UNIVERSIDADE ESTADUAL DA PARAÍBA

CENTRO DE CIÊNCIAS E TECNOLOGIA

DEPARTAMENTO DE MATEMÁTICA

CURSO DE LICENCIATURA EM MATEMÁTICA

Os Números Primos e o Crivo de Eratóstenes

JOSENILDO FERREIRA GALDINO

CAMPINA GRANDE - PB

Dezembro de 2011

Josenildo Ferreira Galdino

Os Números Primos e o Crivo de Eratóstenes

Trabalho Acadêmico Orientado apresentado ao curso de Licenciatura em Matemática do Departamento de Matemática do Centro de Ciências e Tecnologia da Universidade Estadual da Paraíba em cumprimento às exigências legais para obtenção do título de licenciado em Matemática.

Orientador: Dr. Aldo Trajano Lourêdo

CAMPINA GRANDE-PB

Dezembro de 2011

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA CENTRAL – UEPB

G131n Galdino, Josenildo Ferreira.

Os números primos e o crivo de Eratóstenes [manuscrito] / Josenildo Ferreira Galdino. – 2011.

49 f. : il. color.

Digitado.

Trabalho de Conclusão de Curso (Graduação em Matemática) – Universidade Estadual da Paraíba, Centro de Ciências Tecnológicas, 2011.

"Orientação: Prof. Dr. Aldo Trajano Lourêdo, Departamento de Matemática e Estatística".

1. Matemática. 2. Números Primos. 3. Eratóstenes. 4. Criptografia. I. Título.

21. ed. CDD 510.7

JOSENILDO FERREIRA GALDINO

Os Números Primos e o Crivo de Eratóstenes

Aprovado em: 09/12/2011

COMISSÃO EXAMINADORA

Aldo Trajano Lourêdo

Prof. Dr. Aldo Trajano Lourêdo
Dpto. Matemática - CCT/UEPB
ORIENTADOR

Fernando Luiz Tavares da Silva

Prof. Ms. Fernando Luiz Tavares da Silva
Dpto. Matemática - CCT/UEPB
EXAMINADOR

Prof. Dr. Vandenberg Lopes Vieira
Dpto. Matemática - CCT/UEPB
EXAMINADOR

Dedicatória

Dedico este trabalho a toda minha família, e em especial ao meu pai, o Sr. José Galdino Fernandes, e a minha mãe, a Srª Aurenir de Feitas Fernandes.

Agradecimentos

Desejo expressar os meus sinceros agradecimentos.

Primeiramente, agradeço a DEUS por proporcionar a conclusão de mais uma etapa da minha vida que se consuma neste trabalho.

Aos meus pais: José Galdino Fernades e Aurenir Freitas Fernandes e aos meus queridos irmãos: Juraci, Jurandir e Joelma, agradeço todo o amor, carinho e motivação.

Ao Dr Aldo Trajano Lourêdo, sou grato pela orientação e confiança em mim depositada. Agradeço pelas discussões e reflexões que possibilitaram o enriquecimento e realização deste trabalho.

Ao Dr Vandenberg Lopes Viera e Ms Fernando Luiz Tavares da Silva pelas valiosas criticas e sugestões.

Aos funcionários da coordenação e departamento de matemática.

Epígrafe

"A mente que se abre a uma nova idéia jamais voltará ao seu tamanho original"

(Albert Einstein)

Resumo

Este trabalho aborda alguns resultados e problemas relacionados aos números primos, destacando o método clássico do *Crivo de Eratóstenes* que tem a finalidade de determinar se um dado número é primo. Alguns fundamentos da criptografia são apresentados. Além disso, apresentam-se alguns conceitos de álgebra abstrata, tais como: congruência, classes residuais, conjunto quociente, função de Euler e, principalmente, a correlação e relevância dos números primos na criptografia RSA.

Palavras chave: Números Primos, Eratóstenes e Criptografia.

Abstract

This paper discusses some results and problems related to prime numbers, highlighting the classic method of Riddle Eratostenes which has the purpose of determining whether a given number is cousin. Some fundamentals of cryptography are presented. beyond addition, it presents some concepts of abstract algebra, such as: congruence classes residual quotient set, function of Euler and, especially, the correlation and significance of prime numbers in RSA encryption.

Keywords: Primes, Eratostenes and encryption

Lista de Figuras

Lista de Tabelas

Sumário

Capítulo 1

Números Primos

Neste capítulo apresentaremos alguns conceitos e definições sobre números primos. Além disso, destacaremos alguns de seus teoremas e resultados elementares.

1.1 Introdução

A Teoria dos Números é considerada um dos ramos mais antigos da matemática e estuda as propriedades e relações entre os números. É uma área que vem ganhando destaque na literatura especializada e, principalmente, pela grande utilidade na engenharia e na matemática aplicada. Por exemplo, na engenharia, os sistemas criptográficos utilizam primos gigantes.

1.2 Definições

Definição 1. *Um inteiro p diz-se primo se tem exatamente dois divisores positivos, 1 e* $\mid p \mid$.

Definição 2. *Um inteiro a diz-se composto se não é primo e for diferente de 0,1 e -1.*

Definição 3. *(Primos Gêmeos)*
Seja p um primo maior que 2. Os pares de primos da forma $(p, p+2)$ *são chamados de primos gêmeos. Alguns exemplos de primos gêmeos são*

$$(3,5),(5,7),(11,13),(17,19)$$

Definição 4. *(Número Perfeito) Um número é dito perfeito, se for igual à soma de seus*

divisores, excluindo o próprio número. [5] Alguns exemplos de números perfeitos são

$$\boldsymbol{6} = 1 + 2 + 3 \qquad \boldsymbol{28} = 1 + 2 + 4 + 7 + 14$$

Definição 5. *(Número de Mersenne) Um número é dito número de Mersenne se ele for da forma* $M_n = 2^n - 1$ *com* $n \in \mathbb{N}$. *O número de Mersenne é uma homenagem ao matemático francês Marin Mersenne*[1] .

Figura 1.1: Marin Mersenne (1588-1648)

Definição 6. *(Primo de Mersenne) Um número* M_p *se diz primo de Mersenne se* M_p *for primo, na qual*

$$M_p = 2^p - 1 \tag{1.1}$$

para um primo positivo p.

A busca de números de Mersenne incentivou a criação de alguns grupos de pesquisa. É o caso do GIMPS[2]. Este grupo encontrou os 13 maiores primos de Mersenne. Além disso, no site http://mersenne.org são disponiblizados alguns programas computacionais que podem ser utilizados por amadores ou especialistas na área. Uma lista completa de todos os números de Mersenne encontrados é apresentada nas tabelas (1.1) e (1.2).

[1]**Marin Mersenne** - Teólogo, filósofo e matemático francês (1588-1648). Estudou no colégio dos padres jesuítas de La Flèche em Paris, onde conheceu Descartes, com quem manteve laços de amizade até a morte. Em 1611 ingressou na Ordem dos Franciscanos. Lecionou filosofia em Nevers (1614-1620) e Paris. A partir de 1630, aproximadamente, após publicar algumas obras filosóficas e teológicas, dedicou-se especialmente ao estudo da Matemática e da Física. Exerceu grande influência nos movimentos filosóficos e científicos de seu tempo, principalmente por ser o animador de um grupo de intelectuais, como Galileu, Torricelli, Gassendi, Descartes, Roberval e Pascal. Foi o primeiro a medir experimentalmente a velocidade do som e a determinar a frequência das notas musicais. Traduziu para o latim diversos tratados científicos gregos. Escreveu, entre outras obras: *Questiones celeberrimae in Genesim* (1623), *L'impiété des déistes, athées et libertins* (1624), *La vérité des sciences contre les Sceptiques et les Pyrrhoniens* (1625), *L'harmonic universelle, contenant la théorie et la pratique de la musique.*[6]

[2]**GIMPS** - Great Internet Mersenne Prime Search (Grande Pesquisa pela Internet sobre os números de Mersenne.)

