Universidade Federal de Mato Grosso
Instituto de Ciências Exatas e da Terra
Departamento de Matemática

Criptografia RSA: uma abordagem para o ensino médio

Fabricia Auxiliadora Queiroz

Mestrado Profissional em Matemática: PROFMAT/SBM

Orientador: **Prof. Dr. Aldi Nestor de Souza**

Trabalho financiado pela Capes

Cuiabá - MT

Maio de 2018

Criptografia RSA: uma abordagem para o ensino médio

Este exemplar corresponde à redação final da dissertação, devidamente corrigida e defendida por Fabricia Auxiliadora Queiroz e aprovada pela comissão julgadora.

Cuiabá, 23 de maio de 2018.

Prof. Dr. Aldi Nestor de Souza
Orientador

Banca examinadora:

Prof. Dr. Aldi Nestor de Souza
Prof. Dr. Reinaldo de Marchi
Prof. Dr. Junior Cesar Alves Soares

Dissertação apresentada ao curso de Mestrado Profissional em Matemática – PROFMAT, da Universidade Federal de Mato Grosso, como requisito parcial para obtenção do título de **Mestre em Matemática**.

Dados Internacionais de Catalogação na Fonte.

Q3c Queiroz, Fabricia Auxiliadora.
Criptografia RSA: uma abordagem para o ensino médio / Fabricia Auxiliadora Queiroz. -- 2018
ix, 80 f. : il. color. ; 30 cm.

Orientador: Aldi Nestor de Souza.
Dissertação (mestrado profissional) - Universidade Federal de Mato Grosso, Instituto de Ciências Exatas e da Terra, Programa de Pós-Graduação em Matemática, Cuiabá, 2018.
Inclui bibliografia.

1. Criptografia. 2. Proposta de ensino. 3. Algoritmo da divisão. I. Título.

Ficha catalográfica elaborada automaticamente de acordo com os dados fornecidos pelo(a) autor(a).

MINISTÉRIO DA EDUCACÃO
UNIVERSIDADE FEDERAL DE MATO GROSSO
PRÓ-REITORIA DE ENSINO DE PÓS-GRADUACÃO
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA EM REDE NACIONAL - PROFMAT
Av. Fernando Corrêa da Costa, 2367 - Boa Esperança – 78.060-900 - Cuiabá/MT
Fone: (65) 3615-8576 – E-mail: profmat@ufmt.br

FOLHA DE APROVAÇÃO

Título: "Criptografia RSA: uma abordagem para o Ensino Médio"

Autor: Fabrícia Auxiliadora Queiroz

defendida e aprovada em 30/04/2018.

Composição da Banca Examinadora:

Presidente Banca/Orientador Doutor Aldi Nestor de Souza
Instituição : Universidade Federal de Mato Grosso

Examinador Interno Doutor Reinaldo de Marchi
Instituição : Universidade Federal de Mato Grosso

Examinador Externo Doutor Junior Cesar Alves Soares
Instituição : UNEMAT - Barra do Bugres

Cuiabá, 30/04/2018.

Agradecimentos

Agradeço primeiramente à Deus por estar presente sempre junto comigo.

Ao meu esposo, Juciano Carlos Gama, por todo apoio e compreensão, sem ele não conseguiria alcançar mais esse objetivo em minha vida.

Aos meus filhos Gabriel e Tiago, foi por eles meu maior sofrimento durante o mestrado, pois as vezes precisava ficar longe deles para poder me dedicar aos estudos.

Aos meus pais, José Gonçalves e Maria Auxiliadora que sempre me ajudaram e cuidaram dos meus filhos para que eu pudesse me dedicar ao mestrado.

Às minhas amigas, Luluzinhas, Adriana Soares, Cristiany Marinho, Edinalda Gomes, Giseula Maccarini (em memória), Glaciela Alvares, Jacksandra Leite e Marcella Duarte que estiveram comigo nesta fase da minha vida e que por muitas vezes não me deixaram desanimar. Excelentes professoras, cujo trabalho sempre admirei, excelentes pessoas que me faz sorrir diante das dificuldades e acreditar em um futuro melhor para educação.

Aos meus colegas do Profmat, que me acompanharam e me ajudaram diante das dificuldades de aprendizagem.

Ao meu orientador Professor Aldi Nestor, excelente profissional ao qual admiro desde a graduação.

À CAPES pelo apoio financeiro.

À SEDUC pelo apoio a qualificação profissional.

Resumo

A comunicação pela internet necessita de segurança para que as informações que circulam pela rede não estejam no domínio de pessoas não autorizadas. A criptografia tem a função de proteger essas informações. Sendo assim, é importante compreender a criptografia RSA, propondo um estudo no ensino médio da educação básica. Um tipo de criptografia assimétrica utilizada no comércio eletrônico e transações financeiras que necessita da matemática, especificamente da teoria dos números estudada desde o ensino fundamental, para o seu desenvolvimento. Duas experiências foram realizadas, sendo uma delas com alunos do ensino fundamental abordando alguns conteúdos básicos de teoria dos números, e outra com alunos do ensino médio com o conteúdo de criptografia RSA. Percebeu-se interesse dos alunos pelo assunto e ao invés de ensinar os cálculos de codificação e decodificação com aritmética modular, foi ensinado utilizando algoritmo da divisão de Euclides.

Palavras chave: criptografia, proposta de ensino, algoritmo da divisão.

Abstract

The communication by internet demands security in order that information that circulates over the networks does not be in the domain of unauthorized people. The cryptography has the function of protecting this information. Therefore, it is important to comprehend the RSA cryptography, proposing a study in high school. A type of asymmetrical cryptography used in electronic commerce and financial transactions that demand the mathematics, especially the theory of numbers has been studied since elementary school, for its development. Two experiences were performed, one of them with elementary school students approaching some basic contents of theory of numbers, and the other with high school students with the RSA cryptography content. It was perceived interest from the students by the subject and instead teaching the coding and decoding calculations with modular arithmetic, was taught using Euclidean division algorithm.

Keywords: Cryptography; teaching proposal; division algorithm.

Sumário

Lista de Figuras

Introdução

As pessoas cada vez mais utilizam os computadores para realizarem diversos trabalhos, como por exemplo, fazer compras, pagar contas, enviar mensagens, enfim para que a comunicação ocorra de maneira confidencial é importante que as informações naveguem pela rede sem serem decifradas por pessoas que não sejam o destinatário autorizado. A criptografia, inicialmente, era mais utilizada entre militares e governantes, passou a fazer parte da população no geral, principalmente, com a criação do computador e o desenvolvimento da internet.

> A teoria moderna da criptografia está baseada nas ciências exatas e os estudos científicos de criptografia estão ficando cada vez mais avançados e importantes . Criptografia é um dos tópicos mais antigos do conhecimento. Ela existia, não necessariamente como uma ciência, mas como um conhecimento, principalmente nos assuntos da natureza militar (guerras, armamentos) ou nos assuntos políticos para transmitir informações secretas, mantê-las em segredo e em segurança contra as fontes não autorizadas, como inimigos, espiões, espionagens,etc. (Shokranian, 2012)

Existem dois tipos de criptografia utilizada até hoje: a simétrica e a assimétrica. A criptografia assimétrica garante confidencialidade e autenticidade. Uma delas é a criptografia RSA, baseada em teoria dos números.

Ao iniciar o ano letivo pode-se utilizar a criptografia RSA como motivação para revisão de conteúdos básicos da matemática, com o objetivo de ensinar um conteúdo da atualidade, recordar conteúdos matemáticos e ao mesmo tempo fazer um diagnóstico da turma. Muitos conteúdos matemáticos são vistos pelos alunos como "não servem para nada". A teoria dos números durante algum tempo também era vista como uma parte da matemática que não tinha aplicação, mas os matemáticos viram nessa área uma solução para proteger as informações na internet. Mostrar para os alunos que a aplicação de um conteúdo pode ser descoberto após alguns anos é importante.

> Os matemáticos encontraram uma maneira de conectar o difícil problema da fatoração de números aos códigos que protegem as finanças do mundo na internet. Essa tarefa aparentemente inocente e tão difícil de realizar em números de 100 algarismos que os bancos e o comércio eletrônico depositam a segurança de suas transações financeiras no tempo inviavelmente longo necessário - hoje- para encontrar os fatores primos. (du Sautoy, 2007)

O mundo dos negócios depositou sua confiança em uma área da matemática que poucos se dedicaram a examinar por conta própria. (du Sautoy, 2007)

Os Parâmetros Curriculares Nacionais afirmam que a matemática no ensino médio deve ser vista pelo aluno como um conjunto de técnicas e estratégias para serem aplicadas a outras áreas do conhecimento, assim como para a atividade profissional. Portanto o ensino da criptografia RSA atende a esta expectativa. (MEC, 2000)

No capítulo 1 são apresentados os conteúdos matemáticos que são bases para criptografia RSA, uma abordagem para ser trabalhada na educação básica, mais especificamente no ensino fundamenntal

De acordo com os Parâmetros Curriculares Nacionais, no Ensino Fundamental os alunos devem se aproximar de vários campos do conhecimento matemático e agora no ensino médio estão em condições de utilizá-los e ampliá-los e desenvolver de modo mais amplo capacidades tão importantes quanto as de abstração, raciocínio em todas as suas vertentes, resolução de problemas de qualquer tipo, investigação, análise e compreensão de fatos matemáticos e de interpretação da própria realidade. (MEC, 2000)

No capítulo 2 é descrito um pouco da história da criptografia até o surgimento da criptografia RSA.

No capítulo 3 apresenta-se um exemplo de codificação e decodificação com uma abordagem para o ensino médio. Sendo assim, optou-se por não escrever na forma da aritmética modular, mas sim pelo algoritmo da divisão de Euclides.

No capítulo 4 relata-se a experência realizada com alunos do ensino fundamental e médio, sendo realizadas aulas para o ensino fundamental onde foram abordados conteúdos do capítulo 1 deste trabalho, bem como algumas demonstrações. E no ensino médio trabalhados os capítulos 2 e 3. Para que assim pudesse analisar a possibilidade de ensinar um conteúdo que muitas vezes só é citado como exemplo de aplicação, mas que não é explorado a tal ponto de ser um auxílio para revisão de conteúdo e motivação para o processo de ensino-aprendizagem.

Capítulo 1

Números inteiros na educação básica

Neste capítulo será feito uma breve exposição de teoria básica dos números como proposta de abordagem para a educação básica. A intenção é, trabalhar essa teoria no ensino fundamental para que ao chegar no ensino médio os alunos possam ir além do conteúdo em si com a criptografia RSA.

1.1 Números inteiros

É fundamental ao iniciar um conteúdo considerar os conhecimentos prévios dos alunos acerca do assunto. Até esta etapa escolar, ao qual inicia-se os números inteiros, eles estão acostumados a resolverem subtrações, cujo significado pode ser explicado de forma concreta, retirar uma quantidade menor de uma quantidade maior. No entanto, não é possível subtrair quaisquer dois números naturais e dizer que o resultado é natural, por exemplo, 2 - 5 não existe nos naturais, mas é possível fazer essa subtração no conjunto dos números inteiros, dando significado a essa expressão.

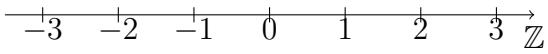
Os números naturais representavam quantidades sendo associados a contagem ou medidas, nesta etapa é introduzido os números negativos dando um novo significado aos números, uma quantidade orientada, ou seja, tem-se quantidades maiores que zero e menores que zero.

O conjunto dos números inteiros é representado por:

$$\mathbb{Z} = \{\ldots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots\}$$

1.1.1 Representação geométrica

Os números inteiros podem ser representados numa reta. O zero passa a ser compreendido como um referencial e não apenas a ausência de quantidade.



A distância entre dois números consecutivos quaisquer é sempre 1. O zero é o referencial que determina a orientação dos números positivos e dos números negativos. É importante ressaltar que o zero não é positivo e nem negativo.

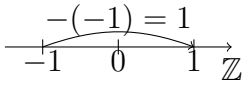
1.1.2 Oposto de um número inteiro

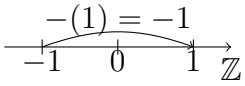
A representação dos números inteiros na reta numerada transmite a ideia de oposição a partir do referencial, ou seja, a partir do ponto zero. Dois números são opostos quando estão à uma mesma distância do zero. Por exemplo: 2 e -2 são opostos. Logo se x é um número inteiro $-x$ é o seu oposto.

Exemplo 1.

$-(-1)$, indica o oposto do número negativo (-1) que é o número positivo $+1$ ou 1.

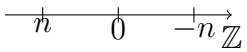
$-(+1)$, indica o oposto do número positivo 1 que é o número negativo -1.

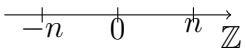




Para Refletir 1. *Se n é um número inteiro, -n é negativo ou positivo?*

Depende do valor de n, se n for negativo $-n$ será positivo, se n for positivo, $-n$ será negativo.





1.1.3 Módulo ou valor absoluto

O número inteiro $|a|$ é chamado de módulo ou valor absoluto de a e é definido por:

$$|a| = \begin{cases} -a, & \text{se} \quad a \leq 0, \\ a, & \text{se} \quad a > 0. \end{cases}$$

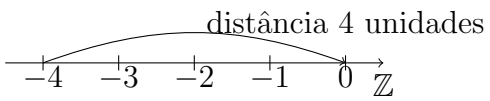
Exemplo 2.

a) $|3| = 3$

b) $|-3| = 3$, pois $-(-3) = 3$

Pode-se utilizar a reta numerada para definir o módulo de um número inteiro, como sendo a distância desse número até o zero, ou seja, geometricamente, o módulo de um número inteiro a, na reta, é definido como sendo a distância desse ponto a até a origem. Logo como distâncias são sempre positivas é fácil verificar que $|a|$ é sempre maior ou igual a zero.

Exemplo 3. $|-4| = 4$



Curiosidade 1. *Desigualdade Triangular*

Para a e $b \in \mathbb{Z}$ temos

- $|a + b| \leq |a| + |b|$

Demonstração. Para todo $x \in \mathbb{Z}$ tem-se que $x = |x|$ ou $x = -|x|$, sendo assim

$$-|a| \leq a \leq |a|$$

e

$$-|b| \leq b \leq |b|.$$

Logo $-|a| - |b| \leq a + b \leq |a| + |b| \Rightarrow -(|a| + |b|) \leq a + b \leq |a| + |b|$.
Divide-se em duas desigualdades $a + b \leq |a| + |b|$ e $a + b \geq -(|a| + |b|)$.

Se $a+b \geq 0$, segue que $|a+b| = a+b$ então $|a+b| \leq |a|+|b|$. Se $a+b \leq 0$, segue que $|a+b| = -(a+b)$, então $|a+b| \leq |a|+|b|$

Portanto $|a+b| \leq |a|+|b|$. □

- $|a-b| \geq |a|-|b|$

Demonstração. $|a| = |a+b-b| = |(a-b)+b|$. Pela desigualdade triagular tem-se $|a| \leq |a-b|+|b|$.

Logo $|a| \leq |a-b|+|b| \Rightarrow |a-b| \geq |a|-|b|$. □

- $|a \cdot b| = |a| \cdot |b|$

Demonstração. Esta demonstração será dividida em seis casos:

i) $a = 0$ e $b \neq 0$ tem-se $|a \cdot b| = |0 \cdot b| = 0$ e $|a| \cdot |b| = 0 \cdot |b| = 0$. Logo $|a \cdot b| = |a| \cdot |b|$.

ii) $a \neq 0$ e $b = 0$ tem-se $|a \cdot b| = |a \cdot 0| = 0$ e $|a| \cdot |b| = |a| \cdot 0 = 0$. Logo $|a \cdot b| = |a| \cdot |b|$.

iii) $a > 0$ e $b > 0$ tem-se $|a \cdot b| = a \cdot b$ e $|a| \cdot |b| = a \cdot b$. Logo $|a \cdot b| = |a| \cdot |b|$.

iv) $a > 0$ e $b < 0$ tem-se $|a \cdot b| = -(a \cdot b)$ e $|a| \cdot |b| = a \cdot (-b) = -(a \cdot b)$.
Logo $|a \cdot b| = |a| \cdot |b|$.

v) $a < 0$ e $b < 0$ tem-se $|a \cdot b| = a \cdot b$ e $|a| \cdot |b| = (-a) \cdot (-b) = a \cdot b$. Logo $|a \cdot b| = |a| \cdot |b|$.

vi) $a < 0$ e $b > 0$ tem-se $|a \cdot b| = -(a \cdot b)$ e $|a| \cdot |b| = -a \cdot b$.Logo $|a \cdot b| = |a| \cdot |b|$.

Para todos os casos tem-se $|a \cdot b| = |a| \cdot |b|$, portanto $|a \cdot b| = |a| \cdot |b|$ para todo $a, b \in \mathbb{Z}$. □

Em seguida será feito alguns exemplos tomando valores particulares para a e $b \in \mathbb{Z}$.

- $|a+b| \leq |a|+|b|$

Sejam $a = 3$ e $b = 5$, tem-se $|3+5| = 8$ e $|3|+|5| = 8$, logo $|3+5| = |3|+|5|$.

Sejam $a = -4$ e $b = 2$, tem-se $|-4+2| = |-2| = 2$ e $|-4|+|2| = 4+2 = 6$, logo $|-4+2| < |-4|+|2|$.

- $|a - b| \geq |a| - |b|$

  Sejam $a = 10$ e $b = -6$, tem-se $|10 - (-6)| = 16$ e $|10| - |-6| = 10 - 6 = 4$, logo $|10 - (-6)| > |10| - |-6|$.

  Sejam $a = 9$ e $b = 4$, tem-se $|9 - 4| = |5| = 5$ e $|9| - |4| = 9 - 4 = 5$, logo $|9 - 4| = |9| - |4|$.

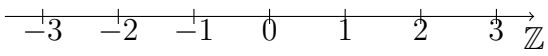
- $|a \cdot b| = |a| \cdot |b|$

  Sejam $a = -7$ e $b = 3$, tem-se $|-7 \cdot 3| = |-21| = 21$ e $|-7| \cdot |3| = 7 \cdot 3 = 21$, logo $|-7 \cdot 3| = |-7| \cdot |3|$.

  Sejam $a = -8$ e $b = -5$, tem-se $|-8 \cdot (-5)| = |40| = 40$ e $|-8| \cdot |-5| = 8 \cdot 5 = 40$, logo $|-8 \cdot (-5)| = |-8| \cdot |-5|$.

1.1.4 Comparação de números inteiros

Observe a figura abaixo



A "setinha" para direita marca a orientação da reta, ou seja, o sentido crescente. Sendo assim, afirma-se por exemplo que $-3 < -2$, $-1 < 0$, $0 < 3$ e $-1 < 3$.

1.1.5 Adição de números inteiros

A operação de adição possui as seguintes propriedades:

1. Comutativa: Para todos a e $b \in \mathbb{Z}$, $a + b = b + a$.
2. Associativa: Para todos a, b e $c \in \mathbb{Z}$, $(a + b) + c = a + (b + c)$.
3. Elemento Neutro: Para todo $a \in \mathbb{Z}$, $a + 0 = a$.
4. Elemento oposto ou inverso aditivo: Para todo $a \in \mathbb{Z}$, existe o oposto de a, denotado por $(-a)$ tal que $a + (-a) = 0$.

Os cálculos do exemplo a seguir serão realizados utilizando a ideia de juntar e acrescentar.

Exemplo 4.

a) $3 + 5 = 8$,

b) $-5 + (-2) = -7$,

c) $2 + 7 = 9$,

d) $-10 + (-8) = -18$.

Agora utilizando a propriedade 4 (Inverso aditivo) será feito os cálculos a seguir:

e) $2+(-5) = 2+(-2)+(-3) = -3$, observe que (-5) pode ser escrito como $(-2)+(-3)$ e pela propriedade 4 tem-se $2 + (-2) = 0$.

f) $-6 + 3 = -3 + (-3) + 3 = -3$, observe que $(-6) = (-3) + (-3)$ neste caso tem-se $(-3) + 3 = 0$.

g) $5 + (-2) = 3 + 2 + (-2) = 3$, neste caso tem-se $5 = 3 + 2$ e $2 + (-2) = 0$.

h) $-7 + 3 = -4 + (-3) + 3 = -4$, neste caso tem-se $(-7) = (-4) + (-3)$ e $-3 + 3 = 0$.

1.1.6 Subtração de inteiros

Dados dois números inteiros a e b, a subtração é dada pelo resultado de $b - a$. No entanto a subtração pode ser interpretada como adição, pois $b - a = b + (-a)$, a propriedade do inverso aditivo possibilita que toda subtração seja escrita como a adição .

Exemplo 5.

a) $5 - 3 = 5 + (-3) = 2 + 3 + (-3) = 2$,

b) $-3 - 2 = -3 + (-2) = -5$,

c) $2 - 7 = 2 + (-7) = 2 + (-2) + (-5) = -5$,

d) $8 - 3 = 8 + (-3) = 5 + 3 + (-3) = 5$.

Observação 1. *A expressão* $5 - 3$ *já era conhecida ao estudar números naturais , porém no conjunto dos naturais ela não poderia ser expressa como adição pois* (-3) *não pertence aos naturais.*

Importante 1. *Seja p um número inteiro qualquer*

$$-(-p) = p.$$

Esta afirmação é consequência intuitivamente da propriedade do inverso aditivo, isto é, $-p$ é o inverso aditivo de p, o inverso aditivo de $-p$ é p, logo $-(-p) = p$.

Utilizando este fato pode-se realizar os cálculos abaixo e obter os seguintes resultados:

- $5 - (-4) = 5 + 4 = 9$, pois o oposto de -4 é 4,
- $-(-3) - 2 = 3 - 2 = 1$,
- $7 - (-1) = 7 + 1 = 8$.

1.1.7 Multiplicação de inteiros

Propriedades da multiplicação

1. Comutativa: Para todos a e $b \in \mathbb{Z}$, $a \cdot b = b \cdot a$.
2. Associativa: Para todos a, b e $c \in \mathbb{Z}$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
3. Elemento Neutro: Para todo $a \in \mathbb{Z}$, $a \cdot 1 = a$.
4. Distributiva: Para todos a, b e $c \in \mathbb{Z}$, tem-se $a \cdot (b + c) = a \cdot b + a \cdot c$.

Importante 2. *Para todo $p \in \mathbb{Z}$, temos $p \cdot 0 = 0$.*

Talvez esse resultado pareça óbvio, mas nenhuma criança nasce sabendo que todo número inteiro multiplicado por zero é zero. Esta afirmação tem uma demonstração, que parte do princípio das propriedades das operações de adição e de multiplicação em $\mathbb{Z}$ e não do fato que ouvi-se muito que 0 somado p vezes é igual a zero.

Demonstração. $p \cdot 0 = p \cdot (0 + 0)$, pela propriedade distributiva tem-se $p \cdot 0 = p \cdot 0 + p \cdot 0$. Então somando $-(p \cdot 0)$, em ambos os lados da igualdade obtem-se

$$p \cdot 0 + [-(p \cdot 0)] = p \cdot 0 + p \cdot 0 + [-(p \cdot 0)].$$

Note que $-(p \cdot 0)$ é o inverso aditivo de $p \cdot 0$, sendo asim $p \cdot 0 + [-(p \cdot 0)] = 0$. Portanto

$$0 = p \cdot 0$$

□

Agora, é possível mostrar que dado p um número inteiro qualquer $-(-p) = p$.

