UNIVERSIDADE FEDERAL DA PARAÍBA
CENTRO DE CIÊNCIAS EXATAS E DA NATUREZA
MESTRADO PROFISSIONAL EM MATEMÁTICA
EM REDE NACIONAL - PROFMAT

Teoria dos números e Criptografia RSA

por

Wélisson Martins Mota

2023

UNIVERSIDADE FEDERAL DA PARAÍBA
CENTRO DE CIÊNCIAS EXATAS E DA NATUREZA
MESTRADO PROFISSIONAL EM MATEMÁTICA
EM REDE NACIONAL - PROFMAT

Teoria dos números e Criptografia RSA [†]

por

Wélisson Martins Mota

sob a orientação do

Prof. Dr. José Laudelino de Menezes Neto

Dissertação apresentada ao Corpo Docente do Mestrado Profissional em Matemática em Rede Nacional - PROFMAT/CCEN/UFPB, como requisito parcial para a obtenção do título de Mestre em Matemática.

Fevereiro/ 2023
João Pessoa - PB

[†]O presente trabalho foi realizado com apoio da CAPES, Coordenação de Aperfeiçoamento de Pessoal de Nível Superior.

Catalogação na publicação
Seção de Catalogação e Classificação

M917t Mota, Wélisson Martins.
Teoria dos números e Criptografia RSA / Wélisson Martins Mota. - João Pessoa, 2023.
58 f. : il.

Orientação: José Laudelino de Menezes Neto.
Dissertação (Mestrado) - UFPB/CCEN.

1. Teoria dos números. 2. Criptografia - Ensino. 3. RSA - Rivest-Shamir-Adleman. I. Menezes Neto, Jose Laudelino de. II. Título.

UFPB/BC CDU 511(043)

Elaborado por ANNA REGINA DA SILVA RIBEIRO - CRB-15/24

Teoria dos números e Criptografia RSA

por

Wélisson Martins Mota

Dissertação apresentada ao Corpo Docente do Mestrado Profissional em Matemática em Rede Nacional - PROFMAT/CCEN/UFPB, como requisito parcial para a obtenção do título de Mestre em Matemática.

Área de Concentração: Matemática

Aprovada por:

Prof. Dr. José Laudelino de Menezes Neto - UFPB (Orientador)

Prof(a). Dr(a). Adecarlos Costa Carvalho - UFMA

Prof(a). Dr(a). Wallace Mangueira de Sousa - UFPB

Fevereiro/ 2023

Agradecimentos

Gostaria de agradecer a todos que de forma direta ou indiretamente me deram forças para concluir essa jornada.

Dedicatória

A minha mãe Ana Maria e meu pai João Bosco

Resumo

Neste trabalho, fazemos uma abordagem de alguns conceitos básicos de teoria dos números visando o entendimento dos modelos de criptografia. Apresentamos inicialmente tópicos de divisibilidade, congruências, números primos e funções aritméticas. Em seguida, fazemos um breve estudo sobre criptografia, com ênfase no sistema RSA (Rivest-Shamir-Adleman). Após o estudo de criptografia, apresentamos duas propostas de atividades a serem desenvolvidas em sala de aula que abordam criptografia com função afim e congruência de números inteiros.

Palavras-chaves: Teoria dos Números; Criptografia; Ensino.

Abstract

In this work, we approach some basic concepts of number theory in order to understand cryptography models. We initially present topics of divisibility, congruences, prime numbers and arithmetic functions, then we make a brief study on cryptography, with emphasis on the RSA system (Rivest-Shamir-Adleman). After the study of cryptography, we present two proposals for activities to be developed in the classroom that address cryptography with linear function and congruence of integers.

Key-words: Number Theory; Cryptography ; Teaching

Sumário

Introdução

Neste trabalho realizamos um estudo de teoria dos números e sua aplicação em modelos de criptografia, buscando atrelar isso ao ensino de matemática, visando levar curiosidades e tecnologia para sala de aula.

No capítulo 1 resgatamos alguns conceitos de divisibilidade, apresentando algorítimos fundamentais sobre divisibilidade e fazendo uma checagem sobre o processo de busca de números primos, o que é a chave do sucesso do sistema criptográfico RSA (Rivest-Shamir-Adleman). Um tópico interessante deste capítulo é o Teorema 1.6 que nos ensina a gerar critérios de divisibilidade para qualquer número primo, isso é interessante pois também pode ser adaptado para o uso em sala de aula, evitando assim o "decoreba"(ato de decorar várias fórmulas ou procedimentos).

Abordamos a aritmética dos restos no segundo capítulo, apresentando o conceito de congruências de números inteiros e quatro funções aritméticas particularmente interessantes. As funções $\tau(n)$ e $\sigma(n)$ que tratam respectivamente da quantidade e da soma dos divisores positivos de um número inteiro, a função $\pi(n)$ que estuda a frequência dos números primos e a famosa função $\phi(n)$ (Função de Euler) que é fundamental para os sistemas de criptografia RSA. Vale ressaltar que as duas primeiras funções podem ser aplicadas no ensino médio atreladas ao estudo das progressões geométricas e análise combinatória, as mesmas já foram abordadas em algumas questões da Olimpíada Brasileira de Matemática das Escolas Públicas (OBMEP).

No capítulo 3 estudamos sobre criptografia. Abordamos um pouco do contexto histórico da criptografia, apresentamos um sistema simétrico simples fazendo o uso de função afim e o sistema assimétrico RSA em duas formas, a primeira visa codificação de letras em números e a segunda letras em letras. O processo é essencialmente o mesmo em ambos, com nível de segurança se bem aplicados. A escolha do qual usar fica a critério do gosto de linguagem a ser ser usada, só números? ou letras? qual o menos trabalhoso para minha perspectiva de uso?

No capítulo 4 apresentamos duas aplicações do estudo de criptografia em sala de aula, tratam-se de dois planos de aula para primeira e segunda séries do ensino médio. O primeiro plano trata da construção de um sistema de criptografia simples utilizando função afim, o segundo plano acrescenta o conceito de congruência de

números inteiros e cria um pequeno programa como forma de aplicação prática. O principal objetivo desses planos é instigar a curiosidade no processo de aprendizado de matemática, o que para estudiosos da Educação como Paulo Freire [6] e Hugo Assmann [1] é muito importante.

Capítulo 1

Conceitos básicos de divisibilidade e números primos

Neste capítulo apresentamos conceitos básicos de divisibilidade de números inteiros, algoritmo da divisão, critérios de divisibilidade, números primos e o processo de busca de números primos. No decorrer do capítulo enunciaremos alguns resultados que envolvem a definição de congruência de números inteiros, tal conteúdo é abordado no capítulo 2.

1.1 Divisibilidade

Estudamos nessa secção algumas características básicas da divisibilidade de números inteiros.

Definição 1.1 *Dados os números inteiros a e b (com $b \neq 0$), dizemos que a divide b (em símbolos $a \mid b$) quando existir um número inteiro c, tal que*

$$b = a \cdot c$$

Neste caso, dizemos que b é múltiplo de a, ou de maneira equivalente b é divisível por a.

De maneira um tanto mais elegante, temos que:

$$a \mid b \Leftrightarrow b = a \cdot c$$

Para algum $c \in \mathbb{Z}$.

Denotamos o conjunto de divisores positivos de a por $D_a = \{n \in \mathbb{N} : n \mid a\}$ e o conjunto de múltiplos de a por $M_a = \{n \in \mathbb{N} : a \mid n\}$.

Exemplo 1.1 *Determinar todos os números inteiros n para os quais $3n+1$ divide $9n^3+11n+12$.*

Solução: *É fácil ver que $9n^3+11n+12 = (3n^2-n+4)\cdot(3n+1)+8$, daí podemos concluir que:*

$$\frac{9n^3+11n+12}{3n+1} = 3n^2-n+4+\frac{8}{3n+1}$$

Como $3n^2-n+4 \in \mathbb{Z}$, então $3n+1$ divide $9n^3+11n+12$ se, e somente se, $3n+1$ divide 8. Como $D_8 = \{\pm1, \pm2, \pm4, \pm8\}$, devemos ter:

$$3n+1 = \pm1,\ 3n+1 = \pm2,\ 3n+1 = \pm4,\ 3n+1 = \pm8$$

De onde obtemos $n=-3$, $n=-1$, $n=0$ e $n=1$ como as soluções inteiras.

Proposição 1.1 *Se $b \mid a$ com $a \neq 0$, então $|b| \leq |a|$.*

Demonstração: Como $b \mid a$, por definição $a = b\cdot c$ com $c \in \mathbb{Z}$ e $c \neq 0$, logo $|a| = |b|\cdot|c| = |b\cdot c|$. Pelo fato de $c \neq 0$, resulta que $1 \leq |c|$ multiplicando essa desigualdade por $|b|$ obtemos $|b| \leq |b|\cdot|c| = |a|$. Como queríamos. ■

Perceba que decorre imediatamente da Proposição 1.1 que os únicos divisores de 1 são -1 e 1.

Teorema 1.1 *A divisibilidade de números inteiros satisfaz as seguintes propriedades:*
(1) $1 \mid a$, $a \mid a$ e $a \mid 0$ para todo $a \in \mathbb{Z}$
(2) Se $a \mid b$ e $b \mid a$, então $a = \pm b$
(3) Se $a \mid b$ e $b \mid c$ então $a \mid c$
(4) Se $a \mid b$ e $c \mid d$ então $a\cdot c \mid b\cdot d$
(5) Se $a \mid (b \pm c)$. Então, $a \mid b \Leftrightarrow a \mid c$
(6) Se $a_1, a_2, ..., a_n$ são números inteiros divisíveis por a, então:

$$a \mid (a_1\cdot b_1 + a_2\cdot b_2 + ... + a_n\cdot b_n)$$

para quaisquer que sejam os inteiros $b_1, b_2, ..., b_n$.

As demonstrações dos itens 1,3,4,5 e 6 do Teorema 1.1 decorrem imediatamente da definição de divisibilidade, já o item 2 é imediato da Proposição 1.1. As mesmas podem ser encontradas no livro do Abramo [7] e no livro do Vandemberg [14]. A seguir, resolvemos três exemplos, que podem ser excelentes artifícios para solução de questões que envolvem divisibilidade de números inteiros.

Exemplo 1.2 *Sejam, $a, b \in \mathbb{Z}$ (com $a - b \neq 0$) e $n \in \mathbb{N}$. Mostre que $a - b$ divide $a^n - b^n$.*

Solução: *Quando $n = 1$ o resultado é óbvio, sendo assim, nos resta mostrar para $n \geq 2$. Ora, mas isso é equivalente a mostrar que a sentença*

$$\frac{a^n - b^n}{a - b} = a^{n-1} + a^{n-2} \cdot b + ... + a \cdot b^{n-2} + b^{n-1}$$

é válida para todo $n \geq 2$. Para isso usemos indução matemática. Perceba que a sentença é valida quando $n = 2$, pois,

$$\frac{a^2 - b^2}{a - b} = \frac{(a - b) \cdot (a + b)}{a - b} = a + b$$

Suponhamos a validade da mesma para um certo $n \in \mathbb{N}$, ou seja,

$$\frac{a^n - b^n}{a - b} = a^{n-1} + a^{n-2} \cdot b + ... + a \cdot b^{n-2} + b^{n-1}$$

Devemos mostrar que também valerá para $n + 1$. De fato, multiplicando ambos os membros da igualdade acima por a, obtemos:

$$\frac{a^{n+1} - a \cdot b^n}{a - b} = a^n + a^{n-1} \cdot b + ... + a^2 \cdot b^{n-2} + a \cdot b^{n-1}$$

Agora somando b^n a ambos os lados da igualdade, resulta que:

$$\frac{a^{n+1} - a \cdot b^n}{a - b} + b^n = \frac{a^{n+1} - a \cdot b^n}{a - b} + \frac{b^n \cdot (a - b)}{a - b} = a^n + a^{n-1} \cdot b + ... + a^2 \cdot b^{n-2} + a \cdot b^{n-1} + b^n$$

o que equivale a

$$\frac{a^{n+1} - b^{n+1}}{a - b} = a^n + a^{n-1} \cdot b + ... + a^2 \cdot b^{n-2} + a \cdot b^{n-1} + b^n$$

Logo a sentença também vale para $n+1$, com isso obtemos o resultado que desejamos.

Exemplo 1.3 *Sejam, $a, b \in \mathbb{Z}$ (com $a + b \neq 0$) e $n \in \mathbb{N}$. Mostre que $a + b$ divide $a^{2n+1} + b^{2n+1}$.*

Solução: *Analogamente ao Exemplo 1.2, basta usar indução para mostrar que:*

$$\frac{a^{2n+1} + b^{2n+1}}{a + b} = a^{2n} - a^{2n-1} \cdot b + ... - a \cdot b^{2n-1} + b^{2n}$$

De fato, quando $n = 1$ temos que,

$$\frac{a^{2n+1} + b^{2n+1}}{a+b} = \frac{a^3 + b^3}{a+b} = \frac{(a+b)\cdot(a^2 - a\cdot b + b^2)}{a+b} = a^2 - a\cdot b + b^2$$

Tomando por hipótese a validade para n, e multiplicando por a^2 e depois somando $-a\cdot b^{2n+1} + b^{2n+2}$ a ambos os membros da igualdade:

$$\frac{a^{2n+1} + b^{2n+1}}{a+b} = a^{2n} - a^{2n-1}\cdot b + ... - a\cdot b^{2n-1} + b^{2n}$$

Obtemos:

$$\frac{a^{2(n+1)+1} + b^{2(n+1)+1}}{a+b} = a^{2(n+1)} - a^{2n+1}\cdot b + ... - a^3\cdot b^{2n-1} + a^2\cdot b^{2n} - a\cdot b^{2n+1} + b^{2(n+1)}$$

E com isso, pelo princípio de indução está provada a igualdade para todo número natural, como queríamos.

Exemplo 1.4 *Sejam, $a, b \in \mathbb{Z}$ (com $a + b \neq 0$) e $n \in \mathbb{N}$. Mostre que $a + b$ divide $a^{2n} - b^{2n}$.*

Solução: *De modo semelhante ao Exemplo 1.2, basta usar indução para mostrar que:*

$$\frac{a^{2n} - b^{2n}}{a+b} = a^{2n-1} - a^{2n-2}\cdot b + ... + a\cdot b^{2n-2} - b^{2n-1}$$

De fato, quando $n = 1$ temos:

$$\frac{a^2 - b^2}{a+b} = \frac{(a+b)\cdot(a-b)}{a+b} = a - b$$

Supondo a validade para n e multiplicando por a^2 e depois somando $a\cdot b^{2n} - b^{2n+1}$ a ambos os membros da igualdade:

$$\frac{a^{2n} - b^{2n}}{a+b} = a^{2n-1} - a^{2n-2}\cdot b + ... + a\cdot b^{2n-2} - b^{2n-1}$$

Obtemos,

$$\frac{a^{2(n+1)} - b^{2(n+1)}}{a+b} = a^{2n+1} - a^{2n}\cdot b + ... + a^3\cdot b^{2n-2} - a^2\cdot b^{2n-1} + a\cdot b^{2n} - b^{2n+1}$$

E com isso, pelo princípio de indução está provada a igualdade para todo número natural, como queríamos.