Nº	**n (expoente)**	**Nº de Digitos de M_n**	**Ano**	**Pesquisador**
1	2	1		
2	3	1		
3	5	2		
4	7	3		
5	13	4		
6	17	6	1588	Cataldi
7	19	6	1588	Cataldi
8	31	10	1772	Euler
9	61	19	1883	Pervushin
10	89	27	1911	Powers
11	107	33	1914	Powers
12	127	39	1876	Lucas
13	521	157	1952	Robinson
14	607	183	1952	Robinson
15	1279	386	1952	Robinson
16	2203	664	1952	Robinson
17	2281	687	1952	Robinson
18	3217	969	1957	Riesel
19	4253	1281	1961	Hurtwitz
20	4423	1332	1961	Hurwitz
21	9689	2917	1963	Gillies
22	9941	2993	1963	Gillies
23	11213	3376	1963	Gillies
24	19937	6002	1971	Tuckerman

Tabela 1.1: Tabela de Números de Mersenne de 1 a 24.

Nº	**n (expoente)**	**Nº de Digitos de M_n**	**Ano**	**Pesquisador**
25	21701	6533	1978	Noll & Nickel
26	23209	6987	1979	Noll
27	44497	13395	1979	Nelson & Slowinski
28	86243	25962	1982	Slowinski
29	110503	33265	1988	Colquitt & Wilsh
30	132049	39751	1983	Slowinski
31	216091	65050	1985	Slowinski
32	756839	227832	1992	Slowinski & Gage et al.
33	859433	258716	1994	Slowinski & Gage
34	1257787	378632	1996	Slowinski & Gage
35	1398269	420921	1996	Armengaud, Woltman, et al. (GIMPS)
36	2976221	895932	1997	Spence, Woltman, et al. (GIMPS)
37	3021377	909526	1998	Clarkson, Woltman, Kurowski et al. (GIMPS)
38	6972593	2098960	1999	Hajratwala, Woltman, Kurowski et al. (GIMPS)
39	13466917	4053946	2001	Cameron, Woltman, Kurowski et al. (GIMPS)
40	20996011	6320430	2003	Shafer, Woltman, Kurowski et al. (GIMPS)
41	24036583	7235733	2004	Findley, Woltman, Kurowski et al. (GIMPS)
42	25964951	7816230	2005	Novak, Woltman, Kurowski et al. (GIMPS)
43	30402457	9152052	2005	Cooper, Boone, Woltman, Kurowski et al. (GIMPS)
44	32582657	9808358	2006	Cooper, Boone, Woltman, Kurowski et al. (GIMPS)
45	37156667	11185272	2008	Elvenich, Woltman, Kurowski et al. (GIMPS)
46	42643801	12837064	2009	Strindmo, Woltman, Kurowski et al. (GIMPS)
47	43112609	12978189	2008	Smith, Woltman, Kurowski et al. (GIMPS)

Tabela 1.2: Tabela de Números de Mersenne de 25 a 47.

Definição 7. *(Números de Fermat) Todo número escrito na forma* $F_n = 2^{2^n} + 1$ *é chamado de Número de Fermat.*

Em 1640, Fermat[3] percebeu que os quatro primeiros números de Fermat eram primos, isto é, F_n para $n = 1, 2, 3, 4$. Sendo assim, ele conjecturou que todo os números de Fermat eram primos. Demorou quase 100 anos para invalidar a conjectura de Fermat, pois em 1739, Euler demonstrou que o quinto número de Fermat, F_5, é divisível por 641. A seguir mostraremos a prova de que F_5 é divisivel por 641 usando o conceito e algumas propriedades de congruências.

$$F_5 = 2^{2^5} + 1 = 2^{32} + 1$$

$$2^{16} = 65536$$

Ao dividir o número 65536 por 641, obtemos um resto igual a 154. Usando, congruências podemos escrever este fato como

$$2^{16} \equiv 154 (mod\, 641)$$

Da Teoria dos Números temos o seguinte resultado.

Proposição 1. *Sejam a, b inteiros arbitrários e m, n inteiros positivos. Se* $a \equiv b (mod\, m)$ *então* $a^n \equiv b^n (mod\, m)$*, para todo inteiro positivo n.*

[3]Pierre de Fermat - Matemático Francês (1601-1665). Foi um dos grandes nomes da Matemática, tendo influenciado muito na criação do ramo chamado Cálculo, com seu estudo sobre máximos, mínimos e tangentes de curvas. Essas tangentes são chamadas atualmente de taxas de variação de uma quantidade ou simplemente de derivada. Tal a importância de seu trabalho que, baseado nele, Newton desenvolveu o cálculo diferencial, base matemática para sua lei da gravidade e as leis da Mecânica. Outro ramo que ajudou a desenvolver , juntamente com Pascal, foi a Teoria das Probabilidades.

A maior contribuição de Fermat foi na Teoria dos Números, forma mais pura e antiga da Matemática. Porém, tinha uma maneira nada acadêmica de mostrar seus conhecimentos e progressos. Na maioria das vezes, em suas anotações e cartas, dava indícios de como provar determinadas propriedades e teoremas, mas não os fazia por completo. Ás vezes, após a descoberta de uma propriedade, escrevia a amigos matemáticos desafiando-os a prová-la. Seu mais célebre problema, conhecido como o *Ultimo Teorema de Fermat*, foi escrito como uma anotação incompleta nas margens do livro Aritmética, de Diofante. Dizia ele:

> É impossivel para um cubo ser escrito como a soma de dois cubos ou um número elevado à quarta potência ser escrito como a soma de dois números elevados à quarta potência, ou, em geral, para qualquer número que seja elevado a uma potência maior que dois ser escrito como a soma de duas potências semelhantes. Ou seja:
>
> $$x^n + y^n = z^n \quad \textit{é impossível para } n > 2$$

Logo após esse desafio, Fermat escreveu. Tenho uma demonstração realmente maravilhosa para essa proposição, mas esta mmargem é muito estreita para contê-la.

A fama do Ultimo Teorema de Fermat veio da sua grande dificuldade de ser demonstrado, bem como do fato de Fermat ter afirmado poder demonstrá-lo. Não se sabe se com os conhecimentos da época ele o faria, mas esse teorema levou 355 anos para ser finalmente demonstrado pelo matemático Andrew Wiles.

Daí,

$$2^{16} \equiv 154 (mod\, 641) \quad \Rightarrow \quad (2^{16})^2 \equiv 154^2 (mod\, 641)$$

Note que $154^2 = 23716$, e dividindo por 641 obtemos umn resto igual a 640. Sendo assim, temos a seguinte congruência.

$$154^2 \equiv 640 (mod\, 641).$$

Outro resultado da Teoria dos Números sobre congruências é dado a seguir.

Proposição 2. *Sejam a, b e c inteiros arbitrários e m um inteiro positivo. Se* $a \equiv b (mod\, m)$ *e* $b \equiv c (mod\, m)$ *então* $a \equiv c (mod\, m)$

Como $2^{32} \equiv 154^2 (mod\, 641)$ e $154^2 \equiv 640 (mod\, 641)$. Então,

$$2^{32} \equiv 640 (mod\, 641)$$

Por fim, utilizaremos o seguinte resultado

Proposição 3. *Sejam a, b e c inteiros arbitrários e m um inteiro positivo. Se* $a \equiv b (mod\, m)$ *então* $a + c \equiv b + c (mod\, m)$

Portanto,

$$2^{32} \equiv 640 (mod\, 641) \quad \Rightarrow \quad 2^{32} + 1 \equiv 641 (mod\, 641)$$

Logo, concluímos que 641 divide $2^{32} + 1$.

1.3 Resultados sobre primos

Proposição 4. *Seja p um número primo e* $a, b \in \mathbb{Z}$

1. *Se* $p \dagger a$, *então mdc(p,a) = 1.*
2. *Se* $p \mid ab$, *então* $p \mid a$ *ou* $p \mid b$

Demonstração:

1. Como p é primo, então seus divisores são 1 e p. Se $p \dagger a$, consequentemente, o único divisor comum positivo de a e p é 1, o que implica que $mdc(p, a) = 1$.

