*Adição*) Note que se $a \equiv a' \bmod m$ e $b \equiv b' \bmod m$ temos válida a seguinte igualdade

$$(a-a')+(b-b')=(a+b)-(a'-b').$$

Além disso $(a+b)-(a'-b')$ é múltiplo de m, portanto $\overline{a+b}=\overline{a'+b'}$.

(*Multiplicação*) Se $\bar{a}=\bar{a'}$, digamos $a=a'+r\cdot m$, $r\in\mathbb{Z}$ e se $\bar{b}=\bar{b'}$, isto é, $b=b'+s\cdot m$, $s\in\mathbb{Z}$. Segue que,

$$a\cdot b=(a'+rm)\cdot(b'+sm)=a'b'+(a's+rb'+smr)\cdot m$$

Logo $ab-a'b'$ é múltiplo de m e $\overline{a\cdot b}=\overline{a'\cdot b'}$.

A seguir apresentaremos as propriedades da adição e multiplicação da aritmética modular, cuja demosntração segue diretamente do uso das respectivas definições.

Propriedades: Sejam $\bar{a}$, $\bar{b}$ e $\bar{c}$ elementos de $\mathbb{Z}_m$, temos:

1. Adição:

   Associativa: $(\bar{a}+\bar{b})+\bar{c} = \bar{a}+(\bar{b}+\bar{c})$

   Comutativa: $\bar{a}+\bar{b} = \bar{b}+\bar{a}$

   Elemento neutro: $\bar{a}+\bar{0} = \bar{a}$

   Elemento simétrico: $\bar{a}+\overline{-a} = \bar{0}$

2. Multiplicação:

   Associativa: $(\bar{a}\cdot\bar{b})\cdot\bar{c} = \bar{a}\cdot(\bar{b}\cdot\bar{c})$

   Comutativa: $\bar{a}\cdot\bar{b} = \bar{b}\cdot\bar{a}$

   Elemento neutro: $\bar{a}\cdot\bar{1} = \bar{a}$

3. Distributiva: $\bar{a}\cdot(\bar{b}+\bar{c}) = \bar{a}\cdot\bar{b}+\bar{a}\cdot\bar{c}$

3.4.2.1 Inverso em $\mathbb{Z}_m$

Diremos que a classe $\bar{\alpha} \in \mathbb{Z}_m$ é o inverso de $\bar{a}$ se a equação $\bar{a}\cdot\bar{\alpha} = 1$ é verificada em $\mathbb{Z}_m$.

Exemplo 8. Temos que $\bar{2}$ é o inverso de $\bar{4}$ em $\mathbb{Z}_7$, pois $2\cdot 4 \equiv 1 \bmod 7$.

Teorema 4 (Inversão)**.** A classe $\bar{a}$ tem inverso em $\mathbb{Z}_m$ se, e somente se, a e m são primos entre si.

Demonstração. ($\Rightarrow$) Se $\bar{a}$ é invertível, então existe um $\bar{b} \in \mathbb{Z}_m$ tal que $\bar{1} = \bar{a}\cdot\bar{b} = \overline{a\cdot b}$. Logo $a\cdot b \equiv 1 \bmod m$, isto é, existe $t \in \mathbb{Z}$ tal que $a\cdot b + t\cdot m = 1$ e, assim $(a,m) = 1$.

($\Leftarrow$) Se $(a,m) = 1$, existem $b,t \in \mathbb{Z}$ tais que $\bar{1} = \overline{ab+mt} = \overline{ab}+\overline{mt} = \overline{ab}+\bar{0} = \bar{a}\cdot\bar{b}$. Portanto $\bar{a}$ é invertível. □

Observe que para encontrar o inverso $\bar{\alpha}$ de $\bar{a}$ em $\mathbb{Z}_m$, temos a que resolver a equação

$$\bar{a}\cdot\bar{\alpha} = \bar{1},$$

que equivale a dizer que $a\cdot\alpha - 1$ é divisível por m. Isto é,

$$a\cdot\alpha + k\cdot m = 1$$

E para resolver essa equação e encontrarmos α podemos empregar o Algoritmo Euclidiano Estendido.

Exemplo 9. Vamos calcular o inverso multiplicativo de $\bar{3}$ em $\mathbb{Z}_{32}$. Note que tal número existe pois $mdc(3,32) = 1$. Usando o Algoritmo Euclidiano, escrevemos a cada etapa das divisões efetuadas o resto em termos do quociente, divisor e dividendo, ou seja, ao dividirmos a por b obtendo um quociente q e um resto r, escreveremos $r = a - bq$. Desse modo temos,

$$32 = 3 \cdot 10 + 2 \Rightarrow 2 = 32 - 3 \cdot 10,$$

$$3 = 2 \cdot 1 + 1 \Rightarrow 1 = 3 - 2 \cdot 1.$$

O próximo passo é, substituir a última expressão obtida para um resto, substituir nas expressões anteriores. Por exemplo,

$$1 = 3 - 2 \cdot 1,$$

$$1 = 3 - (32 - 3 \cdot 10) \cdot 1,$$

$$1 = 11 \cdot 3 - 32.$$

Logo, se reduzimos a módulo 32, temos $\overline{-32} = \bar{0}$. O que nos resta é $11 \cdot 3 \equiv 1$, que é equivalente a $\bar{3} \cdot \overline{11} = \bar{1}$, que nos diz que o inverso de 3 em $\mathbb{Z}_{32}$ é 11. O inverso de 3 em $\mathbb{Z}_{81}$, por exemplo, não existe, já que $mdc(3,81) = 3 \neq 1$.

Definição 4. O conjunto dos elementos de $\mathbb{Z}_m$ que tem inverso denotamos por

$$\mathscr{U}(m) = \{\bar{a} \in \mathbb{Z} \ : \ mdc(a,m) = 1\}.$$

Observação 4. $\mathscr{U}(p) = \mathbb{Z}_p \backslash \{\bar{0}\}$ quando p é primo.

Exemplo 10. Exemplo de classes inversíveis:

$$\mathscr{U}(4) = \{\bar{1}, \bar{3}\};$$

$$\mathscr{U}(8) = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\};$$

$$\mathscr{U}(11) = \{\bar{1}, \bar{2}, ..., \bar{9}, \bar{10}\}.$$

3.4.2.2 Divisões em $\mathbb{Z}_m$

Nesta seção veremos a operação de divisão em $\mathbb{Z}_m$. Nos reais, dividir a por b é equivalente a $a \cdot \frac{1}{b}$, sendo $\frac{1}{b}$ o inverso de b, e tal operação sempre está definida para $b \neq 0$.

De maneira similar, para dividir $\bar{a}$ por $\bar{b}$, é preciso saber se $\bar{b}$ possui inverso, ou seja, se $b \in \mathscr{U}(m)$.

Se $b \in \mathscr{U}(m)$, calculamos o inverso de $\bar{b}$ em $\mathbb{Z}_m$ (digamos β) e dividir $\bar{a}$ por $\bar{b}$, é calcular $\bar{a} \cdot \bar{\beta}$. Se b não possui inverso em $\mathbb{Z}_m$ então a divisão não está bem definida.

Exemplo 11. Vamos efetuar a divisão de $\bar{2}$ por $\bar{3}$ em $\mathbb{Z}_8$. Como $mdc(3,8) = 1$, então $\bar{3}$ tem inverso em $\mathbb{Z}_8$. Note que o fato de 2 não ter inverso em $\mathbb{Z}_8$ é importante pois 2 não é o divisor.

Observe que o inverso de $\bar{3}$ em $\mathbb{Z}_8$ é o próprio $\bar{3}$ (como se tratava de números pequenos encontramos o inverso por tentativa e erro, caso contrário poderíamos ter aplicado o Algoritmo Euclidiano Estentido para encontrar o inverso como fizemos anteriormente). Assim o resultado da divisão de $\bar{2}$ por $\bar{3}$ em $\mathbb{Z}_8$ é $\bar{6}$.

3.4.3 Congruência Linear

Toda equação da forma

$$ax \equiv b \bmod m, \text{ onde } (a,m) = 1,$$

é chamada de congruência linear. Para resolvê-la, encontramos o inverso de a (digamos α), assim

$$\alpha \cdot ax \equiv \alpha \cdot b \bmod m,$$

ou,

$$x \equiv \alpha \cdot b \bmod m.$$

Observação 5. Se $mdc(a,m) = 1$ então a congruência linear $ax \equiv b \bmod m$ tem uma, e uma só, solução em $\mathbb{Z}_m$.

Exemplo 12. Vamos resolver a congruência $7x \equiv 3 \bmod 15$.