1.1.1 Algoritmo da divisão e Algoritmo Euclidiano

Antes de enunciar os resultados desta seção, é de fundamental importância saber do que trata um algoritmo. Pois bem, de maneira essencial um algoritmo é uma "receita"para resolver determinado tipo de problema. Imagine que temos a tarefa de fazer um yakisoba, se pesquisarmos a receita, encontramos uma lista de ingredientes e um conjunto de instruções a seguir para conseguirmos alcançar nosso objetivo. Depois de conseguir os ingredientes e seguir as instruções, temos como resultado o yakisoba. Assim é o algoritmo, quando formos especificá-lo devemos deixar claro qual é a sua entrada e sua saída. Ou seja, definimos a entrada (como os ingredientes) e listamos as operações e passos a serem executados que nos levam a um determinado resultado (saída que desejamos: "o produto"). Podemos então enunciar o algoritmo como um fato ou teorema, deixando claro os ingredientes e os passos a serem executados em busca do produto final, como podemos ver nos algoritmos fundamentais que são apresentados nessa secção.

Algoritmo da divisão

Teorema 1.2 *Sejam a e b inteiros com $b > 0$, então existem únicos inteiros q e r tais que:*

$$a = b \cdot q + r$$

com $0 \leq r < b$.

Demonstração: Seja o conjunto $L = \{x = a - b \cdot q;\ q \in \mathbb{Z} \text{ e } a - b \cdot q \geq 0\}$. Podemos afirmar que L não é vazio, pois $|a| \cdot b \geq |a| \Rightarrow a + |a| \cdot b \geq a + |a| \geq 0$. Daí, $x = a - (-|a|) \cdot b$ é da forma $a - bq$ com $q = -|a|$, com isso $x \in L$.
Sendo L limitado inferiormente por 0, pelo Principio da boa ordenação existe $r =$min L, com isso temos que $r \geq 0$ e

$$r = a - b \cdot q, \text{ com } q \in \mathbb{Z}.$$

E ainda, $r < b$ pois, caso contrário $r - b = a - b \cdot q - b = a - b(q+1) > 0$ $(r - b \in L)$ e $r - b < b$, o que contraria a minimalidade de r. Isso nos garante a existência de q e r.
A unicidade é garantida pelo fato que se existissem $q', r' \in \mathbb{Z}$ tais que

$$a = b \cdot q' + r', \text{ com } 0 \leq r' < b.$$

Com isso, $b \cdot q + r = b \cdot q' + r'$ o que equivale a

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

Ou seja, $b \mid (r - r')$. E pela Proposição 1.1 $|r - r'| < b$, segue que $r - r' = 0$, logo, $r = r'$, o que resulta $q' = q$, uma vez que $b \neq 0$. ∎

Corolário 1.1 ***(versão geral do Algoritmo da divisão):*** *Sejam a e b números inteiros, com $b \neq 0$, então, existem únicos inteiros q e r tais que*

$$a = b \cdot q + r, \text{ com } 0 \leq r < |b|.$$

A demonstração pode ser encontrada [7].

Exemplo 1.5 *Determine o quociente e o resto da divisão de a por b quando:*
a) $a = 73$ e $b = 21$
b) $a = -73$ e $b = 21$
c) $a = -73$ e $b = -21$
d) $a = 73$ e $b = -21$

Solução:
a) Como $73 = 21 \cdot 3 + 10$ e $10 < 21$, então $q = 3$ e $r = 10$.
b) Pelo item anterior temos que $73 = 21 \cdot 3 + 10$, então

$$-73 = -21 \cdot 3 - 10 = -21 \cdot 3 - 10 - 21 + 21 = 21 \cdot (-4) + 11$$

Logo, $q = -4$ e $r = 11$.
c) Como $73 = 21 \cdot 3 + 10$, então

$$-73 = -21 \cdot 3 - 10 - 21 + 21 = -21 \cdot (3 + 1) + 11 = -21 \cdot 4 + 11.$$

Logo, $q = 4$ e $r = 11$.
d) Como $73 = 21 \cdot 3 + 10$, então

$$73 = -21 \cdot -3 + 10$$

Logo, $q = -3$ e $r = 10$.

Algoritmo Euclidiano

Definição 1.2 ***(Máximo divisor comum:)*** *Sejam $a, b \in \mathbb{Z}$. Dizemos que $d \geq 0$ é um máximo divisor comum (mdc) de a e b, se*

1) $d \mid a$ e $d \mid b$;

2) Se $c \in \mathbb{Z}$ é tal que $c \mid a$ e $c \mid b$ então $c \mid d$.

É fácil ver que se o mdc existir ele é único, pois, caso contrário, se d e d' fossem mdc's de a e b, teríamos que $d \mid d'$ e $d' \mid d$ com $d, d' \geq 0$, logo $d = d'$. Ou seja, na existência de d ele é único. Usualmente usaremos a notação $d = \text{mdc}(a, b)$.

Em alguns casos particulares é imediato calcular o mdc. Por exemplo, se a é um número inteiro não nulo é imediato que:

I) $\text{mdc}(0, a) = |a|$.

II) $\text{mdc}(1, a) = 1$.

III) $\text{mdc}(a, a) = |a|$.

IV) Se $b \in \mathbb{Z}$, então $a \mid b \Leftrightarrow \text{mdc}(a, b) = |a|$.

V) $\text{mdc}(a, b) = \text{mdc}(-a, b) = \text{mdc}(-a, -b) = \text{mdc}(a, -b)$.

Perceba que os itens acima decorrem imediatamente da definição de mdc unida com a definição de divisibilidade, note ainda que o item V) nos permite assumir sem perda de generalidade $\text{mdc}(a, b) = \text{mdc}(|a|, |b|)$, isso facilitará o trabalho de encontrar o mdc de dois inteiros quaisquer.

Teorema 1.3 *(**Teorema de Bachet-Bézout:**) Seja d o mdc de dois inteiros a e b, então existem inteiros x_0 e y_0 tais que $a \cdot x_0 + b \cdot y_0 = d$.*

Demonstração: Como comentado anteriormente, adotemos $a, b \geq 0$. Seja o conjunto

$$X_+ = \{a \cdot x + b \cdot y;\ x, y \in \mathbb{Z} \text{ e } a \cdot x + b \cdot y > 0\}.$$

É fácil ver que X_+ não é vazio, pois quando $x, y > 0$ e a, b não ambos nulos, temos $a \cdot x + b \cdot y > 0 \in X_+$. Assim sendo, pelo princípio da boa ordenação X_+ possui um menor elemento, seja $k = \min X_+$. Note que

$$k = a \cdot x_0 + b \cdot y_0 \text{ com } x_0, y_0 \in \mathbb{Z} \qquad \star$$

Pelo algoritmo da divisão, temos que:

$$a = k \cdot q + r, \text{ com } 0 \leq r < k. \qquad \star\star$$

Substituindo o valor de k em $\star$ na igualdade de $\star\star$, obtemos:

$$r = a - k \cdot q = a - (a \cdot x_0 + b \cdot y_0)q = a - a \cdot q \cdot x_0 - b \cdot q \cdot y_0$$
$$\Rightarrow r = a(1 - q \cdot x_0) + b(-q \cdot y_0)$$

Logo, concluímos que $r = a \cdot u + b \cdot v$, com $u = (1 - q \cdot x_0)$ e $v = (-q \cdot y_0)$. Com isso, $r = 0$, pois caso contrário $r > 0$, e por conseguinte $r \in X_+$, o que contraria a

minimalidade de k (absurdo). Daí de $\star\star$ $a = k \cdot q$, ou seja, $k \mid a$. De modo análogo, podemos constatar que $k \mid b$.

Sendo $d = \text{mdc}\ (a, b)$, então $a = d \cdot k_1$ e $b = d \cdot k_2$ e por $\star$ deduzimos que:

$$k = (d \cdot k_1)x_0 + (d \cdot k_2)y_0 = d(k_1 \cdot x_0 + k_2 \cdot y_0)$$

Ou seja, $d \mid k$, e como $k \mid d$, pois $d = \text{mdc}\ (a, b)$, segue que $d = k$. Portanto,

$$a \cdot x_0 + b \cdot y_0 = d$$

■

Corolário 1.2 *Se $d = mdc(a, b)$ então*

$$X = \{a \cdot x + b \cdot y; x, y \in \mathbb{Z}\} = M_d$$

onde M_d é o conjunto dos múltiplos de d.

Teorema 1.4 ***(Lema de Gauss):*** *Sejam a, b e c números inteiros. Se $a \mid b \cdot c$ e $mdc(a, b) = 1$, então $a \mid c$.*

Demonstração: Se $a \mid b \cdot c$ então $b \cdot c = a \cdot x$ com $x \in \mathbb{Z}$. Se $\text{mdc}(a, b) = 1$ pelo teorema de Bachet-Bézout, temos que existem $x_0, y_0 \in \mathbb{Z}$ tais que

$$x_0 \cdot a + y_0 \cdot b = 1$$

Multiplicando ambos os membros da igualdade acima por c, obtemos:

$$x_0 \cdot a \cdot c + y_0 \cdot b \cdot c = c$$

E como $b \cdot c = a \cdot x$ temos que

$$c = x_0 \cdot a \cdot c + y_0 \cdot a \cdot x = a(x_0 \cdot c + y_0 \cdot x)$$

E portanto, $a \mid c$. ■

Lema 1.1 *Sejam $a, b, n \in \mathbb{Z}$. Se existir o $mdc(a, b - n \cdot a)$, então o $mdc(a, b)$ existe, e ainda,*

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

Demonstração: Seja $\text{mdc}(a, b - n \cdot a) = d$, pela definição de mdc, temos que $d \mid a$ e $d \mid (a - b \cdot n)$. E a partir disso, o conceito de divisibilidade nos permite concluir que $d \mid (b - n \cdot a) + n \cdot a$, o que equivale a $d \mid b$. Assim, $d \mid a$ e $d \mid b$. Suponhamos agora que $c \mid a$ e $c \mid b$, para algum $c \in \mathbb{N}$, disso resulta que c também divide $(b - n \cdot a)$, logo pela definição de mdc, como $c \mid a$ e $c \mid (b - n \cdot a)$, temos que $c \mid d$.
Portanto,

$$d = \text{mdc}(a, b - n \cdot a) = \text{mdc } (a, b)$$

Como queríamos. ■

Teorema 1.5 ***(Algoritmo Euclidiano)*** *Para todos $a, b \in \mathbb{Z}$. Existe $mdc(a, b) = d$.*

Demonstração: Note que é equivalente mostrar para $a, b \in \mathbb{N}$, pois como vimos $\text{mdc}(a, b) = \text{mdc}(|a|, |b|)$, e ainda, como $\text{mdc}(a, b) = a$ quando $a \mid b$, nos resta analisar o caso em que $1 < a < b$ e $a \nmid b$. Pois bem, aplicando o Algoritmo da divisão, temos que:

$$b = a \cdot q_1 + r_1, \text{ com } 0 < r_1 < a.$$

Assim, se $r_1 \mid a$, então

$$\text{mdc}(a, b) = \text{mdc}(a, b - a \cdot q_1) = \text{mdc}(a, r_1) = r_1$$

Se $r_1 \nmid a$, então

$$a = r_1 \cdot q_2 + r_2 \text{ com } 0 < r_2 < r_1 \ (r_2 = a - r_1 \cdot q_2)$$

Assim, se $r_2 \mid r_1$ então,

$$\text{mdc}(a, b) = \text{mdc}(a, r_1) = \text{mdc}(a - r_1 \cdot q_2, r_1) = \text{mdc}(r_2, r_1) = r_2$$

Caso contrário de $r_2 \nmid r_1$, então

$$r_1 = r_2 \cdot q_3 + r_3 \text{ com } 0 < r_3 < r_2 \ (r_3 = r_1 - r_2 \cdot q_3).$$

E assim continuamos o procedimento, até que pare (quando encontrarmos o mdc). Note que isso sempre ocorre, pois do contrário, teríamos uma sequência de números naturais $a > r_1 > r_2 > ...$ que não possui menor elemento, o que é um absurdo pelo princípio da boa ordenação. Sendo assim, para algum k, temos que $r_k \mid r_{k-1}$, o que nos dá $\text{mdc}(a, b) = r_k$. ■

De modo simples, podemos dizer que o $\text{mdc}(a, b) = r_k$ onde r_k é o último resto não nulo das divisões sucessivas elencadas anteriormente.

Exemplo 1.6 *Determine o valor de d, tal que $mdc(551, 874) = d$ e determine inteiros x e y tais que $a \cdot x + b \cdot y = d$.*

Solução: Aplicando o Algoritmo Euclidiano, temos

$$\begin{gathered} 874 = 551 \cdot 1 + 323 \\ 551 = 323 \cdot 1 + 288 \\ 323 = 228 \cdot 1 + 95 \\ 228 = 95 \cdot 2 = 38 \\ 95 = 38 \cdot 2 + \mathbf{19} \\ 38 = 19 \cdot 2 + 0. \end{gathered}$$

Logo, o mdc$(551, 874)$=19.

E a partir disso, temos:

$$\begin{gathered} 19 = 95 - 38 \cdot 2 = 95 - (228 - 95 \cdot 2) \cdot 2 = \\ = 95 \cdot 5 - 228 \cdot 2 = (323 - 228) \cdot 5 - 228 \cdot 2 = \\ = 323 \cdot 5 - 228 \cdot 7 = 323 \cdot 5 - (551 - 323) \cdot 7 = \\ = 323 \cdot 12 - 551 \cdot 7 = (874 - 551) \cdot 12 - 551 \cdot 7 = \\ = 874 \cdot 12 - 551 \cdot 19 \end{gathered}$$

Logo, $551 \cdot (-19) + 874 \cdot 12 = 19 = \text{mdc}(551, 874)$, como queríamos.

Portanto, $x = -19$ e $y = 12$ é uma solução.

Comentário 1.1 *Esse resultado é de fundamental importância para o processo de busca se soluções de equações diofantinas lineares, que tem importantes aplicações. Uma delas é a busca do inverso multiplicativo módulo m, ou seja, encontrar x tal que* $a \cdot x \equiv 1$ *mod m, o que é de fundamental importância para sistemas de criptografia como o RSA.*

1.2 Números primos

"Grande parte dos resultados sofisticados da teoria dos números deve-se ao estudo feito sobre números primos"[14]. Como o objetivo desse trabalho é analisar o funcionamento dos sistemas de criptografia, dando ênfase ao RSA, nesse capítulo estudaremos alguns fatos sobre os números primos, tendo em vista que a segurança do RSA depende de fato de sermos capazes de escolher dois números primos extremamente grandes, como veremos a última secção.