2. Suponhamos que $p \mid ab$. Agora, pelo Teorema de Euclides se $mdc(p, a) = 1$, então $p \mid b$. Da mesma forma, se $mdc(p, b) = 1$, então $p \mid a$.

Teorema 1.1. ***(Principio de Indução Completa - 1ª Forma)*** *Seja a um inteiro dado. Suponhamos que para cada inteiro $n \geq a$ está dada uma afirmação A(n) de forma que*

- *A(a) é verdadeira.*
- *Se para um inteiro $k \geq a$ A(k) é verdadeira, então A(k+1) é verdadeira.*

Então A(n) é verdadeira para todo inteiro $n \geq a$.

Iremos utilizar o princípio de indução completa - 2ª forma

Teorema 1.2. ***(Principio de Indução Completa - 2ª Forma)*** *Suponhamos que para cada inteiro $n \geq a$ está dada uma afirmação A(n) de forma que*

- *A(a) é verdadeira.*
- *Se A(m) é verdadeira para todo inteiro m tal que $a \leq m \leq k$, então A(k+1).*

Então A(n) é verdadeira para todo inteiro $n \geq a$.

Lema 1.1. *Todo inteiro $a > 1$ pode ser escrito como produto de números primos.*

Demonstração:

Para $a = 2$ o resultado é válido, visto que 2 é um número primo. Suponhamos agora que o resultado seja verdadeiro para todo inteiro b, $2 \leq b \leq a$. Devemos mostrar que o resultado também vale para a.

Note que se a é primo, o lema está demonstrado. Caso contrário, a admite um divisor positivo b tal que $1 < b < a$. Isto é, $a = bc$, e temos também $1 < c < a$. Pela hipótese de indução, b e c podem ser escrito como produto de primos, na forma

$$b = p_1 \dots p_r \quad c = q_1 \dots q_s$$

Como a = bc, temos

$$a = p_1 \dots p_r q_1 \dots q_s.$$

Portanto, o resultado também vale para a.

Teorema 1.3. *O conjunto dos números primos é infinito.*

Demonstração:

Suponhamos que o conjunto dos primos é finito e os números $p_1, p_2, \ldots, p_n$ são primos. Agora, considere o número P dado por

$$P = p_1 p_2 \ldots p_n + 1.$$

Pelo lema anterior, P admite um divisor positivo primo p_i. Sendo assim, p_i divide o produto $p_1 p_2 \ldots p_n$. Então, p_i divide também $1 = P - p_1 p_2 \ldots p_n$, uma contradição.

■

Proposição 5. *Se $a^n - 1$ é primo com $n \in \mathbb{N}$, então $a = 2$ e n é primo.*

Demonstração:

Seja um primo qualquer p, ele é fatorado da forma $1 \cdot p$, isto é, $p = 1 \cdot p$. Se $a^n - 1$ é primo então seus fatores são 1 e o proprio número.

$$a^n - 1 = (a-1)(1 + a + a^2 + \cdots + a^{n-1}).$$

Note que $1 + a + a^2 + \cdots + a^{n-1} > 1$. Sendo assim, $a - 1 = 1$, isto é, a = 2.

Mostremos agora que n é primo. Sejam r, s inteiros positivos.

$$2^r - 1 = (2-1)(2^{r-1} + 2^{r-2} + \cdots + 2^1 + 1)$$

Agora, substitua 2 por 2^s.

$$(2^s)^r - 1 = (2^s - 1)[(2^s)^{r-1} + (2^s)^{r-2} + \cdots + (2^s)^1 + 1]$$

$$2^{rs} - 1 = (2^s - 1)[(2^s)^{r-1} + (2^s)^{r-2} + \cdots + (2^s)^1 + 1]$$

$$2^{rs} - 1 = (2^s - 1)[2^{s(r-1)} + 2^{s(r-2)} + \cdots + 2^{s \cdot 1} + 1]$$

Faça $n = rs$. Suponha que n é composto, isto é, tem dois fatores diferentes de 1.

Note que $2^{s(r-1)} + 2^{s(r-2)} + \cdots + 2^{s \cdot 1} + 1 > 1$. Como $2^n - 1$ é primo então $2^s - 1 = 1$, isto é, $s = 1$. Como deveriamos encontrar dois fatores diferentes de 1 então a suposição de que n é composto é falsa. Logo, n é primo.

■

1.4 Conjecturas

1.4.1 Conjectura de Goldback

Conjectura 1. *(Conjectura de Goldback) Todo inteiro positivo par maior que dois pode ser escrito como soma de dois primos.*

A seguir listamos alguns exemplos que satisfazem a conjectura de Goldback.

$$\begin{aligned} \mathbf{4} &= 2+2 \qquad \mathbf{12} = 7+5 \\ \mathbf{6} &= 3+3 \qquad \mathbf{14} = 11+3 \\ \mathbf{8} &= 5+3 \qquad \mathbf{16} = 13+3 \\ \mathbf{10} &= 7+3 \qquad \mathbf{18} = 13+5 \end{aligned}$$

1.4.2 Conjectura de Polignac

Conjectura 2. *(Conjectura de Polignac) Para todo par na forma $2n$ existem infinitas duplas de primos consecutivos, isto é, primos que diferem de $d =\mid 2n \mid$*

Quando $n = 1$ e $d = 2$ temos um caso particular da conjectura de Polignac que é conhecida na literatura como conjectura dos primos gêmeos.

Capítulo 2

Biografia e Crivo de Eratóstenes

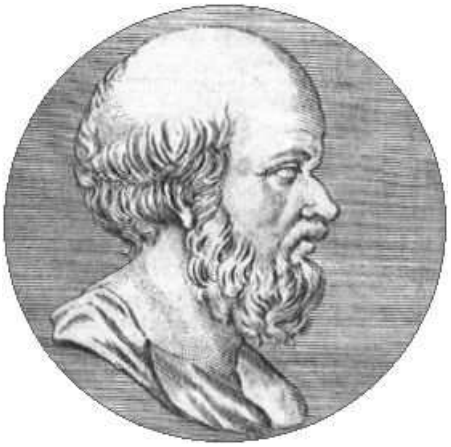

Figura 2.1: Eratóstenes (276 a.C a 196 a.C)

Filósofo, geógrafo e matemático ($276a.C.196a.C.$) foi criado em Cirene, cidade grega localizada ao norte da África. Eratóstenes estudou em Alexandria, no Egito, e posteriormente, em Atenas, retornando a Alexandria em 255 a.C. Ele escreveu sobre matemática, astronomia, geografia e história. Além disso, Eratóstenes ensinou em Alexandria, e por seu vasto conhecimento nas diversas áreas do conhecimento tornou-se diretor da famosa biblioteca de Alexandria em 240 a.C.

Naquela época, Ptolomeu III governava Alexandria e partes do Egito e ordenou que todos os navios e caravanas fossem revistados em busca de livros, mapas ou documentos interessantes para serem copiados. A biblioteca de Alexandria se tornou fonte dos vastos conhecimentos do mundo antigo.

Com as riquezas do mundo intelectual prontamente disponíveis, Eratóstenes compilou um

mapa do mundo conhecido, que se estendia das ilhas Britânicas ao Sri Lanka e incluía todos os países que faziam fronteira com o mar Mediterrâneo. O mapa foi útil por 200 anos. Ele também percebeu que o calendário solar egípcio ficava atrasado em um dia a cada quatro anos com relação às estações e sugeriu que se acrescentasse um dia extra de quatro em quatro anos.

Eratóstenes é mais conhecido por ter calculado o tamanho da Terra, conclusão a que chegou usando um método engenhoso. Ele sabia que o Sol fica mais alto ao meio-dia de 22 de junho, o solstício de verão. Nessa hora especial, uma vara vertical projeta a menor sombra. Se o sol estiver diretamente acima, a vara não projeta sombra nenhuma. Isto acontece em Syene, cidade ao sul de Alexandria, onde se encontra hoje a represa de Aswan. Como Eratóstenes descobriu que o Sol estava diretamente acima de Syene naquela hora única? Ele sabia, através das informações contidas na biblioteca, que ao meio-dia de 22 de junho, a luz do sol brilhava diretamente até o fundo de um poço profundo em Syene e era refletida de volta para cima, em linha reta, mostrando, desta forma, que o sol estava diretamente acima. Usando geometria simples, Eratóstenes mostrou que existe um ângulo de $7,2$ graus entre Alexandria e Syene, o que corresponde a $1/50$ de um círculo. Viajava-se de Syene a Alexandria com freqüência e sabia-se que a distância media 5 mil estádios. Então, Eratóstenes calculou que a Terra tinha 50 x 5 mil estádios, ou cerca de 250 mil estádios. Esta medida é incrivelmente próxima à circunferência da Terra aceita modernamente, cerca de 39.490 quilômetros.