Primeiramente precisamos multiplicá-la pelo inverso de $\overline{7}$ em $\mathbb{Z}_{15}$. Como $15 - 2 \cdot 7 = 1$, o inverso de $\overline{7}$ é $\overline{-2} = \overline{13}$. Multiplicando a congruência por 13, temos

$$x \equiv 13 \cdot 3 \equiv 39 \equiv 9 \mod 15$$

Voltaremos falar sobre congruência na seção 3.6, onde tratamos de algumas propriedades e inciamos o estudo de sistemas de congruências lineares.

3.5 Teorema de Fermat

O Teorema de Fermat é um resultado importante na Criptografia. Para estudá-lo necessitamos do lema a seguir.

Lema 3. (HEFEZ,) Seja p um número primo. Os números $\begin{pmatrix} p \\ i \end{pmatrix}$, onde $0 < i < p$, são todos divisíveis por p.

Demonstração. O resultado vale trivialmente para $i = 1$. Portanto, podemos supor que seja verdadeiro para $1 < i < p$. Neste caso, $i!|p(p-1)\cdots(p-i+1)$. Como $(i!, p) = 1$, decorre que $i!|(p-1)\cdots(p-i+1)$, e

$$\left(\begin{array}{c} p \\ i \end{array} \right) = p\frac{(p-1)\cdots(p-i+1)}{i!},$$

donde segue o lema. □

Teorema 5 (Pequeno Teorema de Fermat)**.** Seja p um número primo e a um número inteiro, então

$$a^p \equiv a \bmod p$$

Demonstração. Vamos mostrar o resultado para $a \geq 0$ e a prova é feita por indução sobre a. O resultado vale claramente para $a = 0$, pois $p|0$.

Supondo o resultado válido para a, iremos prová-lo para $a+1$. Pela fórmula do binômio de Newton, temos

$$(a+1)^p - (a+1) = a^p - a + \left(\begin{array}{c} p \\ 1 \end{array} \right) a^{p-1} + \cdots + \left(\begin{array}{c} p \\ p-1 \end{array} \right) a.$$

Pelo Lema 3 e a hipótese de indução, o segundo membro da igualdade acima é divisível por p. Logo o resultado segue. □

Segundo o teorema, se p é primo e a é um inteiro qualquer, então $a^p \equiv a \bmod p$. Se p não divide a, então a é inversível módulo p (pelo Teorema da Inversão). Seja a' um inteiro positvo tal que $aa' \equiv 1 \bmod p$. Multiplicando ambos os lados da igualdade de $a^p \equiv a \bmod p$ por a' obtemos

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

Substituindo $a'a \equiv 1 \bmod p$ nesta equação, ficamos com

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

esta é a nova versão do Teorema de Fermat.

Teorema 6 (Pequeno Teorema de Fermat - II)**.** Seja p um número primo e a um inteiro que não é divisível por p. Então $a^{p-1} \equiv 1 \bmod p$.

3.6 Sistemas de Congruências

Nesta seção vamos estudar como resolver congruências lineares ou sistemas de congruências.

3.6.1 Equações Lineares

Dada a equação

$$ax \equiv b \bmod m,\ m \in \mathbb{Z}, \tag{3.3}$$

já discutimos anteriormente que esse tipo de equação "é fácil de resolver" se $\bar{a}$ é invertível em $\mathbb{Z}_m$. Em particular, se m é primo e $a \not\equiv 0 \bmod m$ então (3.3) sempre tem solução. Se $\bar{a}$ não tem inverso em $\mathbb{Z}_m$, o problema se torna mais complicado. Dizer que $\bar{a}$ não tem inverso em $\mathbb{Z}_m$ é equivalente a dizer que $mdc(a,m) \neq 1$.

Se a equação (3.3) tem solução, isto é, existem $x, y \in \mathbb{Z}$ tal que

$$ax - my = b,$$

então o $mdc(a,m)$ divide b.

Proposição 7. A equação (3.3) tem solução se e somente, se b é divisível pelo $mdc(a,m)$.

Demonstração. De fato, seja a equação

$$ax - my = b \tag{3.4}$$

e suponha que $d = mdc(a,m)$ divide b, ou seja, $b = d \cdot b'$, $a = d \cdot a'$ e $m = d \cdot m'$. Substituindo em (3.4) temos

$$a'dx - dm'y = db',$$

$$a'x - m'y = b'.$$

ou seja,

$$a'x \equiv b' \bmod m'.$$

Por outro lado, observe que $mdc(a', m') = 1$, portanto a nova equação tem solução. □

Note que neste caso o módulo mudou, e para encontrar a solução da primeira equação temos que retornar ao módulo m, e dessa forma encontrar a solução, isso em algumas vezes se torna um empecilho. O próximo exemplo mostra que pode ocorrer quando mudamos o módulo de uma equação.

Exemplo 13. Encontre a solução da seguinte equação

$$6x \equiv 4 \bmod 8. \tag{3.5}$$

Observe que $mdc(6,8) = 2 \neq 1$, portanto $\bar{6}$ não possui inverso em $\mathbb{Z}_8$. Então podemos escrever a equação (3.5) da forma

$$6x - 8y = 4, \quad \Leftrightarrow \quad 3x - 4y = 2.$$

Como $3x \equiv 2 \bmod 4$ ($\bar{3}$ é seu próprio inverso em $\mathbb{Z}_4$,) segue que

$$x \equiv 2 \bmod 4. \tag{3.6}$$

Mas observe que (3.6) está em $\mathbb{Z}_4$, assim temos que reescrevê-la em $\mathbb{Z}_8$. Podemos escrever

$$x = 2 + 4k, \;\; k \in \mathbb{Z}$$

Assim temos duas possibilidades para k.

- Se k par $(k = 2n)$ então $x \equiv 2 \bmod 8$ é uma solução
- Se k ímpar $(k = 2n+1)$ então $x = 6 + 8n$, isto é, $x \equiv 6 \bmod 8$.

Dessa forma a equação $6x \equiv 4 \bmod 8$ tem duas soluções.

3.6.2 Teorema Chinês do Resto

Nessa seção veremos como calcular um inteiro que satisfaz simultanenamente a várias congruências com módulos distintos: o resultado é conhecido como Algoritmo Chinês do Resto. Iniciamos a introdução desse algoritmo através de exemplo. Basicamente utilizamos várias substituições para resolver o sistema de congruências.

Exemplo 14. Determine o menor inteiro positivo que deixa resto 1 na divisão por 3 e resto 2 na divisão por 5.

Observe que podemos escrever o problema da seguinte forma:

$$x \equiv 1 \bmod 3,$$

$$x \equiv 2 \bmod 5.$$

Além disso, temos que $x = 3q + 1$, $q \in \mathbb{Z}$ e substituindo na segunda congruência obtemos;

$$3q + 1 \equiv 2 \bmod 5.$$

Subtraindo 1 dos dois lados da congruência chegamos a

$$3q \equiv 1 \bmod 5$$

Multiplicando a congruência por 2 temos

$$6q \equiv 2 \bmod 5.$$

Veja que $6 \equiv 1 \bmod 5$, e então

$$q \equiv 2 \bmod 5, \quad \text{ou seja} \quad q = 5k + 2, \;\; k \in \mathbb{Z}.$$

Substituindo em $x = 3q + 1$, concluímos que

$$x = 3(5k+2)+1 \quad \text{ou ainda} \quad x = 15k+7.$$

Observe, contudo, que o resultado obtido não é uma solução, mas sim uma família de soluções. De fato, obtemos uma solução diferente para cada valor inteiro k fixado.

O próximo exemplo trata de um sistema de três congruências, a forma de resolver será semelhante ao exemplo anterior.

Exemplo 15. (ENQ-2016..., 2016) A secretaria de educação de um município recebeu uma certa quantidade de livros para distribuir entre as escolas do município. Sabe-se que a quantidade é superior a 1000, inferior a 2000, que se dividi-lo entre 7 escolas sobram 4, entre 9 sobram 2 e entre 6 sobram 6. Encontre a quantidade de livros.

Seja x a quantidade de livros recebida pela secretaria. Temos que x deve satisfazer as seguintes equações.

$$\begin{aligned}(i)\, x &\equiv 4 \mod 7,\\ (ii)\, x &\equiv 2 \mod 9,\\ (iii)\, x &\equiv 6 \mod 13.\end{aligned}$$

Por *(i)* segue que $x = 7k+4$, $k \in \mathbb{Z}$. Substituindo em *(ii)* vemos que $7k+4 \equiv 2 \mod 9$, somando 5 de ambos os lados temos $7k \equiv 7 \mod 9$, ou seja, $k \equiv 1 \mod 9$. Logo, $k = 9n+1$ e assim $x = 7k+4 = 7(9n+1)+4 = 63n+11$. Colocando essa informação na terceira equação segue que $63n+11 \equiv 6 \mod 13$. Isso implica que $11n \equiv 8 \mod 13$. Multiplicando essa equação por 6 temos que $66n \equiv 48 \mod 13$, ou seja, $n \equiv 9 \mod 13$. Assim segue que $n = 13t+9$ e $x = 63n+11 = 63(13t+9)+11 = 819t+518$, com $t \in \mathbb{Z}$ que é a solução geral do problema.