Definição 1.3 *Um número natural* $p \neq 1$ *é dito um número primo, quando seus únicos divisores positivos são* 1 *e p. Caso contrário, p será composto.*

Exemplo 1.7 *Os números* $2, 5$ *e* 11 *são primos, equanto os números* $4 = 2 \cdot 2, 10 = 5 \cdot 2$ *e* $12 = 2 \cdot 6$ *são compostos.*

Exemplo 1.8 *O número* $11^{9999999} - 7^{9999999}$ *é composto, pois pelos Exemplos 1.2 e 1.3 da secção de divisibilidade 11-7=4 e 11+7=18 são divisores do mesmo.*

Observação 1.1 *Um número n é composto se existe* $1 < k_1 < n$ *tal que* $k_1 \mid n$ *e pela definição de divisibilidade decorre que existe* $1 < k_2 < n$ *tal que* $n = k_1 \cdot k_2$.

Observação 1.2 *É imediato da definição que se p e p' são dois números primos e $a \in \mathbb{N}$, então:*

(I) $p \mid p'$ se, e somente se $p = p'$;

(II) Se $p \nmid a$, então $mdc(a, p) = 1$.

Proposição 1.2 ***(Lema de Euclides):*** *Sejam $a, b, p \in \mathbb{Z}$, com p primo. Se $p \mid a \cdot b$ então $p \mid a$ ou $p \mid b$.*

Demonstração: Suponhamos que $p \mid a \cdot b$ e $p \nmid a$, logo $\text{mdc}(a, p) = 1$ e pelo Lema de Gauss (Teorema 1.4) concluímos que $p \mid b$. Se $p \mid a \cdot b$ e $p \nmid b$, temos que $\text{mdc}(b, p) = 1$ logo pelo Lema de Gauss $p \mid a$. Com Isso provamos que $p \mid a$ ou $p \mid b$. ■

Corolário 1.3 *Sejam $p, p_1, p_2, ..., p_n$ números primos. Se $p \mid p_1 \cdot p_2 \cdot ... \cdot p_n$, então $p = p_i$ para algum $i = 1, 2, ..., n$.*

Demonstração: Seja p um número primo. Considere a seguinte sentença aberta:

$$P(n) : p, p_1, p_2, ..., p_n \text{ números primos e } p \mid p_1 \cdot p_2 \cdot ... \cdot p_n \Rightarrow p \mid p_i \text{ para algum } i = 1, 2, ..., n.$$

Vamos mostrar por indução que $P(n)$ é verdadeira para todo $n \in \mathbb{N}_{>1}$. Inicialmente note que pela proposição anterior garantimos a validade de $P(2)$. Suponhamos então a validade de $P(n)$, e assim devemos provar que $P(n) \Rightarrow P(n+1)$.

Ora pois, sejam $p'_1, p'_2, ..., p'_n, p'_{n+1}$ números primos tais que $p \mid p'_1 \cdot p'_2 \cdot ... \cdot p'_n \cdot p'_{n+1}$ isso equivale à $p \mid (p'_1 \cdot p'_2 \cdot ... \cdot p'_n) \cdot p'_{n+1}$ que ocorre se, e somente se, $p \mid p'_1 \cdot p'_2 \cdot ... \cdot p'_n$ ou $p \mid p'_{n+1}$ atrelando a hipótese resulta que $[p \mid p_i$ para algum $i = 1, 2, ..., n]$ ou $[p \mid p'_{n+1}]$ ou seja, $p \mid p'_i$ para algum $i = 1, 2, ..., n+1$, com isso provamos que $P(n) \Rightarrow P(n+1)$. Portanto, pelo princípio de indução finita está provada a sentença.

E por fim, unindo a validade de $P(n)$ a Observação 1.2 concluímos a demonstração. ■

Teorema 1.6 ***(Teorema Fundamental da Aritmética)*** *Todo número natural maior que 1 ou é primo ou se escreve de modo único (a menos da ordem dos fatores) como um produto de fatores primos.*

Demonstração: Considere a seguinte sentença aberta:

$P(n)$: Dado $n \in \mathbb{N}_{>1}$, n é primo ou pode ser escrito como um produto de primos.

Note que $P(2)$ é verdadeira, pois 2 é um número primo. Suponhamos a validade de $P(k)$ para todo $k < n$. Devemos mostrar que $P(n)$ também é verdadeira. Ora, mas se n for primo não temos o que fazer. Suponhamos então que n é composto, ou seja, existem $1 < k_1, k_2 < n$ tais que $n = k_1 \cdot k_2$. Por hipótese de indução temos que $k_1 = p_1 \cdot ... \cdot p_r$ e $k_2 = q_1 \cdot ... \cdot q_s$, com p_i e q_j primos para $i = 1, 2, ..., r$ e $j = 1, 2, .., s$. Assim,

$$n = k_1 \cdot k_2 = p_1 \cdot ... \cdot p_r \cdot q_1 \cdot ... \cdot q_s$$

Ou seja, n é escrito como produto de primos. Logo pelo princípio de indução finita está provado que $n \in \mathbb{N}_{>1}$, n é primo ou pode ser escrito como produto de números primos.

Veja que com isto, nos resta mostrar a unicidade da decomposição em fatores primos. Para isso, tomemos a seguinte sentença:

$$W(n) : \text{a decomposição de } n \in \mathbb{N}_{>1} \text{ em fatores primos é única.}$$

É fácil ver que $W(2)$ é válida. Suponhamos agora que $W(k)$ é válida para todo $k < n$. Agora, seja $n = p_1' \cdot ... \cdot p_r'$ e $n = q_1' \cdot ... \cdot q_s'$, donde p_i' e q_j' são primos. Pelo corolário anterior, segue que,

$$p_1' \cdot ... \cdot p_r' = q_1' \cdot ... \cdot q_s' \Rightarrow p_1' \mid q_1' \cdot ... \cdot q_s' \Rightarrow p_1' = q_{j(1)}'.$$

Assim, podemos reordenar os índices e supor que $j(1) = 1$. Daí, $p_2' \cdot ... \cdot p_r' = q_2' \cdot ... \cdot q_s'$. Como $p_2 \cdot ... \cdot p_r < n$, então por hipótese de indução temos que $r = s$ e que p_i' e q_j' são iguais aos pares. Segue por Indução que $W(n)$ é verdadeira para todo $n \in \mathbb{N}_{>1}$. Logo, está provada que a decomposição de n em fatores primos é única.

Logo, a validade de $P(n)$ e $W(n)$ prova o que gostaríamos. ■

Por meio de uma ordenação e agrupamento dos primos da decomposição apresentada no teorema anterior, podemos enunciar o seguinte resultado:

Corolário 1.4 *Dado $n \in \mathbb{Z} - \{-1, 0, 1\}$, existem primos $p_1 < ... < p_r$ e $\alpha_1, ..., \alpha_r \in \mathbb{N}$ univocamente determinados, tais que:*

$$n = \pm p_1^{\alpha_1} \cdot ... \cdot p_r^{\alpha_r}.$$

Um importante resultado em teoria dos números que decorre imediatamente do Teorema Fundamental da Aritmética, trata da infinidade dos números primos.

Teorema 1.7 *Existem infinitos números primos.*

Demonstração: Suponhamos por absurdo que existem finitos números primos, a saber $p_1, ..., p_r$ e seja o número

$$n = p_1 \cdot ... \cdot p_r + 1$$

Por hipótese, n não pode ser primo. Mas, pelo Teorema Fundamental da Aritmética, n possui um fator primo p, tal que $p \mid p_1 \cdot ... \cdot p_r + 1$ e por hipótese $p = p_i$ para algum $i = 1, 2, ...r$, o que resulta $p \mid p_1 \cdot ... \cdot p_r$ e $p \mid 1$, o que é um absurdo, logo devem existir infinitos números primos. ■

1.2.1 Alguns critérios de divisibilidade

Em teoria dos números são conhecidos alguns critérios de divisibilidade. Os mesmos visam facilitar o processo de decomposição de um número em fatores primos. Aqui, apresentamos alguns casos particulares conhecidos e enunciamos um teorema que nos permite encontrar um critério de divisibilidade de um número inteiro por um número primo p de modo geral.

Proposição 1.3 *(**Divisão por 2, 5 e 10**) Seja $w \in \mathbb{Z}$, temos que w é divisível por 2,5 e 10 se, e somente se, o algarismo das unidades (a_0) de w for divisível por 2,5 e 10 respectivamente.*

Demonstração: Basta verificar que $w = a_n 10^n + a_{n-1} 10^{n-1} + ... + a_1 10 + a_0$ para todo $w \in \mathbb{Z}$ com $a_i \in \{0, \pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \pm 6, \pm 7, \pm 8, \pm 9\}$ e $n \in \mathbb{N}$. ■

Proposição 1.4 *(**Divisão por 3 e 9**) Dado um número inteiro $w = a_n a_{n-1} ... a_1 a_0$ com $a_i \in 1, 2, 3, 4, 5, 6, 7, 8, 9$, temos que w é divisível por 3 e por 9 se, e somente se, $a_0 + a_1 + ... + a_n$ for divisível por 3 e por 9 respectivamente.*

Demonstração: Basta tomar $w = a_n 10^n + a_{n-1} 10^{n-1} + ... + a_1 10 + a_0$ e unir a fato que $9 \mid 10^n - 1$ (pode ser verificado por indução) para todo $n \in \mathbb{N}$. ■

Proposição 1.5 *(**Divisibilidade por 7**) Seja $w = a_n 10^n + a_{n-1} 10^{n-1} + ... + a_1 10 + a_0$ que de modo equivalente pode ser escrito como $w = 10k + a_0$, com $k = a_1 + a_2 10 + ... + a_n 10^{n-1}$. Temos que:*

$$7 \mid w \Leftrightarrow 7 \mid k - 2a_0$$

A demonstração pode ser encontrada [14].

Exemplo 1.9 *5887 é divisível por 7, pois:*

$$7 \mid 5887 \Leftrightarrow 7 \mid 588 - 2 \cdot 7 = 574 \Leftrightarrow 7 \mid 57 - 2 \cdot 4 = 49 = 7 \cdot 7.$$

Poderíamos passar anos enunciando proposições sobre critérios de divisibilidade de um número inteiro por um número primo específico. Surge então a dúvida: será que vale a pena aprender tantos critérios de divisibilidade? Será que existe um padrão de divisibilidade para todos os primos? A resposta para essa pergunta encontra-se no teorema a seguir:

Teorema 1.8 ***(Quebra da unidade):*** *Sejam* $n = a_r a_{r-1} a_{r-2} ... a_2 a_1 a_0$ *com* $a_i \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ *um número natural,* p *um número primo (diferente de* 2 *e* 5*) e* $x \in \mathbb{Z}$ *tal que* $10 \cdot x \equiv 1$ *mod* p*. Ou seja,* x *é um inverso multiplicativo de* 10 *módulo* p*. O critério de divisibilidade então é o seguinte: se* $m = a_r a_{r-1} a_{r-2} ... a_2 a_1 + x \cdot a_0$ *então* p *divide* n *se, e somente se,* p *divide* m*.*

Demonstração: Sendo $n = a_r 10^r + a_{r-1} \cdot 10^{r-1} + ... + a_1 \cdot 10 + a_0$ e $m = a_r \cdot 10^{r-1} + a_{r-1} \cdot 10^{r-2} + ... + a_1 + x \cdot a_0$. Perceba inicialmente que:

$$n = 10 \cdot m + (1 - 10x) \cdot a_0$$

Como x é um inverso multiplicativo de 10 módulo p, então o termo $1 - 10 \cdot x$ é divisível por p. Portanto, para qualquer que seja a_0, temos:

$$n \equiv 10 \cdot m \bmod p$$

Disso resulta que n é divisível por p se, e somente se, $10 \cdot m$ também é divisível por p. No entanto, como p é primo e p não divide 10 (já que p não é igual a 2 nem 5), então temos que p divide n se, e somente se, p divide m. ■

Exemplo 1.10 *Note que* $10 \cdot 1 \equiv 1$ *mod* 3*, daí, pelo teorema anterior* $n = a_r a_{r-1} a_{r-2} ... a_2 a_1 a_0$ *é divisível por 3 se, e somente se,* $m = a_r a_{r-1} a_{r-2} ... a_2 a_1 + a_0$ *é divisível por 3. Testando a divisibilidade de 12345 por 3 usando esse novo critério temos:*

$$12345 \equiv 1234 + 5 = 1239 \equiv 123 + 9 = 132 \equiv$$
$$13 + 2 = 15 \equiv 1 + 5 = 6 \equiv 3 \equiv 0 \ mod\ 3.$$

Logo 12345 é divisível por 3.

Observação 1.3 *Como o inverso não é único, note que pelo Teorema 1.8 existem diversos critérios a serem criados de acordo com o inverso adotado para gerar o critério de divisibilidade desejado. Com isso, surge a dúvida de qual seria o melhor inverso? A resposta, é o que tornar o critério mais rápido, para determiná-lo devemos colocar na balança o tamanho do número a ser verificado e a quantos dígitos queremos reduzir o número. Pois quando o inverso for negativo quanto maior for em módulo, mais rápido será o processo, por isso é interessante usar um inverso negativo com número de dígitos equivalente a o máximo de dígitos que queremos reduzir os números testados. Outro fato interessante, é que existem outros teoremas que permitem criar critérios de divisibilidade por meio da quebra da dezena e centena, no entanto, esses métodos são trabalhosos, não sendo tão práticos se comparados a quebra da unidade, os mesmos podem ser encontrados no artigo [10].*

1.2.2 Encontrando números primos

Ao iniciar o estudo dos números primos, um dos primeiros questionamentos a surgir é sobre como encontrar números primos? Qual o padrão dos números primos? O processo de busca por números primos é antigo e as respostas para o padrão dos números primos são vagas ou complexas demais sem aplicação prática, sendo em cima disso que reside a segurança de sistemas de criptografia que vemos no final deste trabalho.

Fórmulas Polinomiais

O uso de fórmulas polinomiais é antigo no processo de obtenção de números primos, podemos citar a conjectura que afirma a existência de infinitos primos da forma $n^2 + 1$ (com $n \in \mathbb{N}$), que até então ainda não foi provada. Perceba que $1^2 + 1 = 2$, $2^2 + 1 = 5$, $4^2 + 1 = 17$ são exemplos de primos dessa forma. Mas, será que existem infinitos?

Um teorema interessante, nos garante que não existe uma função polinomial com coeficientes inteiros que gere apenas números primos, como segue:

Teorema 1.9 *Dado um polinômio $P(x)$, como coeficientes inteiros, existe uma infinidade de inteiros positivos n tais que $P(n)$ é composto.*

A Demonstração desse teorema pode ser encontrada no livro do Coutinho [2].

Exemplo 1.11 *Mostre que 7 é o único primo da forma $x^3 - 1$, com $x \in \mathbb{N}$.*

Solução: *A infinidade de números compostos da forma $x^3 - 1$ é garantida pelo teorema anterior, no entanto queremos mostrar que 7 é o único primo que pode ser escrito dessa forma. Note que isso realmente ocorre, pois $7 = 2^3 - 1$ e ainda, $x^3 - 1 = (x - 1) \cdot (x^2 + x + 1)$ o que mostra que $x^3 - 1$ é composto para todo $x \neq 2$, tendo em vista que se $x > 2$, $(x - 1) \geq 2$ e $(x^2 + x + 1) > 2$ e se $x = 1$, $x^3 - 1 = 0$, isso implica a composição de $x^3 - 1$ como queríamos.*

Números de Mersenne

Definição 1.4 *Seja $n \in \mathbb{N}$, o número*

$$M(n) = 2^n - 1$$

é dito número de Mersene.