Eratóstenes mostrou que a Terra é um lugar muito maior do que os gregos imaginavam. Eles ficaram confusos, porque isso fazia o mundo conhecido parecer comparativamente muito pequeno, e rejeitaram o número de Eratóstenes a favor de um tamanho menor e impreciso.

No campo das ciências matemáticas, destaca-se o método conhecido como *Crivo de Eratóstenes*. Este Crivo de Eratóstenes é considerado um algoritmo simples e prático para encontrar números primos.

Infelizmente, apesar de seu sucesso como estudioso e escritor, o fim da vida de Eratóstenes foi trágica. Ele ficou cego e, aos 80 anos de idade, induziu sua própria morte parando de comer.

2.1 Crivo de Eratóstenes

Eratóstenes elaborou um método para determinar todos os primos menores que um dado número $N > 0$. Este método é conhecido como o Crivo de Eratótenes.

Inicialmente escrevemos todos os inteiros positivos menores ou iguais a N. Por exemplo, se escolhermos N = 100 teríamos a seguinte tabela dada a seguir.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Tabela 2.1: Números de 1 a 100.

Agora, eliminamos todos os múltiplos de 2, excetuando-se o próprio 2.

1	2	3	~~4~~	5	~~6~~	7	~~8~~	9	~~10~~
11	~~12~~	13	~~14~~	15	~~16~~	17	~~18~~	19	~~20~~
21	~~22~~	23	~~24~~	25	~~26~~	27	~~28~~	29	~~30~~
31	~~32~~	33	~~34~~	35	~~36~~	37	~~38~~	39	~~40~~
41	~~42~~	43	~~44~~	45	~~46~~	47	~~48~~	49	~~50~~
51	~~52~~	53	~~54~~	55	~~56~~	57	~~58~~	59	~~60~~
61	~~62~~	63	~~64~~	65	~~66~~	67	~~68~~	69	~~70~~
71	~~72~~	73	~~74~~	75	~~76~~	77	~~78~~	79	~~80~~
81	~~82~~	83	~~84~~	85	~~86~~	87	~~88~~	89	~~90~~
91	~~92~~	93	~~94~~	95	~~96~~	97	~~98~~	99	~~100~~

Tabela 2.2: Múltiplos de 2 eliminados.

Agora, eliminamos todos os múltiplos de 3, excetuando-se o próprio 3.

1	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	25	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	35	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	49	~~50~~
~~51~~	~~52~~	53	~~54~~	55	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	65	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	77	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	85	~~86~~	~~87~~	~~88~~	89	~~90~~
91	~~92~~	~~93~~	~~94~~	95	~~96~~	97	~~98~~	~~99~~	~~100~~

Tabela 2.3: Múltiplos de 3 eliminados.

Continuando com este procedimento

1	**2**	**3**	~~4~~	**5**	~~6~~	**7**	~~8~~	~~9~~	~~10~~
11	~~12~~	**13**	~~14~~	~~15~~	~~16~~	**17**	~~18~~	**19**	~~20~~
~~21~~	~~22~~	**23**	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	**29**	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	**37**	~~38~~	~~39~~	~~40~~
41	~~42~~	**43**	~~44~~	~~45~~	~~46~~	**47**	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	**53**	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	**59**	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	**67**	~~68~~	~~69~~	~~70~~
71	~~72~~	**73**	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	**79**	~~80~~
~~81~~	~~82~~	**83**	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	**89**	~~90~~
91	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	**97**	~~98~~	~~99~~	~~100~~

Tabela 2.4: Crivo de Eratóstenes para $N = 100$.

2.2 Implementação do Crivo de Eratóstenes

Para utilizarmos o Crivo de Eratóstenes foi criado uma função chamada *crivo* em linguagem Matlab que referido método. A função *crivo* determina se o número N é primo e também fornece o número de primos menores que N. Na tabela (2.5) apresentamos alguns resultados de simulação para diferentes valores de N.

N	**Número de primos menores que N**
10	4
100	25
1000	168
10000	1229
100000	9592
1000000	78498

Tabela 2.5: Quantidade de primos de 1 a N.

Capítulo 3

Conjectura de Goldback

Neste capítulo apresentaremos a famosa conjectura de Goldback que é um dos problemas em aberto[1] sobre os números primos. Geralmente, os problemas que envolvem números primos são de áreas bem específicas da matemática. Uma área bastante interessante e que aborda vários problemas e resultados sobre os números primos é a *Teoria dos Números*.[2] Nesta área contempla diversos problemas em aberto de fácil entendimento e qualquer pessoa tendo algumas noções sobre números poderá entender o enunciado do problema.

Um dos problemas mais conhecidos é a Conjectura de Goldback[3] que abordaremos na próxima seção.

[1]Problema em aberto são problemas matemáticos que não foram resolvidos ainda.

[2]Segundo (Shokranian, Soares e Godinho, 1998) Teoria dos Números é a ciência na qual se estudam propriedades e relações entre os números.

[3]Matemático prussiano-russo nascido em Königsberg, Prússia, hoje Kaliningrado, Rússia, amigo de Euler a quem este confiou a descoberta de que uma potência imaginária de um número imaginário pode ser um número real. Filho de um pastor, estudou leis e matemática e tornou-se professor de matemática e história e viajou praticamente por toda a Europa, encontrando-se pessoalmente com muitos matemáticos famosos, entre eles Leibniz, Nicolaus (I) Bernoulli, Nicolaus (II) Bernoulli, de Moivre, Daniel Bernoulli e Hermann. da Academia Imperial de São. Petersburgo (1725). Depois, foi trabalhar para a recém-criada Academia de Ciências de São Petersburgo (1728) e tornou-se tutor daquele que mais tarde viria a ser o Czar Pedro II. Especialista em teoria dos números criou conjecturas como a sobre números primos (1742), em que todo inteiro maior que 2 pode ser representado pela soma de dois primos, enviada numa correspondência para Euler. Também estudou somas infinitas, teoria das curvas e teoria das equações e morreu em Moscou, Rússia. Realizou, assim, trabalho importante na matemática e hoje, é a conjectura de Goldbach que mais contribui para a sua fama. [7]

3.1 Conjectura de Goldback

Figura 3.1: Leonhard Euler (1707-1785)

Em 1742, o matemático alemão Christian Goldback (1690-1764) propôs o seguinte problema em uma correspondência enviada a Euler.[4]

Provar que todo inteiro positivo par pode ser escrito como soma de dois primos e todo inteiro maior que dois pode ser escrito como soma de três números primos.

[4]Leonhard Euler (1707-1785), matemático suiço, dominou praticamente todas as áreas da Matemática. Seu pai, o pastor protestante Paul Euler, enviou-o, aos 14 anos, à Universidade de Basiléia para estudar Teologia e preparar-se para ser pastor. Lá, o professor Johann Bernoulli cedo descobriu o potencial de Euler para a Matemática.

Em 1723, Euler formou-se em Filosofia, tendo comparado as idéias filosóficas de Descartes e Newton. No outono do mesmo ano, seguindo os desejos de seu pai, iniciou o curso de Teologia. No entanto, não encontrou entusiasmo suficiente para estudar, embora fosse um cristão devotado. Com o auxílio de Johann Bernoulli, persuadiu seu pai a deixá-lo estudar Matemática. Sob a tutela de Bernoulli concluiu, em 1726 seus estudos.