Demonstração. $-1 \cdot [p + (-p)] = -1 \cdot 0 = 0$, logo $-1 \cdot [p + (-p)] = 0$. Pela propriedade distributiva tem-se $-1 \cdot p + (-1)(-p) = 0$.

Note que $(-1)p + p = (-1)p + 1 \cdot p = [(-1) + 1]p = 0 \cdot p = 0$, sendo assim, $(-1) \cdot p + p = 0$, pela propriedade do inverso aditivo $(-1) \cdot p$ é o inverso aditivo de p, ou seja, $(-1) \cdot p = -p$.

Com esse resultado segue que $-1 \cdot p + (-1)(-p) = -p + [-(-p)] = 0$. Somando p em ambos os lados tem-se $p + (-p) + [-(-p)] = p$, mas $p + (-p) = 0$.

Portanto $-(-p) = p$. □

Para o conjunto dos números naturais a multiplicação $n \cdot b$ é a soma de n parcelas iguais a b, por exemplo, $3 \cdot 5 = 5 + 5 + 5 = 15$, é possível utilizar este mesmo procedimento para multiplicação dos inteiros positivos, mas quando se tratar de negativos, por exemplo $3 \cdot (-5)$? Para isso tem-se a seguinte afirmação:

Importante 3. *Sejam a e $b \in \mathbb{Z}$. Então $a \cdot (-b) = (-b) \cdot a = -(a \cdot b)$.*

Para provar esta afirmação, primeiro será provado que $a \cdot (-b) = -(a \cdot b)$. Esta igualdade significa que $a \cdot (-b)$ é o oposto de $a \cdot b$, ou seja, para mostrar que

$$a \cdot (-b) = -(a \cdot b)$$

basta mostrar que

$$a \cdot (-b) + a \cdot b = 0.$$

Demonstração. Pela propriedade da distributividade pode-se escrever

$$a \cdot (-b) + a \cdot b = a(-b + b).$$

Além disso, $-b + b = 0$, pois $-b$ é o inverso aditivo(elemento oposto) de b. Portanto

$$a \cdot (-b) + a \cdot b = a \cdot 0 = 0.$$

Concluindo que $a \cdot (-b) = -(a \cdot b)$. De forma análoga será provado que $(-b) \cdot a = -(a \cdot b)$, neste caso tem-se $(-b) \cdot a$ o oposto de $a \cdot b$.

$$(-b) \cdot a + (a \cdot b) = (-b) \cdot a + (b \cdot a) = (-b + b) \cdot a = 0 \cdot a = 0.$$

Concluindo assim que $(-b) \cdot a$ é o oposto de $a \cdot b$, portanto $(-b) \cdot a = -(a \cdot b)$. □

Agora já se tem condições de calcular $3 \cdot (-5)$, veja os passos,
$3 \cdot (-5) = -(3 \cdot 5)$, a multiplicação $3 \cdot 5 = 15$ já é conhecida, sendo assim tem-se

$$3 \cdot (-5) = -(3 \cdot 5) = -15.$$

Exemplo 6.

a) $4 \cdot (-6) = -(4 \cdot 6) = -24$,

b) $(-5) \cdot 2 = -(5 \cdot 2) = -10$,

c) $(-6) \cdot 3 = -(6 \cdot 3) = -18$,

d) $7 \cdot (-2) = -(7 \cdot 2) = -14$.

Quanto é $(-2) \cdot (-3)$? Para este caso tem-se a seguinte afirmação:

Importante 4. *Sejam a e $b \in \mathbb{Z}$. Então $(-a) \cdot (-b) = a \cdot b$.*

A demonstração desta afirmação segue do fato que foi provado ser verdade: dados a, b e $p \in \mathbb{Z}$

$$a \cdot (-b) = (-b) \cdot a = -(a \cdot b)$$

e

$$-(-p) = p,$$

segue que

$$(-a) \cdot (-b) = -(a \cdot (-b)) = -(-(a \cdot b)) = a \cdot b.$$

Logo $(-2) \cdot (-3) = -(2 \cdot (-3)) = -(-(2 \cdot 3)) = 2 \cdot 3 = 6$.

Conclusão: o produto de dois números positivos ou de dois números negativos é positivo. E o produto entre um número positivo e um número negativo é negativo.

1.2 Divisibilidade

Dados dois números inteiros a e b, a dividido por b é um número inteiro se a for um múltiplo de b. Neste caso b é denominado divisor de a.

Exemplo 7.

a) $\frac{6}{2} = 3$, logo 2 é um divisor de 6, ou seja, 6 é um múltiplo de 2.

b) $\frac{10}{2} = 5$, logo 2 é um divisor de 10, ou seja, 10 é um múltiplo de 2.

c) $\frac{8}{4} = 2$, logo 4 é um divisor de 8, ou seja, 8 é um múltiplo de 4.

Observe que se 2 divide 4 e 2 divide 6, então 2 também divide $4 + 6$, além disso, 2 divide $4.3 + 6.4 = 36$.

Curiosidade 2. *Sejam a, b e $d \in \mathbb{Z}$ tem-se que se d divide a e d divide b, então d divide $ax + by$ para qualquer combinação linear $ax + by$ de a e b com coeficientes $x, y \in \mathbb{Z}$.*

Demonstração. Se d divide a e d divide b então a e b são múltiplos de d, ou seja, $a = dp$ e $b = dq$, com $p, q \in \mathbb{Z}$, logo $ax + by = dpx + dqy = d(px + qy)$. Como $px + qy \in \mathbb{Z}$, temos que d divide $ax + by$. □

Importante 5. *Propriedade da transitividade: Sejam a, b e $c \in \mathbb{Z}$, se a divide b e b divide c, então a divide c.*

Demonstração. Se a divide b e b divide c ,então $b = ar$ e $c = bs$, com $r, s \in \mathbb{Z}$. Logo $c = ars$, ou seja, c é um múltiplo de a, portanto a divide c. □

Exemplo 8. *Se 5 divide 10 e 10 divide 30, então 5 divide 30.*

Curiosidade 3. *Sejam a, b e $c \in \mathbb{Z}$, tais que a divide $(b + c)$ ou a divide $(b - c)$. Então se a divide b tem-se que a também divide c, reciprocamente se a divide c então a também divide b.*

Demonstração. Suponha que a divide $(b+c)$ e a divide b, ou seja, existem p, $q \in \mathbb{Z}$ tais que $b + c = ap$ e $b = aq$, sendo assim tem-se $aq + c = ap$, somando $-(aq)$ em ambos os lados da igualdade resulta em $c = ap + (-aq) = a(p - q)$, como p e q são números inteiros então

$p - q$ também é inteiro, logo c é um múltiplo de a, ou seja a divide c. Reciprocamente se a divide c, pode-se escrever $c = ak$, $k \in \mathbb{Z}$, substituindo na igualdade $b + c = ap$ tem-se $b + ak = ap$, consequentemente $b = a(p - k)$, concluindo assim que b é um múltiplo de a, ou seja, a divide b. De maneira análoga suponha que a divide $(b - c)$ e a divide b, ou seja, existem p, $q \in \mathbb{Z}$ tais que $b - c = ap$ e $b = aq$, sendo assim tem-se $aq - c = ap$, somando c em ambos os lados da igualdade resulta em $aq = c + ap$, somando ainda $(-ap)$ segue a igualdade $aq + (-ap) = c$, colocando a em evidência obtem-se $a(q - p) = c$, como p e q são números inteiros então $q - p$ também é inteiro, logo c é um múltiplo de a, ou seja a divide c. Reciprocamente se a divide c, pode-se escrever $c = ak$, $k \in \mathbb{Z}$, substituindo na igualdade $b - c = ap$ tem-se $b - ak = ap$, o que implica $b = a(p + k)$, concluindo assim que b é um múltiplo de a, ou seja, a divide b. □

1.2.1 Divisão Euclidiana

A divisão Euclidiana garante a existência de dois números inteiros q e r, chamados, respectivamente, de quociente e resto da divisão de dois números inteiros a e b com $b \neq 0$, tal que $a = bq + r$ com $0 \leq r < |b|$. Esse resultado é antigo e pode ser encontrado no livro *Os Elementos* de Euclides, é considerado uma importante ferramenta para teoria dos números. (Hefez, 2014)

Exemplo 9.

Ao dividir 19 por 5,tem-se os seguintes resultados $q = 3$ e $r = 4$, logo

$$19 = 5.3 + 4,$$

observe que esta divisão já era praticada para o conjunto dos números naturais. No caso de -19 dividido por 5, como fica?

Neste caso o resultado será $q = -4$ e $r = 1$, logo $-19 = 5.(-4) + 1$. É importante ressaltar que o quociente e o resto são únicos e o resto é sempre positivo ou igual a zero.

A seguir será demonstrado a unicidade do quociente e do resto da divisão Euclidiana.

Demonstração. Suponha que dados dois números inteiros a e b tem-se $a = bq + r$, com $0 \leq r < |b|$ e $a = bq' + r'$, com $0 \leq r' < |b|$. Deve-se mostrar que $q = q'$ e $r = r'$.

Observe que r e r' são números inteiros, logo um deles é maior ou igual ao outro. Suponha que $r \geq r'$.

$$a = bq + r \Rightarrow r = a - bq,$$
$$a = bq' + r' \Rightarrow r' = a - bq'.$$

Subtraindo as duas igualdades obtem-se:

$$r - r' = b(q' - q).$$

Note que $r \geq r'$, sendo assim $r - r' \geq 0$, além disso, $r < |b|$ e $r' < |b|$.

Segue que $0 \leq r - r' < |b| \Rightarrow 0 \leq b(q' - q) < |b|$.

Como b, q' e q são números inteiros esta desigualdade só se verifica se $q' - q = 0$, ou seja, $q' = q$.

Logo $r - r' = b(q' - q) = 0$, portanto $r = r'$. □

Sabendo que o quociente e o resto da divisão de a por b são únicos, é possível determiná-los pelo método de divisão por subtrações sucessivas.

Exemplo 10. *Determinar o quociente e o resto da divisão de* 123 *por* 9.

$123 = 9 \cdot q + r$, com q e $r \in \mathbb{Z}$ e $0 \leq r < 9$. Podemos escrever $r = 123 - 9 \cdot q$.

Atribuindo valores para q determina-se r, até que se obtenha $0 \leq r < 9$.

$$q = 10 \Rightarrow \quad r = 123 - 90 = 33,$$
$$q = 11 \Rightarrow \quad r = 123 - 99 = 24,$$
$$q = 12 \Rightarrow \quad r = 123 - 108 = 15,$$
$$q = 13 \Rightarrow \quad r = 123 - 117 = 6.$$

Observe que foram feitas subtrações sucessivas, como 123 é bem maior que 9, pode-se retirar $10 \cdot 9$ de 123, sendo assim tem-se $123 - 90 = 33$, depois $33 - 9 = 24$, em seguida $24 - 9 = 15$ e por último $15 - 9 = 6$.

Portanto, como $0 < 6 < 9$ segue que o resto é 6 e o quociente é 13.

Exemplo 11. *Determinar o quociente e o resto da divisão de* -418 *por* 16.

$-418 = 16 \cdot q + r$, com q e $r \in \mathbb{Z}$ e $0 \leq r < 16$. Pode-se escrever

$$r = -418 - 16 \cdot q.$$

Atribuindo valores para q determina-se r, tal que $0 \leq r < 16$. Observe que se $q \geq 0$ então $r \leq 0$.

$$\begin{aligned}
q = -10 \Rightarrow \quad & r = -418 - 16 \cdot (-10) = -418 + 160 = -258, \\
q = -20 \Rightarrow \quad & r = -418 - 16 \cdot (-20) = -418 + 320 = -98, \\
q = -26 \Rightarrow \quad & r = -418 - 16 \cdot (-26) = -418 + 416 = -2, \\
q = -27 \Rightarrow \quad & r = -418 - 16 \cdot (-27) = -418 + 432 = 14.
\end{aligned}$$

Portanto, como $0 < 14 < 16$ segue que o resto é 14 e o quociente é -27.

Saiba Mais 1. *Determinar o resto da divisão de* 3^{800} *por* 13.

Para isso observe o seguinte:

$$\begin{aligned}
&(a+b) = a + b^1, \\
&(a+b)^2 = a^2 + 2ab + b^2 = a \cdot (a + 2b) + b^2, \\
&(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3 = a \cdot (a^2 + 3ab + 3b^2) + b^3.
\end{aligned}$$

Geralmente trabalha-se até o expoente 3 no ensino fundamental, para $n \geq 4$ calcula-se $(a+b)^n$ pelo Binômio de Newton ver Hefez (2014) encontrado também em livros didáticos de ensino médio, pelo binômio é possível afirmar que para todo $n \in \mathbb{N}$, $(a+b)^n = a \cdot t + b^n$, $t \in \mathbb{Z}$.

Para determinar o que foi proposto escreve-se

$$\begin{aligned}
3^3 &= 13 \cdot 2 + 1 \\
(3^3)^{266} &= (13 \cdot 2 + 1)^{266}
\end{aligned}$$

Pelo Binômio de Newton tem-se $(13 \cdot 2 + 1)^{266} = 13 \cdot t + 1^{266}$, com $t \in \mathbb{Z}$

Logo $(3^3)^{266} = 3^{798} = 13t + 1$

Como $3^2 = 13 \cdot 0 + 9$, segue o resultado

$$3^{798} \cdot 3^2 = (13 \cdot t + 1)(13 \cdot 0 + 9) = 13 \cdot s + 9,\ s \in \mathbb{Z}$$

Portanto $3^{800} = 13s + 9$, logo o resto é 9.

1.2.2 Máximo divisor comum

Em uma divisão quando o resto é 0 tem-se um divisor, por exemplo, 2 é um divisor de 4, 5 é um divisor de 10. É possível ter divisores que são comuns a dois, três ou mais números, por exemplo 2 é divisor de 4 e de 8, 5 é divisor de 10, de 15 e de 20.

Sendo assim segue a definição:

Dados dois números inteiros a e b, um número inteiro d será dito divisor comum de a e b, se d divide a e d divide b.

Além disso, é definido o máximo divisor comum:

Dados dois números inteiros a e b, um número inteiro d maior que zero será dito máximo divisor comum de a e b, indicado por $d = mdc(a, b)$, se satisfaz as seguintes propriedades:

i) *d é um divisor comum de a e b, e*

ii) *d é divisível por todo divisor comum de a e b, ou seja, ele é o maior dos divisores comuns.*

Exemplo 12.

a) $mdc(12, 18) = 6$,

b) $mdc(25, 30) = 5$.

Uma maneira de calcular o mdc é utilizando o *algoritmo de Euclides*, para isso tem-se o seguinte lema

Lema 1. *(Euclides) Seja $a = bq + r$, tal que $b \neq 0$ e $0 \leq r < |b|$ então*

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

Demonstração. Sejam $a = bq + r$, $d = mdc(a, b)$ e $s = mdc(b, r)$, sendo assim tem-se que d divide a e d divide b. Consequentemente d divide $a - bq$, mas $r = a - bq$, logo d divide r. Conclui-se que d divide b e d divide r, mas $s = mdc(b, r)$, então d divide s. Além disso, s divide b e s divide r, então s divide $bq + r$, ou seja, s divide a. Logo s divide a e s divide b, mas $d = mdc(a, b)$, então s divide d. Portanto $d = s$. □

O algoritmo de Euclides consiste em aplicar o lema 1, repetindo o processo, onde q e r são o quociente e o resto na divisão de a por b. Como a cada repetição do processo o resto se torna cada vez menor, o algoritmo para quando atingimos o resto 0.

Exemplo 13. *Calcule $mdc(372, 162)$.*

$$\begin{aligned} 372 &= 162 \cdot 2 + 48, \\ 162 &= 48 \cdot 3 + 18, \\ 48 &= 18 \cdot 2 + 12, \\ 18 &= 12 \cdot 1 + 6, \\ 12 &= 6 \cdot 2 + 0. \end{aligned}$$

Segue que

$$mdc(372, 162) = mdc(162, 48) = mdc(48, 18) = mdc(18, 12) = mdc(12, 6) = mdc(6, 0) = 6$$

Saiba Mais 2. *Sejam a e $b \in \mathbb{Z}$ não simultaneamente nulos e $d = mdc(a, b)$, existem números inteiros x e y tais que $ax + by = d$, sendo d o menor número que pode ser escrito dessa forma.*

Exemplo 14. *Determinar os números inteiros x e y tais que $372x + 162y = 6$.*

Utilizando o algoritmo de Euclides do exemplo 13 tem-se

$6 = 18 - 12$, mas $12 = 48 - 18 \cdot 2$, logo

$6 = 18 - (48 - 18 \cdot 2) = 18 - 48 + 18 \cdot 2 = 18 \cdot 3 - 48$, ou seja,

$6 = 18 \cdot 3 - 48$ note que $18 = 162 - 48 \cdot 3$,

$6 = (162 - 48 \cdot 3) \cdot 3 - 48 = 162 \cdot 3 - 48 \cdot 9 - 48 = 162 \cdot 3 - 48 \cdot 10$, ou seja,

$6 = 162 \cdot 3 - 48 \cdot 10$, mas $48 = 372 - 162 \cdot 2$, segue que

$6 = 162 \cdot 3 - (372 - 162 \cdot 2) \cdot 10 = 162 \cdot 3 - 372 \cdot 10 + 162 \cdot 20 = 162 \cdot 23 + 372 \cdot (-10)$.

Logo$6 = 162 \cdot 23 + 372 \cdot (-10)$

Portanto $x = -10$ e $y = 23$

Um resultado útil e que pode facilitar os cálculos é o seguinte:

Quaisquer que sejam a, $b \in \mathbb{Z}$, não nulos, e $n \in \mathbb{N}$, tem-se que

$$mdc(na, nb) = n \cdot mdc(a, b).$$

Segue a prova desse resultado.

Demonstração. Sejam $k = mdc(na, nb)$ e $t = mdc(a, b)$. Como t divide a e t divide b então nt divide na e nt divide nb, logo $nt \leq k$, pois $k = mdc(na, nb)$. Existem números inteiros x e y tais que $ax + by = t$, multiplicando por n ambos os lados da igualdade obtem-se $nax + nay = nt$, logo $k \leq nt$, pois $k = mdc(na, nb)$, sendo assim é o menor

número que pode ser escrito como essa soma. Portanto $k = nt$, concluindo assim que $mdc(na, nb) = n \cdot mdc(a, b)$. □

Exemplo 15. $mdc(175, 200) = mdc(25 \cdot 7, 25 \cdot 8) = 25 \cdot mdc(7, 8) = 25$

Importante 6. *Em particular, se dados dois números inteiros a e b tais que mdc(a,b)=1, ou seja, o único divisor comum a ambos é o 1, então pode-se dizer que a e b são primos entre si ou coprimos.*

Saiba Mais 3.

Uma aplicação do mdc que difere um pouco das aplicações apresentadas nos livros didáticos, é a resolução das equações diofantinas lineares, que recebe esse nome em homenagem a Diofanto de Alexandria (aprox. 300d.C.). Dados a, b e $c \in \mathbb{Z}$ as equações diofantinas são do tipo

$$aX + bY = c.$$

Observe a seguinte equação: $4X + 6Y = 3$, não possui nenhum valor inteiro para X e para Y que dê como resultado 3, pois ao somar $4X + 6Y$ nos inteiros os resultados possíveis são números pares, portanto nunca igual a 3.

Mas como isso esta relacionado com mdc? Veja bem a seguinte proposição: Sejam a, b e $c \in \mathbb{Z}$. A equação $aX + bY = c$ admite solução em números inteiros se, e somente se, $mdc(a, b)$ divide c. Demonstração desse resultado em Hefez (2014).

Exemplo 16.

É possível determinar valores inteiros X e Y tais que $24X + 14Y = 18$, pois o $mdc(24, 14) = 2$ divide 18, ou seja, a equação diofantina linear tem solução. Já sabe-se quando terá solução, agora será determinado uma solução particular e consequentemente a solução geral, para isso dividi-se a equação pelo $mdc(24, 14) = 2$ para obter a seguinte equação equivalente,

$$12X + 7Y = 9.$$

Pelo algoritmo de Euclides pode-se escrever

$$\begin{aligned} 12 &= 7.1 + 5, \\ 7 &= 5.1 + 2, \\ 5 &= 2.2 + 1. \end{aligned}$$

Substituindo as equações acima uma nas outras tem-se

$$\begin{aligned} 1 = &\quad 5 - 2.2, \\ 1 = &\quad 5 - 2.(7 - 5), \\ 1 = &\quad 5 - 2.7 + 2.5, \\ 1 = &\quad 3.5 - 2.7, \\ 1 = &\quad 3.(12 - 7) - 2.7, \\ 1 = &\quad 3.12 - 3.7 - 2.7, \\ 1 = &\quad 3.12 - 5.7. \end{aligned}$$

Multiplicando por 9 obtem-se a seguinte equação:

$$9 = 12.27 - 7.45.$$

Assim $x_0 = 27$ e $y_0 = -45$ é uma solução particular da equação

$$12X + 7Y = 9,$$

consequentemente será solução particular da equação $24X + 14Y = 18$. Para determinar a solução geral será utilizado a seguinte proposição: sejam x_0 e y_0 uma solução particular da equação $aX + bY = c$, onde $mdc(a, b) = 1$. Então, as soluções x, y em $\mathbb{Z}$ da equação são $x = x_0 + tb$, $y = y_0 - ta$; $t \in \mathbb{Z}$. Demonstração dessa proposição encontra-se em Hefez (2014).

Usando esta proposição a solução geral da equação diofantina

$$24X + 14Y = 18,$$

será dada por $x = 27 + 7t$ e $y = -45 - 12t$; $t \in \mathbb{Z}$. Basta atribuir valores para t para determinar novas soluções para a equação, ou seja, há infinitas soluções.

1.3 Números primos

Curiosidade 4.

Segundo Coutinho (2014) o nome "números primos" é uma herança grega e naturalmente, não se refere a nenhuma relação de parentesco. Os gregos

> classificavam os números em *primeiros* ou *indecomponíveis* e *secundários* ou *compostos*. Os números compostos são secundários por serem formados a partir dos primos. Os romanos apenas traduziram literalmente a palavra grega para primeiro, que em latim é *primus*. E daí que vêm nossos números primos.

Número primo é todo número inteiro maior que 1 que possui exatamente dois divisores: o 1 e ele mesmo. No entanto um número que não é primo é denominado composto.

Exemplos de números primos: 3, 5, 17 e 23.

Exemplos de números compostos: 4, 9, 25 e 30.

Existe um teste para saber se um número inteiro b é primo, basta verificar quais são os divisores de b de 1 ao maior inteiro inferior a $\sqrt{b}$. Por exemplo, para saber se 41 é primo basta verificar quais são seus divisores do 1 ao 6, e portanto 41 só tem como divisores o 1 e ele mesmo, logo 41 é primo. Observe que se b for um número muito grande esse teste vai precisar de muito tempo.