Note que $M(2) = 2^2 - 1 = 3$, $M(3) = 2^3 - 1 = 7$, $M(5) = 2^5 - 1 = 31$ são primos. No entanto, ainda não temos garantia que existem infinitos primos dessa forma e uma conjectura que encontra-se em aberto é a que segue:

Conjectura 1.1 *Existem infinitos primos de Mersenne.*

Os números de Mersenne, tem sua devida importância nessa teoria, pois existem diversas maneiras de testar se um número de Mersenne é primo, tanto que alguns dos maiores números primos conhecidos são de Mersenne. A título de curiosidade, veja o capítulo 9 do livro do Coutinho [2].

Números de Fermat

Definição 1.5 *Seja $n \in \mathbb{N} \bigcup \{0\}$, o número*

$$F(n) = 2^{2^n} + 1$$

é dito número de Fermat.

Assim, os cinco primeiros números de Fermat são $F(0) = 2^{2^0} + 1 = 3$, $F(1) = 2^{2^1} + 1 = 5$, $F(2) = 2^{2^2} + 1 = 17$, $F(3) = 2^{2^3} + 1 = 257$, $F(4) = 2^{2^4} + 1 = 65537$. Todos esses números são primos. Observando esse comportamento, Fermat afirmou que todos os números dessa forma são primos, até que em 1732, Leonhard Euler mostrou que

$$F(5) = 2^{2^5} + 1 = 4294967297$$

é divisível por 641. Com os recursos que temos hoje, testar a primalidade de $F(5)$ torna-se fácil, no entanto na época de Fermat, esse tipo de decisão ainda era muito difícil.

Crivo de Eratóstenes

O crivo de Eratóstenes é o mais antigo dos métodos para achar primos e um dos mais simples. O mesmo nos permite listar os números primos $p \leq n$ para um $n \in \mathbb{N}$ qualquer. Fazendo uma implementação a programas computacionais convenientes, o mesmo pode fazer a lista de primos menores ou iguais a $n \in \mathbb{N}$, para um n consideravelmente grande.

Teorema 1.10 *Se $n > 1$ for composto, então n possui um divisor primo p, tal que $p \leq \sqrt{n}$.*

Demonstração: Sendo n um número composto, então $n = a \cdot b$, com $1 < a, b < n$. Note que, se $a > \sqrt{n}$ e $b > \sqrt{n}$, então

$$n = a \cdot b > \sqrt{n} \cdot \sqrt{n} = n$$

O que é um absurdo. Logo $a \leq \sqrt{n}$ ou $b \leq \sqrt{n}$. Suponhamos então que $b \leq \sqrt{n}$. Pelo teorema fundamental da aritmética, existe p primo, tal que $p \mid b$ e como $b \mid n$,

por transitividade $p \mid n$ com $p \leq b \leq \sqrt{n}$. ■

O Teorema 1.10 mostra que, para verificar se um dado $n > 1$ é primo, é suficiente verificar sua divisibilidade pelos primos $p \leq \sqrt{n}$.

Perceba que o teste de primalidade dado pelo Teorema 1.10 perde sua eficiência quando n é muito grande, e que mesmo de um ponto de vista computacional torna-se inviável pois $\sqrt{n}$ vai para o infinito a mediada que n vai para o infinito. Ainda não possuímos um algoritmo de grande eficácia do ponto de vista computacional.

O método de Eratóstenes para um $n > 2$ consiste nos seguintes passos:

Passo 1: Como 2 é um número primo, faça a lista de 2 unido com os números ímpares menores ou iguais a n;

Passo 2: Excluímos da lista todos os múltiplos de 3 maiores que 3;

Passo 3: Excluímos da lista todos os múltiplos de 5 maiores que 5;

$\vdots$

Passo k: Excluímos da lista todos os múltiplos de p maiores que p, onde p é o maior número primo menor que $\sqrt{n}$.

Após concluir esses passos, teremos todos os primos menores ou iguais a n.

Exemplo 1.12 *Liste todos os primos menores ou iguais a 100.*

Solução: *Como* $\sqrt{100} = 10$ *basta eliminar todos os múltiplos de* 2 *maiores que 2, todos os múltiplos de 3 maiores que 3,todos os múltiplos de 5 maiores que 5 e todos os múltiplos de 7 maiores que 7 da lista dos 100 primeiros naturais, obtendo:*

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97$$

Fatoração de Fermat

Apresentamos a seguir um algoritmo de fatoração que é muito eficiente quando n tem um fator primo que não é muito menor que $\sqrt{n}$, tal método foi apresentado por Fermat para decompor um número composto em fatores primos. A ideia consiste em determinar divisores para cada divisor impar b de n. O algoritmo é o que segue:

Algoritmo de fatoração de Fermat: Se $n \in \mathbb{N}$ é um número composto, então podemos escrevê-lo na forma:

$$n = 2^k \cdot b$$

Sendo b um número impar e $k \in \mathbb{N} \cup \{0\}$. Se b for primo então a fatoração de n em primos é dada por $n = 2^k \cdot b$, caso contrário procedemos da seguinte forma:

Etapa 1: Determine $a = [\sqrt{n}]$ (a parte inteira da $\sqrt{n}$).
Etapa 2: Se $a^2 - b = r^2$, então $b = (a + r) \cdot (a - r)$
Etapa 3: Caso $a^2 - b \neq r^2$, então somamos 1 a a e voltamos a etapa 2.

Comentário 1.2 *A prova da validade do algoritmo de Fermat não é difícil, no entanto é um tanto longa, por isso não apresentamos nesse trabalho. A mesma pode ser encontrada no livro do Vandeberg [14].*

Na prática, procedemos da seguinte forma, supondo que já conhecemos um algoritmo para o cálculo da raiz quadrada:

Exemplo 1.13 *Determine a decomposição em fatores primos de 572.*

Solução: *Como 572 é par, percebemos facilmente que* $572 = 2^2 \cdot 143$. *Com isso temos que* $b = 143$ *agora é só aplicar as etapas do algoritmo:*

Etapa 1: *Temos que* $a = 11$.
Etapa 2: *Como* $11^2 - 143 = -22$, *e -22 não é quadrado perfeito, usamos 11+1. Daí temos* $12^2 - 143 = 1$ *e 1 é quadrado perfeito, então:*

$$143 = (12 + 1) \cdot (12 - 1)$$

E como $572 = 2^2 \cdot 143$, *obtemos a decomposição de 572 em fatores primos como sendo:* $572 = 2^2 \cdot 11 \cdot 13$.

Exemplo 1.14 *Determine a decomposição em fatores primos de 49283.*

Solução:*: Como trata-se de um número impar, temos que* $b = 49283$. *Aplicando as estapas do algoritmo, temos:*

Etapa 1: *Temos que* $a = 221$.
Etapa 2: *Temos que:* $221^2 - 49283 = -442$ *não é quadrado perfeito, daí fazemos* $222^2 - 49283 = 1^2$. *Logo*

$$49283 = (222 + 1) \cdot (222 - 1) = 223 \cdot 221. \qquad (*)$$

Como 223 *é primo, devemos repetir o algoritmo para* $b = 221$, *ora pois, neste caso:*

Etapa 1: $a = 14$.

Etapa 2: *Temos que* $14^2 - 221 = -25$ *que não é quadrado perfeito, seguindo o processo temos que* $15^2 - 221 = 2^2$*, e com isso*

$$221 = (15 + 2) \cdot (15 - 2) = 17 \cdot 13. \qquad (**)$$

E por fim, unindo $*$ *a* $**$ *resulta que* $49283 = 13 \cdot 17 \cdot 223$.

Comentário 1.3 *Perceba que o metódo de Fermat possui eficiência quando a diferença em módulo entre os divisores iniciais de n relativamente pequena, caso contrário, o número de etapas aumentará consideravelmente tornando o algoritmo ineficaz.*

Capítulo 2

Aritmética dos restos

Neste capítulo estudamos congruência de números inteiros, classes de resíduos e funções aritméticas.

2.1 Congruências

Uma das áreas de estudo mais importantes da teoria dos números são as congruências módulo m, pois tem fundamental importância no processo de checagem da divisibilidade de um número por outro e ainda tem importante aplicação nos sistemas de criptografia mais seguros da atualidade. Nesta secção faremos um estudo de congruências de números inteiros e classes de resíduos.

Definição 2.1 *Dados a, b e m números inteiros com $m > 1$ dizemos que a é congruente a b módulo m, em notação $a \equiv b \ mod \ m$, se a e b deixam mesmos restos quando divididos por m.*

Exemplo 2.1 $7 \equiv 2 \ mod \ 5$ *pois,* $7 = 5 \cdot 1 + 2$ *e* $2 = 5 \cdot 0 + 2$.

Proposição 2.1 $a \equiv b \ mod \ m \Leftrightarrow m \mid a - b$

A demonstração é imediata das Definições 1.1 e 2.1.

Proposição 2.2 ***(Lei do cancelamento)*** *Se $a \cdot c \equiv b \cdot c \ mod \ m$ com $mdc(c, m) = 1$, então $a \equiv b \ mod \ m$.*

Demonstração: Se $a \cdot c \equiv b \cdot c \bmod m$, pela proposição 1 temos que $m \mid ac - bc = c(a - b)$, como $\text{mdc}(c, m) = 1$, pelo Teorema 1.4 resulta que $m \mid a - b$, ou seja, $a \equiv b \bmod m$. ■

Proposição 2.3 *Seja $m, n \in \mathbb{N}$. Dados a, b, c e d números inteiros, temos:*
(i) $a \equiv a \ mod \ m$
(ii) se $a \equiv b \ mod \ m$, *então* $b \equiv a \ mod \ m$
(iii) Se $a \equiv b \ mod \ m$ *e* $c \equiv d \ mod \ m$, *então* $a \equiv c \ mod \ m$
(iv) Se $a \equiv b \ mod \ m$ *e* $c \equiv d \ mod \ m$ *então* $a + c \equiv b + d \ mod \ m$
(v) Se $a \equiv b \ mod \ m$ *e* $c \equiv d \ mod \ m$ *então* $a \cdot c \equiv b \cdot d \ mod \ m$
(vi) Se $a \equiv b \ mod \ m$ *então* $a^n \equiv b^n \ mod \ m$
(vii) $a + c \equiv b + c \ mod \ m \Leftrightarrow a \equiv b \ mod \ m$
(viii) Se $a \equiv b \ mod \ m$ *e* $n \mid m$ *então* $a \equiv b \ mod \ n$
(ix) Se $a \equiv b \ mod \ m$ *então* $mdc \ (a, m) = mdc \ (b, m)$
(x) $a \equiv b \ mod \ m_i \ \forall i = 1, 2, ..., k \Leftrightarrow a \equiv b \ mod \ mmc \ (m_1, m_2, ...m_r)$

Observação 2.1 *A volta da implicação do item (v) só vale quando o* $mdc \ (c, m) = 1$

Observação 2.2 *As demonstrações dos itens acima decorrem imediatamente da definição de congruência, sendo assim não farei as mesmas aqui, haja vista que o objetivo deste trabalho é outro. As mesmas podem ser encontradas em [7] e [14].*

Teorema 2.1 ***(Pequeno Teorema de Fermat)*** *Se p é um número primo e $a \in \mathbb{Z}$ tal que $p \nmid a$, então:*

$$a^p \equiv a \ mod \ p$$

Demonstração: Sejam $a, 2a, ..., (p-1) \cdot a$ os primeiros $p-1$ múltiplos de a, note que esses números são dois a dois incongruentes módulo p, pois caso contrário, se $ak_1 \equiv ak_2 \bmod p$, com $1 \leq k_1 < k_2 \leq p-1$, pelo fato do $\text{mdc}(a, p) = 1$, pela lei do cancelamento $k_1 \equiv k_2 \bmod p$ isto é, $p \mid k_2 - k_1$, o que é impossível. Além disso, se $1 \leq w \leq p-1$ e $p \mid wa$, então $p \mid a$ ou $p \mid w$, o que também não é possível. Logo, $p \nmid wa \ \forall w = 1, 2, ...p-1$.

Pelo algoritmo da divisão, cada inteiro é congruente módulo p a um, e somente um, número da sequência, $1, 2, ..., p-1$, daí temos que em uma determinada ordem:

$$a \equiv w_1 \bmod p$$

$$2a \equiv w_2 \bmod p$$

$$\vdots$$

$$(p-1)a \equiv w_{p-1} \bmod p$$

Com $w_i \in \{1, 2, .., p-1\}$ para $i = 1, 2, ..., p-1$. Multiplicando membro a membro as congruências acima obtemos:

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

E pela lei do cancelamento,

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

E por fim, multiplicando ambos os membros por a obtemos:

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

■

Adotemos sem demonstração os seguintes lemas, cujas demonstrações podem ser encontradas em [7] e [14].

Lema 2.1 *Seja p um número primo, então as únicas soluções módulo p da congruência $x^2 \equiv 1$ mod p são 1 e $p-1$.*

Lema 2.2 *Sejam p um número primo e $A = \{1, 2, ..., p-1\}$. Então, para cada $a \in A$ existe um único $b \in A$ tal que $ab \equiv 1$ mod p.*

Lema 2.3 *Seja $n \in \mathbb{Z}$, com $n > 4$, temos que n é composto se, e somente se, $n \mid (n-2)!$.*

Teorema 2.2 ***(Teorema de Wilson)*** *Um número natural p é primo se, e somente se,*

$$(p-1)! \equiv -1 \text{ mod } p.$$

Demonstração: O resultado é trivialmente satisfeito para $p = 2, 3$, suponhamos que é válido para $p \geq 5$. Pelo lema 2.2, temos que para cada $a \in \{1, 2, ..., p-1\}$, existe um único $b \in \{1, 2, ..., p-1\}$ tais que $ab \equiv 1 \bmod p$. De modo particular, pelo lema 2.1, os únicos valores de a que satisfazem $a^2 \equiv 1 \bmod p$ são $a = 1$ ou $a = p-1$. Daí, se $a \in \{2, ..., p-2\}$ então existe um único $b \in \{2, ..., p-2\}$, diferente de a, tal que $ab \equiv 1 \bmod p$. Fazendo o produto de todos eles obtemos:

$$2 \cdot 3 \cdot ... \cdot (p-2) \equiv 1 \bmod p$$

Disso resulta que

$$1 \cdot 2 \cdot 3 \cdot ... \cdot (p-2) \cdot (p-1) \equiv (p-1) \equiv -1 \bmod p$$

Portanto,

$$(p-1)! \equiv -1 \bmod p$$

A recíproca resulta imediatamente do lema 2.3. Veja que para $p = 2, 3, 4$ é imediato. Supondo, $p > 4$ não primo, teriamos que $p \mid (p-1)!$ e com isso, $p \nmid [(p-1)! + 1]$ ou seja, $(p-1)! \not\equiv -1 \bmod p$, o que é um absurdo. Logo, p é primo.