Em 1727, assumiu um cargo na divisão de Matemática-Física na recém-inaugurada Academia de São Petersburgo, onde, em contato com grandes cientistas, pôde desenvolver-se em várias áreas do conhecimento (Matemática aplicada, Teoria dos números, Astronomia, Trigonometria, Geografia ...).

No ano de 1735, após um surto de febre muito alta, perdeu a visão do olho direito. Nos dois anos seguintes, Euler publicou vários artigos e o livro de Mecânica, no qual utilizou análise matemática para o estudo da dinâmica newtoniana.

Em torno de 1740, Euler tinha grande reputação em toda a Europa. Aceitando o convite para ingressar na Academia de Ciências de Berlim, mudou-se para essa cidade em julho daquele ano. Durante os vinte e cinco anos que passou em Berlim, publicou em torno de 380 artigos e vários livros em diversas áreas, uma quantidade invejável para qualquer gênio.

Em 1766, devido à interferência do rei Frederico nos rumos da Academia, Euler decidiu voltar para São Petersburgo. Próximo de seu retorno à Russia, ficou completamente cego. Devido a sua incrível memória, continuou fazendo seus trabalhos. Para isso, teve a ajuda de seus filhos, Johann Euler e Christoph Euler, que anotavam suas observações, além de outros matemáticos da Academia, como Lexell, Krafft, Albrecht, que receberam os créditos por sua ajuda na obra de 775 páginas sobre o movimento da Lua. Seus amigos diziam: a cegueira ampliou os horizontes de sua imaginação. Seu trabalho matemático e científico foi tão vasto que ele é considerado o maior escritor matemático de todos os tempos.

A primeira sentença do problema de Goldback, ou seja, todo número par maior que 2 é soma de dois primos é conhecida hoje como *conjectura de Goldback*. Alguns pesquisadores da área de matemática tentaram resolver esse problema. Em 1966, o matemático chinês Jeng-Run Chen provou parcialmente a conjectura de Goldback. Chen mostrou que a partir de algum n, todo número par maior que dois ou é soma de dois primos, ou a soma de um primo com o produto de dois primos. Vale ressaltar que o argumento de Chen não nos diz qual é o n. Só que tal número existe.

Já a segunda sentença do problema de Goldback foi demonstrada em parte. Em 1937, o matemático soviético I. M. Vinogradov demonstrou, usando somas trigonométricas adequadas, que qualquer número ímpar suficientemente grande é soma de três números primos.

Apesar da simplicidade do enunciado do problema de Goldback este problema continua ainda sem solução, isto é, até o momento ninguém conseguiu provar ou encontrar um contra-exemplo para o problema.

Capítulo 4

Criptografia

4.1 História

O primeiro registro do uso da criptografia foi em 1900 a.c., quando os egípcios escreveram os famosos hieróglifos, que eram códigos. Já os romanos usavam os códigos para comunicar planos de batalha. Alguns dos primeiros relatos sobre escritas secretas datam de Heródoto, "o pai da história", de acordo com o filósofo e estadista romano Cícero. Heródoto que escreveu *As Histórias*, narrou os conflitos entre a Grécia e a Pérsia ocorridos no quinto século antes de Cristo. De acordo com Heródoto, foi a arte da escrita secreta que salvou a Grécia de ser conquistada por Xerxes, Rei dos Reis, o déspota líder dos Persas.

Depois da Segunda Guerra surgiu o computador, a área floresceu, e surgiram códigos mais rápidos, práticos e seguros, com o auxilio de algoritmos matemáticos.

A palavra *criptografia* é derivada do grego *kryptos* e *graphos*, os quais significam "oculto"e "escrita". O objetivo da criptografia não é ocultar a existência de uma mensagem, e sim esconder o seu significado. A vantagem da Criptografia é que, se o inimigo interceptar a mensagem codificada, ela será ilegível e seu conteúdo não poderá ser percebido. Sem conhecer o protocolo de codificação, o inimigo achará difícil, se não impossível, recriar a mensagem original a partir do texto cifrado.

Atualmente, o termo criptografia refere-se a ciência e a arte da transformação de mensagens tornando-as seguras e imunes a ataques. Na criptografia comumente são utilizados alguns nomes para facilitar o entedimento de sistemas criptográficos, sendo eles: Alice, Bob e Eve. Alice é a personagem que necessita transmitir dados com segurança. Bob é o personagem re-

ceptor dos dados. Eve é a personagem que, de algum modo, perturba a comunicação entre Alice e Bob, interceptando mensagens ou enviando mensagens dissimuladas próprias. O objetivo da criptografia é garantir que a mensagem original enviada por Alice seja acessada apenas por Bob.

A criptografia lida com as transformações de uma mensagem para a forma codificada através de *codificação* e recuperação da mensagem original por meio de *decodificação*. A mensagem original, isto é, antes de sofrer transformação, é denominada **texto limpo** ou **texto em claro**. Na etapa de codificação da mensagem original, é utilizada um algoritmo de crifagem que transforma o texto limpo em texto cifrado. Já na etapa de decodificação é utilizado um algoritmo de decifragem que reverte o processo, ou seja, transforma o texto cifrado em texto limpo.

A palavra criptografia é derivada da palavra grega *kriptos*, que significa "oculto".

Conceito de Criptografia: É a arte ou ciência de escrever mensagens em cifras ou em códigos, de modo que somente a pessoa autorizada possa decifrar e ler mensagens.

Cada cifra pode ser considerada em termos de um método geral de codificação conhecido como *algoritmo* e usa uma *chave*, que especifica os detalhes exatos de uma codificação em particular. O algoritmo consiste em substituir o alfabeto original pelo cifrado, e a chave define o alfabeto cifrado que será usado em uma codificação em particular. Assim se o inimigo interceptar uma mensagem em código, ele pode suspeitar qual seja o algoritmo, mas espera-se que ele não conheça a chave.

A palavra, criptografia, ainda evoca imagens de agentes secretos sorrateiramente transferindo informações sigilosas a nações rivais, entretanto, a principal missão da criptografia moderna é proteger as informações referentes a transações bancárias e comerciais que transitam entre computadores numa rede.

Capítulo 5

Cifra de Substituição

5.1 Cifra de César

O primeiro registro da cifra de substituição é atribuído a Júlio Cesar e, assim, ficou conhecido como *cifra de César*. Na cifra de César, cada letra da mensagem do texto que será cifrado é substituído pela k-ésima letra sucessiva do alfabeto. Por exemplo, se k = 4, então a letra *a* fica sendo a letra *d* no texto cifrado; a letra *b* se transforma na letra *f* no texto cifrado, e assim por diante. A seguir mostramos o alfabeto e o texto cifrado usando a cifra de César com k = 4.

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

U	V	W	X	Y	Z
Y	Z	A	B	C	D

As letras A do texto comum são substituídas por E, as letras B do texto comum por F e assim por diante. Com essa cifra a mensagem do texto comum:

A ESCADA DA SABEDORIA SE FAZ COM NÚMEROS

fica da seguinte forma

E IWGEHE HE WEFIHSVME WI JEV GSQ RYQIVSW

Apesar do texto cifrado não ter nenhum nexo é bastante fácil quebrar o código supondo que saibamos que o texto foi cifrado com a cifra de César. Na verdade, no pior dos casos teríamos que testar 25 valores para o deslocamento, isto é, $k = 1, 2, \ldots, 25$.

5.2 Cifra Monoalfabética

Ao longo do tempo, a idéia de César de codificar o texto foi sendo adotada por outros e alterada para que o código ficasse mais difícil de ser quebrado. Um aperfeiçoamento da cifra de César é a **cifra monoalfabética**, que substitui uma letra do alfabeto por outra. Ao contrário da cifra de César que é feita uma substituição seguindo um padrão regular (por exemplo, substituição por um deslocamento de k para todas as letras), na cifra monoalfabética, qualquer letra pode ser substituída por qualquer outra, contanto que cada letra tenha uma única letra substituta e vice-versa.