Outra maneira de verificar se um número é primo é pelo crivo de Eratóstenes, uma tabela na qual se escreve os números naturais do 2 até um valor N e se descobre quais são os números primos até esse valor limite. Além disso, é possível identificar os fatores primos dos números compostos também determinados pelo crivo.

Segue como exemplo o Crivo de Eratóstenes, para $N = 100$. Primeiramente se escreve em forma de tabela números naturais de 2 a 100. Em seguida se risca todos os múltiplos de 2 maiores que 2, depois se risca os múltiplos de 3 maiores que 3, depois observa-se que o quatro já estará riscado, então o novo passo é riscar os múltiplos do menor inteiro ainda não riscado, prosseguindo dessa forma se tem como exemplo a tabela abaixo.

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

Figura 1.1: Tabela: Crivo de Eratóstenes

Ao observar a tabela chega-se a conclusão que os seguintes números naturais menores que 100 são primos: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89 e 97. No entanto esse método também requer tempo, dependendo do valor de N não se torna eficaz descobrir se um número é primo tomando como algoritmo o Crivo de Eratóstenes.

Saiba Mais 4. *Números primos gêmeos: se p e $p+2$ são dois números primos então eles recebem o nome de primos gêmeos. No entanto ainda não se sabe se existem infinitos primos gêmeos.*

Exemplos de primos gêmeos: $(3,5)$, $(5,7)$,$(7,9)$,$(17,19)$.

Curiosidade 5. *Segundo Ribenboim (2014):*

> O maior número primo conhecido cujos algarismos são todos ímpares tem como algarismo inicial o 7 seguido de 74318 algarismos iguais a 9. O maior número primo conhecido tendo o maior número de algarismos iguais a 0 é $207777 \times 10^{207777} + 1$, descoberto por G. LÖH e Y. GALLOT em 2010. E o menor número com 1000 algarismos é $10^{999}+7$, a sua primaridade foi verificada por P. MIHAILESCU em 1998.

1.4 Teorema Fundamental da Aritmética

Um número inteiro maior que 1 será primo ou composto, porém se ele for composto ele poderá ser escrito de modo único (não importando a ordem dos fatores) como um produto de primos. Esse resultado é denominado de Teorema Fundamental da Aritmética. Portanto se pode fatorar um número composto, transformando-o em uma multiplicação de fatores primos.

Exemplo 17.

a) $24 = 2 \cdot 2 \cdot 2 \cdot 3 = 2^3 \cdot 3$,

b) $30 = 2 \cdot 3 \cdot 5$,

c) $100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 \cdot 5^2$.

Saiba Mais 5. *O teorema Fundamental da Aritmética é utilizado para mostrar a irracionalidade de vários números como por exemplo* $\sqrt{2}$.

Demonstração. Suponha que $\sqrt{2}$ seja um número racional, então existem números inteiros p e q tais que $\sqrt{2} = \frac{p}{q}$. Elevando esta equação ao quadrado tem-se $\left(\sqrt{2}\right)^2 = \left(\frac{p}{q}\right)^2$. Assim, é possível escrever $2 = \left(\frac{p}{q}\right)^2$. Logo $2q^2 = p^2$. Observe que se q tiver como fator primo em sua decomposição o 2 e o p também, do lado esquerdo da igualdade terá uma quantidade ímpar de dois e do lado direito uma quantidade par, contradição, pelo TFA. Se q não tiver como fator primo o 2, tanto faz o p tendo ou não o 2 como fator primo, também terá o mesmo caso, do lado esquerdo uma quantidade ímpar e do lado direito uma quantidade par, contradição pelo TFA, pois um número se escreve de maneira única como produto de primos. Portanto, $\sqrt{2}$ é um número irracional. □

É possível fazer uma demonstração semelhante para $\sqrt{10}$, provando que também é irracional.

1.4.1 Quantidade de divisores positivos de um número inteiro

Para todo número inteiro positivo n defini-se $d(n)$ como o número de divisores positivos de n.

Exemplo 18.

a) Divisores de 1: 1; $d(1) = 1$.

b) Divisores de 2: 1 e 2; $d(2) = 2$.

c) Divisores de 3: 1 e 3; $d(3) = 2$.

d) Divisores de 4: 1,2 e 4; $d(4) = 3$.

e) Divisores de 5: 1 e 5; $d(5) = 2$.

f) Divisores de 6: 1, 2, 3 e 6; $d(6) = 4$.

Contudo, dado um número $n > 1$ que não seja tão simples escrever seus divisores e depois contá-los precisa-se do teorema fundamental da aritmética para calcular $d(n)$. Todo número inteiro $n > 1$ pode ser escrito como $n = p_1^{k_1} \cdot p_2^{k_2} \dots p_s^{k_s}$, onde $p_1, p_2, \dots, p_s$, são números primos e $k_1, k_2, \dots, k_s$, são inteiros positivos. Note que qualquer divisor de n não pode ter em sua fatoração primos distintos aos que aparecem na fatoração de n. Além disso, o expoente de cada primo tem que ser menor ou igual ao expoente deste primo correspondente na fatoração de n, ou seja, todo divisor de n é da forma

$$p_1^{l_1} \cdot p_2^{l_2} \dots p_s^{l_s}$$

onde $0 \leq l_j \leq k_j$ para todo $j = 1, \dots, s$.. Sendo assim l_1 pode assumir qualquer um dos valores $0, 1, \dots, k_1$, l_2 pode assumir qualquer um dos valores $0, 1, \dots, k_2$ e assim por diante. Note que cada l_j terá $k_j + 1$ possiblidades. Pelo príncipio multiplicativo da contagem tem-se

$$d(n) = (k_1 + 1)(k_2 + 1) \dots (k_s + 1)$$

.

Exemplo 19. *Determine a quantidade de divisores positivos de* 1000.

$$1000 = 2^3.5^3$$

Logo $d(1000) = (3 + 1)(3 + 1) = 4.4 = 16$

Em particular, para todo número primo p, os únicos divisores de p são 1 e p, logo $d(p) = 2$ e para toda potência de um primo p^k temos que os divisores de p^k são $1, p, p^2, \dots, p^k$, logo $d(p^k) = k + 1$.

Saiba Mais 6. ***Números perfeitos:*** *o que tem em comum número perfeito com divisibilidade? Um número é dito perfeito se ele for igual a soma de seus divisores naturais distintos dele mesmo.*

Talvez para o nosso cotidiano isso não faz um número ser perfeito, mas para matemática essa é a definição e deve-se segui-la rigorosamente tomando cuidado em sala de aula com certas palavras que matematicamente pode ter outro significado.

Exemplos de números perfeitos: 6, pois $6 = 1 + 2 + 3$, note que 1, 2 e 3 são divisores de 6.

$28 = 1 + 2 + 4 + 7 + 14$, neste caso tem-se 1, 2, 4, 7 e 14 como divisores de 28. Até a idade média, conheciam-se apenas os seguintes números perfeitos:

$$6,\ 28,\ 496,\ 8128 \text{ e } 33550336.$$

Observe que para os valores 496, 8128 é melhor fazer a verificação semelhante o exemplo 19, sendo assim tem-se $496 = 2^4 \cdot 31$, logo $d(496) = (4+1) \cdot (1+1) = 5 \cdot 2 = 10$, são eles 1, 2, 4, 8, 16, 31, 62, 124, 248 e 496.

Note que $496 = 1 + 2 + 4 + 8 + 16 + 31 + 62 + 124 + 248$, portanto 496 é um número perfeito.

$$8128 = 2^6 \cdot 127,$$

logo $d(8128) = (6+1) \cdot (1+1) = 7 \cdot 2 = 14$, são eles

$$1, 2, 4, 8, 16, 32, 64, 127, 254, 508, 1016, 2032, 4064, 8128$$

Note que $8128 = 1 + 2 + 4 + 8 + 16 + 32 + 64 + 127 + 254 + 508 + 1016 + 2032 + 4064$, portanto 8128 é um número perfeito.

Ainda não se sabe se existem números perfeitos ímpares, todos os números perfeitos conhecidos são pares, além disso, se os números perfeitos pares são infinitos.

Curiosidade 6. ***Conjectura de Goldbach***

Todo número inteiro par maior que 2 pode ser escrito como a soma de dois números primos. Todo inteiro ímpar maior que 5 é a soma de três números primos. Em 1742, Goldbach escreveu essas observações em carta para Euler, a primeira ficou conhecida

como conjectura forte e a segunda como conjectura fraca. A primeira até hoje não foi provada para todo inteiro par maior que dois . No entanto "o peruano Harald Helfgott em 2005 começou a estudar o trabalho de outros cientistas que haviam provado a conjectura fraca para determinados números e, em junho de 2013, resolveu um problema que já durava três séculos, provou que a conjectura fraca de Goldbach estava certa, ou seja, todo número ímpar maior que 5 é a soma de três números primos."(Notícias r7, 2015)

Pode até se pensar que para o dia a dia essa demonstração não sirva para resolver nenhum problema, porém para a teoria dos números, para o desenvolvimento interno da matemática representa muito. Pode ser que as ideias utilizadas na demonstração sirva como ferramenta para outras demonstrações.

Para Refletir 2. *Quantos são os números primos? Não existe uma quantidade definida de números primos pois existem infinitos números primos, ou seja, é possível tomar um número primo maior do que qualquer outro número primo dado.*

A seguir uma demonstração atribuída a Euclides.

Demonstração. Suponha que existe uma quantidade finita de números primos, ou seja, existem m números primos $p_1, p_2, \ldots, p_m$. Dado um inteiro N tal que, $N = p_1.p_2.p_m + 1 > 1$. N não é divisível por nenhum primo p_i, porque se fosse o 1 também seria divisível por algum p_i, mas 1 não é primo e 1 só é divisível por ele mesmo. Isso nos leva a afirmar que N não é composto, pois não pode ser escrito como produto de primos ou seja, a quantidade de números primos não é finita. □

Curiosidade 7. *Há uma busca pelos números primos, sabendo que são infinitos e fundamentais para a segurança da criptografia RSA. Contudo com auxílio da tecnologia buscam encontrar os maiores números primos. Nesse contexto que em 26 de dezembro de 2017 o engenheiro elétrico Jonathan Pace de 51 anos morador de uma cidade no sudeste americano descobriu o maior número primo conhecido por toda humanidade. O número primo descoberto por ele tem 23.249.425 dígitos. Para garantir que o número é realmente primo foi verificado independentemente em quatro programas diferentes em execução em várias configurações de hardware. (Mersenne, 2018)*

> Com o ritmo cada vez mais acelerado da internet e a consequente demanda por números primos cada vez maiores, a prova de Euclides de que os primos nunca se esgotarão adquiriu subitamente um significado comercial inesperado. (du Sautoy, 2007)

Capítulo 2

Surgimento da criptografia RSA

Heródoto, um historiador grego foi um dos primeiros a relatar a comunicação por meio da escrita secreta. Para ele foi essa escrita que salvou a Grécia dos ataques da Pérsia. Uma escrita que consistia na ocultação da mensagem, por exemplo, mensagens em tabuletas coberta com cera, em couro cabeludo, nesse caso esperava o cabelo crescer para esconder a mensagem, ou então em seda fina e coberta com cera formando uma pequena bola.

Esse tipo de comunicação secreta é denominada de esteganografia, ao qual também inclui a técnica da escrita com tinta invisível.

A esteganografia possui uma certa fragilidade, pois se o portador da mensagem for interceptado e a mensagem descoberta tudo que está escrito será revelado.

Enquanto a esteganografia deriva das palavras gregas *Steganos*, que significa coberto e *graphein*, que significa escrever . A criptografia que evoluiu paralelamente deriva da palavra grega *kriptos* que significa oculto. Segundo Singh (2014) o objetivo da criptografia não é ocultar a existência de uma mensagem, e sim esconder o seu significado - um processo conhecido como *encriptação*.

A esteganografia e a criptografia podem estar juntas de tal modo a tornar a comunicação mais segura, mas ainda sim a criptografia é mais vantajosa, pois impede que a informação caia em mãos erradas.

A criptografia é uma ciência que estuda técnicas que transformam mensagens legíveis em mensagens ilegíveis, de forma que possa ser compreendida apenas pela pessoa autorizada, seu destinatário. As técnicas são divididas em dois tipos: transposição e substituição. A transposição consiste no rearranjo das letras, como anagramas. Se ela for

feita de modo aleatório oferecerá um nível alto de segurança, porém fica difícil até mesmo para o receptor a decodificação. Contudo para que a transposição seja feita de tal modo que o destinatário consiga decodificar a mensagem, o rearranjo das letras deve seguir um sistema acertado por ele e pelo remetente.

No século V a.C. temos a **Cítala** o primeiro aparelho criptográfico militar de criptografia de transposição, sendo um bastão de madeira ao qual é enrolado uma tira de couro. Com a tira de couro enrolada no bastão o remetente escreve a mensagem, depois desenrola a tira, ficando assim uma sequência de letras sem significado, o destinatário para decodificar a mensagem enrola a tira em uma cítala de mesmo diâmetro.

Figura 2.1: Cítala. (Fonte: Wordpress (2013))

O outro tipo de criptografia é a de substituição, consiste em substituir cada letra da mensagem original por uma letra diferente ou por um símbolo. Se ao substituir a letra original o alfabeto cifrado é deslocado um número fixo de posições em relação ao alfabeto original (2.2) é chamado cifra de César em homenagem ao general romano Julio Cesar que utilizava um deslocamento de três casas em relação ao alfabeto original.

Alfabeto original	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Alfabeto cifrado	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
Texto original	t	e	o	r	i	a		d	o	s		n	u	m	e	r	o	s								
Texto cifrado	W	H	R	U	L	D		G	R	V		Q	X	P	H	U	R	V								

Figura 2.2: Exemplo de cifra de César

Pode-se deslocar entre uma e vinte e cinco casas, usando a cifra de substituição de César, nesse caso é possível criar 25 códigos diferentes, o que não o torna seguro, pois quem o interceptar terá apenas 25 possibilidades (desde que o interceptador suspeite que a cifra seja de César) para testar e conseguir decifrar a mensagem. Contudo se for feito qualquer rearranjo das letras, não apenas um deslocamento, tem-se um número maior de cifras.

> Cada cifra pode ser considerada em termos de um método geral de codificação conhecido como *algoritmo* e uma *chave*, que especifica os detalhes exatos de uma codificação em particular. Neste caso, o algoritmo consiste em substituir cada letra do alfabeto original por uma letra do alfabeto cifrado, e o alfabeto cifrado pode consistir em qualquer rearranjo do alfabeto original. A chave define o alfabeto cifrado exato que será usado em uma codificação em particular. (Singh, 2014, p.27)

O inimigo pode até interceptar uma mensagem e descobrir o algoritmo utilizado, mas para conseguir decifrar ele precisará conhecer a chave. Veja o esquema abaixo:

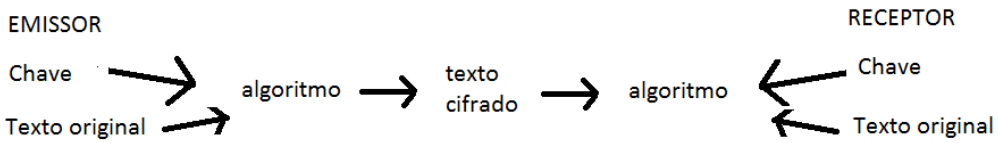


Figura 2.3: Chave para cifrar e decifrar

Quanto mais chaves e quanto mais for mantido em segredo essas chaves, mais será seguro um sistema de código.

A figura 2.4 apresenta um texto cifrado de tal forma que a chave definida pelo alfabeto cifrado consiste de um rearranjo qualquer.

Alfabeto original	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Alfabeto cifrado	J	L	K	A	I	X	B	D	C	Z	P	T	E	U	Q	F	V	W	M	G	O	N	Y	S	H	R
Texto original	m	a	t	e	m	a	t	i	c	a		e		c	r	i	p	t	o	g	r	a	f	i	a	
texto cifrado	E	J	G	I	E	J	G	C	K	J		I		K	W	C	F	G	Q	B	W	J	X	C	J	

Figura 2.4: Exemplo texto cifrado de forma que a chave definida pelo alfabeto cifrado consiste de um rearranjo qualquer

A chave deve ser conhecida pelo remetente e pelo destinatário e para evitar que caia em mãos erradas é necessário evitar registrar no papel, sendo assim rearranjar de forma aleatória fica difícil memorizar. Então, para facilitar o remetente escolhia uma palavra-chave ou frase-chave para dar início ao alfabeto cifrado. Por exemplo, escolhe-se como frase-chave "teoria dos números", em seguida remove-se as letras repetidas e os espaços, obtendo TEORIADSNUM, e este será o início do alfabeto cifrado.

Alfabeto original	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Alfabeto cifrado	T	E	O	R	I	A	D	S	N	U	M	P	Q	V	W	X	Y	Z	B	C	F	G	H	J	K	L

Figura 2.5: Exemplo alfabeto cifrado iniciando com a frase-chave "teoria dos números"

A forma como a mensagem era cifrada é considerada simples, mas para alguém que interceptasse a mensagem, sem o conhecimento da chave, seria impossível decifrá-la. Portanto, a cifra de substituição dominou a arte da escrita secreta durante o primeiro milênio.

Os árabes também utilizavam a criptografia para codificar os segredos de Estado. Eles usavam um rearranjo do alfabeto original e também símbolos para cifra de substituição. Além disso, os árabes foram capazes de decifrar uma mensagem sem conhecer a chave, inventando assim a ciência denominada *criptoanálise*.

O primeiro avanço dessa ciência está relacionado com a frequência de vezes que uma letra aparece em um texto, ou seja, quais letras são mais comuns. Portanto, a análise de frequência era utilizada para quebrar um texto cifrado.

Enquanto a Europa utilizava o básico da criptografia com os monges que a introduziram no ocidente durante a Idade Média, os árabes já lutavam com a criptoanálise. No entanto, por volta do século XIV os alquimistas e cientistas utilizavam a criptografia para manter suas descobertas em segredo, colaborando assim para o crescimento da criptografia na Europa. Junto com esse crescimento temos a descoberta da criptoanálise. Sendo assim as cortes européias começaram a empregar criptoanalistas para que decifrassem mensagens interceptadas.

Por um lado tinham os criptógrafos com a responsabilidade de manter as mensagens em segredo por meio da cifra de substituição denominada monoalfabética (utilizava apenas um alfabeto cifrado), por outro lado os criptoanalistas com o objetivo de decifrar as mensagens usando a análise de frequência.

A quebra de códigos fez surgir novos métodos para cifra de substituição, um deles foi acrescentar símbolos e letras que não representavam nada, contudo, o receptor da mensagem já saberia quais letras não representavam letras verdadeiras, eram nulas, bem como os símbolos.

Outro método desenvolvido foi escrever as palavras com a grafia errada e depois codificar a mensagem. Esses dois métodos dificultariam a análise de frequência das letras pelos criptoanalistas.

Na disputa entre os criptógrafos e os criptoanalistas, os criptógrafos se sentiram pressionados a desenvolverem uma nova cifra, mais segura, pois a cifra de substituição monoalfabética já não conseguia guardar segredos.

No final do século XVI surge uma nova cifra, denominada cifra de Vigenère, em honra ao francês Blaise de Vigenère.

Alfabeto correto	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Figura 2.6: Quadrado de Vigenére

Para dar um exemplo da cifra de Vigenère vamos cifrar a frase "guardar segredos". Primeiro define-se uma palavra-chave ou frase-chave, por exemplo a palavra FORTE. De acordo com a palavra-chave, a letra F representa a linha 5 do quadrado de Vigenère, sendo assim o G será representado por L, o O representa a linha 14, logo o U será representado por I, o R representa a linha 17, logo o A será representado por R, e assim até chegar na fileira do E e depois repetimos o processo.

Palavra-chave	F	O	R	T	E	F	O	R	T	E	F	O	R	T	E
Texto original	g	u	a	r	d	a	r	s	e	g	r	e	d	o	s
Texto cifrado	L	I	R	K	H	F	F	J	X	K	W	S	U	H	W

Figura 2.7: Exemplo: frase "guardar segredos" cifrado com a cifra de Vigenére

A cifra de Vigenère usava vários alfabetos cifrados, conhecida como cifra de subs-

tituição polialfabética , tornando-o mais seguro, no entanto, mais complicado e, não foi bem aceito pelos militares, pois precisavam de rapidez e simplicidade em suas comunicações, o tempo para eles em muitas situações era essencial. Observe que nessa cifra a mesma letra pode ser cifrada de maneiras diferentes, ou seja, podemos ter mais de um símbolo ou letra representando uma letra da mensagem original. Mas apesar da dificuldade, essa cifra também apresentava fragilidade, para a mensagem ser cifrada iniciava-se com palavra-chave, desse modo se a palavra for composta de 4 letras, por exemplo, ela irá determinar 4 alfabetos cifrados. Sendo assim ao longo do texto cifrado pode haver repetições de letras, figura 2.8.

Palavra-chave	T	U	D	O	T	U	D	O	T	U	D	O	T	U	D	O
Texto original	p	a	r	a	c	a	s	a	p	a	r	a	v	i	d	a
Texto cifrado	I	U	U	O	V	U	V	O	I	U	U	O	O	C	G	O

Figura 2.8: Exemplo: frase “para casa para vida” cifrado com a cifra de Vigenére

No século XIX o britânico Charles Babbage, conseguiu quebrar a cifra de Vigenère analisando essas repetições junto com os espaçamentos de cada repetição para que assim pudesse descobrir o comprimento da palavra-chave. Com o comprimento da palavra-chave podemos dividir o texto de acordo com as cifras de substituição monoalfabética, definida por cada letra da palavra-chave.

A quebra da cifra de Vigenère produziu um grande avanço na criptoanálise desde que a cifra de substituição monoalfabética foi decifrada pelos arábes no século IX. Mas apesar de ter sido decifrada no século XIX, esta descoberta só foi divulgada no século XX.

Babbage poderia não ter divulgado anteriormente por displicência ou por interesse na segurança nacional, mantendo em segredo para dar vantagem aos britânicos sobre os demais. Independentemente e diferente de Babbage um oficial da reserva do exército prussiano Friedrich Wilhelm Kasiski, publicou em 1863 este avanço na criptoanálise e segundo Singh (2014) desde então a técnica tem sido conhecida como teste de Kasiski e, a contribuição de Babbage é geralmente ignorada. Portanto, ao descobrirem uma técnica, a cifra de Vigenère não era mais segura

Durante a segunda metade do século XIX houve um crescimento no interesse pelas pessoas pelas cifras, pois até então os grandes interessados eram os militares e o Estado. Com o desenvolvimento do telégrafo, as pessoas queriam manter as suas mensagens em segredo despertando assim um interesse comercial pela criptografia. Mesmo

que as cifras das pessoas comuns fossem decifradas pelos criptoanalistas, o que importava era que quem olhasse diretamente o que estava escrito não conseguisse ler imediatamente. Consequentemente de acordo como as pessoas iam se familiarizando com as cifras, elas começaram a criptografar de várias maneiras.