Portanto, um número natural p é primo se, e somente se,

$$(p-1)! \equiv -1 \bmod p.$$

■

2.2 Classes de resíduos

Definição 2.2 *Seja $m > 1$ um número inteiro, temos que todo conjunto de números inteiros cujos restos da divisão por m são os números $0, 1, 2, .., m-1$ sem repetições, independentemente da ordem, é dito um sistema completo de resíduos módulo m.*

Exemplo 2.2 *0,1,2,3,4,5,6 é um sistema completo de resíduos módulo 7. 700, 22, 1402, 10, 704, 2105, 2106 também o é.*

Proposição 2.4 *Sejam a, k e $m \in \mathbb{Z}$ com $m > 1$ e $mdc\ (k, m) = 1$ se $r_1, r_2, ..., r_m$ é um sistema completo de resíduos módulo m, então*

$$a + k \cdot r_1, a + k \cdot r_2 + ... + a + k \cdot r_m$$

também é um sistema completo de resíduos módulo m.

Demonstração: Da Lei do cancelamento e da Proposição 2.3 (v), obtemos que para $i, j = 0, 1, 2, ..., m-1$, temos que

$$\begin{aligned} a + k \cdot r_i \equiv a + k \cdot r_j \bmod m &\Leftrightarrow k \cdot r_i \equiv k \cdot r_j \bmod m \\ &\Leftrightarrow r_i \equiv r_j \bmod m \Leftrightarrow r_i = r_j. \end{aligned}$$

Disso concluímos que $a+k\cdot r_1, a+k\cdot r_2+...+a+k\cdot r_m$ são dois a dois não congruentes módulo m e, portanto, formam um sistema completo de resíduos módulo m. ■

Definição 2.3 *Seja $m \in \mathbb{Z}$ com $m > 1$. Um sistema reduzido de resíduos módulo m é um conjunto de números $r_1, r_2, ..., r_s$ tais que:*

(i) $mdc(r_i, m) = 1$ para todo $i = 1, 2, ..., s$;

(ii) $r_i \not\equiv r_j \ mod\ m$, se $i \neq j$;

(iii) Para cada $n \in \mathbb{Z}$ tal que $mdc(n, m) = 1$, existe i tal que $n \equiv r_i \ mod\ m$.

Observação 2.3 *Para qualquer $m \in \mathbb{Z}$, com $m > 1$ existe um sistema reduzido de resíduos módulo m, para encontrá-lo é só tomar o sistema completo e eliminar os elementos que não são coprimos com m. Qualquer sistema reduzido terá o mesmo número de elementos, o qual é a quantidade de elementos do conjunto $\{1, 2, ..., m-1\}$ que são coprimos com m.*

Exemplo 2.3 *Dado $m = 10$ um sistema reduzido de resíduos módulo m seria $\{1, 3, 7, 9\}$.*

Definição 2.4 *Seja $m \in \mathbb{Z}$, com $m > 1$. Considere $\phi(m)$ o número de elementos de um sistema reduzido de resíduos módulo m. Para $m = 1$ escrevemos $\phi(1) = 1$, e assim temos a função:*

$$\phi : \mathbb{N} \longmapsto \mathbb{N}$$

Denominada função fi de Euler.

Observação 2.4 *Note que m é primo se, e somente se, $\phi(m) = m - 1$, além disso, $\phi(m) \leq m - 1$ para todo $m \geq 2$.*

Proposição 2.5 *Sejam $k, d \in \mathbb{N}$ e $n = kd$ então a quantidade de números naturais m, tais que $1 \leq m \leq n$ e $mdc(m, n) = d$ é $\phi(k)$.*

Demonstração: Perceba que $1 \leq m \leq n$ e $\text{mdc}(m, kd) = d$ se, e somente se, $m = \alpha d$, com $1 \leq \alpha \leq k$ e $\text{mdc}(\alpha, k) = 1$. Sendo assim, a quantidade de naturais m com as condições acima é igual a quantidade α tal que $1 \leq \alpha \leq k$ e $\text{mdc}(\alpha, k) = 1$, o que equivale a $\phi(k)$. ■

Corolário 2.1 *Seja $n \in \mathbb{N}$, então,*

$$\sum_{d \in \mathbb{N}; d|n} \phi(d) = n.$$

Comentário 2.1 ***Sobre a demonstração do corolário 2.1*** *Sendo $I = \{1, 2, ..., n\}$, basta notar que para cada $d \in \mathbb{N}$ tal que $d \mid n$ sendo $I_d = \{m \in I, mdc(m, n) = d\}$, temos que se $d \neq d'$ então $I_d \cap I_{d'} = \emptyset$ e*

$$\bigcup_{d \in \mathbb{N}; d|n} I_d = I$$

com isso, é só usar a proposição 2.5 para chegar no resultado que queremos.

Lema 2.4 *Sejam $r_1, ..., r_{\phi(m)}$ um sistema reduzido de resíduos módulo m e seja $a \in \mathbb{Z}$ tal que $mdc(a, m) = 1$. Então $ar_1, ..., ar_{\phi(m)}$ é um sistema reduzido de resíduos módulo m.*

Demonstração: Seja $a_1, ..., a_m$ o sistema completo de resíduos do qual foi retirado o sistema reduzido $r_1, ..., r_{\phi(m)}$. Pelo fato do $\text{mdc}(a, m) = 1$, tem-se que o $\text{mdc}(a_i, m) = 1$ se, e somente, se $\text{mdc}(aa_i, m) = 1$. Donde segue o resultado. ■

Teorema 2.3 ***(Teorema de Euler)*** *Sejam $a, m \in \mathbb{Z}$, com $m > 1$ e $mdc(a, m) = 1$. Então:*

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

Demonstração: Seja $r_1, ..., r_{\phi(m)}$ um sistema reduzido de resíduos módulo m. Pelo lema 2,4, temos que $ar_1, ..., ar_{\phi(m)}$ também forma um sistema reduzido de resíduos módulo m. Com isso,

$$ar_1 \cdot ar_2 \cdot ... \cdot ar_{\phi(m)} \equiv r_1 \cdot r_2 \cdot ... \cdot r_{\phi(m)} \bmod m$$

O que equivale a

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

Aplicando a lei do cancelamento, obtemos:

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

Como queríamos. ∎

A seguir serão enunciados alguns resultados de utilidade futura, os quais não faremos as demonstrações. As demonstrações podem ser encontradas em [7].

Proposição 2.6 *Sejam $m, m' \in \mathbb{N}$ tais que $mdc(m, m') = 1$. Então, $\phi(m \cdot m') = \phi(m) \cdot \phi(m')$.*

Corolário 2.2 *Seja $m \in \mathbb{Z}$ livre de quadrados, então para todo $a \in \mathbb{Z}$ e $k \in \mathbb{N}$ tem-se que*

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

Proposição 2.7 *Sejam $p, r \in \mathbb{N}$, com p primo. Então,*

$$\phi(p^r) = p^r - p^{r-1} = p^r \left(1 - \frac{1}{p}\right)$$

Atrelando as proposições 2.6 e 2.7, podemos enunciar o seguinte teorema:

Teorema 2.4 *Seja $m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ...p_r^{\alpha_r}$ a decomposição em fatores primos de m em fatores primos. Então*

$$\phi(m) = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_r^{\alpha_r} \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot ... \cdot \left(1 - \frac{1}{p_r}\right)$$

2.3 Funções aritméticas

Algumas funções em teoria dos números merecem destaque devido a sua importância, são elas:

1. $\tau(n)$: número de divisores positivos de n.
2. $\sigma(n)$: Soma dos divisores positivos de n
3. $\pi(n)$: número de primos menores ou iguais a n.
4. $\phi(n)$: Função ϕ de Euler.

Definição 2.5 *Toda função $f : \mathbb{N} \longmapsto \mathbb{R}$ é dita uma função aritmética.*

2.3.1 A função $\tau(n)$: número de divisores positivos de n

Seja $n \in \mathbb{N}$, temos que n pode ser escrito como $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_k^{\alpha_k}$ com p_i números primos distintos $\forall i \ 1 \leq i \leq k$. Usando o princípio fundamental da contagem podemos definir a função $\tau(n)$, como segue:

Definição 2.6 *A função $\tau(n)$ é dada pela aplicação:*

$$\begin{aligned} f : \mathbb{N} &\to \mathbb{R} \\ n &\mapsto \tau(n) = (\alpha_1 + 1) \cdot (\alpha_2 + 1) \cdot ... \cdot (\alpha_k + 1) \end{aligned}$$

Exemplo 2.4 *Determine o número de divisores positivos de $2^6 \cdot 3^4 \cdot 5^8 \cdot 13^2 \cdot 17$. Quantos desses divisores são ímpares?*

Solução: *o número de divisores é dado por: $\tau(2^6 \cdot 3^4 \cdot 5^8 \cdot 13^2 \cdot 17) = 7 \cdot 5 \cdot 9 \cdot 3 \cdot 2 = 1890$. Como os números ímpares não são divisíveis por 2, o número de divisores ímpares de $2^6 \cdot 3^4 \cdot 5^8 \cdot 13^2 \cdot 17$ é dado por $\tau(3^4 \cdot 5^8 \cdot 13^2 \cdot 17) = 5 \cdot 9 \cdot 3 \cdot 2 = 270$.*

2.3.2 A função $\sigma(n)$: soma dos divisores positivos de n

Seja $n \in \mathbb{N}$, decomposto em fatores primos, sob a forma: $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_k^{\alpha_k}$, por meio da fórmula da soma dos termos de uma PG não é tão difícil deduzir o resultado apresentado na definição da função $\sigma(n)$ que segue:

Teorema 2.5 *A função $\sigma(n)$ é dada pela seguinte lei*

$$\begin{aligned} f : \mathbb{N} &\to \mathbb{R} \\ n &\mapsto \sigma(n) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot ... \cdot \frac{p_k^{\alpha_k+1} - 1}{p_k - 1} \end{aligned}$$

Demonstração: Seja $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_k^{\alpha_k}$. Note que o produto

$$(1 + p_1 + p_1^2 + ... + p_1^{\alpha_1}) \cdot (1 + p_2 + p_2^2 + ... + p_2^{\alpha_2}) \cdot ... \cdot (1 + p_k + p_k^2 + ... + p_k^{\alpha_k})$$

é igual a soma dos divisores positivos de n. Para visualizar isso, basta checar a expansão desse produto, onde cada divisor positivo de n aparece uma única vez. Perceba também que para cada α_i, $(1 + p_i + p_i^2 + ... + p_i^{\alpha_i})$ representa a soma dos $\alpha_i + 1$ primeiros termos de uma progressão geométrica de primeiro termo $a_1 = 1$ e razão $q = p_i$. Sendo assim,

$$1 + p_i + p_i^2 + ... + p_i^{\alpha_i} = \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}$$

E daí concluímos que

$$\sigma(n) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot ... \cdot \frac{p_k^{\alpha_k+1} - 1}{p_k - 1}$$

. ■

Exemplo 2.5 *a soma dos divisores de* $3^4 \cdot 5^8 \cdot 13^2$ *é dada por*

$$\sigma(3^4 \cdot 5^8 \cdot 13^2) = \frac{3^5 - 1}{3 - 1} \cdot \frac{5^9 - 1}{5 - 1} \cdot ... \cdot \frac{13^3 - 1}{13 - 1} = 121 \cdot 488281 \cdot 183 = 10812006183$$

2.3.3 A função $\pi(n)$: número de primos menores ou iguais a n

A frequência de números primos menores ou iguais a n é dada por $\pi(n)$, ou seja selecionando ao acaso um número $p \leq n$, a probabilidade de p ser um número primo é dada por $\frac{\pi(n)}{n}$.

Como podemos ver em [11], não é simples determinar valores $\pi(n)$, visando facilitar, Legendre e Gauss, analisando tabelas, chegaram a conclusão que esse quociente se aproxima de $\frac{1}{\ln n}$. Esse fato veio a ser provado por volta de 1900, quando J. Hadamard e Ch. de la Valléc-Poussin, independentemente, provaram o profundo teorema dos números primos, cujo enunciado é:

$$\lim_{n\to\infty} \frac{\pi(n)}{n} \cdot \frac{1}{\ln x}^{-1} = 1$$

Uma fórmula para $\pi(n)$ dada por Willians em 1964 é a que que segue:

Para todo $k \in \mathbb{N}$, Seja

$$F(k) = \left[\cos^2 \pi \frac{(k-1)! + 1}{k}\right]$$

Donde $[x]$ é o maior inteiro menor ou igual a x.

Então, para $k > 1$, $F(k) = 1$ quando k é primo e caso contrário $F(k) = 0$, além disso, $F(1) = 1$.(isso é garantido pelo teorema de Wilson)

Disso resulta que

$$\pi(n) = -1 + \sum_{k=1}^{n} F(k)$$

Observação 2.5 *Willians também expressou* $\pi(n)$ *de modo semelhante usando o seno, mas não apresentarei aqui, pois, o trabalho das duas fórmulas é equivalente.*

Mináč, estabeleceu outra fórmula, que foi publicada pela primeira vez em [11], na qual não existem valores de cossenos e senos, como segue:

$$\pi(n) = \sum_{k=2}^{n} \left[\frac{(k-1)! + 1}{k} - \left[\frac{(k-1)!}{k} \right] \right]$$

A demonstração é simples, e pode ser encontrada em [11].

O autor afirma que disso, obtém-se a fórmula de Willans para o enésimo número primo, a dedução pode ser encontrada em [8]. A fórmula é a que segue:

$$p_n = 1 + \sum_{m=1}^{2^n} \left[\left(\frac{n}{\sum_{k=1}^{m} F(k)} \right)^{\frac{1}{n}} \right]$$

A mesma tem aplicação muito difícil e se torna inviável quando tratamos de números grandes.

2.3.4 A função $\phi(n)$: função ϕ de Euler

Trata-se do número de elementos de um sistema reduzido de resíduos módulo $n > 1$, em outras palavras, trata-se da quantidade de números naturais entre 0 e $n-1$, que são primos com n. Com isso, tomando $\phi(1) = 1$, e unindo a Definição 2.4 ao Teorema 2.4 podemos enunciar a seguinte função:

$$\phi : \mathbb{N} \to \mathbb{N}$$

E ainda, Seja $n \in \mathbb{N}$, decomposto em fatores primos, sob a forma: $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_k^{\alpha_k}$, pelo teorema 2.4 temos que:

$$\phi(n) = p_1^{\alpha_1 - 1} \cdot ... \cdot p_k^{\alpha_k - 1} \cdot (p_1 - 1) \cdot ... \cdot (p_k - 1)$$

.

Essa função é de grande utilidade no sistema de criptografia RSA. Vejamos sua aplicabilidade no capítulo seguinte.

Capítulo 3

Criptografia

3.1 Introdução

"Essas mensagens estão criptografadas de ponta a ponta", essa é a mensagem que vemos em nosso WhatsApp quando vamos enviar uma mensagem para alguém pela primeira vez. Mas, o que significa isso? Bem, significa que só quem saberá do que se trata a mensagem é quem está enviando e quem está recebendo, pois caso um terceiro intercepte a mensagem, não saberá do que se trata, pois a mesma se encontrará embaralhada de modo que o processo para desembaralhar sem a chave de embaralhamento torna-se praticamente impossível.