Observe que nesse caso temos a restrição, $1000 < x < 2000$, dessa forma concluímos que nossa solução vale apenas para $t = 1$ e a resposta é "A secretaria de educação recebeu 1397 livros para serem distribuídos".

Exemplo 16. (PROFMAT-AV3-ARITMETICA, 2011) Quando um macaco sobe uma escada de dois em dois degraus, sobra um degrau, quando sobe de três em três degraus, sobram dois degraus e quando sobe de cinco em cinco degraus, sobram três degraus. Quantos degraus possui a escada, sabendo que o número de degraus está entre 150 e 200?

Seja o número x de degraus. Temos que x é a solução do seguinte sistema

$$\begin{aligned}(i)\, x &\equiv 1 \mod 2,\\ (ii)\, x &\equiv 2 \mod 3,\\ (iii)\, x &\equiv 3 \mod 5.\end{aligned}$$

De *(i)* $x = 2k+1$, $k \in \mathbb{Z}$. Substituindo em *(ii)* temos que $2k+1 \equiv 2 \mod 3$. Subtraindo uma unidade de ambos os lados temos $2k \equiv 1 \mod 3$. Multiplicando essa equação por 2 temos que

$4k \equiv 2 \bmod 3$, ou seja, $k \equiv 2 \bmod 3$. Logo, $k = 3n+2$ e assim $x = 2k+1 = 2(3n+2)+1 = 6n+5$. Colocando essa informação em *(iii)* segue que $6n+5 \equiv 3 \bmod 5$, ou seja, $n \equiv 3 \bmod 5$. Assim segue que $n = 5t+3$ e $x = 6n+5 = 6(5t+3)+5 = 30t+23$, com $t \in \mathbb{Z}$ é a solução geral do problema.

Observe que nesse caso temos a restrição, $150 < x < 200$, dessa forma concluímos que nossa solução vale apenas para $t = 5$ e a resposta é "A escada tem 173 degraus".

O *Algoritmo Chinês do Resto* apenas sistematiza o resultado final do método utilizado nos problemas anteriores. Vamos enunciar o teorema e analisá-lo com mais cuidado.

Teorema 8 (Teorema Chinês do Resto)**.** (COUTINHO, 1997) Sejam m e n inteiros positivos primos entre si. Se a e b são inteiros quaisquer, então o sistema

$$x \equiv a \bmod m,$$

$$x \equiv b \bmod n,$$

admite uma solução x. Além disso, a solução é única em $\mathbb{Z}_{mn}$.

Demonstração. Considere o sistema

$$x \equiv a \bmod m \tag{3.7}$$

$$x \equiv b \bmod n \tag{3.8}$$

Vamos reescrever (3.7) na forma $x = a+my$, onde y é um inteiro qualquer. Substituindo o resultado de (3.7) em (3.8) obtemos $a+my \equiv b \bmod n$, ou ainda

$$my \equiv b-a \mod n \tag{3.9}$$

Além disso, $mdc(m,n) = 1$, isto é, $\overline{m}$ tem inverso em $\mathbb{Z}_n$. Chamando de $\bar{\alpha}$ o inverso de m em $\mathbb{Z}_n$, a solução da equação (3.9) é $y \equiv \alpha(b-a) \bmod$ n. Isto é, $y = \alpha(b-a)+nz$, onde z é um número inteiro. Substituindo na equação (3.7), temos

$$x = a+m\alpha(b-a)+mnz$$

Ou seja, para todo z, o número inteiro $a+m\alpha(b-a)+mnz$ é solução do nosso sistema proposto. Resta mostrar que esta solução é única em $\mathbb{Z}_{mn}$. Suponha que são x e y duas soluções do sistema. Então

$$x \equiv a \bmod m,$$

$$y \equiv b \bmod m.$$

Subtraindo uma equação da outra, encontramos $x-y \equiv 0 \bmod m$, ou seja, $x-y \equiv 0 \bmod n$.

Como $mdc(m,n) = 1$, temos que $m \cdot n$ divide $x-y$. Logo se x e y são soluções do sistema então $x \equiv y \bmod mn$. Ou seja, o sistema possui uma única solução em $\mathbb{Z}_{mn}$. □

No caso desse teorema, o sistema é composto de duas equações, porém de maneira análoga é possível generalizá-lo. Vamos enunciar o resultado geral.

Teorema 9. Sejam $n_1, \ldots, n_k$ inteiros positivos dois a dois primos entre si. Então o sistema

$$\begin{aligned} x &\equiv a_1 \bmod n_1, \\ x &\equiv a_2 \bmod n_2, \\ &\vdots \\ x &\equiv a_k \bmod n_k. \end{aligned}$$

tem uma única solução em $\mathbb{Z}_{n_1 \ldots n_k}$.

3.7 Grupos

3.7.1 Definição e exemplos

Definição 5. Seja G um conjunto não vazio e seja $*$ uma operação em G. O par $(G, *)$ é um grupo se satisfaz as seguintes propriedades:

(i) Associativa: dados, $a, b, c \in G$ temos que

$$a * (b * c) = (a * b) * c.$$

(ii) Elemento neutro: existe $e \in G$ tal que para todo $g \in G$ temos

$$g * e = e * g = g.$$

(iii) Elemento inverso: dado um elemento $g \in G$ qualquer, existe um elemento $g' \in G$ (inverso de g), tal que

$$g * g' = g' * g = e.$$

Exemplo 17.

1. $(\mathbb{N}, +)$ não é um grupo, pois dado $n \in \mathbb{N}$, com $n \geq 1$ não possui inverso na adição em $\mathbb{N}$.
2. $(\mathbb{Z}, +)$ é um grupo onde o elemento neutro é o 0 e o elemento oposto da adição para cada $a \in \mathbb{Z}$ é o seu oposto $-a$.
3. $(\mathbb{Z}, \cdot)$ não é um grupo, pois $a \in \mathbb{Z}, a \neq 1$ não admite inverso em $\mathbb{Z}$.
4. $(\mathbb{Z}_n, +)$ é um grupo de elemento neutro $\bar{0}$, e o elemento inverso de $\bar{a} \in \mathbb{Z}_n$ é $\overline{-a}$.
5. $(\mathbb{R}, +)$ é um grupo.
6. $(\mathbb{R} - \{0\}, \cdot)$ é um grupo.

Definição 6 (Ordem de um grupo)**.** Sendo $(G;*)$ um grupo, dizemos que a ordem de G é igual a n, se G é um conjunto finito de n elementos. Se o conjunto G possui infinitos elementos então sua ordem será infinita.

Quase todos grupos que destacamos acima possuem ordem infinta, o único exemplo que vimos de grupo finito é $\mathbb{Z}_n$ com a soma; este grupo tem ordem n.

3.7.2 Grupos Aritméticos

Como vimos anteriormente, denotamos por $\mathscr{U}(n)$ o conjunto dos elementos inversíveis de $\mathbb{Z}_n$, ou seja,

$$\mathscr{U}(n) = \{\bar{a} \in \mathbb{Z}_n;\ mdc(a,n) = 1\}.$$

Afirmamos que $\mathscr{U}(n)$ é um grupo em relação à multiplicação de classes de $\mathbb{Z}_n$. De fato, a operação $(\cdot)$ está bem definida em $\mathscr{U}(n)$, ou seja, o produto de dois elementos de $\mathscr{U}(n)$ é um elemento de $\mathscr{U}(n)$. Sejam $\bar{a}$ e $\bar{b} \in \mathscr{U}(n)$ e seus inversos $\bar{a'}$ e $\bar{b'}$. Então temos,

$$\overline{ab} \cdot \overline{a'b'} = \overline{aa'} \cdot \overline{bb'} = \bar{1},$$

ou seja, no conjunto $\mathscr{U}(n)$ está bem definida a operação produto de classes. Resta agora verificar que $(\cdot)$ satisfaz as propriedades de grupo. A propriedade associatividade segue facilmente em $\mathbb{Z}_n$, o elemento neutro é $\bar{1}$ que pertence a $\mathscr{U}(n)$, e segue da própria definição de $\mathscr{U}(n)$ que cada elemento desse conjunto possui inverso.