> No fim do século XIX, a criptografia vivia uma época de confusão. Desde que Babbage e Kasiski tinham destruído a segurança da cifra de Vigenère, os criptógrafos buscavam por uma nova cifra, algo que pudesse restabelecer as comunicações secretas, permitindo que os homens de negócios e os militares explorassem a rapidez do telégrafo sem que seus comunicados fossem roubados ou decifrados. (Singh, 2014, p.119)

Em 1894 temos a invenção do rádio pelo físico italiano Guglielmo Marconi. Esse novo meio de comunicação sem fio enviava as mensagens com mais facilidade, podendo ser interceptadas sem dificuldades pelo inimigo, desse modo para enviar mensagens secretas através do rádio era necessário uma codificação confiável. Portanto, com o surgimento do rádio e o início da Primeira Guerra Mundial aumentou a necessidade de uma cifragem mais segura.

Segundo Singh (2014) embora houvesse um fluxo de novas cifras, estas eram todas variações ou combinações das cifras do século XIX que já tinham sido quebradas.

O desafio dos criptoanalistas estava na quantidade de mensagens interceptadas, pois antes do rádio elas eram raras, mas depois desse meio de comunicação o fluxo aumentou, ocupando cada vez mais as mentes dos criptoanalistas durante a Primeira Guerra Mundial. Ao decifrarem a cifra de Vigenère os criptógrafos estavam preocupados e perto do fim da guerra, os cientistas da América descobriram que poderiam utilizar a cifra de Vigenère para uma forma nova de cifragem. Haviam percebido que mesmo que as palavras-chave fossem longas, não eram impossíveis de serem decifradas as mensagens, portanto se essas palavras fossem significativas o trabalho do criptoanalista era facilitado. De acordo com Singh (2014) em 1918 os criptógrafos começaram a experimentar com chaves que eram desprovidas de estrutura. E o resultado era uma cifra indecifrável.

Nesse contexto temos o bloco de cifras de uma única vez. Ao qual as chaves eram compostas por uma sequência de letras aleatória e para cifrar uma mensagem era utilizada a cifra de Vigenère. O remetente e o destinatário tinham posse da chave. Haviam centenas de chaves, cada uma em uma folha de papel formando um bloco, cada vez que era cifrada uma mensagem e enviada e o destinatário a ter decifrado a folha com a chave utilizada

era destruída.

Apesar da segurança, na prática não funcionava perfeitamente, pois havia problema na produção das chaves aleatórias em grande quantidade.

Para que as mensagens fossem enviadas com mais segurança, os criptógrafos viram a necessidade de abandonar o lápis e o papel, e começarem a explorar a tecnologia para mandar mensagem.

De acordo com Singh (2014) a primeira máquina criptográfica é o disco de cifras, inventado no século XV pelo arquiteto italiano Leon alberti, um dos pais da cifra polialfabética.

Figura 2.9: Disco de cifras dos confederados utilizado na Guerra Civil americana . (Fonte:Wordpress (2014))

O disco de cifra poderia ser utilizado para cifrar uma mensagem com uma cifra de César ou uma cifra polialfabética com o uso da palavra-chave. O disco é mais rápido se comparado com o quadrado de Vigenère, seria uma versão mecanizada do quadrado. Porém assim como a cifra de Vigenère foi quebrada por Babbage e Kasiski essa nova versão também poderia ser decifrável por interceptadores.

No século XX o alemão Arthur Scherbius desenvolveu uma máquina criptográfica, uma versão elétrica do disco de cifras de Alberti, denominada Enigma.

Figura 2.10: Máquina Enigma. (Fonte: Brasil Escola (2018))

O remetente e o destinatário de posse da máquina Enigma e do livro de códigos, necessário para ajustar a máquina diariamente, as mensagens poderiam ser cifradas e decifradas com facilidade.

Scherbius não foi o único a inventar uma máquina de cifra, porém nenhum teve sucesso nas vendas, exceto ele, que vendeu sua máquina para comerciantes e militares alemães.

Segundo Singh (2014) a invenção de Scherbius deu aos alemães o sistema mais seguro de criptografia do mundo. Com ele, no início da Segunda Guerra Mundial, as comunicações estavam protegidas por um nível sem igual de cifragem.

O serviço secreto francês conseguiu informações importantes sobre o uso da máquina Enigma, bem como os aspectos internos. Contudo, mesmo construindo uma réplica da máquina, isso não era suficiente para decifrar as mensagens, pois era necessário obter a chave (ajuste inicial da máquina). Esta chave era trocada diariamente, por isso o livro de códigos era construído com várias chaves cada uma para um dia específico. Sendo assim os franceses entregaram as informações para o departamento de cifras Biuro Szyfrów dos poloneses, estes temendo uma invasão tinham uma motivação para decifrar as mensagens da Enigma.

> A Enigma era uma cifra mecânica, e o Biuro Szyfrów concluiu que uma mente mais científica poderia ter uma chance melhor de quebrá-la. O Biuro organizou um curso de criptografia e convidou vinte matemáticos, após cada um deles prestar um juramento de sigilo. (Singh, 2014, p.169)

O que mais se destacou no curso de criptografia foi o matemático Marian Rejewski, que começou a enfrentar o grande desafio de decifrar mensagens cifradas pela Enigma. Rejewski passou um ano fazendo um catálogo de comprimentos de correntes, para que assim pudesse determinar a chave diária antes que o dia terminasse, conseguindo assim decifrar a Enigma, ganhando mais uma batalha para os criptoanalistas, batalha esta que exigiu muito esforço e poder intelectual. A Enigma não era considerada mais indecifrável.

Os poloneses contribuiram ao mostrarem que os matemáticos eram valiosos como decifradores de códigos, pois muitos criptoanalistas eram linguistas e especialistas nos clássicos.

Em 1938 os criptógrafos aumentaram a segurança da Enigma. Rejewski não tinha recursos suficiente para avançar e não podia mais encontrar as chaves diárias. Se a

Polônia não tinha condições de avançar no desenvolvimento da decifragem da Enigma, a França e a Grã-Bretanha poderiam se beneficiar com tais descobertas. Os quebradores de códigos britânicos tinham mais recursos e uma equipe maior do que os poloneses, dessa forma conseguiram decifrar a enigma mesmo com os avanços na segurança da máquina. No entanto, precisava de mais avanços na criptoanálise, pois a máquina Enigma evoluia.

De acordo com Singh (2014) Alan Turing identificou a maior fraqueza da Enigma e graças a ele foi possível quebrar a cifra da Enigma mesmo sob as circunstâncias mais difíceis. Turing foi para Escola de Cifras e Códigos do Governo em Bletchley e começou a desenvolver o trabalho como criptoanalista.

Ao decifrar a Enigma os criptoanalistas da Escola de Códigos e Cifras de Bletchley Park na Inglaterra fez com que a Segunda Guerra Mundial terminasse antes do tempo previsto, salvando vidas caso a guerra continuasse.

Depois da guerra tudo que havia em Bletchley foi destruído, os avanços desenvolvidos na criptoanálise foram mantidos em segredo, contudo, três décadas depois , em 1970 foi permitido a divulgação de informações sobre o trabalho feito em Bletchley.

> Durante a Segunda Guerra Mundial os decifradores de códigos britânicos levaram a melhor sobre os fazedores de códigos alemães, porque os homens e mulheres em Bletchley Park seguiram a iniciativa dos poloneses, desenvolvendo algumas das primeiras máquinas de quebra de códigos. Além das bombas de Turing, usadas para quebrar a cifra Enigma, os britânicos inventaram outro aparelho decifrador, o Colossus, para combater uma forma ainda mais poderosa de cifra, a cifra alemã Lorenz. (Singh, 2014, p.267)

Os criptoanalistas contribuíram para o desenvolvimento do computador e eles o utilizavam para quebrar todo tipo de cifra. O computador era utilizado tanto para cifrar quanto para decifrar uma mensagem. Primeiramente, as cifragens por computadores eram feitas pelo governo e militares, pois os computadores não eram acessíveis.

Em 1960 os computadores ficaram mais baratos, as empresas eram capazes de comprar e as cifragens entre elas se difundiam. Uma preocupação a mais para os criptógrafos, pois cada empresa tinha modos particulares de cifragens e para se comunicar de modo seguro com organizações externas, necessitava de um sistema padrão de cifragem.

Horst Feistel, um emigrante alemão, que chegara aos Estados Unidos e durante o início da década de 1970 desenvolveu o sistema Lucifer, sendo este um sistema padrão disponível comercialmente.

A Agência de segurança Nacional (NSA), organização responsável pela segurança das comunicações militares e do governo interferiu no desenvolvimento desse sistema de cifragem, pois temiam que a grande quantidade de chaves disponíves para cifrar seria uma dificuldade para que a NSA pudesse decodificar. Com isso, limitaram o número de chaves, acreditando que a comunidade civil não teria computador desenvolvido para analisar todas as chaves possíveis em tempo razoável. Contudo, a NSA tinha acesso aos maiores sistemas de computação e conseguiria decifrar a mensagem.

Em 23 de novembro de 1976 a cifra Lucifer, adotada como padrão, foi batizada de DES(Data Encryption Standard). A adoção da DES como padrão possibilitou uma comunicação segura para as empresas, porém um grande problema era a distribuição das chaves.

> O problema da distribuição de chaves tem prejudicado a criptografia ao longo de sua história. Por exemplo, durante a Segunda Guerra Mundial, o alto comando alemão precisava distribuir o livro mensal de chaves diárias para todos os seus operadores da Enigma, o que também era um enorme problema logístico. Os submarinos costumavam passar longos períodos longe de suas bases e, de algum modo, precisavam obter um suprimento regular de chaves. Em uma época anterior, os usuários da cifra de Vigenère tinham que encontrar um meio de levar a palavra-chave do emissor ao receptor. Não importa tão segura seja uma cifra em teoria, na prática ela pode ser prejudicada pelo problema da distribuição de chaves. (Singh, 2014, p.276)

O governo para garantir a segurança gastava o que fosse preciso para distribuir as chaves e, além do emissor e do receptor deveriam confiar na pessoa que distribuia as chaves. Se as empresas gastassem dinheiro com a distribuição das chaves poderiam entrar em falência.

O desafio da criptografia era desenvolver técnicas para superar o problema da distribuição das chaves.

O criptógrafo Whitfield Diffie contou com o apoio de Martin Helman, um professor da Universidade de Stanford, na Califórnia. Juntos começaram a pesquisar sobre a distribuição das chaves, para que assim pudessem encontrar uma solução para o problema.

Para se transmitir uma mensagem cifrada, o emissor e o receptor antes devem trocar em segredo a chave, ou seja, para se comunicar uma mensagem em segredo, antes devem partilhar outro segredo. Essa é uma característica da criptografia denominada simétrica.

A criptografia simétrica é aquela em que o processo de decifragem é o oposto da cifragem. Tanto o emissor quanto o receptor compartilham do mesmo conhecimento e utilizam a mesma chave para cifrar e decifrar. Contudo a chamada criptografia assimétrica utilizam chaves diferentes para cifrar e para decifrar. Nesse sistema tanto o emissor quanto o receptor tem sua chave particular e há uma chave pública que pode ser divulgada para todos. A pessoa de posse da chave pública poderá enviar uma mensagem cifrada para o receptor, e apenas este terá a chave de decifragem para tal chave pública.

Diffie e Helman publicaram um artigo em 1975 propondo a criptografia de chave pública, mas para colocá-la em prática era necessário encontrar uma função de mão única apropriada para determinar uma cifra assimétrica. Depois da divulgação a busca para encontrar a cifra assimétrica foi vencida pelos cientistas da computação Ron Rivest e Adi Shamir e o matemático Leonard Adleman. Enquanto os cientistas apresentavam as ideias, o matemático era responsável por detectar as falhas. Em abril de 1977 Rivest tinha feito uma descoberta, sendo possível com ajuda de Adleman e Shamir depois de muitas tentativas fracassadas. A descoberta ficou conhecida como sistema RSA (Rivest, Shamir, Adleman) tornando-se a cifra mais influente da criptografia moderna e nesse sistema se encontra a função de mão única baseada nos números primos e na fatoração.

No RSA cada pessoa pode escolher um valor n, obtido pela multiplicação de dois números primos p e q, n será a chave pública e p e q as chaves particulares. Com os valores de p e q para determinar n, leva-se alguns segundos, mas se for dado o valor de n muito grande, para determinar p e q levará muito mais tempo. A fatoração é um cálculo trabalhoso, por isso quanto maior o número, mais tempo será necessário para escrevê-lo como produto de primos.

Singh (2014) afirma que "para importantes transações bancárias, n tende a ser em torno de 10^{308} e os esforços combinados de cem milhões de microcomputadores levariam mais de mil anos para quebrar esta cifra". Com valores suficientemente grandes de p e q a RSA é invencível. Enquanto não se descobre um método para que a fatoração seja feita de forma rápida, a RSA estará segura.

Com o RSA o problema com a distribuição das chaves foi solucionado, pois não precisa trocar as chaves emissor e receptor ou até mesmo ter que confiar em uma terceira pessoa para distribuir a chave, pois a RSA é uma criptografia de chave pública.

Em agosto de 1977 Martin Gardener anunciou pela primeira vez a existência da

RSA ao escrever um artigo intitulado “Um novo tipo de cifra que levará milhões de anos para ser decifrado”.

> De acordo com o governo britânico, a criptografia de chave pública foi inventada, originalmentente, no Quartel-General de Comunicações do Governo (GCHQ) em Cheltenham, o estabelecimento altamente secreto que foi formado a partir dos remanescentes de Bletchley Park, depois da Segunda Guerra mundial. (Singh, 2014, p.305)

James Ellis, um dos principais criptógrafos do governo chegou a conclusão em 1969 que a criptografia de chave pública era possível, ele também sabia que era necessário uma função que só pudesse ser revertida se o receptor tivesse um elemento específico da informação. Clifford Cocks um matemático entrou para GCHQ, e mesmo sabendo pouco sobre cifragem, ele começou a formular a descoberta da cifra assimétrica, mais tarde conhecida como RSA.

Cocks por trabalhar com teoria dos números e ao pensar em funções de mão única ele pensou nos números primos e na fatoração. Em 1974 Cocks contou com a ajuda de Malcolm Williamson, além de velhos amigos, Williamson entrara para GCHG como criptógrafo. Porém, mesmo os três criptógrafos descobrindo o sistema de criptografia de chave pública eles não podiam divulgar, pois as descobertas da GCHQ eram mantidas em segredo. No entanto, a descoberta feita por Adleman, Rivest e Shamir foi totalmente independente e a desenvolveram contribuindo para um avanço digital.

Na Era da Informação, as mensagens digitais são comuns na sociedade. O comércio por meio da internet se desenvolve, portanto é necessário proteger as informações que circulam pelo mundo. Durante dois mil anos quem utilizava a criptografia eram os militares e o governo, mas hoje qualquer pessoa que utiliza a internet para negócios, transações bancárias, entre outros, precisam proteger suas informações.

Uma empresa pode distribuir sua chave pública a todos que queiram enviar, por exemplo, o número do cartão de crédito. No entanto, mesmo que todos utilizem a mesma chave para codificar seus dados, estes só serão lidos pela empresa que administra a página virtual, nem os clientes conseguem mais lê-los, nem os seus dados e nem dos demais. “Se você estiver fazendo compras pela internet do conforto de sua casa, usando um computador pessoal com muita memória e um processador rápido, nem se dará conta do tempo necessário para codificar o número de seu cartão de crédito.”(du Sautoy, 2007)

De acordo com Singh (2014) “a cifra RSA é usada para proteger as mais importantes comunicações militares, diplomáticas, comerciais e criminosas. Mas para desafiar uma cifragem RSA forte, os criptoanalistas precisarão de um salto teórico ou tecnológico.”

Capítulo 3

Criptografia RSA pelo método da divisão Euclidiana

A criptografia RSA envolve um par de chave pública e um par de chave privada, estas chaves são geradas da seguinte maneira:

1. Escolhe-se dois números primos grandes p e q. Segundo Stallings (2015) para uma chave (n) com 309 dígitos decimais, tanto p quanto q deverão estar na ordem de grandeza de 10^{75} a 10^{100}.

2. Calcula-se $n = p \cdot q$.

3. Calcula-se $(p-1) \cdot (q-1)$.

4. Escolhe-se um inteiro positivo e talque $mdc(e, (p-1)(q-1)) = 1$.

5. Determina-se um inteiro positivo d tal que o resto da divisão de $e \cdot d$ por $(p-1)(q-1)$ seja 1, com $1 \leq d < (p-1)(q-1)$.

Portanto a chave pública será o par (n, e) e a chave privada o par (n, d).

A seguir tem-se as etapas de pré-codificação, codificação e decodificação de uma mensagem.

3.1 Pré-codificação de uma mensagem

A pré-codificação é a etapa em que se converte as letras em números, ou seja, a mensagem original é convertida em uma sequência de números. Para esta etapa geral-

mente é utilizada a tabela de conversão ASCII(American Standard Code for Information Interchange), um Código Padrão Americano para o Intercâmbio de Informação. Nele contém letras, números, acentos e sinais diversos representados numericamente. Porém, para exemplificar será feito a conversão utilizando a seguinte tabela

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

Figura 3.1: Conversão de letras em números

Além das letras os espaços entre as palavras será substituído pelo número 99. Observe que as letras correspondem a um número de dois algarismos, pois caso tivesse números com um e dois algarismos poderia causar confusão. Para que se possa entender melhor o processo de pré-codificação segue um exemplo.

Exemplo 20. *Texto original: DIREITOS E DEVERES.*
Texto convertido em números 13182714182924289914991314311427142 8.

Em seguida é preciso determinar os parâmetros do sistema RSA, que são dois primos distintos p e q, tal que $n = p \cdot q$.

O processo final da pré-codificação consiste em dividir em blocos o número produzido ao converter o texto em número. Sendo que os blocos devem ser números menores que n, evitando que o bloco comece por 0, pois pode ocorrer problema na decodificação (Dado o bloco 024, por exemplo, ao decodificar pode ser que apareça apenas 24, o que dá problema para obter o texto original).

Utilizando o exemplo 20 e escolhendo $p = 11$ e $q = 13$ então $n = 143$. Neste caso tem-se os seguintes blocos:

131 - 82 - 71 - 41 - 82 - 92 - 42 - 89 - 91 - 49 - 91 - 31 - 43 - 114 - 27 - 142 - 8

É importante ressaltar que a maneira de escolher os blocos não é única e os blocos não precisam ter o mesmo número de dígitos, independente dos números representados pelos blocos, estes serão calculados normalmente, sem nenhum problema, o fundamental é que o valor do bloco seja menor que n, pois a fundamentação matemática do RSA (seção 3.4) é necessário ter como hipótese que o número do bloco seja menor que n.

3.2 Codificação de uma mensagem

Para o processo de codificação é necessário o valor de n, com $n = p.q$, e de um número inteiro positivo e tal que $mdc(e, (p-1)(q-1)) = 1$.

Os valores de p e q são mantidos em segredo, já os valores de n e e podem ser divulgados, pois são os números necessários para cifragem. A chave de codificação do sistema RSA é dado pelo par (n, e), denominado chave pública.

Ao passar pelo processo de pré-codificação a mensagem estará convertida numa sequência de números ou blocos. Os blocos serão codificados separadamente e assim permanecerão para não impossibilitar a decodificação.

Seja b um bloco, logo b é um inteiro positivo menor que n. Para determinar o bloco b codificado, denotado por $C(b)$, é preciso calcular o resto da divisão de b^e por n.

Considerando o exemplo 20, dado $p = 11$, $q = 13$, logo $n = 143$, além disso, $(p-1)(q-1) = 10 \cdot 12 = 120$. Escolhendo $e = 7$, pois $mdc(7, 120) = 1$ fazendo as contas obtem-se cada bloco codificado. Para observar as contas em termos de congruências ver (A.2).

$$
\begin{aligned}
131^2 &= 17161 \\
17161 &= 143 \cdot 120 + 1 \\
\left(131^2\right)^3 &= (143 \cdot 120 + 1)^3 \\
131^6 &= 143 \cdot q_1 + 1^6 \\
131^6 &= 143 \cdot q_1 + 1 \\
131^6 \cdot 131 &= 143 \cdot q_1 \cdot 131 + 131 \\
131^7 &= 143 \cdot q_2 + 131
\end{aligned}
\qquad
\begin{aligned}
82^2 &= 6724 \\
6724 &= 143 \cdot 47 + 3 \\
\left(82^2\right)^3 &= (143 \cdot 47 + 3)^3 \\
82^6 &= 143 \cdot p_1 + 27 \\
82^6 \cdot 82 &= 143 \cdot p_1 \cdot 82 + 27 \cdot 82 \\
82^7 &= 143 \cdot p_2 + 2214 \\
82^7 &= 143 \cdot p_2 + 143 \cdot 15 + 69 \\
82^7 &= 143 \cdot p_3 + 69
\end{aligned}
$$

Logo $C(131) = 131$ e $C(82) = 69$

$$
\begin{aligned}
71^2 &= 5041 \\
5041 &= 143 \cdot 35 + 36 \\
\left(71^2\right)^3 &= (143 \cdot 35 + 36)^3 \\
71^6 &= 143 \cdot t_1 + 36^3 \\
71^6 &= 143 \cdot t_1 + 46656 \\
71^6 &= 143 \cdot t_1 + 143 \cdot 326 + 38 \\
71^6 &= 143 \cdot t_2 + 38 \\
71^6 \cdot 71 &= 143 \cdot t_2 \cdot 71 + 38 \cdot 71 \\
71^7 &= 143 \cdot t_3 + 2698 \\
71^7 &= 143 \cdot t_3 + 143 \cdot 18 + 124 \\
71^7 &= 143 \cdot t_4 + 124
\end{aligned}
\qquad
\begin{aligned}
41^3 &= 68921 \\
68921 &= 143 \cdot 481 + 138 \\
\left(41^3\right)^2 &= (143 \cdot 481 + 138)^2 \\
41^6 &= 143 \cdot n_1 + 138^2 \\
41^6 &= 143 \cdot n_1 + 19044 \\
41^6 &= 143 \cdot n_1 + 143 \cdot 133 + 25 \\
41^6 &= 143 \cdot n_2 + 25 \\
41^6 \cdot 41 &= 143 \cdot n_2 \cdot 41 + 25 \cdot 41 \\
41^7 &= 143 \cdot n_3 + 1025 \\
41^7 &= 143 \cdot n_3 + 143 \cdot 7 + 24 \\
41^7 &= 143 \cdot n_4 + 24
\end{aligned}
$$

Logo $C(71) = 124$ e $C(41) = 24$.