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

U	V	W	X	Y	Z
Y	T	R	E	W	Q

Com essa cifra a mensagem do texto comum:

A ESCADA DA SABEDORIA SE FAZ COM NÚMEROS

fica da seguinte forma

M CIBMVM VM IMNCVKOSM IC XMQ BKH JYHCOKI

A cifra monoalfabética requer 26! (aproximadamente 10^{26}) possibilidades para codificar o alfabeto, um número estrondoso em comparação à 25 possibilidades para o alfabeto da cifra de César. Uma abordagem pelo método de força bruta que testa todas as possibilidades demandaria um esforço computacional grande e isto impediria que este código fosse quebrado. No entanto, a cifra monoalfabética tem um ponto fraco com relação a codificação de maneira única para cada letra do alfabeto. Observe no exemplo anterior que: se a letra A é cifrada como a

letra M, significa que toda letra A do texto original vai ser substituida pela letra M. Portanto, pela análise estatística da linguagem do texto e sabendo que as letras A, E e O são as mais frequentes nos textos em português, é possivel quebrar esse código.

5.3 Cifra Polialfabética

Na cifra polialfabética, cada ocorrência de um caractere pode ter um substituto diferente. Em outras palavras, cada caractere do texto original pode ser cifrado por diferentes caracteres. A idéia da cifra polialfabética é utilizar várias cifras monoalfabéticas com uma cifra monoalfabética específica para codificar uma letra em uma posição específica do texto. Assim, uma mesma letra, quando aparece em diferentes posições no texto, pode ser codificada de maneira diferente. Por exemplo, considere um esquema criptográfico polialfabético composto por duas cifras de César ($k = 5$ e $k = 19$). Uma opção é utilizar essas duas cifras de César, C_1 e C_2, seguindo o modelo de repetição $C_1C_2C_2C_1C_2C_1C_2C_2C_1C_1$. A seguir temos um esquema de uma cifra polialfabética que utiliza duas cifras de César.

$$\begin{aligned} Alfabeto &: A\,B\,C\,D\,E\,F\,G\,H\,I\,J\,K\,L\,M\,N\,O\,P\,Q\,R\,S\,T\,U\,V\,W\,X\,Y\,Z \\ C_1(k=5) &: F\,G\,H\,I\,J\,K\,L\,M\,N\,O\,P\,Q\,R\,S\,T\,U\,V\,W\,X\,Y\,Z\,A\,B\,C\,D\,E \\ C_2(k=19) &: T\,U\,V\,W\,X\,Y\,Z\,A\,B\,C\,D\,E\,F\,G\,H\,I\,J\,K\,L\,M\,N\,O\,P\,Q\,R\,S \end{aligned}$$

Com essa cifra a mensagem do texto comum:

MATEMATICA

fica da seguinte forma

RTMJFFMBHT

Capítulo 6

Aritmética Modular

6.1 Congruência

Definição 8. *Seja $m > 1$ um número inteiro. Dados $a, b \in \mathbb{Z}$, dizemos que a é congruente a b módulo m se, e somente se, $m|(a-b)$ e usamos a notação:$a \equiv b(mod m)$.*

Exemplo:

$$21 \equiv 1(\text{mod } 5) \qquad \text{pois} \qquad 21 - 1 = 20 \text{ que é divisível por } 5$$

Propriedades:

- Reflexiva: $a \equiv a(\text{mod } m)$;
- Simétrica: Se $a \equiv b(\text{mod } m)$ então $b \equiv a(\text{mod } m)$;
- Transitiva: Se $a \equiv b(\text{mod } m)$ e $b \equiv c(\text{mod } m)$, então $a \equiv c(\text{mod } m)$.

Além destas, a congruência módulo m goza das seguintes propriedades:

- Se $a \equiv a(\text{mod } m)$ e $c \equiv d(\text{mod } m)$, então $a + c \equiv b + d(\text{mod } m)$;
- Se $a \equiv b(\text{mod } m)$ e $c \equiv d(\text{mod } m)$, então $a.c \equiv b.d(\text{mod } m)$;
- Se $a \equiv b(\text{mod } m)$ então $a^n \equiv b^n(\text{mod } m)$ para todo $n \in \mathbb{N}$.

6.2 Classes Residuais

Definição 9. *Toda classe de equivalência em $\mathbb{Z}$ determinada pela congruência módulo m, chama-se classe residual módulo m.*

A classe residual módulo m de um inteiro a é o conjunto de todos os números inteiros x tais que $x \equiv a(\text{mod } m)$, ou seja, tais que $x - a = k.m$, $k \in \mathbb{Z}$ e representada por $\overline{a}$ que se lê: "a barra". Portanto, simbolicamente:

$$\begin{aligned} \overline{a} &= \{x \in \mathbb{Z}; x \equiv a(\text{mod } m)\} \\ \overline{a} &= \{x \in \mathbb{Z}; x = m.k + a\} \end{aligned}$$

6.3 Conjunto Quociente

O conjunto quociente de $\mathbb{Z}$ pela conguência módulo m, isto é, o conjunto de todas as classes residuais módulo m, indica-se por $\mathbb{Z}_m$. Portanto, simbolicamente:

$$\mathbb{Z}_m = \{\overline{a} \mid \ a \in \mathbb{Z}\}$$

Como $a = q.m+r$, onde $0 \leq r < m$, qualquer $a \in \mathbb{Z}$ é congruente módulo m a um dos elementos $\overline{0}, \overline{1}, \overline{2}, ..., \overline{m-1}$ e mostra-se que:

$$\mathbb{Z}_m = \{\overline{0}, \overline{1}, \overline{2}, ..., \overline{m-1}\}$$

Em $\mathbb{Z}_m$ definimos as seguintes operações:

- Adição: $\overline{a} + \overline{b} = \overline{a+b}$
- Multiplicação: $\overline{a}.\overline{b} = \overline{a.b}$

Um elemento $\overline{a} \in \mathbb{Z}_m$ é dito invertível se existir $\overline{x} \in \mathbb{Z}_m$ tal que:

$$\overline{a}.\overline{x} = \overline{x}.\overline{a} = 1$$

ou equivalente,

$$ax \equiv 1(\text{mod } m)$$

Proposição 6. *Um elemento $\overline{a} \in \mathbb{Z}_m$ é invertível, se e somente se, $mdc(a, m) = 1$.*

6.4 Função de Euler

Seja $\phi : \mathbb{N} \longrightarrow \mathbb{N}$ a função de Euler, isto é, a função definida por

$$\phi(n) = \#\{1 \leq r \leq n; mdc(r, n) = 1\}$$

Exemplo: $\phi(6) = 2$, pois $mdc(1, 6) = 1$, $mdc(2, 6) = 2$, $mdc(3, 6) = 3$, $mdc(4, 6) = 2$, $mdc(5, 6) = 1$, $mdc(6, 6) = 6$.

Proposição 7. *Se p e q, são primos, então*

$$\phi(p.q) = (p - 1)(q - 1)$$

Capítulo 7

Cifras de Hill

Uma desvantagem de cifras de substituição é que elas preservam as frequências de letras individuais, tornando relativamente fácil quebrar o código por métodos estatísticos. Uma maneira de superar este problema é dividir o texto em grupos de letras e criptografar o texto comum por grupo, em vez de uma letra de cada vez. Um sistema poligráfico é um sistema de criptografia no qual o texto comum é dividido em conjuntos de n letras, cada um dos quais é substituído por um conjunto de n letras cifradas. Estudaremos agora uma classe de sistemas poligráficos chamados *Cifras de Hill* que são baseados em trasformações matriciais. (O nome é em referência a Lester S. Hill que introduziu estes sistemas em dois artigos: "Cryptography in na Algebraic Alphabet", American Mathematical Monthly, vol. 36, Junho-Julho de 1929 e "Conserning Certain Linear Transmation Apparatus of Cryptography", American Mathematical Monthly, vol. 38, Março de 1931, páginas 135-154).

Nos casos mais simples de cifras de Hill, tranformamos pares sucessivos de texto comum em texto cifrado pelo seguinte procedimento:

Passo 1: Escolha uma matriz 2×2

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \qquad \text{em} \qquad \mathbb{Z}_m$$

com entradas $a_{ij} i, j = 1, 2$ inteiras para efetuar a codificação.