3.7.3 Função ϕ de Euler (Ordem de $\mathscr{U}(n)$)

Definição 7. A função ϕ de Euler associa a cada elemento em $n \in \mathbb{N}$ o número de elementos de $\mathscr{U}(n)$, ou seja, a quantidade de números naturais entre 0 e $n-1$ que são primos com n.

Denotando a ordem de $\mathscr{U}(n)$ por $\phi(n)$, vamos calcular ϕ. Primeiro começaremos por um caso mais trivial.

Proposição 7. Sendo p um número primo e k um número natural, temos que $\phi(p^k) = p^k - p^{k-1}$.

Demonstração. $\phi(p^k)$ é o número de números naturais menores que p^k que são primos com p^k. Como p é primo, os números naturais que não são primos com p^k são aqueles que tem p como divisor, ou seja, p, $2p$, $3p$, $\ldots$ $p^{k-1}p$. Assim temos p^{k-1} números que são divisíveis por p menores que p^k. Logo existem $p^k - p^{k-1}$ números que não são divisíveis por p. Isto é,

$$\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1).$$

□

Corolário 4. Se p é um número primo então $\phi(p) = p-1$.

Demonstração. Segue imediatamente de proposição anterior, tomando $k = 1$. □

Observação 6. Note que $(t, m\cdot m') = 1$ se, e somente se, $(t,m') = (t,m) = 1$: De fato, $(t,m\cdot m') = 1$ implica que existem $a,b \in \mathbb{Z}$ tais que $at + bmm' = 1$, logo $at + (bm)m' = 1$ e $at + (bm')m = 1$, o que implica $(t,m) = 1$ e $(t,m') = 1$. Reciprocamente, se $(t,m) = (t,m') = 1$, segue que $(t,mm') = (t,m') = 1$.

Teorema 10. (HEFEZ, 2010) Se m, n são inteiros positivos tais que $mdc(m,n) = 1$, então

$$\phi(mn) = \phi(m)\phi(n).$$

Demonstração. Considere a seguinte tabela formada pelos números naturais de 1 a $m\cdot m'$:

$$\begin{array}{ccccccc} 1 & 2 & \dots & k & \dots & m' \\ m'+1 & m'+2 & \dots & m'+k & \dots & 2m' \\ \vdots & \vdots & & \vdots & & \vdots \\ (m-1)m'+1 & (m-1)m'+2 & \dots & (m-1)m'+k & \dots & m\cdot m' \end{array}$$

Segue da observação acima que $(t, m\cdot m') = 1$ se, e somente se, $(t,m') = (t,m) = 1$, asiim para calcular $\phi(m\cdot m')$, devemos determinar os inteiros na tabela acima que são simultaneamente primos com m e m'.

Se o primeiro elemento de uma coluna não for primo com m' então todos os elementos da coluna também não são primos com m'. Portanto, os elementos primos com m' estão necessariamente nas colunas restantes que são em número $\phi(m')$, cujos elementos são primos com m'. Vejamos agora quais são os elementos primos com m em cada uma dessas colunas.

Como $(m,m') = 1$, a sequência

$$k, m'+k, \dots, (m-1)m'+k,$$

forma um sistema completo de resíduos módulo m (veja Proposição 6) e, portanto $\phi(m)$ desses elementos são primos com m. Logo, o número de elementos simultaneamente primos com m' e m é $\phi(m)\cdot\phi(m')$. □

Teorema 11. Se $n = p_1^{e_1}\dots p_k^{e_k}$ é a decomposição de n em fatores primos, então

$$\phi(n) = p_1^{e_1}\dots p_k^{e_k}\left(1-\frac{1}{p_1}\right)\dots\left(1-\frac{1}{p_k}\right).$$

Demonstração. Pelo Teorema 10 temos,

$$\phi(n) = \phi(p_1^{e_1})\dots\phi(p_k^{e_k}).$$

E pela Proposição 7, onde utilizamos o cálculo de ϕ para potências de primos, encontramos

$$\phi(n) = p_1^{e_1-1} \dots p_k^{e_k-1}(p_1-1)(p_k-1),$$

como queríamos. □

Exemplo 18. Vamos calcular $\phi(120)$. Temos que $120 = 2^3 \cdot 3 \cdot 5$, assim

$$\phi(120) = 2^3 \cdot 3 \cdot 5 \left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right) = 32$$

3.7.4 Subgrupos

Definição 8. (SAMPAIO, 2008) Sejam G um grupo e H um subconjunto de G. Dizemos que H é um subgrupo de G se:

- Para todo $a, b \in H$ temos $a * b \in H$.
- O elemento neutro de G está em H.
- Para todo $a \in H$, seu inverso a' também está em H.

Observação 7. Qualquer grupo tem pelo menos dois subgrupos: o próprio grupo e o subgrupo formado apenas pelo elemento neutro.

Exemplo 19.

- $(\mathbb{Q}^*, \cdot)$ é um subgrupo de $(\mathbb{R}^*, \cdot)$;
- $(\mathbb{Z}, +)$ é um subgrupo de $(\mathbb{Q}, +)$;
- $(\mathbb{N}, \cdot)$ não é um subgrupo de $(\mathbb{Q}^*, \cdot)$ pois não contém todos os inversos de seus elementos.

CAPÍTULO

4

A CRIPTOGRAFIA RSA

Nesse capítulo descrevemos o processo da Criptografia RSA, ou seja, explicitamos como codificar e decodificar uma mensagem utilizando esse método. Além disso, verificamos que uma vez a mensagem codificada sempre conseguimos retornar a mensagem original. Encerramos o capítulo tratando brevemente sobre a segurança do processo.

Vale destacar novamente que a Criptografia RSA é composta de duas chaves: a pública e a privada, onde a chave pública (chave de codificação) é de conhecimento de todos e a chave privada (chave de decodificação) é mantida em sigilo. Dessa forma só é possível decifrar a mensagem usando a respectiva chave privada do processo de codificação. Na Criptografia RSA o uso das chaves deve obedecer a seguinte regra:

- Chave pública: a forma de criptografia é passada publicamente, para diversas pessoas, porém a maneira de descriptografá-las fica apenas com a pessoa que criou a chave.

- Chave privada: o criador é o único que sabe como codificar e decodificar, somente poderão ler ou esconder a informação a quem ele passar as instruções para fazê-lo.

Iremos então detalhar o processo para gerar e utilizar o par de chaves acima citado.

4.1 Pré-codificação

A primeira coisa a fazer se desejamos usar o método RSA é converter a mensagem em uma sequência de números.

Para simplificar suponha que na mensagem há apenas palavras. Essa primeira etapa é chamada de pré-codificação. Na pré-codificação convertemos as letras em números usando a seguinte tabela de conversão:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

R	S	T	U	V	W	X	Y	Z
27	28	29	30	31	32	33	34	35

O espaço entre duas palavras será substituído pelo número 99. Primeiramente para codificar uma mensagem no sistema RSA precisamos determinar os parâmetros. Estes parâmetros são dois primos distintos, que vamos denotar por p e q. Seja $n = p \cdot q$.

Após converter a mensagem em números, a última fase da pré-codificação consiste em quebrar a mensagem em blocos. Estes blocos devem ser números menores do que n. Para exemplificar esse processo de codificação, utilizamos a seguinte frase:

MATEMÁTICA É LEGAL

Utilizando a tabela de números para conversão temos:

22102914221029181210991499211416102l

Se escolhermos os números $p = 13$ e $q = 17$, então $n = 221$. Neste caso a mensagem acima pode ser quebrada em blocos cujo número formado seja menor que 221, uma possibilidade é a seguinte

22-10-29-142-210-29-181-210-99-149-92-114-16-10-21.

Observação 8. A maneira de escolher os blocos não é única, ou seja, há várias formas de pré-codificar a mensagem, e quando decodificarmos a mensagem original será a mesma. Alguns cuidados devem ser tomados na pré-codificação, como por exemplo não iniciar um bloco com 0, pois isso nos traria problemas na decodificação, uma vez que faltariam letras. Além disso é interessante que tomemos blocos diferentes daquele que formamos quando fizemos a pré-codificação, para tornar a mensagem mais difícil de ser decodificada.

Note que para este exemplo a escolha para o primeiro bloco foi 22. Não poderíamos ter escolhido o primeiro bloco como 221, mas poderíamos escolhê-lo como 2. Se o primeiro bloco fosse o 2, o segundo seria necessariamente 210, para evitar que o terceiro bloco começasse com zero.