$$
\begin{aligned}
92^3 &= 778688 \\
778688 &= 143 \cdot 5445 + 53 \\
\left(92^3\right)^2 &= 143 \cdot m_1 + 53^2 \\
92^6 &= 143 \cdot m_1 + 2809 \\
92^6 &= 143 \cdot m_1 + 143 \cdot 19 + 92 \\
92^6 &= 143 \cdot m_2 + 92 \\
92^6 \cdot 92 &= 143 \cdot m_2 \cdot 92 + 92^2 \\
92^7 &= 143 \cdot m_3 + 8464 \\
92^7 &= 143 \cdot m_3 + 143 \cdot 59 + 27 \\
92^7 &= 143 \cdot m_4 + 27
\end{aligned}
\qquad
\begin{aligned}
42^3 &= 74088 \\
74088 &= 143 \cdot 518 + 14 \\
\left(42^3\right)^2 &= (143 \cdot 518 + 14)^2 \\
42^6 &= 143 \cdot b_1 + 14^2 \\
42^6 &= 143 \cdot b_1 + 196 \\
42^6 &= 143 \cdot b_1 + 143 + 53 \\
42^6 &= 143 \cdot b_2 + 53 \\
42^6 \cdot 42 &= 143 \cdot b_2 \cdot 42 + 53 \cdot 42 \\
42^7 &= 143 \cdot b_3 + 2226 \\
42^7 &= 143 \cdot b_3 + 143 \cdot 15 + 81 \\
42^7 &= 143 \cdot b_4 + 81
\end{aligned}
$$

Logo $C(92) = 27$ e $C(42) = 81$

$$
\begin{aligned}
89^3 &= 704969 \\
704969 &= 143 \cdot 4929 + 122 \\
\left(89^3\right)^2 &= (143 \cdot 4929 + 122)^2 \\
89^6 &= 143 \cdot c_1 + 122^2 \\
89^6 &= 143 \cdot c_1 + 14884 \\
89^6 &= 143 \cdot c_1 + 143 \cdot 104 + 12 \\
89^6 &= 143 \cdot c_2 + 12 \\
89^6 \cdot 89 &= 143 \cdot c_2 \cdot 89 + 12 \cdot 89 \\
89^7 &= 143 \cdot c_3 + 1068 \\
89^7 &= 143 \cdot c_3 + 143 \cdot 7 + 67 \\
89^7 &= 143 \cdot c_4 + 67
\end{aligned}
\qquad
\begin{aligned}
91^3 &= 753571 \\
753571 &= 143 \cdot 5269 + 104 \\
\left(91^3\right)^2 &= (143 \cdot 5269 + 104)^2 \\
91^6 &= 143 \cdot d_1 + 104^2 \\
91^6 &= 143 \cdot d_1 + 10816 \\
91^6 &= 143 \cdot d_1 + 143 \cdot 75 + 91 \\
91^6 &= 143 \cdot d_2 + 91 \\
91^6 \cdot 91 &= 143 \cdot d_2 \cdot 91 + 91^2 \\
91^7 &= 143 \cdot d_3 + 8281 \\
91^7 &= 143 \cdot d_3 + 143 \cdot 57 + 130 \\
91^7 &= 143 \cdot d_4 + 130
\end{aligned}
$$

Logo $C(89) = 67$ e $C(91) = 130$

$$
\begin{aligned}
49^3 &= 117649 \\
117649 &= 143 \cdot 822 + 103 \\
\left(49^3\right)^2 &= (143 \cdot 822 + 103)^2 \\
49^6 &= 143 \cdot x_1 + 103^2 \\
49^6 &= 143 \cdot x_1 + 10609 \\
49^6 &= 143 \cdot x_1 + 143 \cdot 74 + 27 \\
49^6 &= 143 \cdot x_2 + 27 \\
49^6 \cdot 49 &= 143 \cdot x_2 \cdot 49 + 27 \cdot 49 \\
49^7 &= 143 \cdot x_3 + 1323 \\
49^7 &= 143 \cdot x_3 + 143 \cdot 9 + 36 \\
49^7 &= 143 \cdot x_4 + 36
\end{aligned}
\qquad
\begin{aligned}
31^3 &= 29791 \\
29791 &= 143 \cdot 208 + 47 \\
\left(31^3\right)^2 &= (143 \cdot 208 + 47)^2 \\
31^6 &= 143 \cdot y_1 + 47^2 \\
31^6 &= 143 \cdot y_1 + 2209 \\
31^6 &= 143 \cdot y_1 + 143 \cdot 15 + 64 \\
31^6 &= 143 \cdot y_2 + 64 \\
31^6 \cdot 31 &= 143 \cdot y_2 \cdot 31 + 64 \cdot 31 \\
31^7 &= 143 \cdot y_3 + 1984 \\
31^7 &= 143 \cdot y_3 + 143 \cdot 13 + 125 \\
31^7 &= 143 \cdot y_4 + 125
\end{aligned}
$$

Logo $C(49) = 36$ e $C(31) = 125$

$$
\begin{aligned}
43^3 &= 79507 \\
79507 &= 143 \cdot 555 + 142 \\
\left(43^3\right)^2 &= (143 \cdot 555 + 142)^2 \\
43^6 &= 143 \cdot d_1 + 142^2 \\
43^6 &= 143 \cdot d_1 + 20164 \\
43^6 &= 143 \cdot d_1 + 143 \cdot 141 + 1 \\
43^6 &= 143 \cdot d_2 + 1 \\
43^6 \cdot 43 &= 143 \cdot d_2 \cdot 43 + 43 \\
43^7 &= 143 \cdot d_3 + 43
\end{aligned}
\qquad
\begin{aligned}
114^3 &= 1481544 \\
1481544 &= 143 \cdot 10360 + 64 \\
\left(114^3\right)^2 &= (143 \cdot 10360 + 64)^2 \\
114^6 &= 143 \cdot t_1 + 64^2 \\
114^6 &= 143 \cdot t_1 + 4096 \\
114^6 &= 143 \cdot t_1 + 143 \cdot 28 + 92 \\
114^6 &= 143 \cdot t_2 + 92 \\
114^6 \cdot 114 &= 143 \cdot t_2 \cdot 114 + 92 \cdot 114 \\
114^7 &= 143 \cdot t_3 + 10488 \\
114^7 &= 143 \cdot t_3 + 143 \cdot 73 + 49 \\
114^7 &= 143 \cdot t_4 + 49
\end{aligned}
$$

Logo $C(43) = 43$ e $C(114) = 49$

$$
\begin{aligned}
27^3 &= 19683 \\
19683 &= 143 \cdot 137 + 92 \\
\left(27^3\right)^2 &= (143 \cdot 137 + 92)^2 \\
27^6 &= 143 \cdot k_1 + 92^2 \\
27^6 &= 143 \cdot k_1 + 8464 \\
27^6 &= 143 \cdot k_1 + 143 \cdot 59 + 27 \\
27^6 &= 143 \cdot k_2 + 27 \\
27^6 \cdot 27 &= 143 \cdot k_2 \cdot 27 + 27^2 \\
27^7 &= 143 \cdot k_3 + 729 \\
27^7 &= 143 \cdot k_3 + 143 \cdot 5 + 14 \\
27^7 &= 143 \cdot k_4 + 14
\end{aligned}
\qquad
\begin{aligned}
142^3 &= 2863288 \\
2863288 &= 143 \cdot 20022 + 142 \\
\left(142^3\right)^2 &= (143 \cdot 20022 + 142)^2 \\
142^6 &= 143 \cdot y_1 + 142^2 \\
142^6 &= 143 \cdot y_1 + 20164 \\
142^6 &= 143 \cdot y_1 + 143 \cdot 141 + 1 \\
142^6 &= 143 \cdot y_2 + 1 \\
142^6 \cdot 142 &= 143 \cdot y_2 \cdot 142 + 142 \\
142^7 &= 143 \cdot y_3 + 142
\end{aligned}
$$

Logo $C(27) = 14$ e $C(142) = 142$

$$
\begin{aligned}
8^3 &= 512 = 143 \cdot 3 + 83 \\
\left(8^3\right)^2 &= (143 \cdot 3 + 83)^2 \\
8^6 &= 143 \cdot z_1 + 83^2 \\
8^6 &= 143 \cdot z_1 + 6889 \\
8^6 &= 143 \cdot z_1 + 143 \cdot 48 + 25 \\
8^6 &= 143 \cdot z_2 + 25 \\
8^6 \cdot 8 &= 143 \cdot z_2 \cdot 8 + 25 \cdot 8 \\
8^7 &= 143 \cdot z_3 + 200 \\
8^7 &= 143 \cdot z_3 + 143 + 57 \\
8^7 &= 143 \cdot z_4 + 57
\end{aligned}
$$

Logo $C(8) = 57$

Portanto ao realizar todos os cálculos codifica-se a mensagem e obtem-se os blocos:

131 - 69 - 124 - 24 - 69 - 27 - 81 - 67 - 130 - 36 - 130 - 125 - 43 - 49 - 14 - 142 - 57

3.3 Decodificação de uma mensagem

Para decodificar uma mensagem é necessário conhecer dois números: n e um inteiro d, tal que o resto da divisão de $e \cdot d$ por $(p-1)(q-1)$ seja 1. Além disso $1 \leq d < (p-1)(q-1)$.

A chave de decodificação é dada pelo par (n, d), o valor d é denominado chave particular ou chave de decifragem. Sendo a um bloco da mensagem codificada, deno-

tando por $D(a)$ o resultado do processo de decodificação, ou seja, o bloco original, para determinar $D(a)$ é preciso calcular o resto da divisão de a^d por n.

Dando continuidade ao exemplo 20, temos $n = 143$ e $e = 7$. Para determinar o valor d, de acordo com o algoritmo da divisão pode-se escrever a seguinte igualdade:

$$\begin{aligned} 7 \cdot d = &\quad 120 \cdot q + 1 \\ d = &\quad \frac{120 \cdot q}{7} + \frac{1}{7}, \text{ note que } 120 = 7 \cdot 17 + 1, \text{ logo} \\ d = &\quad \frac{7 \cdot 17q}{7} + \frac{1q}{7} + \frac{1}{7} \\ d = &\quad 17 \cdot q + \frac{q+1}{7}. \end{aligned}$$

O valor d é um número inteiro, então é necessário que o lado direito da igualdade seja um número inteiro, mas para isso $\frac{q+1}{7}$ deve ser inteiro. Sendo assim $q = 6$ satisfaz esta condição. Segue que $d = 17 \times 6 + 1 = 103$. É importante notar que $1 \leq d < 120$. Portanto $d = 103$.

Com o valor de d determinado inicia-se a decodificação dos blocos, por exemplo, para decodificar o bloco 131 da mensagem codificada calcula-se o resto da divisão de 131^{103} por 143.

Os cálculos a seguir foram realizados com auxílio apenas do lápis e papel com o objetivo de apresentar a matemática que está por trás desse tipo de comunicação sigilosa. No entanto, com números maiores é ineficiente realizar esses cálculos e precisa-se do auxílio do computador.

Em seguida são apresentados os cálculos realizados para decodificação.

$$
\begin{aligned}
69^3 &= 328509 \\
328509 &= 143 \cdot 2297 + 38 \\
\left(69^3\right)^3 &= (143 \cdot 2297 + 38)^3 \\
69^9 &= 143 \cdot g_1 + 38^3 \\
69^9 &= 143 \cdot g_1 + 54872 \\
69^9 &= 143 \cdot g_1 + 143 \cdot 383 + 103 \\
69^9 &= 143 \cdot g_2 + 103 \\
\left(69^9\right)^2 &= (143 \cdot g_2 + 103)^2 \\
69^{18} &= 143 \cdot g_3 + 103^2 \\
69^{18} &= 143 \cdot g_3 + 10609 \\
69^{18} &= 143 \cdot g_3 + 143 \cdot 74 + 27 \\
69^{18} &= 143 \cdot g_4 + 27 \\
\left(69^{18}\right)^5 &= (143 \cdot g_4 + 27)^5 \\
69^{90} &= 143 \cdot g_5 + 27^5 \\
69^{90} &= 143 \cdot g_5 + 14348907 \\
69^{90} &= 143 \cdot g_5 + 143 \cdot 100342 + 1 \\
69^{90} &= 143 \cdot g_6 + 1 \\
69^{90} \cdot 69^9 &= (143 \cdot g_6 + 1)(143 \cdot g_2 + 103) \\
69^{99} &= 143 \cdot g_7 + 103 \\
69^{99} \cdot 69^3 &= (143 \cdot g_7 + 103)(143 \cdot 2297 + 38) \\
69^{102} &= 143 \cdot g_8 + 103 \cdot 38 \\
69^{102} &= 143 \cdot g_8 + 3914 \\
69^{102} &= 143 \cdot g_8 + 143 \cdot 27 + 53 \\
69^{102} &= 143 \cdot g_9 + 53 \\
69^{102} \cdot 69 &= 143 \cdot g_9 \cdot 69 + 53 \cdot 69 \\
69^{103} &= 143 \cdot g_{10} + 3657 \\
69^{103} &= 143 \cdot g_{10} + 143 \cdot 25 + 82 \\
69^{103} &= 143 \cdot g_{11} + 82
\end{aligned}
$$

$$
\begin{aligned}
124^3 &= 1906624 \\
1906624 &= 143 \cdot 13333 + 5 \\
\left(124^3\right)^{10} &= (143 \cdot 13333 + 5)^{10} \\
124^{30} &= 143 \cdot p_1 + 5^{10} \\
124^{30} &= 143 \cdot p_1 + 9765625 \\
124^{30} &= 143 \cdot p_1 + 143 \cdot 68291 + 12 \\
124^{30} &= 143 \cdot p_2 + 12 \\
\left(124^{30}\right)^3 &= (143 \cdot p_2 + 12)^3 \\
124^{90} &= 143 \cdot p_3 + 12^3 \\
124^{90} &= 143 \cdot p_3 + 1728 \\
124^{90} &= 143 \cdot p_3 + 143 \cdot 12 + 12 \\
124^{90} &= 143 \cdot p_4 + 12 \\
124^9 &= 143q + 5^3 = 143q + 125 \\
124^{90} \cdot 124^9 &= (143 \cdot p_4 + 12)(143q + 125) \\
124^{99} &= 143 \cdot p_5 + 12 \cdot 125 \\
124^{99} &= 143 \cdot p_5 + 1500 \\
124^{99} &= 143 \cdot p_5 + 143 \cdot 10 + 70 \\
124^{99} &= 143 \cdot p_6 + 70 \\
124^{99} \cdot 124^3 &= (143 \cdot p_6 + 70)(143 \cdot 13333 + 5) \\
124^{102} &= 143 \cdot p_7 + 70 \cdot 5 \\
124^{102} &= 143 \cdot p_7 + 350 \\
124^{102} &= 143 \cdot p_7 + 143 \cdot 2 + 64 \\
124^{102} &= 143 \cdot p_8 + 64 \\
124^{102} \cdot 124 &= 143 \cdot p_8 \cdot 124 + 64 \cdot 124 \\
124^{103} &= 143 \cdot p_9 + 7936 \\
124^{103} &= 143 \cdot p_9 + 143 \cdot 55 + 71 \\
124^{103} &= 143 \cdot p_{10} + 71
\end{aligned}
$$

Logo $D(69) = 82$ e $D(124) = 71$

$$
\begin{aligned}
24^5 &= 7962624 \\
7962624 &= 143 \cdot 55682 + 98 \\
\left(24^5\right)^2 &= (143 \cdot 55682 + 98)^2 \\
24^{10} &= 143 \cdot s_1 + 98^2 \\
24^{10} &= 143 \cdot s_1 + 9604 \\
24^{10} &= 143 \cdot s_1 + 143 \cdot 67 + 23 \\
24^{10} &= 143 \cdot s_2 + 23 \\
\left(24^{10}\right)^5 &= (143 \cdot s_2 + 23)^5 \\
24^{50} &= 143 \cdot s_3 + 23^5 \\
24^{50} &= 143 \cdot s_3 + 6436343 \\
24^{50} &= 143 \cdot s_3 + 143 \cdot 45009 + 56 \\
24^{50} &= 143 \cdot s_4 + 56 \\
\left(24^{50}\right)^2 &= (143 \cdot s_4 + 56)^2 \\
24^{100} &= 143 \cdot s_5 + 56^2 \\
24^{100} &= 143 \cdot s_5 + 3136 \\
24^{100} &= 143 \cdot s_5 + 143 \cdot 21 + 133 \\
24^{100} &= 143 \cdot s_6 + 133 \\
24^3 &= 13824 = 143 \cdot 96 + 96 \\
24^{100} \cdot 24^3 &= (143 \cdot s_6 + 133)(143 \cdot 96 + 96) \\
24^{103} &= 143 \cdot s_7 + 133 \cdot 96 \\
24^{103} &= 143 \cdot s_7 + 12768 \\
24^{103} &= 143 \cdot s_7 + 143 \cdot 89 + 41 \\
24^{103} &= 143 \cdot s_8 + 41
\end{aligned}
$$

$$
\begin{aligned}
131^2 &= 17161 \\
17161 &= 143 \cdot 120 + 1 \\
\left(131^2\right)^{51} &= (143 \cdot 120 + 1)^{51} \\
131^{102} &= 143 \cdot f_1 + 1^{51} \\
131^{102} &= 143 \cdot f_1 + 1 \\
131^{102} \cdot 131 &= 143 \cdot f_1 \cdot 131 + 131 \\
131^{103} &= 143 \cdot f_2 + 131
\end{aligned}
$$

$$
\begin{aligned}
27^5 &= 14348907 \\
14348907 &= 143 \cdot 100342 + 1 \\
\left(27^5\right)^{20} &= (143 \cdot 100342 + 1)^{20} \\
27^{100} &= 143 \cdot j_1 + 1^{20} \\
27^{100} &= 143 \cdot j_1 + 1 \\
27^3 &= 19683 = 143 \cdot 137 + 92 \\
27^{100} \cdot 27^3 &= (143 \cdot j_1 + 1)(143 \cdot 137 + 92) \\
27^{103} &= 143 \cdot j_2 + 92
\end{aligned}
$$

$$
\begin{aligned}
14^5 &= 537824 = 143 \cdot 3761 + 1 \\
\left(14^5\right)^{20} &= (143 \cdot 3761 + 1)^{20} \\
14^{100} &= 143 \cdot w_1 + 1 \\
14^3 &= 2744 = 143 \cdot 19 + 27 \\
14^{100} \cdot 14^3 &= (143 \cdot w_1 + 1)(143 \cdot 19 + 27) \\
14^{103} &= 143 \cdot w_2 + 27
\end{aligned}
$$

Logo $D(24) = 41$, $D(27) = 92$ e $D(14) = 27$

$$
\begin{aligned}
81^4 &= 43046721 \\
43046721 &= 143 \cdot 301026 + 3 \\
\left(81^4\right)^{10} &= (143 \cdot 301026 + 3)^{10} \\
81^{40} &= 143 \cdot v_1 + 3^{10} \\
81^{40} &= 143 \cdot v_1 + 59049 \\
81^{40} &= 143 \cdot v_1 + 143 \cdot 412 + 133 \\
81^{40} &= 143 \cdot v_2 + 133 \\
\left(81^{40}\right)^2 &= (143 \cdot v_2 + 133)^2 \\
81^{80} &= 143 \cdot v_3 + 133^2 \\
81^{80} &= 143 \cdot v_3 + 17689 \\
81^{80} &= 143 \cdot v_3 + 143 \cdot 123 + 100 \\
81^{80} &= 143 \cdot v_4 + 100 \\
\left(81^4\right)^5 &= (143 \cdot 301026 + 3)^5 \\
81^{20} &= 143 \cdot v_5 + 3^5 \\
81^{20} &= 143 \cdot v_5 + 243 \\
81^{20} &= 143 \cdot v_5 + 143 + 100 \\
81^{20} &= 143 \cdot v_6 + 100 \\
81^{80} \cdot 81^{20} &= (143 \cdot v_4 + 100)\,(143 \cdot v_6 + 100) \\
81^{100} &= 143 \cdot v_7 + 100 \cdot 100 \\
81^{100} &= 143 \cdot v_7 + 10000 \\
81^{100} &= 143 \cdot v_7 + 143 \cdot 69 + 133 \\
81^{100} &= 143 \cdot v_8 + 133 \\
81^3 &= 531441 = 143 \cdot 3716 + 53 \\
81^{100} \cdot 81^3 &= (143 \cdot v_8 + 133)\,(143 \cdot 3716 + 53) \\
81^{103} &= 143 \cdot v_9 + 133 \cdot 53 \\
81^{103} &= 143 \cdot v_9 + 7049 \\
81^{103} &= 143 \cdot v_9 + 143 \cdot 49 + 42 \\
81^{103} &= 143 \cdot v_{10} + 42
\end{aligned}
$$

$$
\begin{aligned}
67^3 &= 300763 \\
300763 &= 143 \cdot 2103 + 34 \\
\left(67^3\right)^4 &= (143 \cdot 2103 + 34)^4 \\
67^{12} &= 143 \cdot h_1 + 34^4 \\
67^{12} &= 143 \cdot h_1 + 1336336 \\
67^{12} &= 143 \cdot h_1 + 143 \cdot 9345 + 1 \\
67^{12} &= 143 \cdot h_2 + 1 \\
\left(67^{12}\right)^8 &= (143 \cdot h_2 + 1)^8 \\
67^{96} &= 143 \cdot h_3 + 1^8 \\
67^{96} &= 143 \cdot h_3 + 1 \\
\left(67^3\right)^2 &= (143 \cdot 2103 + 34)^2 \\
67^6 &= 143 \cdot h_4 + 34^2 \\
67^6 &= 143 \cdot h_4 + 1156 \\
67^6 &= 143 \cdot h_4 + 143 \cdot 8 + 12 \\
67^6 &= 143 \cdot h_5 + 12 \\
67^6 \cdot 67 &= 143 \cdot h_5 \cdot 67 + 12 \cdot 67 \\
67^7 &= 143 \cdot h_6 + 804 \\
67^7 &= 143 \cdot h_6 + 143 \cdot 5 + 89 \\
67^7 &= 143 \cdot h_7 + 89 \\
67^{96} \cdot 67^7 &= (143 \cdot h_3 + 1)\,(143 \cdot h_7 + 89) \\
67^{103} &= 143 \cdot h_8 + 89
\end{aligned}
$$

Logo $D(81) = 42$ e $D(67) = 89$.