Passo 2: Agrupe letras sucessivas do texto comum em pares, adicionando uma letra fictícia para complemetar o último par se o texto comum tem um número ímpar de letras; substitua cada letra do texto comum por seu valor numérico.

Passo 3: Converta cada par sucessivo $p_1\ p_2$ de letras de texto comum em um vetor-coluna.

$$P = \begin{pmatrix} p_1 \\ p_2 \end{pmatrix}$$

e forme o produto AP. Chama-se P de vetor comum e AP o correspondente vetor cifrado.

Passo 4: Converta cada vetor cifrado em seu equivalente alfabético.

Exemplo 7.1. *Use o alfabeto da tabela abaixo e a matriz dada:*

A	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*
0	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	*15*	*16*	*17*	*18*	*19*

U	*V*	*W*	*X*	*Y*	*Z*	*É*	,	*?*
20	*21*	*22*	*23*	*24*	*25*	*26*	*27*	*28*

$$A = \begin{pmatrix} 4 & 1 \\ 0 & 2 \end{pmatrix} \quad em \quad \mathbb{Z}_{29}$$

Para obter a cifra de Hill da mensagem de texto comum

MATEMATICA

Solução: *Agrupamos o texto comum em pares de letras o qual obteremos:*

MA TE MA TI CA

ou, equivalentemente, usando a tabela dada

12 0 19 4 12 0 19 8 2 0

Para codificar o par MA efetua-se o produto matricial

$$\begin{pmatrix} 4 & 1 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 12 \\ 0 \end{pmatrix} = \begin{pmatrix} 48 \\ 0 \end{pmatrix} = \begin{pmatrix} 19 \\ 0 \end{pmatrix}$$

Aqui temos um problema, pois o número 48 não possui equivalente alfabético de acordo com a tabela dada, já que está se usando o conjunto $\mathbb{Z}_{29}$. Para resolver este problema faz-se o seguinte: sempre que ocorrer um inteiro maior que 28, ele será substituído pelo resto da divisão deste

inteiro por 29.

Com o resto da divisão é um dos inteiros $0, 1, 2, ..., 28$*, este procedimento sempre fornece um inteiro com equivalente alfabético.*

Assim substitui-se 48 por 19, que é o resto da divisão deste número por 29 e obtem-se o texto cifrado TA, no lugar de MA.

As contas para os demais vetores cifrados são:

$$\begin{pmatrix} 4 & 1 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 19 \\ 4 \end{pmatrix} = \begin{pmatrix} 80 \\ 8 \end{pmatrix} = \begin{pmatrix} 22 \\ 8 \end{pmatrix}$$

$$\begin{pmatrix} 4 & 1 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 19 \\ 8 \end{pmatrix} = \begin{pmatrix} 84 \\ 16 \end{pmatrix} = \begin{pmatrix} 26 \\ 16 \end{pmatrix}$$

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

Estes vetores correspondem aos pares de texto cifrado TA, WI, TA, ÉQ e IA, respectivamente. Coletando os pares, obtemos a mensagem cifrada completa:

TA WI TA ÉQ IA

Que, normalmente, seria transmitida como uma única cadeia sem espaços:

TAWITAÉQIA

Como o texto comum foi agrupado em pares e criptografado por uma matrix 2×2, diz-se que a cifra de Hill do exemplo é uma **2-cifra de Hill**. Evidentemente também é possível agrupar o texto comum em ternas e criptografar com uma matriz 3×3 com entradas inteiras, isto é chamado de uma **3-cifra de Hill**. Em geral, para uma **n-cifra de Hill** agrupa-se o texto comum em conjuntos de n letras e codifica-se com uma **matriz codificadora n×n** de entradas inteiras.

7.1 Decifração

Para decifrarmos a mensagem codificada acima faz-se o seguinte:

pela tabela dada o equivalente numérico é

19 0 22 8 19 0 26 16 8 0

Para obtermos os pares de texto comum, multiplica-se cada vetor cifrado pela inversa de A, onde a inversa de A é dada por $A^{-1} = (a_{11}a_{22} - a_{21}a_{12})^{-1} \begin{pmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{pmatrix} \pmod{m}$

Tem-se

$$A^{-1} = \begin{pmatrix} 22 & 18 \\ 0 & 15 \end{pmatrix} \quad \text{em} \quad \mathbb{Z}_{29}$$

Logo, para decodificar o par 19 0, faz-se a seguinte operação:

$$\begin{pmatrix} 22 & 18 \\ 0 & 15 \end{pmatrix} \begin{pmatrix} 19 \\ 0 \end{pmatrix} = \begin{pmatrix} 418 \\ 0 \end{pmatrix} = \begin{pmatrix} 12 \\ 0 \end{pmatrix}$$

E, assim por diante, até que todos os vetores tenham sido decifrados.

$$\begin{pmatrix} 22 & 18 \\ 0 & 15 \end{pmatrix} \begin{pmatrix} 22 \\ 8 \end{pmatrix} = \begin{pmatrix} 628 \\ 120 \end{pmatrix} = \begin{pmatrix} 19 \\ 4 \end{pmatrix}$$
$$\begin{pmatrix} 22 & 18 \\ 0 & 15 \end{pmatrix} \begin{pmatrix} 26 \\ 16 \end{pmatrix} = \begin{pmatrix} 860 \\ 240 \end{pmatrix} = \begin{pmatrix} 19 \\ 8 \end{pmatrix} \quad \text{em} \quad \mathbb{Z}_{29}$$
$$\begin{pmatrix} 22 & 18 \\ 0 & 15 \end{pmatrix} \begin{pmatrix} 8 \\ 0 \end{pmatrix} = \begin{pmatrix} 176 \\ 0 \end{pmatrix} = \begin{pmatrix} 2 \\ 0 \end{pmatrix}$$

Pela tabela dada anteriormente temos que os equivalentes alfabéticos desses vetores são:

MA TE MA TI CA

Que fornece a mensagem cifrada anteriormente.

Exercício 7.1. *Usando a cifra de Hill do exemplo acima, como seria codificada a mensagem*

"Deus é fiel"?

Use o alfabeto da tabela abaixo.

A	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*
0	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	*15*	*16*	*17*	*18*	*19*

U	*V*	*W*	*X*	*Y*	*Z*	*É*		*?*
20	*21*	*22*	*23*	*24*	*25*	*26*	*27*	*28*

Capítulo 8

Cripto-Sistemas

A mensagem a ser enviada é chamada de texto-original e a mensagem codificada é chamada de texto-cifrado. O texto-original e o texto cifrado são escritos em algum alfabeto P constituído de um certo número de símbolos. Isto é,

$$\#(P) = n$$

O texto-original e o texto cifrado são divididos em mensagens unitárias, que podem ser um bloco de k símbolos do alfabeto P. O processo de codificação é uma função que associa cada mensagem unitária m do texto-original a uma mensagem unitária c do texto-cifrado. Seja M o conjunto de todas as possíveis mensagens unitárias c do texto-cifrado. Então a correspondência biunívoca

$$f : M \longrightarrow C \qquad \text{tal que} \qquad f(m) = c$$

é o processo de codificação. A correspondência biunívoca

$$f^{-1} : C \longrightarrow M \qquad \text{tal que} \qquad f^{-1}(c) = m$$

é o processo de decodificaçao. Assim, temos o seguinte diagrama

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

8.1 Cripto-sistema

Um cripto-sistema é qualquer bijeção de M sobre C.