4.2 Codificação

Para codificar a mensagem precisamos de n, que é o produto de primos, e de um inteiro positivo e que seja inversível módulo $\phi(n)$. Em outras palavras, $mdc(e, \phi(n)) = 1$. Lembremos que se conhecemos p e q, então $\phi(n) = (p-1)(q-1)$. Chamaremos o par (n, e) de chave de

codificação do sistema RSA que estamos usando. Uma vez que a mensagem foi pré-codificada temos uma sequência de números ou blocos. Codificarmos cada bloco separadamente, e a mensagem será a sequência de blocos codificados.

Dada a chave de codificação (n,e), para codificar um bloco b (lembre-se que $b \in \mathbb{Z}_+$ e é menor que n), vamos fazer o seguinte. Denotando o bloco codificado por $C(b)$. Temos que $C(b)$ é resto da divisão de b^e por n. Em termos de Aritmética modular, $C(b)$ é a forma reduzida de b^e módulo n.

Voltando ao exemplo que estamos considerando, temos $p = 13$ e $q = 17$, logo $n = 221$ e $\phi(n) = (13-1)(17-1) = 192$. Para este exemplo, podemos tomar $e = 5$. Assim o bloco 22 da mensagem é codificado como o resto da divisão de 22^5 por 221. Verificamos que $22^5 \equiv 133 \bmod 221$, por meio de técnicas de aritmética modular e fazendo uso de calculadora eletrônica.

Utilizamos o mesmo raciocínio codificamos toda mensagem e obtemos a seguinte sequência de blocos.

133-108-139-194-58-139-129-58-216-132-79-173-152-108-21.

4.2.1 Decodificação

A informação que precisamos para decodificar a mensagem consiste de dois números: n e o inverso de e em $\phi(n)$, que denotamos por d. Chamamos o par (n,d) de chave de decodificação.

Seja a um bloco de mensagem codificada, então $D(a)$ será o resultado do processo de decodificação e temos que $D(a)$ = resto da divisão de a^d por n. Em aritmética modular, $D(a)$ é a forma reduzida de a^d módulo n. Assim, para decodificar precisamos conhecer o n e o inverso d de e módulo $\phi(n)$.

Em nosso exemplo, temos que $n = 221$ e $e = 5$. Aplicando o Algoritmo Euclidiano Estendido para calcular d, temos:

$$\begin{aligned} 192 &= 5 \cdot 38 + 2, \\ 5 &= 2 \cdot 2 + 1, \end{aligned}$$

Ou ainda,

$$\begin{aligned} 1 &= 5 - 2 \cdot 2, \\ 1 &= 5 - 2(192 - 5 \cdot 38), \\ 1 &= 5 \cdot 77 - 2 \cdot 192. \end{aligned}$$

Logo o inverso de 5 módulo 192 é 77. Assim para decodificar o bloco 133 da mensagem codificada, calculamos 133^{77} módulo 221, e verificamos que $133^{77} \equiv 22$ módulo 221. Observe

que não precisamos conhecer p e q, apenas n e d. E assim, sucessivamente retornamos mensagem a original.

4.3 Por que funciona?

Digamos que temos um sistema RSA de parâmetros p e q com $n = p \cdot q$. Então temos os seguintes dados:

- chave de codificação (chave pública): (n, e),
- chave de decodificação (chave privada): (n, d).

Sendo assim, para mostrar a eficiência do uso de mensagens criptografadas precisamos garantir que nas condições acima a mensagem recebida, quando decodificada, será exatamente igual a mensagem original. Isto equivalente a verificar que se b (bloco gerado na pré-codificação) é um inteiro tal que $1 \leqslant b \leqslant n-1$ então $D(C(b)) = b$, ou seja, $DC(b) \equiv b \bmod n$. Fazendo uso do Teorema de Fermat vamos mostrar que esta igualdade é verificada.

Teorema 12. Seja o par (n, e) a chave de codificação e o par (n, d) a chave de decodificação do sistema RSA. Então $DC(b) \equiv b \bmod n$, para todo inteiro b, com $1 \leqslant b \leqslant n-1$.

Demonstração. De fato, segue da definição de D e C que

$$DC(b) \equiv (b^e)^d \equiv b^{ed} \bmod n. \tag{4.1}$$

Porém d é o inverso de e módulo $\phi(n)$, logo $ed = 1 + k\phi(n)$, para algum inteiro k. Observe ainda que, como e e d são inteiros maiores que 2 e $\phi(n) > 0$, então $k > 0$. Sendo assim temos que

$$b^{ed} \equiv b^{1+k\phi(n)} \bmod n.$$

Como $n = p \cdot q$ (p e q primos) calculamos b^{ed} módulo p e q. Veja que

$$ed = 1 + k\phi(n) = 1 + k(p-1)(q-1),$$

logo,

$$b^{ed} \equiv b \cdot \left(b^{(p-1)}\right)^{k(q-1)} \bmod p.$$

Dessa forma temos dois casos a considerar.

(i) Se p não divide b, então pelo Teorema de Fermat, $b^{p-1} \equiv 1 \bmod p$ então

$$b^{ed} \equiv b \bmod p.$$

(ii) Se p divide b o fato de p ser primo, nos leva a conclusão que $b \equiv 0 \bmod p$ e a congruência é facilmente verificada.

Assim, $b^{ed} \equiv b \bmod p$ se verifica para qualquer b. Analogamente, podemos mostrar que $b^{ed} \equiv b \bmod q$. Em outras palavras, $b^{ed} - b$ é divisível por p e por q. Como $mdc(p,q) = 1$, temos que $p \cdot q$ divide $b^{ed} - b$ pelo Lema 2. Dessa forma, como $n = p \cdot q$, concluímos que $b^{ed} \equiv b \bmod n$, para todo número inteiro b. □

Segue do resultado acima a eficiência do processo de codificação e decodificação, ou seja, a mensagem decodificada por meio deste processo será idêntica a mensagem encaminhada originalmente, sem qualquer perda de informações.

4.4 A segurança do RSA

Apesar de todo avanço tecnológico e de inúmeras tentativas teóricas e algorítmicas, até hoje não existe um método eficiente para determinar a fatoração em primos de um número inteiro muito grande. A falta deste processo eficiente é que torna a Criptografia RSA segura.

Lembramos que no processo da Criptografia RSA precisamos conhecer p e q primos tais que $n = pq$. Sem p e q não conseguimos calcular $\phi(n) = (p-1)(q-1)$. Apesar da chave pública (n,e) ser conhecida, para encontrarmos d, a chave de decodificação, precisamos aplicar o Algoritmo Euclidiano Estendido a $\phi(n)$ e e, tarefa impossível sem conhecermos p e q.

CAPÍTULO

5

CRIPTOGRAFIA EM SALA DE AULA

Nesse capítulo descreveremos a atividade aplicada aos alunos de uma segunda série do Ensino Médio. O objetivo da atividade foi introduzir a noção de criptografia e como ela é importante em nosso dia a dia. Vale destacar que nesse caso não foi utilizada a Criptografia RSA.

5.1 Atividade

A Atividade foi adaptada do livro (DANTE, 2018). Trabalhou-se a ideia de matrizes com criptografia. Num primeiro momento pensávamos em trabalhar superficialmente a teoria dessa dissertação e depois aplicarmos uma atividade direcionada a isso. Porém essa programação demandaria várias aulas e a docente temia atrapalhar os conteúdos programados daquele ano. Dessa forma, optou-se por uso de outro método mais simples através de tabela, porém que engloba-se os principais conceitos da criptografia.

5.2 Plano de aula

Identificação: Atividade prática de Matemática

Prof. Evelyn Gomes da Silva

Etec Paulino Botelho

Série: 2 ano do ensino médio

Tema: Matrizes e Criptografia

Situação problema: Codificar e decodificar uma mensagem usando matrizes e introduzir a noção de criptografia.

Objetivos específicos: Trabalhar a ideia de criptografia através de matrizes.

Conceitos-chave: Matriz. Matriz Inversa. Criptografia.

Conhecimentos prévios: matrizes, matriz inversa e multiplicação de matrizes.

Recursos necessários: Lousa e giz.

Tempo: 2 h/aulas(1h40min)

Avaliação: Envolvimento na atividade e cooperação.

Procedimentos:

- Explicar sobre a importância da criptografia no nosso cotidiano, como por exemplo em compras on-line e mensagens de whatsapp. É importante destacar como funciona a criptografia nesse processo;

- Mostrar um exemplo que está contido no livro (DANTE, 2018), pag.82.