$$
\begin{aligned}
130^2 &= 16900 \\
16900 &= 143 \cdot 118 + 26 \\
\left(130^2\right)^5 &= (143 \cdot 118 + 26)^5 \\
130^{10} &= 143 \cdot a_1 + 26^5 \\
130^{10} &= 143 \cdot a_1 + 11881376 \\
130^{10} &= 143 \cdot a_1 + 143 \cdot 83086 + 78 \\
130^{10} &= 143 \cdot a_2 + 78 \\
\left(130^{10}\right)^3 &= (143 \cdot a_2 + 78)^3 \\
130^{30} &= 143 \cdot a_3 + 78^3 \\
130^{30} &= 143 \cdot a_3 + 474552 \\
130^{30} &= 143 \cdot a_3 + 143 \cdot 3318 + 78 \\
130^{30} &= 143 \cdot a_4 + 78 \\
\left(130^{30}\right)^3 &= (143 \cdot a_4 + 78)^3 \\
130^{90} &= 143 \cdot a_5 + 78^3 \\
130^{90} &= 143 \cdot a_5 + 143 \cdot 3318 + 78 \\
130^{90} &= 143 \cdot a_6 + 78 \\
130^{90} \cdot 130^{10} &= (143 \cdot a_6 + 78)(143 \cdot a_2 + 78) \\
130^{100} &= 143 \cdot a_7 + 78 \cdot 78 \\
130^{100} &= 143 \cdot a_7 + 6084 \\
130^{100} &= 143 \cdot a_7 + 143 \cdot 42 + 78 \\
130^{100} &= 143 \cdot a_8 + 78 \\
130^{100} \cdot 130^2 &= (143 \cdot a_8 + 78)(143 \cdot 118 + 26) \\
130^{102} &= 143 \cdot a_9 + 78 \cdot 26 \\
130^{102} &= 143 \cdot a_9 + 2028 \\
130^{102} &= 143 \cdot a_9 + 143 \cdot 14 + 26 \\
130^{102} &= 143 \cdot a_{10} + 26 \\
130^{102} \cdot 130 &= 143 \cdot a_{10} \cdot 130 + 26 \cdot 130 \\
130^{103} &= 143 \cdot a_{11} + 3380 \\
130^{103} &= 143 \cdot a_{11} + 143 \cdot 23 + 91 \\
130^{103} &= 143 \cdot a_{12} + 91
\end{aligned}
$$

$$
\begin{aligned}
125^2 &= 15625 \\
15625 &= 143 \cdot 109 + 38 \\
\left(125^2\right)^5 &= (143 \cdot 109 + 38)^5 \\
125^{10} &= 143 \cdot m_1 + 38^5 \\
125^{10} &= 143 \cdot m_1 + 79235168 \\
125^{10} &= 143 \cdot m_1 + 143 \cdot 554092 + 12 \\
125^{10} &= 143 \cdot m_2 + 12 \\
\left(125^{10}\right)^2 &= (143 \cdot m_2 + 12)^2 \\
125^{20} &= 143 \cdot m_3 + 12^2 \\
125^{20} &= 143 \cdot m_3 + 144 \\
125^{20} &= 143 \cdot m_3 + 143 + 1 \\
125^{20} &= 143 \cdot m_4 + 1 \\
\left(125^{20}\right)^5 &= (143 \cdot m_4 + 1)^5 \\
125^{100} &= 143 \cdot m_5 + 1^5 \\
125^{100} &= 143 \cdot m_5 + 1 \\
125^{100} \cdot 125^2 &= (143 \cdot m_5 + 1)(143 \cdot 109 + 38) \\
125^{102} &= 143 \cdot m_6 + 38 \\
125^{102} \cdot 125 &= 143 \cdot m_6 \cdot 125 + 38 \cdot 125 \\
125^{103} &= 143 \cdot m_7 + 4750 \\
125^{103} &= 143 \cdot m_7 + 143 \cdot 33 + 31 \\
125^{103} &= 143 \cdot m_8 + 31
\end{aligned}
$$

Logo $D(130) = 91$ e $D(125) = 31$

$$
\begin{aligned}
36^5 &= 60466176 \\
60466176 &= 143 \cdot 422840 + 56 \\
\left(36^5\right)^4 &= (143 \cdot 422840 + 56)^4 \\
36^{20} &= 143 \cdot \alpha_1 + 56^4 \\
36^{20} &= 143 \cdot \alpha_1 + 9834496 \\
36^{20} &= 143 \cdot \alpha_1 + 143 \cdot 68772 + 100 \\
36^{20} &= 143 \cdot \alpha_2 + 100 \\
\left(36^{20}\right)^4 &= (143 \cdot \alpha_2 + 100)^4 \\
36^{80} &= 143 \cdot \alpha_3 + 100^4 \\
36^{80} &= 143 \cdot \alpha_3 + 100000000 \\
36^{80} &= 143 \cdot \alpha_3 + 143 \cdot 699300 + 100 \\
36^{80} &= 143 \cdot \alpha_4 + 100 \\
36^{80} \cdot 36^{20} &= (143 \cdot \alpha_4 + 100)(143 \cdot \alpha_2 + 100) \\
36^{100} &= 143 \cdot \alpha_5 + 100 \cdot 100 \\
36^{100} &= 143 \cdot \alpha_5 + 10000 \\
36^{100} &= 143 \cdot \alpha_5 + 143 \cdot 69 + 133 \\
36^{100} &= 143 \cdot \alpha_6 + 133 \\
36^3 &= 46656 = 143 \cdot 326 + 38 \\
36^{100} \cdot 36^3 &= (143 \cdot \alpha_6 + 133)(143 \cdot 326 + 38) \\
36^{103} &= 143 \cdot \alpha_7 + 133 \cdot 38 \\
36^{103} &= 143 \cdot \alpha_7 + 5054 \\
36^{103} &= 143 \cdot \alpha_7 + 143 \cdot 35 + 49 \\
36^{103} &= 143 \cdot \alpha_8 + 49
\end{aligned}
$$

$$
\begin{aligned}
43^4 &= 3418801 \\
3418801 &= 143 \cdot 23907 + 100 \\
\left(43^4\right)^2 &= (143 \cdot 23907 + 100)^2 \\
43^8 &= 143 \cdot \beta_1 + 100^2 \\
43^8 &= 143 \cdot \beta_1 + 10000 \\
43^8 &= 143 \cdot \beta_1 + 143 \cdot 69 + 133 \\
43^8 &= 143 \cdot \beta_2 + 133 \\
\left(43^8\right)^3 &= (143 \cdot \beta_2 + 133)^3 \\
43^{24} &= 143 \cdot \beta_3 + 133^3 \\
43^{24} &= 143 \cdot \beta_3 + 2352637 \\
43^{24} &= 143 \cdot \beta_3 + 143 \cdot 16452 + 1 \\
43^{24} &= 143 \cdot \beta_4 + 1 \\
\left(43^{24}\right)^4 &= (143 \cdot \beta_4 + 1)^4 \\
43^{96} &= 143 \cdot \beta_5 + 1^4 \\
43^{96} &= 143 \cdot \beta_5 + 1 \\
43^{96} \cdot 43^4 &= (143 \cdot \beta_5 + 1)(143 \cdot 23907 + 100) \\
43^{100} &= 143 \cdot \beta_6 + 100 \\
43^3 &= 79507 = 143 \cdot 555 + 142 \\
43^{100} \cdot 43^3 &= (143 \cdot \beta_6 + 100)(143 \cdot 555 + 142) \\
43^{103} &= 143 \cdot \beta_7 + 100 \cdot 142 \\
43^{103} &= 143 \cdot \beta_7 + 14200 \\
43^{103} &= 143 \cdot \beta_7 + 143 \cdot 99 + 43 \\
43^{103} &= 143 \cdot \beta_8 + 43
\end{aligned}
$$

Logo $D(36) = 49$ e $D(43) = 43$

$$
\begin{aligned}
49^5 &= 282475249 \\
282475249 &= 143 \cdot 1975351 + 56 \\
\left(49^5\right)^4 &= (143 \cdot 1975351 + 56)^4 \\
49^{20} &= 143 \cdot u_1 + 56^4 \\
49^{20} &= 143 \cdot u_1 + 9834496 \\
49^{20} &= 143 \cdot u_1 + 143 \cdot 68772 + 100 \\
49^{20} &= 143 \cdot u_2 + 100 \\
\left(49^{20}\right)^4 &= (143 \cdot u_2 + 100)^4 \\
49^{80} &= 143 \cdot u_3 + 100^4 \\
49^{80} &= 143 \cdot u_3 + 100000000 \\
49^{80} &= 143 \cdot u_3 + 143 \cdot 699300 + 100 \\
49^{80} &= 143 \cdot u_4 + 100 \\
49^{80} \cdot 49^{20} &= (143 \cdot u_4 + 100)(143 \cdot u_2 + 100) \\
49^{100} &= 143 \cdot u_5 + 100 \cdot 100 \\
49^{100} &= 143 \cdot u_5 + 10000 \\
49^{100} &= 143 \cdot u_5 + 143 \cdot 69 + 133 \\
49^{100} &= 143 \cdot u_6 + 133 \\
49^3 &= 117649 = 143 \cdot 822 + 103 \\
49^{100} \cdot 49^3 &= (143 \cdot u_6 + 133)(143 \cdot 822 + 103) \\
49^{103} &= 143 \cdot u_7 + 133 \cdot 103 \\
49^{103} &= 143 \cdot u_7 + 13699 \\
49^{103} &= 143 \cdot u_7 + 143 \cdot 95 + 114 \\
49^{103} &= 143 \cdot u_8 + 114
\end{aligned}
$$

$$
\begin{aligned}
57^4 &= 10556001 \\
10556001 &= 143 \cdot 73818 + 27 \\
\left(57^4\right)^5 &= (143 \cdot 73818 + 27)^5 \\
57^{20} &= 143 \cdot i_1 + 27^5 \\
57^{20} &= 143 \cdot i_1 + 14348907 \\
57^{20} &= 143 \cdot i_1 + 143 \cdot 100342 + 1 \\
57^{20} &= 143 \cdot i_2 + 1 \\
\left(57^{20}\right)^5 &= (143 \cdot i_2 + 1)^5 \\
57^{100} &= 143 \cdot i_3 + 1^5 \\
57^{100} &= 143 \cdot i_3 + 1 \\
57^3 &= 185193 = 143 \cdot 1295 + 8 \\
57^{100} \cdot 57^3 &= (143 \cdot i_3 + 1)(143 \cdot 1295 + 8) \\
57^{103} &= 143 \cdot i_4 + 8
\end{aligned}
$$

$$
\begin{aligned}
142^3 &= 2863288 = 143 \cdot 20022 + 142 \\
\left(142^3\right)^2 &= (143 \cdot 20022 + 142)^2 \\
142^6 &= 143 \cdot \lambda_1 + 142^2 \\
142^6 &= 143 \cdot \lambda_1 + 20164 \\
142^6 &= 143 \cdot \lambda_1 + 143 \cdot 141 + 1 \\
142^6 &= 143 \cdot \lambda_2 + 1 \\
\left(142^6\right)^{17} &= (143 \cdot \lambda_2 + 1)^{17} \\
142^{102} &= 143 \cdot \lambda_3 + 1^{17} \\
142^{102} &= 143 \cdot \lambda_3 + 1 \\
142^{102} \cdot 142 &= 143 \cdot \lambda_3 \cdot 142 + 142 \\
142^{103} &= 143 \cdot \lambda_4 + 142
\end{aligned}
$$

Logo $D(49) = 114$, $D(57) = 8$ e $D(142) = 142$.

Portanto, ao realizar todos os cálculos tem-se os blocos decodificados:

131 - 82 - 71 - 41 - 82 - 92 - 42 - 89 - 91 - 49 - 91 - 31 - 43 - 114 - 27 - 142 - 8.

Ao juntar estes blocos e obter um único número

$$13182714182924289914991314311427142 8$$

tem-se o texto original convertido em números que pela tabela de conversão

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

Figura 3.2: Conversão de letras em números

corresponde a seguinte frase:

"DIREITOS E DEVERES".

Neste exemplo a chave particular poderia ser determinada tendo acesso apenas a chave pública, pois foi escolhido um valor de n com apenas 3 algarismos, desse modo é importante a escolha dos primos p e q para que o RSA seja seguro, pois "o tamanho da chave precisa ser grande o suficiente para tornar o ataque de força bruta impraticável, mas pequeno o suficiente para que a criptografia e a decriptografia sejam viáveis". (Stallings, 2008)

> Evidentemente, um espião que dispuser de um algoritmo de fatoração eficiente poderá utilizá-lo para fatorar n, que é público, obtendo os primos p e q. De posse destes o espião computará $(p-1)(q-1)$ e, conhecido e, que é público, determinará d. Assim, quebrar o RSA não é mais difícil do que fatorar inteiros. Por outro lado, não se conhece nenhum algoritmo eficiente para fatorar. (Lucchesi, 1986)

Para du Sautoy (2007) "a natureza forneceu uma maneira rápida e fácil de produzir os primos com os quais é gerado a criptografia da internet, mas escondeu qualquer maneira rápida de decompor números nos primos que os formam". Existem alguns métodos que permitem determinar se um número é primo ou composto sem fornecer os fatores primos. São chamados testes de primalidade, tais como, teste de Miller Rabin, APR e AKS, para mais exemplos ver Ribenboim (2014).

3.4 Fundamentação matemática do RSA

Suponha p e q números primos distintos, com $n = p \cdot q$, e $e \in \mathbb{N}$, tal que $mdc(e, (p-1)(q-1)) = 1$. Sejam n e e os dados de codificação e n e d os dados de decodificação, com $d \in \mathbb{Z}$ um inteiro definido pelas duas condições:

1. o resto da divisão de $e \cdot d$ por $(p-1)(q-1)$ tem que ser 1.

2. $1 \leq d < (p-1)(q-1)$.

Precisa-se verificar que se b é um inteiro e $1 \leq b \leq n-1$, então $D[C(b)] = b$, ou seja, a decodificação de um bloco b codificado é b. Por definição $D[C(b)]$ é o resto da divisão de $C(b)^d$ por n, então é preciso mostrar que o resto da divisão de $C(b)^d$ por n é b.

Por definição de codificação, $C(b)$ é o resto da divisão de b^e por n, pelo algoritmo da divisão pode-se escrever

$$b^e = nq + C(b), \text{ com } q \text{ e } C(b) \in \mathbb{Z} \text{ talque } 0 \leq C(b) \leq n-1.$$

Elevando ambos os lados da igualdade por d obtem-se

$$b^{ed} = (nq + C(b))^d.$$

Pelo binômio de Newton segue

$$(nq+C(b))^d = (nq)^d + \binom{d}{1}(nq)^{d-1}C(b) + \binom{d}{2}(nq)^{d-2}C(b)^2 + \cdots + \binom{d}{d-1}(nq)C(b)^{d-1} + C(b)^d.$$

Observe que todas as parcelas, exceto a última são múltiplos de n, sendo assim pode-se escrever

$$b^{ed} = (nq + C(b))^d = n \cdot t + C(b)^d,$$

com $t = n^{d-1}q^d + \binom{d}{1}n^{d-2}q^{d-1}C(b) + \binom{d}{2}n^{d-3}q^{d-2}C(b)^2 + \cdots + \binom{d}{d-1}qC(b)^{d-1}$.

Sendo assim

$$C(b)^d = b^{ed} - nt.$$

Pela condição 1, $e \cdot d = (p-1)(q-1)a + 1$, $a \in \mathbb{Z}$, substituindo na equação tem-se

$$C(b)^d = b^{(p-1)(q-1)a+1} - nt,$$
$$C(b)^d = b^{(p-1)(q-1)a} \cdot b - nt.$$

Pelo algoritmo da divisão existem x e y, denominados respectivamente, quociente e resto da divisão de $b^{(p-1)(q-1)a}$ por n, logo $b^{(p-1)(q-1)a} = nx + y$, com $0 \leq y < n$.

Segue que

$$C(b)^d = b^{(p-1)(q-1)a} \cdot b - nt = (nx + y)b - nt,$$
$$C(b)^d = nxb + yb - nt = n(xb - t) + yb.$$

Como $(xb - t) \in \mathbb{Z}$ e $1 \leq b \leq n-1$, logo pela igualdade anterior ao provar que $y = 1$ b será o resto da divisão de $C(b)^d$ por n.

Como $1 \leq b \leq n-1$ e $n = p \cdot q$ então b não pode ser divisível por p e q. Suponha, sem perda de generalidade, que p não divide b.

Será utilizado um resultado denominado pequeno Teorema de Fermat: *dado um número primo p, tem-se que p divide o número $b^p - b$, para todo $b \in \mathbb{Z}$.*

Assim, $b^p - b = b(b^{p-1} - 1)$, logo p divide $b(b^{p-1} - 1)$, mas por hipótese p não divide b, consequentemente, p divide $b^{p-1} - 1$, ou seja, o resto da divisão de b^{p-1} por p é 1.

Escreve-se $b^{p-1} = pk + 1$, elevando ambos os lados dessa igualdade por $(q-1)a$ tem-se

$$b^{(p-1)(q-1)a} = (pk+1)^{(q-1)a},$$

usando binômio de Newton $(pk+1)^{(q-1)a} = ph + 1^{(q-1)a} = ph + 1$, $h \in \mathbb{Z}$.

Portanto $b^{(p-1)(q-1)a} = ph + 1$, isto é, o resto da divisão de $b^{(p-1)(q-1)a}$ por p é 1.

Note que $b^{(p-1)(q-1)a} = nx + y$, como $n = p \cdot q$ tem-se $b^{(p-1)(q-1)a} = p \cdot (qx) + y$, além disso, o resto da divisão de $b^{(p-1)(q-1)a}$ por p é 1, isto implica que $y = 1$, pois $C(b)^d = n(xb - t) + yb = n(xb - t) + b$, pela unicidade do resto e do quociente e como $1 \leq b \leq n-1$, é possível afirmar que o resto da divisão de $C(b)^d$ por n é b, ou seja, $D[C(b)] = b$.

3.5 Assinatura de uma mensagem

Criptografar uma mensagem e envia-lá a alguém é possível por meio da criptografia RSA. Além disso, a mensagem pode ser assinada, de maneira eletrônica. Por exemplo, se um cliente enviasse uma mensagem ao banco solicitando a transferência de um certo valor de uma conta para outra. Como o banco teria certeza que a mensagem foi enviada pelo cliente titular da conta ao qual é realizada a operação? Usando o RSA isso é possível segue o exemplo:

Ana quer mandar uma mensagem para João de modo que João tenha certeza que a mensagem só poderia ser escrita por ela. Sejam C_A e D_A, e C_J e D_J as funções codificação e decodificação de Ana e João, respectivamente. Se fosse para Ana mandar uma mensagem apenas criptografada para João ela pegaria um bloco b da mensagem e

calcularia $C_J(b)$, mas para assinar a mensagem primeiro ela deverá calcular $D_A(b)$ em seguida $C_J[D_A(b)]$. Para obter a mensagem original João aplica a função D_J e obtém $D_A(b)$ e por último aplica a função C_A, que é público. Observe que D_A só é conhecido por Ana, então João pode ficar convencido de que quem escreveu a mensagem realmente foi ela. Em outras palavras, criptografa a mensagem usando a chave privada do emissor (A), servindo para assinatura, em seguida, criptografa novamente usando a chave pública do receptor (B) e assim produz o texto final cifrado. Somente B poderá decifrar a mensagem, pois inicialmente precisará da chave privada de B, garantindo confidencialidade, e para obter o texto original utiliza a chave pública de A. Para Stallings (2008) a desvantagem dessa técnica é que o algoritmo de chave pública, que é complexo, precisa ser usado quatro vezes, em vez de duas, em cada comunicação.

Portanto, alguns algoritmos como o RSA, exibe a seguinte característica: qualquer uma das duas chaves relacionadas pode ser usada para criptografar, com a outra usada para decriptografar. (Stallings, 2008)

Demonstração. Suponha p e q números primos distintos, com $n = p \cdot q$, e $e \in \mathbb{N}$, tal que $mdc(e, (p-1)(q-1)) = 1$. Sejam n e e os dados de decodificação e n e d os dados de codificação, com $d \in \mathbb{Z}$ um inteiro definido pelas duas condições:

1. o resto da divisão de $e \cdot d$ por $(p-1)(q-1)$ tem que ser 1.

2. $1 \leq d < (p-1)(q-1)$

É preciso verificar que se b é um inteiro e $1 \leq b \leq n-1$ então $D[C(b)] = b$. Por definição $D[C(b)]$ é o resto da divisão de $C(b)^e$ por n, então deve-se mostrar que o resto da divisão de $C(b)^e$ por n é b.

Por definição de codificação $C(b)$ é o resto da divisão de b^d por n, pelo algoritmo da divisão pode-se escrever

$$b^d = nq + C(b), \text{ com } q \text{ e } C(b) \in \mathbb{Z} \text{ talque } 0 \leq C(b) \leq n-1.$$

Elevando ambos os lados da igualdade por e obtem-se

$$b^{de} = (nq + C(b))^e.$$

Pelo binômio de Newton tem-se

$$b^{de} = nk + C(b)^e, \text{ com } k \in \mathbb{Z}.$$

Sendo assim

$$C(b)^e = b^{de} - nk.$$

Pela condição 1, $e \cdot d = (p-1)(q-1)a + 1$, $a \in \mathbb{Z}$, substituindo na equação tem-se

$$C(b)^e = b^{(p-1)(q-1)a+1} - nk$$
$$C(b)^e = b^{(p-1)(q-1)a} \cdot b - nk$$

Pelo algoritmo da divisão existem g e j, denominados respectivamente, quociente e resto da divisão de $b^{(p-1)(q-1)a}$ por n, logo $b^{(p-1)(q-1)a} = ng + j$, com $0 \leq j < n$.

Segue que

$$C(b)^e = b^{(p-1)(q-1)a} \times b - nk = (ng + j)b - nk$$
$$C(b)^e = ngb + jb - nk = n(gb - k) + jb$$

Como $(gb - k) \in \mathbb{Z}$ e $1 \leq b \leq n - 1$, logo pela igualdade anterior ao provar que $j = 1$ tem-se que b é o resto da divisão de $C(b)^e$ por n. Para isso usa-se o mesmo argumento utilizado na seção anterior, ao qual prova-se que y=1.

Portanto $C(b)^e = n(gb - k) + jb = n(gb - k) + b$, pela unicidade do resto e do quociente e como $1 \leq b \leq n - 1$, é possível afirmar que o resto da divisão de $C(b)^e$ por n é b, ou seja, $D[C(b)] = b$. □

Assim prova-se que é possível codificar com a chave particular e decodificar com a chave pública.

Capítulo 4

Relato de Experiência

Foram realizadas duas experiências, sendo uma com alunos do 7^{o} ano do ensino fundamental e outra com alunos do 2^{o} ano do ensino médio da Escola Estadual Heliodoro Capistrano da Silva em Cuiabá-MT.

4.1 Ensino Fundamental

Essa experiência consistiu em aulas, sendo um total de 7 horas/aulas, na qual foi trabalhado os conteúdos de divisibilidade (múltiplos, divisores, algoritmo da divisão de Euclides, máximo divisor comum) e números primos (teste para saber se um número é primo, números compostos, decomposição em fatores primos).

A escolha da turma ficou a critério do professor titular, sendo escolhido a turma D. Essa experiência foi feita em horário de aula normal e, estavam presentes a maioria dos alunos. Num primeiro momento conversamos sobre a matemática, sobre o que pensam sobre essa disciplina, quais são suas dificuldades e, para despertar a curiosidade comentei sobre a conjectura de Collatz: *A partir de um certo número n, dividindo-o por* 2 *se for par, ou multiplicando-o por* 3 *e adicionando* 1 *se for ímpar, e fazendo assim sucessivamente chegaremos sempre ao número* 1*, proposta pelo matemático alemão Lothar Collatz em* 1937, para que pudessemos refletir sobre os problemas matemáticos que não tem solução. Fizemos alguns exemplos particulares sobre a conjectura de Collatz e foi mostrado a eles que mesmo tomando valores e fazendo os cálculos para alguns números isso não garante que a conjectura é válida para todos os números naturais, sendo assim não podemos afirmar algo somente mostrando que é válido para alguns números.