É útil substituir os símbolos de uma alfabeto P, por números inteiros $0, 1, 2, ...$, para tornar mais fácil a construção do cripto-sistema f. Uma correspondência que pode ser feita entre o alfabeto

$$P = \{A, B, C, ..., X, Y, Z, \text{É}, , , ?\}$$

e o conjunto dos números inteiros

$$\mathbb{Z}_{29} = \{0, 1, 2, ..., 25, 26, 27, 28\}$$

é a seguinte

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19

U	V	W	X	Y	Z	É	,	?
20	21	22	23	24	25	26	27	28

De forma geral pode-se rotular mensagens unitárias, com blocos de k símbolos, de um alfabeto P de n símbolos, por inteiros do conjunto

$$\mathbb{Z}_{n^k} = \{0, 1, 2, ..., n^k - 1\}$$

do seguinte modo:

$$(x_{k-1}, ..., x_1, x_0) \in \mathbb{Z}_{n^k} \Leftrightarrow x_{k-1}n^{k-1} + ... + x_1 n + x_0 n^0 \in \mathbb{Z}_{n^k},$$

onde cada x_i corresponde a um símbolo do alfabeto P. Por exemplo, a mensagem unitária com blocos de quatro símbolos

"AMOR

corresponde ao inteiro

$$0.29^3 + 12.29^2 + 14.29 + 17.29^0 = 10515 \in \mathbb{Z}_{29^4}$$

Observação 1. *O cripto-sistema*

$$f(x) = ax + b$$

é chamado de transformação afim. O par (a, b) é chamado de chave de codificação ou chave secreta. Quando $n = 27$, $a = 1$ e $b \in \mathbb{Z}_{27}$, o cripto-sistema

$$f(x) = ax + b$$

é chamado de Cifra de César, pois Júlio César a utilizava. Quando $b = 0$*, o cripto-sistema*

$$f(x) = ax$$

é uma transformação linear

Exemplo 8.1. *A correspondência biunívoca entre o alfabeto* P *e os números inteiros é dado pela tabela*

A	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*
0	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	*15*	*16*	*17*	*18*	*19*

U	*V*	*W*	*X*	*Y*	*Z*	*É*	*,*	*?*
20	*21*	*22*	*23*	*24*	*25*	*26*	*27*	*28*

Seja o símbolo $x \in \mathbb{Z}^{29}$ *correspondendo a uma mensagem unitária com blocos de um símbolo do texto-original. Assim, com* $a = 5$ *e* $b = 2$*, temos que a função*

$$f : \mathbb{Z}_{29} \longrightarrow \mathbb{Z}_{29} \qquad \textit{dada por} \qquad f(x) = 5x + 2$$

é um cripto-sistema. Portanto, para decodificar o texto-original

"CRIPTOGRAFIA"

primeiro calculamos

$$f(2) = 12,\ f(17) = 0,\ ...,\ f(8) = 13,\ f(0) = 0,$$

logo a mensagem cifrada é

"MANTKODAC,NC"

Para decodificar a mensagem cifrada, primeiro calculamos

$$f^{-1}(x) = 6x - 12$$

e depois

$$f^{-1}(12) = 2,\ f^{-1}(0) = 17,\ ...,\ f^{-1}(13) = 8,\ f^{-1}(2) = 0,$$

Logo a mensagem decifrada é

"CRIPTOGRAFIA"

Exercício 8.1. *Usando o cripto-sistema acima, como ficaria codificada a mensagem:*

O melhor São João do mundo fica em Campina Grande.

a correspondência biunívoca entre o alfabeto P e os números inteiros é dado pela tabela

A	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*
0	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	*15*	*16*	*17*	*18*	*19*

U	*V*	*W*	*X*	*Y*	*Z*	*Ã*		.
20	*21*	*22*	*23*	*24*	*25*	*26*	*27*	*28*

Exercício 8.2. *Usando o cripto-sistema acima, como ficaria codificada a mensagem*

O melhor da Paraíba, é o Campinense Clube

a correspondência biunívoca entre o alfabeto P e os números inteiros é dado pela tabela

A	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*
0	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	*15*	*16*	*17*	*18*	*19*

U	*V*	*W*	*X*	*Y*	*Í*	,		*É*
20	*21*	*22*	*23*	*24*	*25*	*26*	*27*	*28*

Capítulo 9

Criptografia RSA

A criptografia de chave pública RSA surgiu em 1978 e tem esse nome devido as iniciais dos inventores **R**ivest, **S**hamir e **A**dleman. É considerado o método mais utilizado na criptografia com chave pública.

A criptografia RSA baseia-se no fato da simplicidade de calcular o produto de dois números primos grandes. Em contrapartida, a segurança do RSA reside na inviabilidade de fatorar um número gigantesco.

Na criptografia RSA, utiliza-se duas chaves: uma privada e uma pública. A chave privada é formada por um par de números (N,d). Já a chave pública é formada por outro par (N,e). Note que o número N é comum a ambas as chaves.

Na codificação, Alice utiliza o seguinte algoritmo para cifrar a mensagem

$$C = P^e \, mod \, N$$

na qual, P é o texto original (texto limpo), que é representado por um número; C é um número que representa o texto cifrado. Os números e e N são os componentes da chave pública. O texto limpo é gerado por meio de $P = C^e \, mod \, N$. Deve-se ressaltar que o termo *mod* representa o resto da divisão de P por N, e esse resto é enviado como o texto cifrado.

Na decodificação, Bob usa o seguinte algoritmo para decifrar a mensagem

$$P = C^d \, mod \, N$$

Os números d e N são os componentes da chave privada.

9.1 Chaves Pública e Privada

Uma questão primordial na criptografia RSA é a escolha adequada para os três números N, d e e que compõem as chaves pública e privada. Estes números são fundamentais no processo de cifragem e decifragem do texto. A seguir descreveremos o procedimento padrão para geração dos números das chaves.

1. Escolha dois números primos grandes. Denote-os por p e q.
2. Calcule $N = p \times q$
3. Escolha e (menor que N) tal que e e $(p-1)(q-1)$ sejam primos entre si, isto é, não tem nenhum divisor comum, exceto o número 1.
4. Escolha d tal que $(e \times d)\, mod\, [(p-1)(q-1)] = 1$.

Este procedimento foi desenvolvido pelos inventores da criptografia RSA e é baseado em resultados obtidos da teoria dos números.

Capítulo 10

Conclusão

Com a realização desse trabalho algumas definições, teoremas e conjecturas associados aos números primos foram destacadas. Em especial, a conjectura de Goldback que afirma que todo inteiro positivo par pode ser escrito como soma de dois primos.

O método clássico do Crivo de Eratóstenes foi implementado em linguagem Matlab o que propiciou um bom aprendizado com alguns fundamentos em programação, e sobretudo, explorar os poderosos recursos disponibilizados pelo Matlab que é considerado uma ferramenta essencial para estudantes das ciências exatas. Desta forma, este trabalho pretende contribuir para que outros alunos venham a se interessar a utilizar o Matlab.

No estudo feito sobre criptografia foi apresentado um pouco da história da criptografia, principais tipos de cifras e conceitos matemáticos associados à criptografia.

Referências Bibliográficas

[1] Coelho S. P; Milies C. P. *Números: Uma Introdução a Matemática*. Edusp - Editora da Universidade de São Paulo, 3ª Edição, 2006 - São Paulo - SP - Brasil.

[2] Shokranian S, Soares M e Godinho H. *Teoria dos Números*. Editora Universidade de Brasília, 2ª Edição, 1999.

[3] Forouzan B. A, *Comunicação de Dados e Redes de Computadores.* Editora Bookman, 3ª Edição, 2006. Porto Alegre.

[4] Kurose J. F, Ross K. W. *Redes de Computadores e Internet - Uma abordagem top-down.* Editora Pearson Addison Wesley. 3ª Edição, 2006. São Paulo - SP.

[5] Filho D. C. M, *Um Convite à Matemática - Fundamentos-Lógicos com Técnicas de Demonstração, Notas Históricas e Curiosidades*, Editora Universitária da Universidade Federal de Campina Grande (EDUFCG), 2ª Edição, 2007.

[6] *Enciclopédia Brasileira Globo.* 19ª Edição, Editora Globo, Porto Alegre, 1981.

[7] http://www.dec.ufcg.edu.br/biografias/ChrstiaG.html (Consultado em novembro de 2011).

[8] http://primes.utm.edu/mersenne/index.html (Consultado em novembro de 2011).

[9] Coutinho, S.C., *Números Inteiros e Criptografia RSA*; IMPA, Rio de Janeiro, 2000.

[10] Andrade, A.S.,*Números, Relações e Criptografia*, UFPB, João Pessoa, 1997.

[11] Hefez, A., *Curso de Álgebra*, Volume 1.(3ª edição) IMPA, Rio de Janeiro, 2000.