  Tomamos uma matriz A inversível (a matriz A pode ser qualquer desde que inversível), por exemplo $A = \begin{pmatrix} 3 & 1 \\ 2 & 3 \end{pmatrix}$ e a tabela

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
1	2	3	4	5	6	7	8	9	10	12	13	14	15	16	17	18

R	S	T	U	V	W	X	Y	Z	.
19	20	21	22	23	24	25	26	27	28

Suponhamos que a mensagem que vamos transmitir seja:

MATEMÁTICA É LEGAL

De acordo com a tabela numérica temos: 14-1-21-5-14-1-21-9-3-1-28-5-28-13-5-7-1-13 (substituímos espaços por ·).

Arrumamos a sequência de números numa matriz de duas linhas M:

$$M = \begin{pmatrix} 14 & 1 & 21 & 5 & 14 & 1 & 21 & 9 & 3 \\ 1 & 28 & 5 & 28 & 13 & 5 & 7 & 1 & 13 \end{pmatrix}$$

Utilizamos a matriz A para codificar a mensagem e fazemos N=A·M, desse modo obtemos a seguinte matriz:

$$N = \begin{pmatrix} 43 & 31 & 68 & 43 & 55 & 8 & 70 & 28 & 22 \\ 31 & 86 & 57 & 94 & 67 & 17 & 63 & 21 & 45 \end{pmatrix}$$

Os elementos de N constituem a mensagem codificada: 43-31-68-43-55-8-70-28-22-31-86-57-94-67-17-63-21-45.

Para realizar a decodificação necessitamos da matriz inversa de A (A^{-1}), a matriz $B = \begin{pmatrix} \frac{3}{7} & \frac{-1}{7} \\ \frac{-2}{7} & \frac{3}{7} \end{pmatrix}$ e procedemos da seguinte forma:

$$B \cdot N = \begin{pmatrix} \frac{3}{7} & \frac{-1}{7} \\ \frac{-2}{7} & \frac{3}{7} \end{pmatrix} \cdot \begin{pmatrix} 43 & 31 & 68 & 43 & 55 & 8 & 70 & 28 & 22 \\ 31 & 86 & 57 & 94 & 67 & 17 & 63 & 21 & 45 \end{pmatrix} =$$

$$= \begin{pmatrix} 14 & 1 & 21 & 5 & 14 & 1 & 21 & 9 & 3 \\ 1 & 28 & 5 & 28 & 13 & 5 & 7 & 1 & 13 \end{pmatrix} = M$$

Os elementos da matriz M obtida formam a sequência de números: 14-1-21-5-14-1-21-9-3-1-28-5-28-13-5-7-1-13, cuja decodificação é:

M	A	T	E	M	A	T	I	C	A	·	E	·	L	E	G	A	L
14	1	21	5	14	1	21	9	3	1	28	5	28	13	5	7	1	13

- Demonstrar porque funciona: $B \cdot \underbrace{N}_{A \cdot M} = \underbrace{B \cdot A}_{I} \cdot M = I \cdot M = M$;
- Foram separados grupos de 5 alunos, a atividade foi elaborada em 2 etapas:

  1ªEtapa: Os alunos escolhereram palavras com 8 letras ou mais e determinaram uma matriz e sua inversa. Em seguida realizaram as operações necessárias para determinar a matriz codificada. Numa folha os alunos colocaram a matriz A e a matriz codificada.

  2ªEtapa: Foram entregues para os grupos a atividade da 1ª etapa, esses por sua vez deviam encontrar a matriz inversa e realizar a multiplicação com a matriz N e por fim encontrar a original.

5.3 Ocorrências da atividade

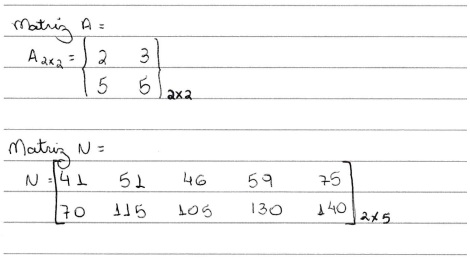
No geral a atividade ocorreu como planejada. Na primerira etapa alguns alunos tiveram dificuldades para encontrar a inversa da matriz, mas quando a professora interviu ocorreu normalmente. A segunda etapa houve mais dificuldades, pois alguns alunos não construíram a matriz M corretamente, o que impossibilitou os alunos do outro grupo encontrar a mensagem codificada.

Contudo, o objetivo geral foi alcançado, pois os alunos mostraram interesse pela criptografia e houve envolvimento de todos os alunos.

5.4 Anexos

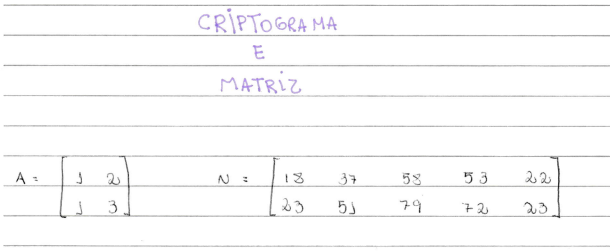
Seguem abaixo as atividades realizadas pelos alunos:

Figura 1 – Grupo 1



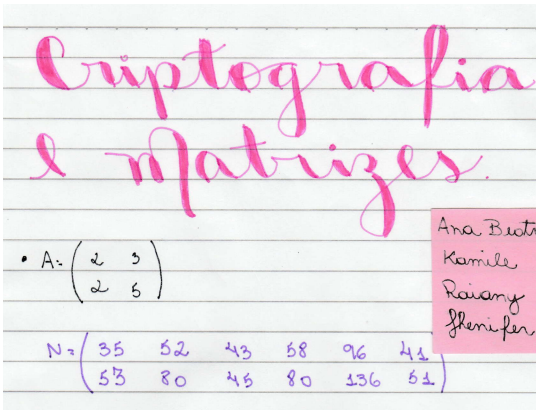
Fonte: Elaborada pelo autor.

Figura 2 – Grupo 2



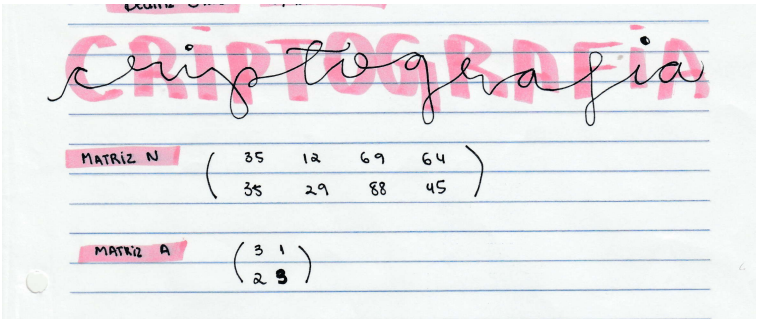
Fonte: Elaborada pelo autor.

Figura 3 – Grupo 3



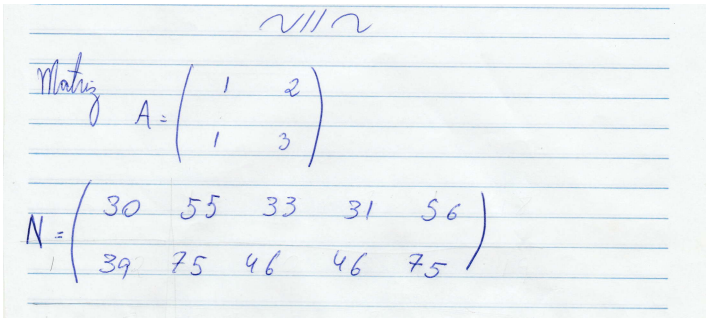
Fonte: Elaborada pelo autor.

Figura 4 – Grupo 4



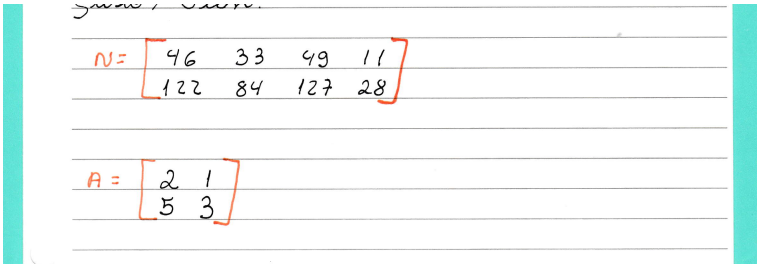
Fonte: Elaborada pelo autor.

Figura 5 – Grupo 5



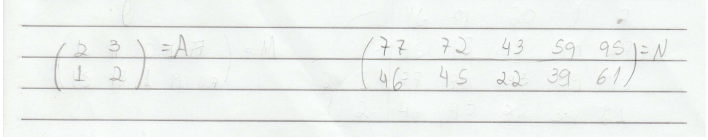
Fonte: Elaborada pelo autor.