Em seguida foi iniciado o conteúdo de divisibilidade, ao serem questionados, por exemplo, sobre como eles sabem que 21 é um múltiplo de 3, eles responderam que 3 vezes 7 é 21, e assim trabalhamos outros exemplos até chegarmos a escrever que qualquer múltiplo de 2 é escrito da forma $2a$, $a \in \mathbb{N}$, múltiplo de 3 é escrito da forma $3b$, $b \in \mathbb{N}$, e assim sucessivamente. No início eles falavam: 2 vezes alguma coisa, 3 vezes alguma coisa, depois já incorporavam as letras.

Foram apresentados vários exemplos sobre múltiplos e divisores, além disso exemplos referente a propriedade da transitividade, um deles foi o seguinte: se 5 divide 10 e 10 divide 30, então 5 divide 30. Depois disso foi proposto aos alunos que eles falassem a propriedade considerando o caso geral e assim eles disseram: se a divide b, e b divide c, então a divide c. Eles haviam entendido a proposta, deixaram de pensar em questões particulares e pensaram de maneira mais abrangente, com o pensamento de que provar uma afirmação na matemática vai além de citar exemplos numéricos. Foi desenvolvido a demonstração dessa propriedade juntamente com eles, é claro que eles precisavam ser questionados, mas de qual maneira? Falei que tínhamos como argumento que a divide b e b divide c e deveríamos provar utilizando esses fatos que a divide c. Com a afirmação de que a divide b, por meio de exemplos como 21 múltiplo de 3 e de 7, pois 21 é igual a $3 \cdot 7$, 12 é múltiplo de 2 e de 6, pois é escrito como $2 \cdot 6$, eles chegaram a conclusão de que b é um múltiplo de a, pois a é um divisor de b, e que $b = ad$, com o mesmo raciocínio eles disseram que c era b vezes alguma coisa, logo após complementaram $c = be$. A substituição $c = ade$ foi feita, com isso observaram que c era escrito como a vezes algum número representado pelas letras, então c é um múltiplo de a. Logo a divide c.

Em nenhum momento foi dado a resposta para eles, mas foram questionados, foram feitos exemplos particulares para que entendessem o raciocício. Não apresentaram nenhuma resistência no momento da demonstração, pelo contrário comemoravam a cada passo acertado.

Estudamos o algoritmo da divisão de Euclides e se espantaram com a data que esse resultado foi criado. Fizemos alguns exemplos e foram questionados sobre os possíveis restos quando dividimos um número natural por dois, por três, por quatro, e assim por diante, até compreenderem que o resto é sempre menor que o divisor. Conversamos sobre os números pares e os números ímpares. Sobre a escrita $2q$, $q \in \mathbb{N}$, para os números pares e a escrita, $2p + 1$, $p \in \mathbb{N}$ para os números ímpares.

Foi proposto um exercício para que verificassem a paridade nas seguintes situações: soma de dois números, diferença de dois números e produto de dois números. A princípio começaram a pensar em números particulares, e dar as respostas, mas quando questionados se poderíamos afirmar que era verdade para todos os números só fazendo alguns exemplos, eles pararam de responder, pensaram e em seguida disseram que não, pois os números são infinitos e não garante que é verdade para todos. Contudo, juntos resolvemos essa questão tomando a forma geral dos pares como $2q$ e a forma geral dos ímpares como $2p+1$. A dificuldade apresentada foi no momento de colocar em evidência, pois disseram que ouviram falar, mas não sabiam do que se tratava.

Calculamos o máximo divisor comum pelo algoritmo de Euclides, o método ao qual estavam acostumados a determinar o mdc era determinando os divisores e depois identificando qual era o maior comum. Nesta etapa demoraram para determinar o quociente e escrever o algoritmo. O tempo exigido foi maior, pois cada um tinha uma estratégia para tabuada.

Os números primos foram o próximo assunto trabalhado, também partindo do conhecimento prévio dos alunos, foi definido números primos, citaram alguns exemplos de números primos e ao perceberem a dificuldade de determinar se um número é primo ou composto, foi proposto o teste que verifica se um número b é primo, testando quais são seus divisores de 1 até o maior inteiro inferior a $\sqrt{b}$. Mesmo assim perceberam que esse método é exaustivo.

Ao falar sobre a fatoração de números compostos eles seguiam os passos do cálculo do mínimo múltiplo comum. Ao propor a fatoração, alguém perguntava: é pra fazer o mmc? Eles demoraram a entender que o mmc se calculava por meio da fatoração, mas a fatoração não significa mmc.

Durante essas 7 horas, sendo duas tardes, em uma sala de aula em média com 24 alunos, passei pela mesma realidade enfrentada diariamente por todos os professores: a falta de interesse, conversas exageradas, discussões, enfim situações que dificultam a aprendizagem. Porém, me deparei com alunos que não diziam que era muito difícil, ou "não vou usar essas coisas" no momento em que o professor começa o conteúdo, sem ao menos tentarem já tem o discurso pronto.

Abaixo estão escritos alguns comentários dos alunos que mostram que o diferente pra eles, as letras que representam números na matemática não os assustam, mas

despertam neles uma certa curiosidade:

"A aula foi muito boa, faltou mais tempo".

"Gostei de conhecer coisas novas que eu não sabia".

"Nós descobrimos que a matemática não era escrita só com números mas também com letras".

Nas últimas aulas os alunos já não diziam ser verdade uma afirmação somente dando um exemplo com números particulares, mas diziam o caso particular e logo em seguida diziam a seguinte frase: "mas não posso dizer né professora que vale pra todos os números, só fazendo pra esse, os números naturais são infinitos."

4.2 Ensino Médio

Foi realizada uma experiência com alunos de quatro turmas, A, B, C e D do segundo ano. Foram um total de sete horas/aulas por turma entre os dias 15/02/2018 à 05/03/2018 no período matutino no horário de aula, não sendo aulas extras.

A princípio foi exposto e dialogado com os alunos sobre a criptografia até o surgimento da criptografia RSA. Eles demonstraram interesse na comunicação secreta, alguns até disseram que fariam isso com os irmãos em casa para que não soubessem seus segredos. Ao relatar a história da criptografia, desde a cifra de César, antes de chegar na criptografia assimétrica já surgiu a seguinte pergunta: onde entra matemática neste assunto? Em seguida foi dito que essa pergunta já seria respondida ao falarmos sobre criptografia assimétrica e mais especificamente, a criptografia RSA.

Depois de dialogarmos sobre o surgimento da criptografia RSA, revisamos os conteúdos matemáticos utilizados para o desenvolvimento desse tipo de comunicação. A partir disso, foi perguntado se alguém sabia o algoritmo da divisão de Euclides. Só de falarmos em divisão já percebeu-se um certo desconforto por parte dos alunos, alguns até comentaram que se tratava de um assunto novo e que fazia parte dos conteúdos do Ensino Médio. Ao fazermos vários exemplos, eles ainda tiveram dificuldades em determinar o resto, pois sempre queriam dar continuidade na divisão, como se tivessem trabalhando com a divisão no conjunto dos números reais. Alguns até disseram que se trava de um conteúdo que já viram há muito tempo e que nem lembravam mais. Ao questioná-los porque o divisor não pode ser zero, não souberam responder, além disso disseram que ao

dividir 3 por 0 a resposta seria 0 e outros que a resposta seria 3.

Logo após foram esclarecidas as dúvidas e feito alguns exemplos sobre algoritmo da divisão passando para a definição de números primos e o teorema fundamental da aritmética.

Poucos souberam definir números primos, mas quando definidos reagiram como algo que tivessem recordado naquele momento. Ao comentar sobre a fatoração, escrever um número como uma multiplicação de fatores primos, a primeira coisa que disseram foi: é pra fazer mmc? A fatoração está tão vinculada ao cálculo do mmc que acreditam que se tratam do mesmo assunto.

Dialogamos sobre algumas curiosidades, por exemplo, sobre o maior número primo encontrado com mais de 23 milhões de dígitos. E para que tivessemos uma noção da dificuldade que se é fatorar um número, foi proposto a fatoração de alguns números, por exemplo, $7519 = 73 \cdot 103$, a princípio disseram que este número era primo, pois não estavam encontrando nenhum divisor, mas foi sugerido que continuassem procurando até pelo menos concluirem o teste para afirmar se o número era primo. E assim fizeram com auxílio da calculadora e, depois de alguns minutos chegaram a solução.

Concluimos após esse exercício a dificuldade encontrada para fatorar um número com apenas 4 algarismos, sendo assim imaginamos a dificuldade para fatorar a chave pública da criptografia RSA que são mais de 100 algarismos.

Comentamos sobre afirmar algo em matemática quando tratamos de infinitos números, por exemplo, ao provar que a soma de dois números pares é par, a soma de dois números ímpares é par, apresentaram certa resistência ao escreverem $2q$ para representar a forma geral dos números pares e $2q+1$ para a forma geral dos números ímpares. Ao fazer a pergunta: a soma de dois números pares é par? Responderam sim, porque $2+2=4$ e 4 é par, a partir disso, foi debatido sobre a questão de se tentar afirmar algo com exemplos particulares e juntos fizemos a demonstração desse fato. No final entenderam o argumento apresentado.

Ao propor o seguinte exercício: sejam p e q números primos, determine todos os valores de p e q, tais que $p - q = 3$, e levá-los a pensarem e resolverem, houve uma certa satisfação, não por todos, mas por uma boa parte dos alunos. De modo satisfatório chegaram ao resultado $p = 5$ e $q = 2$, mas ao serem questionados sobre a existência de mais valores para p e q já que os primos são infinitos, alguns foram testando na tentativa

de encontrar algum e outros já disseram que não sabem. Sozinhos não chegaram no argumento para esta pergunta, porém ao serem motivados a pensarem na questão da paridade de p e q descobriram que q só poderia ser o 2, consequentemente o $p = 5$.

Ao comentar que iriam aprender os cálculos realizados para codificar uma mensagem com a criptografia RSA e que os exemplos seriam com números pequenos, pois na realidade os números tomados para tal função são grandes e os cálculos são realizados por computadores, um dos alunos argumentou: "então para que vamos aprender o cálculo se não é necessário fazer? Se o computador faz eu não preciso fazer."

Algumas resistências foram encontradas, tais como, isso vai cair na prova? Vai valer nota? É matéria de segundo ano? Vai cair no ENEM? Um simples exercício de fatoração os alunos já queriam visto no caderno. Estavam preocupados com nota, isso acaba desanimando qualquer professor e toda aquela empolgação que trazemos para aula é abalada.

Os alunos do $7^{\underline{o}}$ ano não reclamam tanto dos conteúdos, esperam o conteúdo ser apresentado e explicado para depois emitirem alguma opinião. Já os do segundo ano acham tudo difícil, tudo complicado. Antes mesmo de tentarem já falam que não sabem. Parece que tem enraizados que a matemática é um bicho de sete cabeças e quanto mais conteúdos forem apresentados mais feia ela se tornará.

Os alunos apresentaram muita dificuldade com o algoritmo da divisão de Euclides, não conseguiam mesmo depois de alguns exemplos, visualizar o quociente e o resto no algoritmo.

O processo de pré-codificação foi compreendido, mas ao começar a codificação utilizando o algoritmo da divisão as dificuldades foram surgindo e, ao invés de tentarem aprender eles demonstraram desinteresse diante da dificuldade e muitos fugiram do assunto até mesmo atrapalhando os demais.

Depois de ter repedito várias vezes que para codificar um bloco era preciso determinar o resto da divisão de b^e por n, eles compreenderam o que deveria ser feito, mas desenvolverem os cálculos, foi complicado. Foi proposto o uso da calculadora para o desenvolvimento dos cálculos, mas não sabiam determinar resto da divisão utilizando essa ferramenta, pois só sabiam dizer o resultado final da divisão que ela apresentava. Sendo assim, foi ensinado mostrando o algoritmo da divisão e os passos que deveriam seguir ao usar a calculadora para determinar o quociente e o resto da divisão.

A decodificação foi explicada, mas os cálculos também foram difíceis de serem concluídos. A cada etapa era necessário parar e explicar o algoritmo da divisão, regra de potenciação, multiplicação e o uso da calculadora.

Além dessas dificuldades, tinham os problemas de sala de aula: muitos alunos, calor, mau comportamento e avisos da escola. Toda aula alguém perguntava se ia "cair" na prova o conteúdo, enquanto não falava a frase "vai cair na prova" alguns nem mesmo demonstravam algum interesse.

Das quatro turmas em que a experiência foi realizada, duas delas demonstraram maior interesse pelo assunto. Os alunos estavam mais preparados e mesmo aqueles que tinham alguma dificuldade com conteúdo matemático do ensino fundamental, bastava uma explicação.

Ao perguntar o que acharam das aulas e propor que escrevessem, a maioria disse que foi interessante o assunto, relembraram conteúdos matemáticos, como números primos, fatoração e máximo divisor comum e que foi um assunto bem diferente.

No início do ano letivo, geralmente, a coordenação pedagógica propõe para os professores um diagnóstico das turmas e uma revisão de matemática básica. A criptografia RSA pode ser trabalhada com esse objetivo, a partir de um assunto da atualidade, de uma aplicação, trabalhamos conteúdos básicos da matemática, sendo que estes podem auxiliar no diagnóstico da turma. Motiva-se os alunos com a criptografia para que eles possam revisar alguns conteúdos, além disso, aprender os cálculos realizados por essa criptografia assimétrica.

Considerações finais

A criptografia é um ciência que estuda métodos para codificar uma mensagem, de maneira segura, de modo que apenas seu destinatário consegue interpretá-la. Ela está baseada nas ciências exatas e enviar mensagens secretas de modo que as informações que circulam pela internet, por exemplo, não estejam no domínio de pessoas não autorizadas é uma necessidade que exige mais conhecimento nessa área.

Com o desenvolvimento tecnológico a comunicação pela internet é um grande desafio para criptografia, pois as transações comercias ou bancárias ou até mesmo as compras feitas com cartão de crédito necessitam de um dos métodos da criptografia para que as informações não sejam decifradas por alguém que não seja o destinatário legítimo. Um desses métodos é conhecido como RSA, nome este correspondente as inicias dos seus inventores Rivest, Shamir e Adleman. Para o desenvolvimento da criptografia RSA foi fundamental assuntos relacionados a teoria dos números, uma parte da matemática que por algum tempo nenhuma aplicação prática era conhecida. Especificamente, são necessários dois conteúdos matemáticos que ainda aprendemos no Ensino Fundamental: os números primos e a decomposição em fatores primos (fatoração). É seguro pelo fato de não existir um algoritmo eficiente para fatoração e fabricação de primos o que existe são algoritmos que testam se n é um primo e responde que é com uma probabilidade alta próxima de 1. (Terada, 2008)

Se já é difícil e demorado fatorar números com 4 algarismos imagina números com 150 algarismos, isso levaria anos. Portanto estudar números primos, números inteiros não é algo do passado é algo da atualidade e poderemos nos surpreender com muitas outras descobertas.

Na educação básica procura-se mostrar para alunos que a matemática é importante para diversas áreas do conhecimento e ao invés de apenas citar a sua importância é necessário que se mostre algumas aplicações.

O conteúdo de criptografia RSA, pode motivar os alunos em sala de aula no estudo de alguns conteúdos, tais como: fatoração, números primos e divisibilidade.

Percebe-se através da experiência realizada que até os alunos chegarem ao ensino médio muitos conteúdos que foram ensinados anteriormente ficaram perdidos, ou até mesmo não fazem mais sentido. Por exemplo, algoritmo da divisão, não sabem mais fazer divisão com resto, números primos fica apenas na definição, não sabem da sua importância.

Ao propor um ensino mais aprofundado com detalhes da atualidade, pode trazer uma certa satisfação. A grande maioria dos alunos estão acostumados com ensino de matemática com fórmulas e exercícios siga o modelo. Propor que aprendam e raciocinem diante de problemas e situações do cotidiano faz com que eles se assustem.

Pela experiência realizada percebe-se que, o que mais importa é saber a nota que será atribuída para uma determinada proposta de ensino e não o conhecimento que será adquirido.

No ensino fundamental pode-se ensinar aos alunos a matemática com demonstrações e aplicações. Dar sentido aos números primos, a divisibilidade, as propriedades dos números inteiros, não ficando apenas na definição e em listas de exercícios repetitivos. Cobra-se muito a retomada de conteúdos que não foram aprendidos pelos alunos nos anos anteriores, então pode-se retomar esses conteúdos com algo da atualidade. Como é o caso da criptografia RSA, pode-se retomar o assunto de fatoração, divisibilidade e números primos por exemplo. E se esse não for o problema da turma e se forem alunos que não apresentam dificuldades relacionadas com esses assuntos pode-se ensinar a criptografia para o ensino médio como uma nova proposta de conteúdo.

As bibliografias pesquisadas e as leituras realizadas pela internet demonstram que este assunto é trabalhado com aritmética modular e escrevê-lo pelo algoritmo da divisão foi um desafio.

É possível ensinar criptografia RSA para alunos de ensino médio, mas com alguns desafios. Se for possível desenvolver o primeiro capítulo deste trabalho no ensino fundamental de tal modo que não fique perdido com o decorrer do tempo, os cálculos de codificação e decodificação será feito com mais tranquilidade e para que se alcance os objetivos, ou seja, aprendizagem do conteúdo, não será necessário muito tempo. Contudo, se desde o ensino fundamental os conhecimentos adquiridos em um ano são esquecidos no

outro ou nem mesmo façam sentido para o aluno, ensinar criptografia RSA para o ensino médio pode-se exigir muito mais tempo do que previsto.

Com a experiência realizada conclui que revisar um conteúdo matemático com alguma novidade, trazendo novas informações é fundamental, por exemplo, com a criptografia RSA. Ás vezes foca-se no conteúdo, que até já foi revisado nos anos anteriores o que acaba ficando chato, então pode-se fazer uma revisão de conteúdo mais motivadora. É importante pesquisar outros assuntos da atualidade que precisam da matemática para o seu desenvolvimento e que pode ser traduzida em uma linguagem a nível da educação básica. Uma pergunta realizada por um aluno e que é um desafio para nós professores é a seguinte: se o computador faz os cálculos, por que nós precisamos aprender? Outro questionamento, agora por parte do professor é com relação a avaliação: a nota final representa mais para o aluno do que o conhecimento? Além disso, o que dizer para um aluno que chega ao segundo ano do ensino médio e diz que não sabe divisão e pensa que sabe manusear uma calculadora.

O conteúdo de criptografia não se encontra nos livros didáticos por isso é preciso irmos além do que está nesses livros, sendo estes apenas uma das ferramentas de pesquisa e não a rotina de sala de aula.

São muitas as dificuldades de aprendizagem apresentadas pelos alunos, é importante mostrar para eles que ter um conhecimento possibilita a descoberta de novas aplicações, além disso, o que os professores ensinam não é algo que está pronto e acabado, mas sim algo que pode solucionar alguns problemas e responder algumas perguntas que possam surgir em outras áreas do conhecimento.

Referências Bibliográficas

Brasil Escola (2018). Máquina enigma. URL: https://brasilescola.uol.com.br/historiag/maquina-enigma.htm. Acesso em 06/02/2018.

Coutinho, S. (2014). *Números inteiros e criptografia RSA*. IMPA, Rio de Janeiro.

du Sautoy, M. (2007). *A música dos números primos: a história de um problema não resolvido na matemática*. Jorge Zahar, Rio de Janeiro. Tradução de Diego Alfaro.

Hefez, A. (2014). *Aritmética*. SBM, Rio de Janeiro. Coleção PROFMAT.

Lucchesi, C. L. (1986). *Introdução à criptografia computacional*. Editora da UNICAMP, Campinas.

MEC (2000). Parâmetros curriculares nacionais: Ciências da natureza, matemática e suas tecnologias. URL: http://portal.mec.gov.br/seb/arquivos/pdf/ciencian.pdf. Acesso em 28/02/2018.

Mersenne (2018). O maior número primo encontrado. URL: http://www.mersenne.org/. Acesso em 06/02/2018.

Notícias r7 (2015). O matemático peruano que resolveu um problema de quase 300 anos. URL: http://noticias.r7.com/tecnologia-e-ciencia/o-matematico-peruano-que-resolveu-um-problema-de-quase-300-anos-05102015. Acesso em 08/08/2017.

Ribenboim, P. (2014). *Números primos: velhos mistérios e novos recordes*. IMPA, Rio de Janeiro. Coleção matemática universitária.

Shokranian, S. (2012). *Criptografia para iniciantes*. Ciência moderna, Rio de Janeiro.

Singh, S. (2014). *O livro dos códigos*. Record, Rio de Janeiro. Tradução de Jorge Calife.

Stallings, W. (2008). *Criptografia e segurança de redes*. Pearson, São Paulo.

Stallings, W. (2015). *Criptografia e segurança de redes: princípios e práticas*. Pearson, São Paulo.

Terada, R. (2008). *Segurança de dados: criptografia em rede de computador*. Blucher, São Paulo.

Wordpress (2013). Cítala. URL: https://siriarah.wordpress.com/2013/05/13/criptografia–bastao–de–licurgo–scytale–em–python/. Acesso em 8/11/2017.

Wordpress (2014). Disco de cifras. URL: https://archeocomputing.wordpress.com/2014/-01/31/il–disco–di–leon–battista–alberti/. Acesso em 09/11/2017.

Apêndice

.

A.1 Aritmética modular

Este assunto não é trabalhado na Educação Básica, porém pode-se notar a aritmética modular no relógio de ponteiro, por exemplo, se agora são 8 horas daqui 26 horas serão 10 horas, no entanto, fazendo a adição usual como de costume obtem-se $8 + 26 = 34$. Quando o ponteiro do relógio atinge o 12, volta para o 0, neste caso ao invés de dizer 34 horas será dito 10 horas. Essa aritmética pode ser chamada de arimética módulo 12.

A.1 Congruências

A congruência trata-se de cálculos realizados com restos da divisão euclidiana por um número fixado.

Definição 1. *Seja n um número natural. Dois números inteiros a e b são congruentes módulo n se os restos de sua divisão euclidiana por n são iguais. Em símbolos pode-se escrever*

$$a \equiv b \bmod n.$$

Exemplo 21.

a) $7 \equiv 5 \bmod 2$, pois 7 e 5 quando divididos por 2 deixam restos iguais a 1.

b) $22 \equiv 17 \bmod 5$, pois 22 e 17 quando divididos por 5 deixam restos iguais a 2.

Se a relação de congruência $a \equiv b \bmod n$ não for verdadeira, escreve-se

$$a \not\equiv b \bmod n,$$

ou seja, não são congruentes módulo n.

Pela definição de congruência, dados a, b e $c \in \mathbb{Z}$ e $n \in \mathbb{N}$ são verificadas as seguintes propriedades:

i) $a \equiv a \bmod n$.

ii) se $a \equiv b \bmod n$, então $b \equiv a \bmod n$.

iii) se $a \equiv b \bmod n$ e $b \equiv c \bmod n$, então $a \equiv c \bmod n$.

Portanto a relação de congruência é uma relação de equivalência.

Para verificar se dois números são congruentes módulo n sem precisar fazer a divisão de ambos os números por n e determinar os restos, tem-se a seguinte afirmação:

Suponha a, b e $n \in \mathbb{Z}$, com $n > 1$. Tem-se que $a \equiv b$ mod n se, e somente se, n divide $b - a$.