Em resumo, a criptografia é responsável pelo estudo e aplicação de técnicas que possibilitam a codificação e decodificação de mensagens, tornando o processo de troca de informações seguro, evitando fraudes. Noutras palavras, a criptografia define uma chave de entrada na qual as mensagens e dados a serem transitados são embaralhados e uma chave de saída que desembaralha os dados quando recebidos, de modo que só quem tem acesso a chave de entrada é quem está enviando a mensagem e quem tem acesso a chave de saída é quem está recebendo.

Um dos primeiros modelos de criptografia conhecido é denominado Cifras de César, o mesmo se baseia na seguinte correspondência:

Entrada	A	B	C	D	E	...	X	Y	Z
$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	...	$\updownarrow$	$\updownarrow$	$\updownarrow$
Saída	D	E	F	G	H	...	A	B	C

Onde a chave de entrada transforma A em D, B em C, C em F e assim sucessivamente. Já a chave de saída faz o inverso disso, ou seja D em A, E em B e assim sucessivamente.

Nesse sistema a palavra AMOR seria codificada da seguinte forma DPRU e a mensagem PRWR decodificada é MOTO.

Esse tipo de sistema de criptografia é chamado de cifra de substituição simples, onde as letras de um alfabeto são substituídas por outras. O código de César possui pelo menos 25 variantes, que corresponde a iniciar a segunda linha da chave de codificação com qualquer letra diferente de A. Note que a segurança desse sistema não é de qualidade, pois poderíamos decodificar facilmente uma mensagem usando a frequência das letras que mais se repetem. O problema de criar um modelo de criptografia seguro foi muito estudado durante um longo período. Ao longo do tempo surgiram outros métodos, como o de Bellaso que teve sua chave considerada inquebrável por mais de 300 anos, tendo sido quebrada em meados do século XIX, pelo inglês Charles Babbage e pelo polonês Friedrich Kasiski, independentemente. Os detalhes dessa história podem ser encontrados em [13].

Além do processo de troca de mensagens, surgiu o problema de transporte e troca de chaves de decodificação de maneira segura, para que o único destinatário da mensagem seja o único a decodificar a mesma.

No decorrer do processo, chegamos ao advento das máquinas, onde máquinas famosas como a japonesa Purple e a alemã Enigma perduraram por um bom tempo. Uma bela história a ser retratada é a de Alan Turing, o matemático responsável pela quebra das chaves da Enigma que auxiliou ao fim da segunda guerra mundial. Não descreverei aqui os detalhes dessa história espetacular, no entanto recomendo o filme "O jogo da Imitação", que apresenta muito bem essa história.

Todos os sistemas citados até aqui são simétricos, ou seja, a mesma chave é usada para cifrar e decifrar uma mensagem. Por muito tempo pairou sobre a comunidade dos criptologistas o paradigma da impossibilidade da troca de senhas sem a intermediação de um portador. Coube aos norte americanos, Whitfield Driffie, Martin Hellman e Ralph Merkle quebrar esse paradigma trazendo para o campo da criptografia a teoria dos números por meio da noção de congruências. O sistema criado por eles denominado DHM em homenagem aos criadores é bastante engenhoso e foi o primeiro passo na busca para a solução do problema da troca de chaves de modo seguro sem a necessidade de um intermediário. O defeito do sistema é a serventia apenas para a troca de chaves entre dois indivíduos. No entanto, ele serviu de inspiração para o desenvolvimento de sistemas com chaves assimétricas. Na criptografia assimétrica, existem duas chaves, a chave pública e a chave privada. Para cifrar uma mensagem para alguém, precisa-se ter a chave pública, de conhecimento geral, e utilizar esta chave para cifrar a mensagem; o receptor decifra a mensagem secretamente. (A descrição do sistema DHM pode ser encontrada no capítulo 13 do livro [7] de maneira simples por meio de uma troca de mensagens entre "João e Maria").

Hoje em dia o sistema de criptografia mais utilizado é o RSA, o qual vemos detalhadamente neste capítulo.

O sistema RSA é um dos mais seguros atualmente, sendo utilizado nas principais trocas de mensagens de teor privado e/ou sigiloso. Diante de uma sociedade onde

a quantidade de conteúdo é aumentada exponencialmente e grande parte deste conteúdo é sigiloso, como mensagens pessoais, senha de contas bancárias e cartões de crédito, torna-se essencial proteger esse sistema de troca. Com isso, é de suma importância buscar aprimorar o mesmo cada vez mais e estudar técnicas de criação de chaves cada vez mais eficazes.

Para poder implementar o RSA precisamos de dois números primos que vamos chamar de p e q. Para codificar uma mensagem é suficiente saber do produto entre $n = p \cdot q$. Para decodificar a mensagem precisamos conhecer os primos p e q. Cada usuário no método tem sua própria chave de codificação. A chave n é pública, ou seja, todos podem ter conhecimento dela. Já a chave de decodificação constituída por p e q é secreta, logo, deve ser mantida em sigilo por cada usuário ou a segurança do sistema estará comprometida.

Note que o processo de decodificação do RSA é teoricamente simples, pois basta fatorar $n = p \cdot q$ e teremos a chave de decodificação, de fato, na teoria é simples, mas quando usamos números primos muito grandes essa fatoração pode levar alguns milhares de anos, devido aos métodos que dispomos atualmente para fazer isso não serem tão eficazes. Vide [2].

Ora, mas se fatorar é tão difícil, como podemos encontrar primos tão grandes? A resposta é que existem métodos para determinar se um número é primo ou composto sem tentar fatorá-lo. Como exemplo podemos citar os Primos de Mersene que foram estudados no decorrer desse trabalho, sendo que o maior descoberto é $2^{82589933} - 1$ que tem quase 25 milhões de dígitos. Já o número $2^{2^{14}} + 1$ é composto e nenhum de seus fatores é conhecido.

Fazemos a seguir a apresentação de um sistema simétrico de Criptografia estudando um modelo com função afim, e após isso, estudamos o sistema assimétrico RSA em duas de suas variações, com o passo a passo de seu desenvolvimento e exemplos. Também comentamos algumas estratégias que devem ser utilizadas para garantir a segurança do RSA, pois não trata-se apenas de encontrar dois primos grandes, mas sim encontrar dois primos grandes de modo estratégico para tornar os algoritmos de fatoração que dispomos atualmente inúteis.

3.2 Um sistema de criptografia simétrico com Função Afim

Nesta seção, estudamos o desenvolvimento de um sistema simétrico simples de criptografia que faz o uso de Função Afim. Por ser simples e interessante, esse sistema pode render uma excelente prática em sala de aula para o ensino médio, como podemos ver no capítulo 4.

Pré codificação

Inicialmente definimos um alfabeto de S símbolos e fazemos uma correspondência biunívoca entre os símbolos deste alfabeto e os números inteiros do intervalo $[0, S-1]$.

Exemplo 3.1 *Como exemplo prático, se tomarmos nosso alfabeto usual de 26 letras, podemos fazer a seguinte correspondência:*

Entrada	A	B	C	D	E	...	X	Y	Z
$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	...	$\updownarrow$	$\updownarrow$	$\updownarrow$
Saída	0	1	2	3	4	...	23	24	25

O motivo da correspondência ser feita com os números do intervalo $[0, S-1]$ é tornar possível o uso da aritmética dos restos no processo de codificação , como veremos mais a frente. Note ainda que para que isso seja possível poderíamos ter tomado qualquer sistema completo de resíduos módulo S para fazer a correspondência no lugar do intervalo $[0, S-1]$.

O próximo passo é a escolha de uma Função Afim dada por $f(x) = ax + b$ com $a, b \in \mathbb{Z}$ e $\text{mdc}(a, S) = 1$ onde S é o número de símbolos do alfabeto. Como queremos usar congruência módulo S, justifica-se $\text{mdc}(a, S) = 1$, pois caso contrário não existiria inverso de a módulo S (vide capítulo 2), o que é essencial para o processo de decodificação como veremos adiante.

Exemplo 3.2 *Adotando o alfabeto do Exemplo* 3.1 *poderíamos escolher* $f(x) = 3x+7$ *Essa função é a função de codificação, ou simplesmente "chave de codificação".*

Codificando uma mensagem

O processo de codificação de uma mensagem é bem simples. Basta aplicar a função de codificação e usar congruência módulo S para transformar letra em letra.

Exemplo 3.3 *Adotando a função* $f(x) = 3x + 7$ *do Exemplo 3.2 e o alfabeto do Exemplo 3.1 codifique a mensagem "EU SOU O MILIOR".*

Solução: *Associando as letras da frase aos números temos:*

EU	SOU	O	$MILIOR$
$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$
$(4-20)$	$(18-14-20)$	(14)	$(12-8-11-8-14-17)$

Codificamos letra a letra da seguinte forma:

1 Para codificar a letra E=4 fazemos $f(E) = f(4) = 3 \cdot 4 + 7 = 19$ *e* $19 \equiv 19$ *mod 26, como* $19 = T$ *temos que* $E \leftrightarrow T$.

2 Para codificar a letra U=20 fazemos $f(U) = f(20) = 3 \cdot 20 + 7 = 67$ *e* $67 \equiv 15$ *mod 26, como* $15 = P$ *temos que* $U \leftrightarrow P$.

Dos itens 1 e 2 obtemos $EU \leftrightarrow TP$

Seguindo O processo para as demais letras obtemos:

$$EU\ SOU\ O\ MILIOR \leftrightarrow TP\ JXP\ X\ RFOFXG$$

Logo a mensagem codificada é: TP JXP X RFOFXG.

Observação 3.1 *Perceba que podemos tomar infinitas funções de codificação e o processo não vai passar de uma correspondência com uma permutação do alfabeto. Isso se garante pela Proposição 2.4. Usando a chave* $f(x) = 3x + 7$ *para codificar todo o alfabeto do Exemplo 3.1 teremos: H,K,N,Q,T,W,Z,C,F,I,L,O,R,U,X,A,D,G,J,M,P,S,V,Y,B,E como resultado do alfabeto codificado. Isso é interessante pois independente da função tomada (que são infinitas), o Princípio Fundamental da Contagem nos garante que para um alfabeto de* S *símbolos o número de chaves de codificação distintas possíveis é* $S!$.

Decodificando uma mensagem

O processo de decodificação também é simples. Definida a função de codificação $f(x) = ax + b$ basta encontrar a inversa dada por $f^{-1}(x) = a'x + b'$ onde $a \cdot a' \equiv 1 \mod S$ (a' é o inverso de a mod S) e $b' = -a' \cdot b$. Deste modo $f^{-1}(ax + b) = a' \cdot (ax + b) - a' \cdot b = a' \cdot a \cdot x \equiv x \mod S$. Note que $f^{-1}(x)$ sempre existe, uma vez que na pré codificação era exigido que $\text{mdc}(a, S) = 1$. Encontrada $f^{-1}(x)$ o processo de decodificação torna-se semelhante ao de codificação. Veja o Exemplo 3.4

Exemplo 3.4 *Decodifique a mensagem codificada no Exemplo 3.3*

Solução: *Sabendo que* $f(x) = 3x + 7$ *inicialmente devemos encontrar* a' *tal que* $3 \cdot a' \equiv 1$ *mod* 26*, isso equivale a resolver a equação:* $3a' + 26k = 1$*, a qual tem solução garantida pelo Teorema 1.3, seguindo o passo a passo do Exemplo 1.6 temos:*

$$26 = 8 \cdot 3 + 2$$
$$3 = 2 \cdot 1 + 1$$

e consequentemente:

$$1 = 3 - 2 = 3 - 26 + 8 \cdot 3 = 3 \cdot 9 + 26 \cdot (-1).$$

Logo $a' = 9$. *E consequentemente*

$$f^{-1}(x) = 9x - 9 \cdot 7 = 9x - 63$$

Como $-63 \equiv 15$ *mod* 26, *podemos reescrever a inversa como*

$$f^{-1}(x) = 9x + 15$$

Agora, iniciamos a decodificação da mensagem TP JXP X RFOFXG da seguinte forma:

1 Como T=19, fazemos $f^{-1}(T) = f^{-1}(19) = 9 \cdot 19 + 15 = 186$ *e* $186 \equiv 4$ *mod* 26, *como 4=E, temos que* $T \leftrightarrow E$.

2 Como P=15, fazemos $f^{-1}(T) = f^{-1}(15) = 9 \cdot 15 + 15 = 150$ *e* $150 \equiv 20$ *mod* 26, *como 20=U, temos que* $P \leftrightarrow U$.

Dos itens 1 e 2 obtemos

$$TP \leftrightarrow EU$$

Seguindo o processo para as demais letras obtemos:

$$TPJXPXRFOFXG \leftrightarrow EUSOUOMILIOR$$

E temos como mensagem decodificada: "EU SOU O MILIOR".

3.3 O RSA

O método apresentado a seguir pode ser encontrado no livro de Coutinho [2] sendo possível a verificação de sua validade no mesmo.

Pré-codificação

Inicialmente devemos definir o alfabeto a ser utilizado em nosso sistema e fazer cada elemento de nosso alfabeto corresponder a um número. É de fundamental importância ser estrategista nesse momento e buscar evitar ambiguidades. Se o nosso alfabeto tiver menos de 10 caracteres podemos associá-lo aos números 0,1,2,...9. Se tiver até 90 caracteres podemos associar cada elemento a um número de dois dígitos. Se tiver até 900 caracteres podemos associar cada elemento a um número de 3 dígitos e assim sucessivamente. Note que se fosse usada uma correspondência com quantidade de dígitos diferentes podemos gerar ambiguidades do tipo: Na correspondência $A \leftrightarrow 1, B \leftrightarrow 2, C \leftrightarrow 3, ...Z \leftrightarrow 26$ A palavra 191512 Pode ser interpretada como AIAEAB interpretando $A \leftrightarrow 1, I \leftrightarrow 9, E \leftrightarrow 5, B \leftrightarrow 2$ como

SAEL se $S \leftrightarrow 19, A \leftrightarrow 1, E \leftrightarrow 5, L \leftrightarrow 12$, como SOL se $S \leftrightarrow 19, O \leftrightarrow 15, L \leftrightarrow 12$, e assim por diante. Com isso percebemos a importância de deixar bem definido o alfabeto e tornar a correspondência dos caracteres com os números não ambígua.

Vamos definir nosso alfabeto como sendo 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 e façamos a seguinte correspondência:

$A \leftrightarrow 11, B \leftrightarrow 13, C \leftrightarrow 15, D \leftrightarrow 17, E \leftrightarrow 22, F \leftrightarrow 33, G \leftrightarrow 70, H \leftrightarrow 71, I \leftrightarrow 72, J \leftrightarrow 73, K \leftrightarrow 74, L \leftrightarrow 75, M \leftrightarrow 41, N \leftrightarrow 57, O \leftrightarrow 58, P \leftrightarrow 67, Q \leftrightarrow 65, R \leftrightarrow 28, S \leftrightarrow 42, T \leftrightarrow 43, U \leftrightarrow 44, V \leftrightarrow 45, W \leftrightarrow 47, X \leftrightarrow 88, Y \leftrightarrow 83, Z \leftrightarrow 37$

O espaço entre duas palavras será substituído por 99.