Figura 6 – Grupo 5



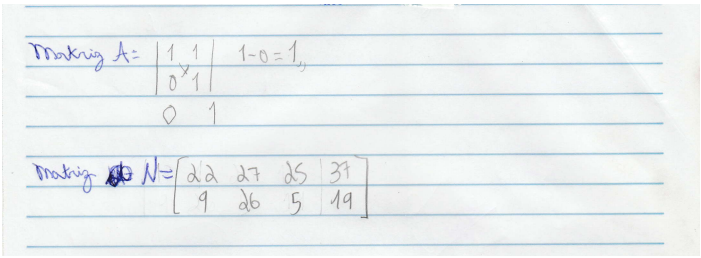
Fonte: Elaborada pelo autor.

Figura 7 – Grupo 5



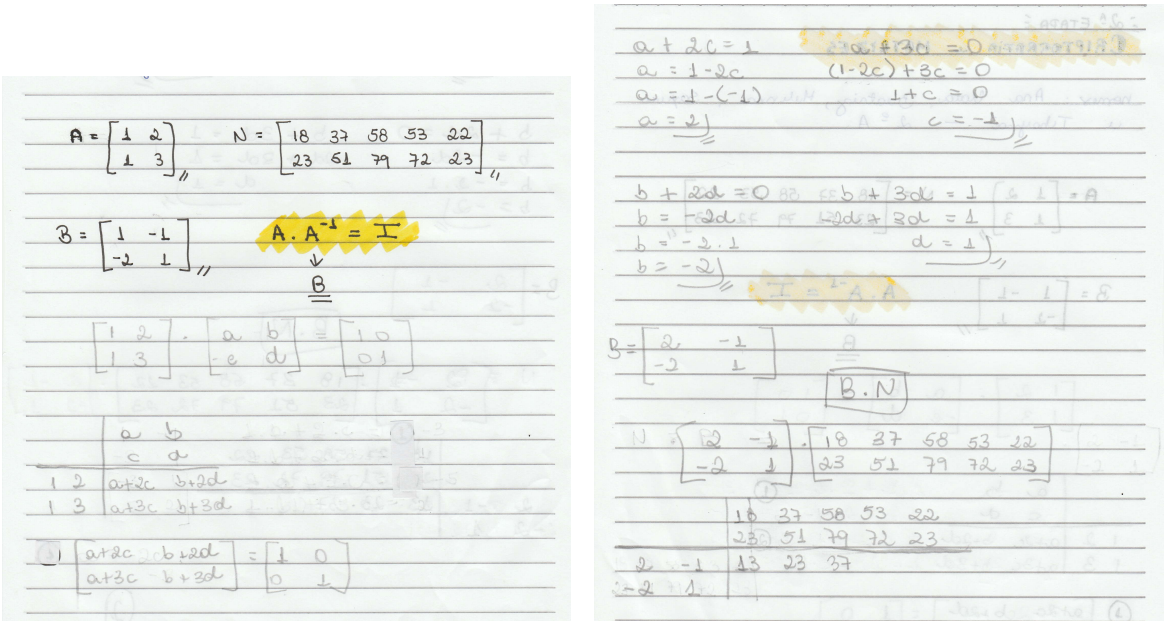
Fonte: Elaborada pelo autor.

Figura 8 – Grupo 5



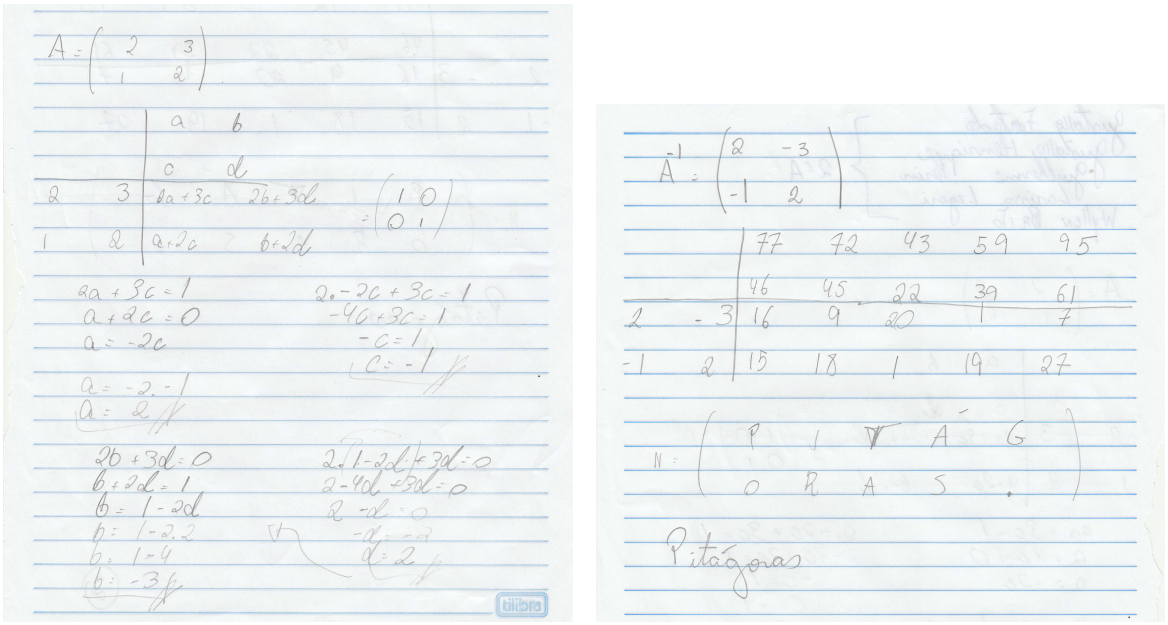
Fonte: Elaborada pelo autor.

Figura 9 – Grupo 1 - 2ª Etapa



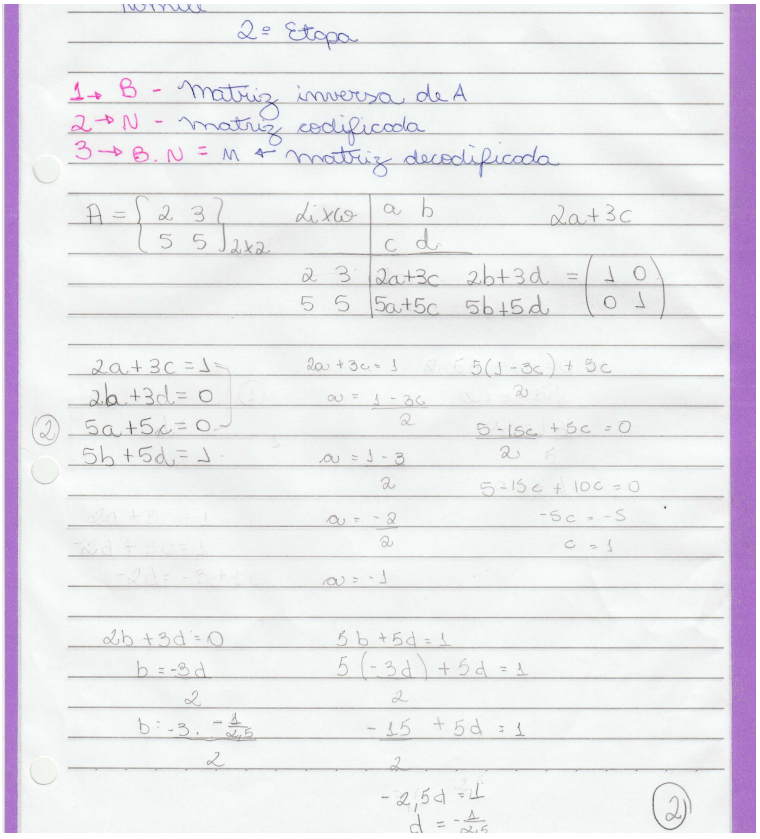
Fonte: Elaborada pelo autor.