Demonstração. Sejam $a = nq + r$, com $0 \leq r < n$ e $b = nq' + r'$, com $0 \leq r' < n$. Fazendo $b - a$, tem-se

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

Por definição $a \equiv b \bmod n$ se, e somente se $r = r'$, mas isto equivale a

$b - a = n(q' - q)$, ou seja, $b - a$ é um múltiplo de n. Portanto n divide $b - a$. □

Observação 2. *O resto da divisão de qualquer número inteiro por 1 é sempre 0, logo $a \equiv b$ mod 1, quaisquer a, $b \in \mathbb{Z}$. Portanto não é interessante trabalhar com $n = 1$, mas sim $n > 1$.*

Exemplo 22.

a) $7 \equiv 1 \bmod 2$ b) $10 \equiv 2 \bmod 4$ c) $41 \equiv 6 \bmod 7$

Note que cada número é congruente ao seu resto, por exemplo, ao dividir 7 por 2, os restos possíveis são 0 e 1, e 2 divide $7 - 1$.

Portanto todo número inteiro é congruente módulo n a um dos números

$$0, 1, \ldots, n - 1.$$

Além disso, dois desses números não são congruentes módulo n.

Exemplo 23.

a) $3 \not\equiv 2 \bmod 5$

b) $4 \not\equiv 1 \bmod 7$

Em relação a adição e a multiplicação envolvendo congruências tem-se dois resultados importantes.

Sejam a, b, c, d *e* $n \in \mathbb{Z}$ *com* $n > 1$.

i) Se $a \equiv b \bmod n$ e $c \equiv d \bmod n$, então $a + c \equiv b + d \bmod n$.

ii) Se $a \equiv b \bmod n$ e $c \equiv d \bmod n$, então $ac \equiv bd \bmod n$.

Demonstração. **i)** Suponha que $a \equiv b \bmod n$ e $c \equiv d \bmod n$, sendo assim tem-se que n divide $b - a$ e n divide $d - c$, ou ainda, $b - a = nq$, $q \in \mathbb{Z}$ e $d - c = nk$, $k \in \mathbb{Z}$. Logo,

$$(b - a) + (d - c) = nq + nk,$$
$$(b + d) - (a + c) = n(q + k).$$

Segue que n divide $(b + d) - (a + c)$.

Portanto, $a + c \equiv b + d \bmod n$.

ii) Suponha que $a \equiv b \bmod n$ e $c \equiv d \bmod n$, assim $b - a = nq$, $q \in \mathbb{Z}$ e $d - c = nk$, $k \in \mathbb{Z}$. Logo,

$$bd - ad = nq' \text{ e } da - ca = nk'$$

Somando as duas igualdades tem-se

$$bd - ca = n(q' + k').$$

Segue que n divide $bd - ca$. Portanto, $ac \equiv bd \bmod n$.

□

Outro resultado importante veja a seguir:

Para todo $m \in \mathbb{N}$, $a, b \in \mathbb{Z}$, *se* $a \equiv b \bmod n$, *então tem-se que* $a^m \equiv b^m \bmod n$.

Demonstração. Para $m = 1$ é verdadeiro, pois $a \equiv b \bmod n$ é a hipótese. Suponha válido para m, ou seja, $a^m \equiv b^m \bmod n$, é preciso mostrar que é válido para $m + 1$.

Note que $a \equiv b \bmod n$ e $a^m \equiv b^m \bmod n$, logo $a^m.a \equiv b^m.b \bmod n$.

Portanto, $a^{m+1} \equiv b^{m+1} \bmod n$. □

O cancelamento com relação a adição é válido para as congruências, segue a demonstração.

Sejam $a, b, c, n \in \mathbb{Z}$, com $n > 1$. Tem-se que

$$a + c \equiv b + c \bmod n \text{ se, e somente se, } a \equiv b \bmod n.$$

Demonstração. Suponha que $a \equiv b \bmod n$, além disso, $c \equiv c \bmod n$ então $a + c \equiv b + c \bmod n$.

Reciprocamente, suponha que $a + c \equiv b + c \bmod n$, logo n divide $(b + c) - (a + c)$ ou ainda, n divide $b - a$.

Portanto, $a \equiv b \bmod n$. □

O cancelamento com relação a multiplicação é válido, mas com uma observação em relação aos valores de c e de n. Segue a afirmação:

Sejam a, b, c, $n \in \mathbb{Z}$, com $n > 1$ e $mdc(c, n) = 1$. tem-se

$$ac \equiv bc \bmod n \text{ se, se somente se, } a \equiv b \bmod n.$$

Demonstração. Suponha $ac \equiv bc \bmod n$ tem-se que n divide $bc - ac = (b - a).c$. Como $mdc(c, n) = 1$ então n não divide c e portanto, n divide $(b - a)$. Logo $a \equiv b \bmod n$.

Reciprocamente, seja $a \equiv b \bmod n$ e $c \equiv c \bmod n$, segue que $ac \equiv bc \bmod n$. □

Definição 2. *Sejam a, b e $n \in \mathbb{Z}$, é dito que a é invertível mod n quando $mdc(a, n) = 1$, neste caso, se $ab \equiv 1$ mod n, b é dito inverso multiplicativo de a módulo n.*

Sejam a, $n \in \mathbb{Z}$, $n > 0$, então existe $b \in \mathbb{Z}$ com $ab \equiv 1$ mod n se , e somente se, $mdc(a, n) = 1$.

Demonstração. Seja $ab \equiv 1 \bmod n$ logo n divide $(1 - ab)$. Existe $k \in \mathbb{Z}$ tal que $nk = 1 - ab$. Pode-se escrever esta equação da seguinte maneira $nk + ab = 1$. Pelo Teorema de Bachet-Bézout isto ocorre se, e somente se, $mdc(a, n) = 1$. □

A.2 Criptografia RSA

A.1 Codificação da mensagem do exemplo 20 da seção 3.1

Dado $p = 11$, $q = 13$, logo $n = 143$ e $(p-1)(q-1) = 10 \cdot 12 = 120$. Escolhendo $e = 7$, pois $mdc(7, 120) = 1$ é feito as contas e obtem-se cada bloco codificado. Denotando por $C(b)$ o bloco codificado e escrevendo em termos de congruência segue

$$C(b) \equiv b^e \bmod n.$$

$$131 \equiv -12 \bmod 143 \qquad 82^2 \equiv 3 \bmod 143$$
$$131^2 \equiv 1 \bmod 143 \qquad 82^6 \equiv 3^3 \equiv 27 \bmod 143$$
$$131^6 \equiv 1 \bmod 143 \qquad 82^6 \cdot 82 \equiv 27 \cdot 82 \bmod 143$$
$$131^6 \cdot 131 \equiv 131 \bmod 143 \qquad 82^7 \equiv 69 \bmod 143$$
$$131^7 \equiv 131 \bmod 143$$

Logo $C(131) = 131$ e $C(82) = 69$

$$71^2 \equiv 36 \bmod 143 \qquad 41^3 \equiv 138 \bmod 143$$
$$71^6 \equiv 36^3 \equiv 38 \bmod 143 \qquad 41^6 \equiv 138^2 \equiv 25 \bmod 143$$
$$71^6 \cdot 71 \equiv 38 \cdot 71 \bmod 143 \qquad 41^6 \cdot 41 \equiv 25 \cdot 41 \bmod 143$$
$$71^7 \equiv 124 \bmod 143 \qquad 41^7 \equiv 24 \bmod 143$$

Logo $C(71) = 124$ e $C(41) = 24$

$$42^3 \equiv 14 \bmod 143 \qquad 89^3 \equiv 122 \bmod 143$$
$$42^6 \equiv 14^2 \equiv 53 \bmod 143 \qquad 89^6 \equiv 122^2 \equiv 12 \bmod 143$$
$$42^6 \cdot 42 \equiv 53 \cdot 42 \bmod 143 \qquad 89^6 \cdot 89 \equiv 12 \cdot 89 \bmod 143$$
$$42^7 \equiv 81 \bmod 143 \qquad 89^7 \equiv 67 \bmod 143$$

Logo $C(42) = 81$ e $C(89) = 67$

$$91^3 \equiv 104 \bmod 143 \qquad 49^3 \equiv 103 \bmod 143$$
$$91^6 \equiv 104^2 \equiv 91 \bmod 143 \qquad 49^6 \equiv 103^2 \equiv 27 \bmod 143$$
$$91^6 \cdot 91 \equiv 91 \cdot 91 \bmod 143 \qquad 49^6 \cdot 49 \equiv 27 \cdot 49 \bmod 143$$
$$91^7 \equiv 130 \bmod 143 \qquad 49^7 \equiv 36 \bmod 143$$

Logo $C(91) = 130$ e $C(49) = 36$

$$31^3 \equiv 47 \bmod 143 \qquad 43^3 \equiv 142 \bmod 143$$
$$31^6 \equiv 47^2 \equiv 64 \bmod 143 \qquad 43^6 \equiv 142^2 \equiv 1 \bmod 143$$
$$31^6 \cdot 31 \equiv 64 \cdot 31 \bmod 143 \qquad 43^6 \cdot 43 \equiv 43 \bmod 143$$
$$31^7 \equiv 125 \bmod 143 \qquad 43^7 \equiv 43 \bmod 143$$

Logo $C(31) = 125$ e $C(43) = 43$

$$114^3 \equiv 64 \bmod 143 \qquad 27^3 \equiv 92 \bmod 143$$
$$114^6 \equiv 64^2 \equiv 92 \bmod 143 \qquad 27^6 \equiv 92^2 \equiv 27 \bmod 143$$
$$114^6 \cdot 114 \equiv 92 \cdot 114 \bmod 143 \qquad 27^6 \cdot 27 \equiv 27 \cdot 27 \bmod 143$$
$$114^7 \equiv 49 \bmod 143 \qquad 27^7 \equiv 14 \bmod 143$$

Logo $C(114) = 49$ e $C(27) = 14$

$$142^3 \equiv 142 \bmod 143 \qquad 8^3 \equiv 83 \bmod 143$$
$$142^6 \equiv 142^2 \equiv 1 \bmod 143 \qquad 8^6 \equiv 83^2 \equiv 25 \bmod 143$$
$$142^6 \cdot 142 \equiv 142 \bmod 143 \qquad 8^6 \cdot 8 \equiv 25 \cdot 8 \bmod 143$$
$$142^7 \equiv 142 \bmod 143 \qquad 8^7 \equiv 57 \bmod 143$$

Logo $C(142) = 142$ e $C(8) = 57$

$$92^3 \equiv 53 \bmod 143$$
$$92^6 \equiv 53^2 \equiv 92 \bmod 143$$
$$92^6 \cdot 92 \equiv 92 \cdot 92 \bmod 143$$
$$92^7 \equiv 27 \bmod 143$$

Logo $C(92) = 27$

A.2 Decodificação da mensagem do exemplo 20 da seção 3.1

Para decodificar uma mensagem é necessário conhecer dois números: n e o inverso multiplicativo de e módulo $(p-1)(q-1)$ denotado por d, ou seja,

$$e \cdot d \equiv 1 \bmod (p-1)(q-1).$$

A chave de decodificação é dada pelo par (n, d) e sendo a um bloco da mensagem codificada, o resto da divisão de a^d por n dá o resultado do bloco original. Denotando por $D(a)$ o resultado do processo de decodificação tem-se

$$a^d \equiv D(a) \bmod n$$

Seja $n = 143$ e $e = 7$. Para determinar o valor d se aplica o algoritmo euclidiano estendido. Ao dividir $(p-1)(q-1) = (11-1)(13-1) = 120$ por 7 obtem-se:

$$120 = 7 \cdot 17 + 1, \text{ ou seja, } 1 = 120 + (-17) \cdot 7.$$

Note que $1 \equiv 1 \bmod 120$, logo $1 \equiv 120 + (-17) \cdot 7 \bmod 120$, mas $120 \equiv 0 \bmod 120$. Portanto,$1 \equiv (-17) \cdot 7 \bmod 120$.

Sendo assim, -17 é o inverso multiplicativo de 7 módulo 120, porém o valor de d tem que ser positivo, pois é utilizado como expoente de potência.

Observe que 120 divide $(-17-103)$, logo $-17 \equiv 103 \bmod 120$. Portanto $d = 103$.

Com o valor de d determinado se inicia a decodificação dos blocos, por exemplo, para decodificar o bloco 131 da mensagem codificada é preciso determinar o resto da divisão de 131^{103} por 143, ou seja, determinar o menor valor de x tal que $131^{103} \equiv x \bmod 143$.

$$\begin{aligned}
69^3 &\equiv 38 \bmod 143 \\
69^9 \equiv 38^3 &\equiv 103 \bmod 143 \\
69^{18} \equiv 103^2 &\equiv 27 \bmod 143 \\
69^{90} \equiv 27^5 &\equiv 1 \bmod 143 \\
69^{90} \times 69^9 \equiv 69^9 &\equiv 103 \bmod 143 \\
69^{99} &\equiv 103 \bmod 143 \\
69^{99} \times 69^3 &\equiv 103 \times 38 \bmod 143 \\
69^{102} &\equiv 53 \bmod 143 \\
69^{102} \times 69 \equiv 69 \times 53 &\equiv 82 \bmod 143 \\
69^{103} &\equiv 82 \bmod 143
\end{aligned}$$

$$\begin{aligned}
131 &\equiv -12 \bmod 143 \\
131^2 &\equiv 1 \bmod 143 \\
131^{102} \equiv 1^{51} &\equiv 1 \bmod 143 \\
131^{102} \times 131 &\equiv 131 \bmod 143 \\
131^{103} &\equiv 131 \bmod 143
\end{aligned}$$

Logo $D(69) = 82$ e $D(131) = 131$

$$124^3 \equiv 5 \bmod 143$$
$$124^{30} \equiv 5^{10} \equiv 12 \bmod 143$$
$$124^{90} \equiv 12^3 \equiv 12 \bmod 143$$
$$124^9 \equiv 5^3 \equiv 125 \bmod 143$$
$$124^{90} \times 124^9 \equiv 12 \times 125 \equiv 70 \bmod 143$$
$$124^{99} \equiv 70 \bmod 143$$
$$124^{99} \times 124^3 \equiv 70 \times 5 \equiv 64 \bmod 143$$
$$124^{102} \times 124 \equiv 64 \times 124 \equiv 71 \bmod 143$$
$$124^{103} \equiv 71 \bmod 143$$

$$24^5 \equiv 98 \bmod 143$$
$$24^{10} \equiv 98^2 \equiv 23 \bmod 143$$
$$24^{50} \equiv 23^5 \equiv 56 \bmod 143$$
$$24^{100} \equiv 56^2 \equiv 133 \bmod 143$$
$$24^3 \equiv 96 \bmod 143$$
$$24^{100} \times 24^3 \equiv 133 \times 96 \bmod 143$$
$$24^{103} \equiv 41 \bmod 143$$

Logo $D(124) = 71$ e $D(24) = 41$

$$27^5 \equiv 1 \bmod 143$$
$$27^{100} \equiv 1^{20} \equiv 1 \bmod 143$$
$$27^3 \equiv 92 \bmod 143$$
$$27^{100} \times 27^3 \equiv 1 \times 92 \bmod 143$$
$$27^{103} \equiv 92 \bmod 143$$

$$14^5 \equiv 1 \bmod 143$$
$$14^{100} \equiv 1^{20} \equiv 1 \bmod 143$$
$$14^3 \equiv 27 \bmod 143$$
$$14^{100} \times 14^3 \equiv 1 \times 27 \bmod 143$$
$$14^{103} \equiv 27 \bmod 143$$

Logo $D(27) = 92$ e $D(14) = 27$

$$81^4 \equiv 3 \bmod 143$$
$$81^{40} \equiv 3^{10} \equiv 133 \bmod 143$$
$$81^{80} \equiv 133^2 \equiv 100 \bmod 143$$
$$81^{20} \equiv 3^5 \equiv 100 \bmod 143$$
$$81^{80} \times 81^{20} \equiv 100 \times 100 \bmod 143$$
$$81^{100} \equiv 133 \bmod 143$$
$$81^3 \equiv 53 \bmod 143$$
$$81^{100} \times 81^3 \equiv 133 \times 53 \bmod 143$$
$$81^{103} \equiv 42 \bmod 143$$

$$67^3 \equiv 34 \bmod 143$$
$$67^{12} \equiv 34^4 \equiv 1 \bmod 143$$
$$67^{96} \equiv 1^{96} \equiv 1 \bmod 143$$
$$67^6 \equiv 34^2 \equiv 12 \bmod 143$$
$$67^6 \times 67 \equiv 12 \times 67 \equiv 89 \bmod 143$$
$$67^7 \equiv 89 \bmod 143$$
$$67^{96} \times 67^7 \equiv 1 \times 89 \bmod 143$$
$$67^{103} \equiv 89 \bmod 143$$

Logo $D(81) = 42$ e $D(67) = 89$

$$130^2 \equiv 26 \bmod 143$$
$$130^{10} \equiv 26^5 \equiv 78 \bmod 143$$
$$130^{30} \equiv 78^3 \equiv 78 \bmod 143$$
$$130^{90} \equiv 78^3 \equiv 78 \bmod 143$$
$$130^{90} \times 130^{10} \equiv 78 \times 78 \bmod 143$$
$$130^{100} \equiv 78 \bmod 143$$
$$130^3 \equiv 91 \bmod 143$$
$$130^{100} \times 130^3 \equiv 78 \times 91 \bmod 143$$
$$130^{103} \equiv 91 \bmod 143$$

$$125^2 \equiv 38 \bmod 143$$
$$125^{10} \equiv 38^5 \equiv 12 \bmod 143$$
$$125^{20} \equiv 12^2 \equiv 1 \bmod 143$$
$$125^{100} \equiv 1^5 \equiv 1 \bmod 143$$
$$125^3 \equiv 31 \bmod 143$$
$$125^{100} \times 125^3 \equiv 1 \times 31 \bmod 143$$
$$125^{103} \equiv 31 \bmod 143$$

Logo $D(130) = 91$ e $D(125) = 31$

$$36^5 \equiv 56 \bmod 143$$
$$36^{20} \equiv 56^4 \equiv 100 \bmod 143$$
$$36^{80} \equiv 100^4 \equiv 100 \bmod 143$$
$$36^{80} \times 36^{20} \equiv 100 \times 100 \bmod 143$$
$$36^{100} \equiv 133 \bmod 143$$
$$36^3 \equiv 38 \bmod 143$$
$$36^{100} \times 36^3 \equiv 133 \times 38 \bmod 143$$
$$36^{103} \equiv 49 \bmod 143$$

$$43^4 \equiv 100 \bmod 143$$
$$43^8 \equiv 100^2 \equiv 133 \bmod 143$$
$$43^{24} \equiv 133^3 \equiv 1 \bmod 143$$
$$43^{96} \equiv 1^4 \equiv 1 \bmod 143$$
$$43^{96} \times 43^4 \equiv 1 \times 100 \equiv 100 \bmod 143$$
$$43^3 \equiv 142 \bmod 143$$
$$43^{100} \times 43^3 \equiv 100 \times 142 \bmod 143$$
$$43^{103} \equiv 43 \bmod 143$$

Logo $D(36) = 49$ e $D(43) = 43$

$$49^5 \equiv 56 \bmod 143$$
$$49^{20} \equiv 56^4 \equiv 100 \bmod 143$$
$$49^{80} \equiv 100^4 \equiv 100 \bmod 143$$
$$49^{80} \times 49^{20} \equiv 100 \times 100 \bmod 143$$
$$49^{100} \equiv 133 \bmod 143$$
$$49^3 \equiv 103 \bmod 143$$
$$49^{100} \times 49^3 \equiv 133 \times 103 \bmod 143$$
$$49^{103} \equiv 114 \bmod 143$$

$$57^4 \equiv 27 \bmod 143$$
$$57^{20} \equiv 27^5 \equiv 1 \bmod 143$$
$$57^{100} \equiv 1^5 \equiv 1 \bmod 143$$
$$57^3 \equiv 8 \bmod 143$$
$$57^{100} \times 57^3 \equiv 1 \times 8 \bmod 143$$
$$57^{103} \equiv 8 \bmod 143$$

Logo $D(49) = 114$ e $D(57) = 8$

$$142^3 \equiv 142 \bmod 143$$
$$142^6 \equiv 142^2 \equiv 1 \bmod 143$$
$$142^{102} \equiv 1^{17} \equiv 1 \bmod 143$$
$$142^{102} \times 142 \equiv 1 \times 142 \bmod 143$$
$$142^{103} \equiv 142 \bmod 143$$

Logo $D(142) = 142$

Portanto ao realizar todos os cálculos decodifica-se a mensagem e obtem-se os blocos: 131 - 82 - 71 - 41 - 82 - 92 - 42 - 89 - 91 - 49 - 91 - 31 - 43 - 114 - 27 - 142 - 8.

Ao juntar estes blocos e obter um único número tem-se o texto original convertido em números.

A.3 Fundamentação matemática do RSA pelo método da aritmética modular

Suponha p e q números primos distintos, com $n = p.q$, n e e, com $e \in \mathbb{N}$, os dados de codificação tal que, $mdc(e, (p-1)(q-1)) = 1$ e n e d os dados de decodificação, com $d \in \mathbb{Z}$ um inteiro definido pelas duas condições:

1. $ed \equiv 1 \bmod (p-1)(q-1)$.
2. $1 \leq d < (p-1)(q-1)$

É preciso verificar que se b é um inteiro e $1 \leq b \leq n-1$ então $D[C(b)] = b$. Para isso basta provar que $D[C(b)] \equiv b \bmod n$, pois tanto $D[C(b)]$ quanto b estão no intervalo que vai de 1 a $n-1$.

Por definição de codificação tem-se que

$$C(b) \equiv b^e \bmod n,$$
$$(C(b))^d \equiv (b^e)^d \bmod n.$$

Logo, $(C(b))^d \equiv b^{ed} \bmod n$.
Além disso, $ed \equiv 1 \bmod (p-1)(q-1)$. Segue que $ed = k(p-1)(q-1)+1$, para algum $k \in \mathbb{Z}$. Então,

$$(C(b))^d \equiv b^{ed} \equiv b^{k(p-1)(q-1)+1} \bmod n$$

Como p e q são dois primos distintos e $b \not\equiv 0 \bmod p$ e $b \not\equiv 0 \bmod q$ pelo Teorema de Fermat pode-se afirmar que $b^{p-1} \equiv 1 \bmod p$. Portanto, $b^{(p-1)(q-1)} \equiv 1 \bmod p$. Da mesma forma $b^{q-1} \equiv 1 \bmod q$, logo $b^{(q-1)(p-1)} \equiv 1 \bmod q$.

Portanto p e q dividem $b^{(p-1)(q-1)} - 1$, ou seja, $b^{(p-1)(q-1)} \equiv 1 \bmod pq$.

Assim tem-se

$$(C(b))^d \equiv b^{k(p-1)(q-1)+1} \equiv (b^{(p-1)(q-1)})^k \times b \equiv 1^k \times b \equiv b \bmod pq.$$

Note que $(C(b))^d = D[C(b)]$ e $pq = n$.

Portanto, $D[C(b)] \equiv b \bmod n$.