Vamos usar como exemplo a frase *"ESSE CARA SOU EU"* que convertida em números torna-se:

$$22424222991511281199425844992244$$

Agora vamos definir os parâmetros do sistema RSA, ou seja, vamos definir os dois primos p e q e tomemos $n = p \cdot q$ como exemplo, tomemos $p = 17$ e $q = 19$, daí $n = 323$.

A última fase do processo é a quebra do número produzido na mensagem em blocos com a condição de que esses blocos devem ser números menores que n. Essa quebra também deve ser estratégica, a primeira coisa que devemos ter cuidado é para que nenhum bloco comece por 0, pois isso traria problemas na hora de decodificar (como vemos mais a frente). Também é interessante fazer com que os blocos não correspondam a nenhuma unidade linguística, pois isso torna a decodificação por contagem de frequência essencialmente impossível. Seguindo essas instruções podemos quebrar o número do exemplo acima nos seguintes blocos:

$$2 - 242 - 4 - 222 - 9 - 91 - 51 - 128 - 119 - 94 - 25 - 84 - 49 - 92 - 244$$

Vale ressaltar que a maneira de escolher os blocos não é única, no entanto devemos sempre tomar os cuidados citados anteriormente para tornar sistema seguro. Com isso encerramos as etapas de pré-codificação do sistema RSA.

Codificando

Para o processo de codificação precisamos do valor de $n = p \cdot q$ (produto dos primos escolhidos) e um número inteiro α tal que $\text{mdc}(\alpha, \phi(n)) = 1$, pois queremos que α seja inversível módulo $\phi(n)$. Chamamos o par (n, α) de chave de codificação, note que para um mesmo n escolhido podemos criar mais de uma chave de codificação, pois α não é único. Note ainda que é fácil encontrar um α,

pois como α depende de $\phi(n)$, pelo que estudamos sobre a função $\phi(n)$ no Teorema 2.4 e na subseção 2.3.4 sabemos que conhecidos os valores de p e q torna-se muito fácil encontrar o valor de $\phi(n = p \cdot q)$ que é dado por $\phi(n) = (p-1) \cdot (q-1)$. Por isso p e q devem ser mantidos em segredo e o sucesso desse sistema depende disso.

Vejamos na prática como funciona a codificação. Para isso, sigamos o exemplo usado na pré codificação, cujos blocos gerados foram:

$$2 - 242 - 4 - 222 - 9 - 91 - 51 - 128 - 119 - 94 - 25 - 84 - 49 - 92 - 244$$

Com $n = 323$, $p = 17$, $q = 19$ e consequentemente $\phi(n) = 17 \cdot 18 = 288$, daí podemos escolher $\alpha = 5$ pois $\text{mdc}(5, 288) = 1$.

Devemos codificar os blocos separadamente e o resultado da codificação de cada bloco deve permanecer separado, visando tornar viável o processo de decodificação. Mas como é o processo de codificação?

Bem, denotando por $C(b)$ um bloco codificado, a receita para chegar a $C(b)$ é $C(b) =$ Resto da divisão de b^α por n (onde b é o bloco a ser codificado), noutras palavras,

$$b^\alpha \equiv C(b) \text{ mod } n \text{ com } C(b) = \text{Mín } \mathbb{N} \text{ que satisfaz a congruência.}$$

Assim, o bloco 2 da mensagem anterior é codificado como o resto da divisão de 2^5 por 323. Como $32 = 2^5 \equiv 32 \text{ mod} 323$, concluímos que $C(2) = 32$. Fazendo as contas para os demais blocos temos:

C(242)=276	C(4)=55	C(222)=52	C(9)=263	C(91)=211
C(51)=204	C(128)=314	C(119)=85	C(94)=246	C(25)=43
C(84)=50	C(49)=121	C(92)=232	C(244)=194	

Logo a mensagem codificada é dada por:

$$32 - 276 - 55 - 52 - 263 - 211 - 204 - 314 - 85 - 246 - 43 - 50 - 121 - 232 - 194$$

e assim, finalizamos a etapa de codificação.

Decodificando

O segredo do sistema RSA está na decodificação, pois a mesma só pode ser feita por quem tem conhecimento dos primos p e q escolhidos. Mesmo conhecendo a chave de codificação e sabendo codificar, não saber os valores de p e q faz com que o processo de decodificação seja praticamente impossível. Por isso, o RSA é dito um sistema de chave pública (Todos podem tem acesso a chave de codificação). Mas como decodificar uma mensagem?

Anteriormente usando $n = 323$, $\alpha = 5$ e $\phi(323) = 288$ chegamos a seguinte mensagem codificada

$$32 - 276 - 55 - 52 - 263 - 211 - 204 - 314 - 85 - 246 - 43 - 50 - 121 - 232 - 194$$

Para decodificar a mensagem precisamos de duas informações, a primeira é $n = p \cdot q$ e a segunda é o inverso de α módulo $\phi(n)$ ao qual denominaremos α'. O par (n, α') é a chave de decodificação. Definindo $D(x)$ como sendo um bloco decodificado, a receita para calcular $D(x)$ é dada por $D(x) =$ resto da divisão de $x^{\alpha'}$ por n(onde x é um bloco codificado), ou de modo equivalente:

$$x^{\alpha'} \equiv D(x) \bmod n, \text{ com } D(x) = \text{mín } \mathbb{N} \text{ que satisfaz a congruência.}$$

Iniciamos o processo calculando o inverso de α módulo $\phi(n)$ resolvendo a congruência $5 \cdot \alpha' \equiv 1 \bmod 288$, isso equivale a $5 \cdot \alpha' - 1 = 288w$ que pode ser reescrito como $5 \cdot \alpha' - 288 \cdot w = 1$, aplicando o Algoritmo Euclidiano temos:

$$288 = 5 \cdot 57 + 3$$
$$5 = 1 \cdot 3 + 2$$
$$3 = 1 \cdot 2 + 1$$

E consequentemente,

$$1 = 3 - 2 = 3 - (5 - 3) = 3 - 5 + 3 = 2 \cdot 3 - 5 = 2(288 - 5 \cdot 57) - 5 = 2 \cdot 288 - 115 \cdot 5$$

Daí $\alpha' = -115 + 288t$ com $t \in \mathbb{Z}$ e com $t = 1$ podemos tomar $\alpha' = 173$.

Agora, aplicando a receita no bloco $x = 32$, temos que encontrar o resto da divisão de 32^{173} por 323, o que pode ser resolvendo a congruência $32^{173} \equiv b \bmod 323$, para isso, basta utilizar as propriedades de congruência, no entanto, fazer isso manualmente é desgastante, por isso é de fundamental importância o uso de uma calculadora algébrica. Para isso usaremos a WolframAlpha que pode ser acessada em www.wolframalpha.com, nela para resolver essa equação basta digitar "32^{173} mod 323"e veremos que o resto que queremos é 2, logo $D(32) = 2$. Repetindo o processo para os demais blocos temos:

D(276)=242	D(55)=4	D(52)=222	D(263)=9	D(211)=91
D(204)=51	D(314)=128	D(85)=119	D(246)=94	D(43)=25
D(50)=84	D(121)=49	D(232)=92	D(194)=244	

E daí a lista de blocos decodificados é dada por:

$$2 - 242 - 4 - 222 - 9 - 91 - 51 - 128 - 119 - 94 - 25 - 84 - 49 - 92 - 244$$

Agora juntando esses blocos formamos o número

$$22424222991511281199425844992244$$

Como na pré codificação cada letra tinha dois dígitos, basta associar o resultado ao alfabeto definido 22-E, 42-S, 99-espaço, 15-C,... chegando a frase "ESSE CARA SOU EU".

3.4 Variação do RSA (codificando palavras em palavras)

Essa variação é encontrada em [8]. O processo é semelhante, inicialmente escolhemos dois primos p e q extremamente grandes e definimos $n = p \cdot q$, calculamos $\phi(n) = (p-1)\cdot(q-1) = n+1-p-q$, escolhemos $1 < \alpha < \phi(n)$ tal que $\text{mdc}(\alpha, \phi(n))=1$ e calculamos o inverso multiplicativo de α módulo $\phi(n)$ resolvendo a congruência $\alpha \cdot \alpha' \equiv 1 \bmod n$. A chave de codificação é (n, α) e a chave de decodificação é (n, α')

Codificação

A receita de codificação para um bloco b é dada por $C(b) \equiv b^{\alpha} \bmod n$, onde $C(b)$ é o resultado do bloco b codificado. A mudança dessa variação com relação a anterior na receita de codificação é que nessa os blocos gerados na pré codificação devem ter a mesma quantidade de caracteres, ou seja, quebramos a mensagem original em blocos de 2, ou 3 ou 4... dígitos uniformemente.

Decodificação

A receita decifradora de um bloco codificado $C(b) = x$ é dada por $D(x) \equiv x^{\alpha'} \bmod n$. Ora, mas até aqui o processo é essencialmente o mesmo se comparado com o descrito anteriormente. O que muda de fato? A mudança é que nessa variação deseja-se codificar uma palavra em um bloco de letras, e não de números, para isso a mudança se dá pelo uso das bases numéricas e a aritmética dos restos implementada a associação de um alfabeto bem organizado no processo de pré codificação.

Pré codificação

Devemos ter um mínimo de organização na escolha do alfabeto, para que assim torne-se viável a associação de números a letras por meio da aritmética dos restos. Se estamos trabalhando com um alfabeto de S símbolos, fazemos uma correspondência biunívoca entre os símbolos do alfabeto e os inteiros do intervalo $[0, S-1]$. Depois disso, dividimos o texto que queremos cifrar (já associado aos números) em blocos de k dígitos e escolhemos a quantidade m de dígitos que os blocos codificados devem ter (ou seja, no processo serão transformados blocos de k dígitos em blocos de m dígitos). Para que não ocorram falhas devemos escolher k e m de modo que $S^k < n < S^m$ se $k < m$ ou $S^m < n < S^k$ caso $m < k$, pois com isso qualquer unidade de texto simples corresponde a um elemento em $\mathbb{Z}_n$ e a unidade codificada $C(b) \equiv b^{\alpha} \bmod n$ que também é um elemento de $\mathbb{Z}_n$ pode ser escrita como um bloco de m letras.

Exemplo 3.5 *Tomemos* $L = 26, k = 3$ *e* $m = 4$*, ou seja, o texto original deve ser dividido em blocos de* 3 *caracteres o texto cifrado em blocos de 4 caracteres. No alfabeto usual, façamos a seguinte associação:*

$$\begin{array}{ccccccccccc} A & B & C & ... & K & L & ... & X & Y & Z \\ \updownarrow & \updownarrow & \updownarrow & ... & \updownarrow & \updownarrow & ... & \updownarrow & \updownarrow & \updownarrow \\ 0 & 1 & 2 & ... & 10 & 11 & ... & 23 & 24 & 25 \end{array}$$

Para enviarmos a mensagem sol, para o usuário A com a chave de codificação: $(n_A, \alpha_A) = (46927, 39423)$ *gerada pelos primos* $p = 167$ *e* $q = 281$*, primeiro determinamos a equivalência numérica:*

$$SOL \leftrightarrow 18 \cdot 26^2 + 14 \cdot 26 + 11 = 12543$$

E então calculamos

$$C(b) \equiv 12543^{39423} \ mod\ 46927$$

Que é $24599 = 1 \cdot 26^3 + 10 \cdot 26^2 + 10 \cdot 26 + 3$ *que equivale a mensagem codificada BKKC.*

O destinatário conhece a chave de decodificação $(46927, 26767)$ *e portanto calcula:*

$$D(x) \equiv 24599^{26767} \ mod\ 46927$$

Que é $12543 = 18 \cdot 26^2 + 14 \cdot 26 + 11$ *e portanto recupera a mensagem SOL.*

Exemplo 3.6 *Usando os mesmos dados do exemplo anterior, vamos analisar como seria o processo para a mensagem "FLAMENGOL".*

Inicialmente dividimos a mensagem em blocos de 3 letras e associamos aos números do alfabeto obtendo:

$$FLA(5\text{-}11\text{-}0 \leftrightarrow 5 \cdot 26^2 + 11 \cdot 26 + 0)$$
$$MEN(12\text{-}4\text{-}13 \leftrightarrow 12 \cdot 26^2 + 4 \cdot 26 + 3)$$
$$GOL(6\text{-}14\text{-}11 \leftrightarrow 6 \cdot 26^2 + 14 \cdot 26 + 11)$$

Ou seja $FLA \leftrightarrow 3666$*,* $MEN \leftrightarrow 8219$ *e* $GOL \leftrightarrow 4431$*.*

Daí calculamos:

1. $C(3666) \equiv 3666^{39423}$ *mod* 46927 *o que resulta em* $C(3666) = 13754 = 0 \cdot 26^3 + 20 \cdot 26^2 + 9 \cdot 26 + 0$ *que equivale a palavra AUJA.*

2. $C(8219) \equiv 8219^{39423}$ *mod* $46927 = 3606 = 0 \cdot 26^3 + 5 \cdot 26^2 + 8 \cdot 26 + 15$ *o que nos dá a palavra AFIP.*

3. $C(4431) \equiv 4431^{39423}$ *mod* $46927 = 15589 = 0 \cdot 26^3 + 23 \cdot 26^2 + 1 \cdot 26 + 15$ *o que gera a palavra AXBP.*

Agora, unindo 1,2 e 3 obtemos a mensagem codificada:

$$FLAMENGOL \leftrightarrow AUJAAFIPAXBP$$

Para decodificar aplicamos a chave $(46927, 26767)$ *e calculamos:*

1. $D(13754) \equiv 13754^{26767}$ *mod* 46927 *o que resulta em* $D(13754) = 3666 = 5 \cdot 26^2 + 11 \cdot 26 + 0 \cdot 26 + 0$ *que equivale a palavra FLA.*

2. $D(3603) \equiv 3603^{26767}$ *mod* $46927 = 8219 = 12 \cdot 26^2 + 4 \cdot 26 + 3$ *o que nos dá a palavra MEN.*

3. $D(15589) \equiv 15589^{26767}$ *mod* 46927 *o que resulta em* $D(15589) = 4431 = 6 \cdot 26^2 + 14 \cdot 26 + 11 \cdot 26 + 0$ *que equivale a palavra GOL.*

E com isso obtemos a mensagem decifrada FLAMENGOL.

3.5 Comentários acerca das duas variações do RSA

Note que em ambos os sistemas apresentados aqui a segurança é equivalente quando tomados dois números primos extremamente grandes. Poderíamos pensar que no segundo método a mensagem poderia ser quebrada por frequência, mas perceba que se a variação do tamanho dos blocos for utilizada de maneira estratégica torna-se inviável a análise por frequência.

Outro fato é que mesmo sendo extremamente grandes, se os números primos não forem escolhidos de maneira estratégica, o sistema pode se tornar fraco. Pois se os números p, q forem escolhidos de modo que p ou q estejam próximos de $\sqrt{n} = \sqrt{p \cdot q}$, a chave pode ser quebrada utilizando uma calculadora algébrica avançada atrelada ao método de fatoração de Fermat visto no capítulo 1.