Figura 10 – Grupo 2 - 2ª Etapa



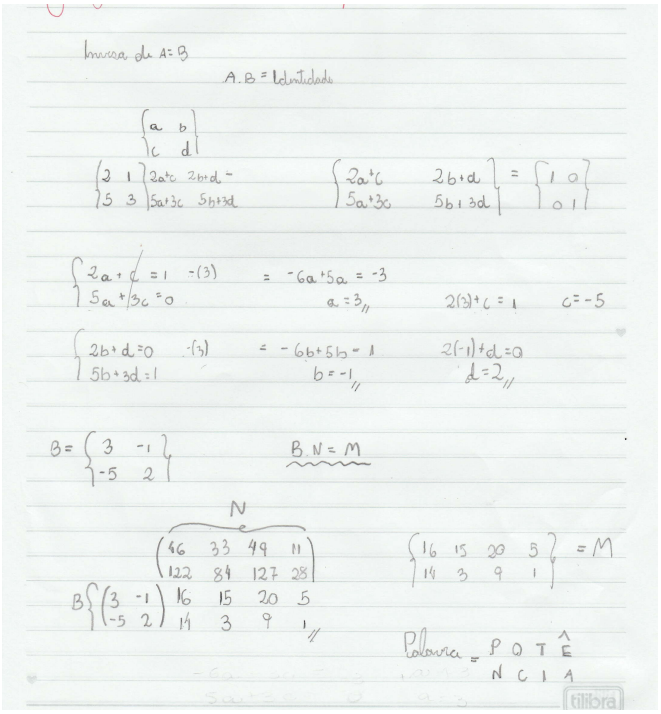
Fonte: Elaborada pelo autor.

Figura 11 – Grupo 3 - 2ªEtapa



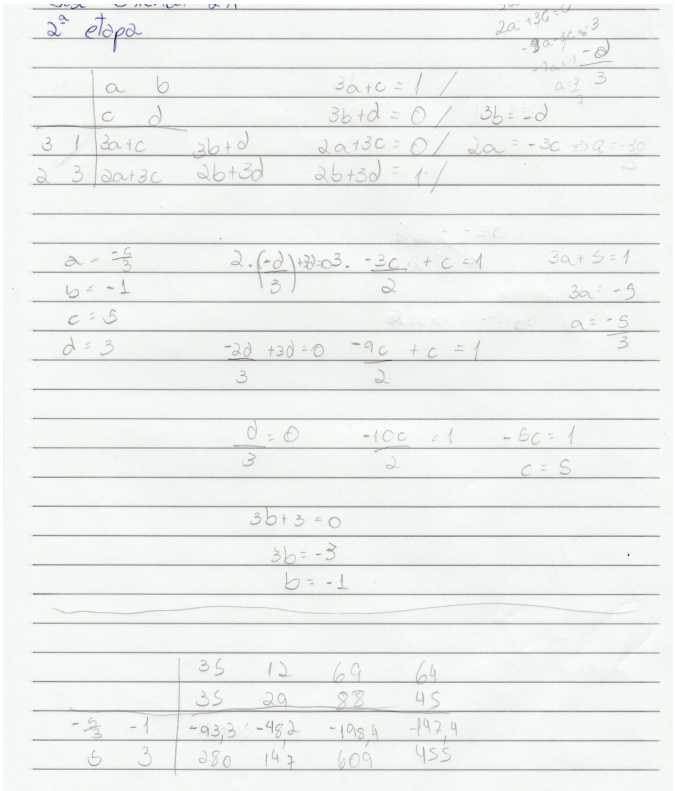
Fonte: Elaborada pelo autor.

Figura 12 – Grupo 4 - 2ªEtapa



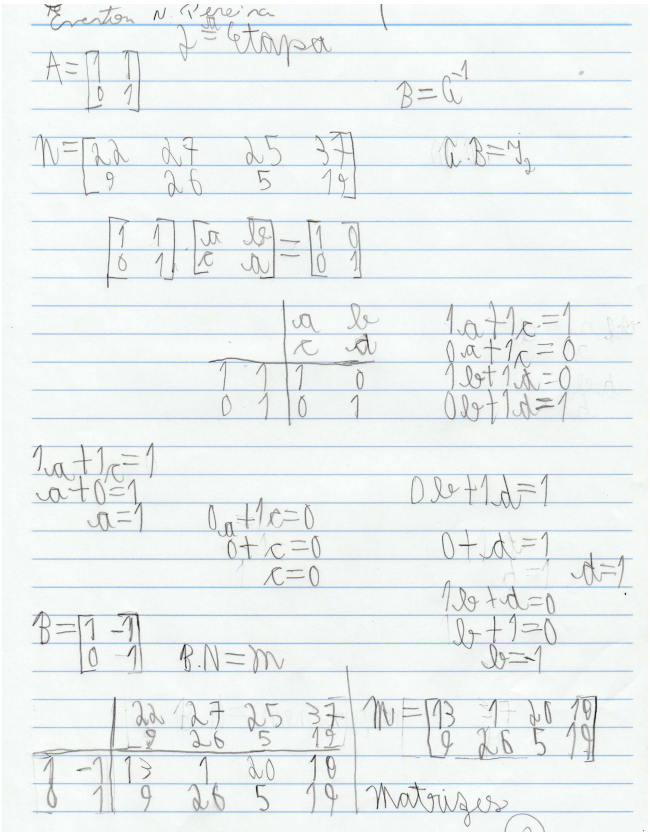
Fonte: Elaborada pelo autor.

Figura 13 – Grupo 5 - 2ªEtapa



Fonte: Elaborada pelo autor.

Figura 14 – Grupo 6 - 2ªEtapa



Fonte: Elaborada pelo autor.

CAPÍTULO

6

CONCLUSÃO

O tema escolhido para a realização desse trabalho mostrou-se muito satisfatório. A criptografia RSA provou-se tão interessante quanto aparentava e os tópicos que foram estudados antes de atingirmos de fato o objetivo foram bastante engrandecedor do ponto de vista matemático, pois me proporcionou trabalhar mais rigorosamnete alguns tópicos da teoria de números. Além do fato, que já mencionamos de se tratar de um tema bastante atual, o que despertou maior interesse ainda.

Ademais, foi possível levar a abordagem da criptografia para sala de aula, apesar de não conseguirmos uma abordagem tão detalhada do método como fomos capazes de realizar neste trabalho, mas a experiência foi enriquecedora, e me incentivou a levar mais aplicações da matemática em sala de aula.

Outro ponto a salientar é a importância do PROFMAT em minha formação como professora, pois os conteúdos das disciplinas e os professores que as lecionaram, me ajudaram muita na preparação das aulas e na maneira de ensinar os alunos, além de estimularem a capacidade de me expressar matematicamente.

REFERÊNCIAS

ANDRADE, E. **A História d a Criptografia.** 2014. Disponível em: <http://www.dsc.ufcg.edu.br/~pet/jornal/abril2014/materias/historia_da_computacao.html>. Citado na página 22.

COUTINHO, S. C. **Números Inteiros e Criptografia RSA**. [S.l.: s.n.], 1997. Citado nas páginas 20 e 41.

____. **Criptografia**. 2015. Disponível em: <http://www.obmep.org.br/docs/apostila7.pdf>. Citado na página 20.

DANTE, L. R. **Matemática: Contexto e Aplicações**. [S.l.: s.n.], 2018. Citado nas páginas 53 e 54.

DIAS, I.; GODOY, S. M. S. de. **Elementos de Matemática - Notas de Aulas**. 2006. Disponível em: <http://conteudo.icmc.usp.br/~iresdias/material/sma341.pdf>. Citado na página 26.

ENQ-2016.2. 2016. Disponível em: <http://www.profmat-sbm.org.br/wp-content/uploads/sites/23/2016/08/ENA-2016-Solucoes-com-Gabarito.pdf>. Citado na página 40.

FIARRESGA, V. M. C. **Criptografia e Matemática**. Dissertação (Mestrado), 2010. Citado na página 27.

HEFEZ, A. **Aritmética - Coleção PROFMat**. [S.l.: s.n.]. Citado na página 36.

____. **Elementos da Aritmética**. [S.l.: s.n.], 2010. Citado na página 44.

IMPA. **Descoberto número primo com quase 25 milhões de dígitos**. 2019. Disponível em: <https://impa.br/page-noticias/descoberto-numero-primo-com-quase-25-milhoes-de-digitos/?utm_source=facebook&utm_medium=post-link&utm_campaign=numero_primo&utm_term=numero_primo%2C%20primo_marsenne%2C%20gimps&fbclid=IwAR0qiQagxnO0q6G9hB5gVVKMofkXoV7M0I51oj9W13AkofE5zTUXi-DOflc>. Citado na página 24.

LIMA, E. L. de. **Análise Real**. [S.l.: s.n.], 2006. Citado na página 25.

PROFMAT-AV3-ARITMETICA. **Profmat- AV3- Aritmetica**. 2011. Disponível em: <http://www.profmat-sbm.org.br/wp-content/uploads/sites/23/2016/08/AV3_MA14_2011.pdf>. Citado na página 40.

SAMPAIO, J. C. V. **Estruturas Algébricas**. 2008. Citado na página 45.

SAMPAIO, J. C. V.; CAETANO, P. A. S. **Introdução à aTeoria dos Números**. [S.l.: s.n.], 2008. Citado na página 29.


ICMC
USP
SÃO CARLOS