Capítulo 4

Sugestões de atividades para sala de aula

4.1 Criando um modelo de Criptografia Simples

Público: Alunos da 1ª série do ensino médio

Material: Lápis, borracha, folhas de papel, celulares, tablets, computadores e projetor multimídia.

Tempo previsto: Quatro horas aulas.

Objetivos

1. Compreender o conceito de função por meio da noção de chaves de entradas e saídas de modelos de criptografia;
2. Fazer o uso de critérios de divisibilidade para definição de primalidade de um número;
3. Mostrar a importância da matemática e sua aplicação em meios tecnológicos e sistemas de segurança;
4. Ampliar o conhecimento histórico sobre a segunda guerra, analisando a importância de Alan Turing para o fim da mesma.
5. Instigar a autonomia e o autodidatismo;
6. Estimular a pesquisa científica.

Pré-requisitos: Noções iniciais do conceito de função, relação, função inversa e relação inversa.

Desenvolvimento da atividade

Inicialmente o professor deve expor o conceito de criptografia e o seu contexto histórico, apresentando os primeiros modelos de criptografia e a sua relação com a ideia de relações e funções por meio das chaves de entrada e relações e funções inversas por meio das chaves de saída.

Em seguida, o professor deve resgatar a disciplina de história de modo interdisciplinar (como propõe o novo ensino médio) e comentar a parte "desconhecida"da segunda guerra mundial onde Alan Turing e sua equipe tiveram um papel importante para quebrar os segredos da Enigma e de maneira estratégica prever os movimentos dos Nazistas, ajudando a por fim na guerra.

Após isso, o professor pode comentar as fragilidades do sistema de Júlio César (cifras de César, vide seção 3.1), e sugerir como atividade para os alunos a criação de um modelo aprimorado baseado na cifra de césar corrigindo algumas de suas fragilidades. É importante que nesse momento os alunos tenham em mente a importância de apresentar de forma clara e objetiva as chaves de entrada e saída do modelo criado, para isso, deve-se solicitar a criação de uma mensagem codificada com esse modelo, à qual deve ser decodificada por um colega.

Perguntas a serem feitas: Quanto mais demorado o processo de decodificação, melhor o modelo? Como reduzir os padrões nas palavras do modelo? É possível fazer a troca de chaves sem contato presencial de modo seguro? É possível converter esse modelo para o sistema binário?

Divisão do tempo

Uma aula será destinada a apresentação do contexto histórico e o conceito de criptografia. Uma aula será destinada a revisão do conceito de função inversa e a sua interligação com os sistemas de criptografia, fazendo associação as chaves de entrada e de saída. Uma aula será destinada a criação de um modelo de criptografia por cada um dos estudantes no qual eles devem associar a relação de função inversa com as chaves de entrada e saída de seus modelos, feito isso cada um deverá escrever uma mensagem com o modelo criado. A última aula será destinada ao processo de decodificação de mensagem e eleição dos modelos mais seguros, fazendo uma análise baseada na dificuldade de codificação e decodificação, nesta aula devem ser apresentadas propostas de melhoria dos modelos por parte do professor e apresentadas indagações que quando respondidas podem dar a ideia de funcionamento de sistemas de criptografia mais complexos.

4.2 Implementando um modelo de criptografia com função afim no Construct

Para aplicação em sala de aula a nível médio o modelo usando função afim torna-se viável e atrativo, pois é simples e aborda uma gama de habilidades já trabalhadas no decorrer do ensino médio. Por isso, implementamos de modo inicial esse sistema simétrico simples (vide seção 3.2), no entanto a aplicação do RSA também pode acontecer, mas com finalidades diferentes como preparação para olimpíadas ou um curso de extensão. Para um melhor detalhamento sobre o a implementação desse modelo em sala de aula e no Construct ver [4], [5] e [9].

Público: Alunos da 1ª série do ensino médio

Material: Lápis, borracha, folhas de papel, celulares, tablets, computadores e projetor multimídea.

Tempo previsto: Quatro horas aulas.

Objetivos

1. Compreender o conceito de função por meio da noção de chaves de entradas e saídas de modelos de criptografia;
2. Usar o algoritmo de Euclides para o cálculo do mdc de dois números inteiros e encontrar o inverso módulo m de um número inteiro;
3. Mostrar a importância da matemática e sua aplicação em meios tecnológicos e sistemas de segurança;
4. Determinar a inversa de uma função afim,
5. Instigar a autonomia e o autodidatismo;
6. Estimular a pesquisa científica.

Pré-requisitos: Noções iniciais do conceito de função, relação, função inversa e relação inversa. Conhecimentos de função afim. Noção de funcionalidade de um sistema de criptografia e aplicação prática do mesmo.

Desenvolvimento da atividade

Inicialmente o professor deve expor o conceito de criptografia e seu contexto histórico, apresentando os primeiros modelos de criptografia e a sua associação com a ideia de relações e funções por meio das chaves de entrada e relações e funções inversas por meio das chaves de saída.

Em Seguida o professor deve apresentar o Algoritmo Euclidiano para o cálculo do mdc de dois inteiros e apresentar a ideia de congruência e inverso multiplicativo na aritmética dos restos.

Após isso, o professor deve juntamente com os alunos definir o alfabeto a ser utilizado no modelo de criptografia a ser criado, criar e fazer ensaios do mesmo utilizando função afim (Vide seção 3.2) e por fim implementá-lo no Costruct e fazer um ensaio de seu funcionamento. O Construct é um programa online, utilizado para criação de jogos, pode ser acessado através do endereço https://editor.construct.net. Mais detalhes e o passo dessa etapa são encontrados em [4].

Perguntas a serem feitas: Esse modelo é eficaz? Qual o nível de segurança desse modelo? É possível fazer a troca de chaves sem contato presencial de modo seguro? É possível converter esse modelo para o sistema binário?

Por fim, é interessante apresentar a ideia de funcionamento do sistema RSA, visando estimular os estudantes a pesquisa. Essa etapa deve ser trabalhada como um fato curioso, para que o estudante estimule-se a pesquisar. Não é necessário aprofundar-se na mesma.

Divisão do tempo

Uma aula será destinada a revisão do conceito de função inversa de uma função afim e a sua interligação com os sistemas de criptografia, fazendo associação as chaves de entrada e de saída. Uma aula será destinada ao estudo da aritmética dos restos, abordando o conceito de congruência, inverso multiplicativo e o Algoritmo Euclidiano. E duas aulas serão destinadas a criação de um modelo de criptografia de função afim e implementação do mesmo no Construct.

Passo a passo: O passo a passo para construção de um modelo de criptografia usando função afim e sua implementação no Construct pode ser encontrado no artigo [4].

4.3 Comentário sobre as aplicações feitas em sala de aula

O desenvolvimento das aulas citadas acima foi feito com 15 estudantes das 1º e 2º séries do ensino médio da escola cidadã integral técnica Lynaldo Cavalcanti de Albuquerque na cidade de Patos-PB.

As práticas permitiram a abordagem dos conceitos de função, função inversa, analise combinatória e aprofundamento de estudos abordando equações diofantinas e congruência de números inteiros (que são conteúdos abordados nas aulas do programa OBMEP na escola da Sociedade Brasileira de Matemática), além de

que, dentro da proposta de nivelamento do novo ensino médio foi possível revisar operações com números inteiros e interpretação gráfica, que são duas das habilidades de propulsão (nivelamento) elencadas pela matriz curricular do novo ensino médio.

Os resultados foram satisfatórios e a avaliação de aprendizagem foi feita por meio de atividades propostas no decorrer do processo como: criação de modelos de criptografia por parte dos alunos, aprimoramento desses modelos por meio da noção de funções e congruências de números inteiros e implementação no Construct. As contas envolvidas no processo em um primeiro instante foram feitas manualmente, depois disso instigou-se o uso de calculadoras algébricas, em específico a Wolframalpha que pode ser acessada em https://www.wolframalpha.com. Os estudantes se mostraram participativos e bastante interessados no desenvolvimento de cada etapa das aulas, inclusive alguns projetos de vida foram despertados dentro das etapas das aula, pois dois dos estudantes afirmaram que as temáticas abordadas influenciaram na formulação de seus projetos de vida, tendo em vista que nas aulas foram abordados temas de interesse deles.

Para ter sucesso na aplicação dessas práticas, deve-se ter planejamento voltado a realidade de cada turma, pois, por ser um conteúdo amplo e com níveis diferentes, podemos estipular finalidades de aprendizado específico, pois tanto podemos trabalhar como prática experimental ou curso de aprofundamento (política da OBMEP na escola), ou até mesmo como nivelamento de conceitos básicos, dentro da proposta de nivelamento do novo ensino médio.

Estas propostas de atividades visam despertar curiosidade no aluno com relação às aplicações da matemática, mostrando a importância do estudo da mesma para si e a importância da mesma no desenvolvimento de tecnologias no decorrer da história. Por que despertar curiosidade sobre a matemática? Estudiosos como Freire [6] e Assmann [1] discutem que a curiosidade faz com que os discentes quebrem as barreiras da sala de aula e busquem o conhecimento de modo amplo. "Alunos curiosos não fazem só perguntas, mas vão em busca de respostas"[1]. A curiosidade prepara o cérebro para aprender, exercita a mente para o novo, isso faz com que a aprendizagem ocorra com excelência, haja vista que segundo a teoria da inteligência multifocal nossa memória necessita de estimulo e emoções para gravar a aprendizagem ao longo prazo [3]. Para estimular, as práticas sugerem um estudo das tecnologias de segurança incorporadas no decorrer da história visando troca de informações de maneira segura.

Observação 4.1 *Mediante formulário impresso aplicado no final do desenvolvimento das aulas acima, constatou-se que obteve-se uma média de aproveitamento de* 80% *de todas as temáticas abordadas. A seguir, nas Figuras 4.1 e 4.2, temos dois dos formulários aplicados com as respostas dos estudantes A e B.*

1. O estudo de criptografia propiciou o aprendizado ou revisão de conceitos de matemática? Se sim, quais conteúdos você aprendeu e\ou revisou?

Sim. Tanto os métodos básicos, como adição, subtração, multiplicação e divisão, e também a parte de função afim.

2. Qual o seu nível de entendimento mediante a metodologia apresentada nas aulas?

( ) não entendi nada ( ) compreendi pouco (X) Foi satisfatório

3. Você julga importante o estudo de criptografia e sistemas de segurança? Se sim, justifique o motivo.

Sim. Para a maior segurança de ~~informações~~ informações.

4. Assinale os temas abordados em que você teve um bom entendimento.

(X) Contexto histórico de criptografia

(X) Cifras de Cézar

(X) Criptografia Com funções afins

(X) Aprimoramento do sistema das funções afins com o conceito de congruência

(X) Implementação no Construct

(X) Uso do WolframAlpha

5. O estudo de Criptografia Contribuiu de alguma forma para a formulação ou estímulo ao seu projeto de vida? Justifique.

No projeto atual não, porém futuramente para a vida adulta, seja para um trabalho fixo, ou apenas uma renda extra.

Figura 4.1: Formulário respondido pelo aluno A

1. O estudo de criptografia propiciou o aprendizado ou revisão de conceitos de matemática? Se sim, quais conteúdos você aprendeu e\ou revisou?

Função, divisão com resto, equação

2. Qual o seu nível de entendimento mediante a metodologia apresentada nas aulas?

( ) **não entendi nada** ( ) **compreendi pouco** (X) **Foi satisfatório**

3. Você julga importante o estudo de criptografia e sistemas de segurança? Se sim, justifique o motivo.

É sempre bom compreender como funcionam sistemas de segurança em diversos ramos da tecnologia, como em programação e hacking. Principalmente pela "ética" envolvida.

4. Assinale os temas abordados em que você teve um bom entendimento.

(X) Contexto histórico de criptografia

(X) Cifras de Cézar

(X) Criptografia Com funções afins

(X) Aprimoramento do sistema das funções afins com o conceito de congruência

( ) Implementação no Construct — Ainda não tentei

(X) Uso do WolframAlpha

5. O estudo de Criptografia Contribuiu de alguma forma para a formulação ou estímulo ao seu projeto de vida? Justifique.

Sim, além de entender melhor como funcionam os computadores e a ética por trás de alguns encontros.

Figura 4.2: Formulário respondido pelo aluno B

Referências Bibliográficas

[1] ASSMANN, Hugo, Curiosidade e Prazer de Aprender – O papel da curiosidade na aprendizagem criativa. – Petropolis, RJ: Editora Vozes, 2004.

[2] COUTINHO, S. C. Números inteiros e criptografia RSA. 2. ed. Rio de Janeiro: IMPA, 2014. 226 p. ISBN 978-85-244-0124-4.

[3] CURY, Augustu. Inteligência Multifocal. São Paulo: Cultrix, 1998.

[4] DE MENEZES NETO, Jose Laudelino. Escrevendo em código: aprendendo a criptografar. 2022. Disponível em: http://dx.doi.org/10.13140/RG.2.2.30266.47044. Acesso em 24/12/2022.

[5] DE MENEZES NETO, José Laudelino, Primeiros Passos em Criptografia. 1. ed. Editora UFPB, 2021. Disponível em: https://laudelino.dcx.ufpb.br/livro

[6] FREIRE, Paulo. Pedagogia do oprimido, 17ª ed., Rio de Janeiro: Paz e Terra, 1987.

[7] HEFEZ, Abramo. Aritmética. 2. ed. Rio de Janeiro: SBM, 2016. 298 p. ISBN 978-85-8337-105-2.

[8] KOBLITZ, Neal. A course in number theory and cryptography. Springer, 1994.

[9] MIRANDA, Ariane Andressa Noronha de Sousa; PAULA, Fernanda Vital de. Uma proposta para o ensino de funções afins por meio da criptografia. REAMEC - Rede Amazônica de Educação em Ciências e Matemática, v.9, n. 2, 2021. DOI: https://doi.org/10.26571/reamec.v9i2.12652

[10] RIBEIRO, Bruno; SILVA, Talysson Paulo da. Montando critérios de divisibilidade diferentes. Professor de matemática, Revista eletrônica da sociedade brasileira de matemática, ano 2020, v. 8, n. 2, p. 170-179.

[11] RIBENBOIM, Paulo. Números primos: Velhos mistérios, novos recordes. 3. ed. Rio de Janeiro: SBM, 2020. 317 p. v. 1. ISBN 978-65-89124-03-0.

[12] RIBENBOIM, Paulo. Números primos, amigos que causam problemas: Um triálogo com o Papa Paulo. 1. ed. aum. Rio de Janeiro: SBM, 2015. 408 p. v. 1. ISBN 978-85-8337-021-5.

[13] SINGH, S. O livros dos Códigos, Editora Record, Terceira Edição, 2003.

[14] VIEIRA, Vandemberg Lopes. Um curso básico em teoria dos números. 1. ed. Campina Grande: Eduepb, 2015. 560 p. v. 1. ISBN 987-85-7879-275-6.