UNIVERSIDADE ESTADUAL DO CEARÁ

CENTRO DE CIÊNCIAS E TECNOLOGIA

CURSO DE MESTRADO PROFISSIONAL EM MATEMÁTICA

RAFAEL PEREIRA DE MELO

NÚMEROS PRIMOS: HISTÓRIA, TÓPICOS, CRIPTOGRAFIA E O ENSINO DA MATEMÁTICA

FORTALEZA – CEARÁ

2014

RAFAEL PEREIRA DE MELO

NÚMEROS PRIMOS: HISTÓRIA, TÓPICOS, CRIPTOGRAFIA E O ENSINO DA MATEMÁTICA

Dissertação apresentada ao Curso de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT do Centro de Ciências e Tecnologia da Universidade Estadual do Ceará, como requisito parcial para a obtenção do título de Mestre em Matemática.

Orientador: Prof. Dr. João Marques Pereira

FORTALEZA – CEARÁ

2014

Dados Internacionais de Catalogação na Publicação

Universidade Estadual do Ceará

Biblioteca Central Prof. Antônio Martins Filho

Bibliotecário(a) Responsável – Meirilane Santos de Morais CRB-3 / 785

M528n Melo, Rafael Pereira de

Números primos: história, tópicos, criptografia e o ensino da matemática / Rafael Pereira de Melo. — 2014.

CD-ROM. 59 f. : il. (alguns color) ; 4 ¾ pol.

“CD-ROM contendo o arquivo no formato PDF do trabalho acadêmico, acondicionado em caixa de DVD Slin (19 x 14 cm x 7 mm)”.

Dissertação (mestrado) – Universidade Estadual do Ceará, Centro de Ciências e Tecnologia, Curso de Mestrado Profissional em Matemática, Fortaleza, 2014.

Orientação: Prof. Dr. João Marques Pereira.

1. Números primos - História . 2. Teoremas. 3. Criptografia. I. Título.

CDD: 510

RAFAEL PEREIRA DE MELO

NÚMEROS PRIMOS: História, Tópicos, Criptografia e Ensino da Matemática

Dissertação apresentada ao Curso de Mestrado Profissional em Matemática em Rede Nacional (PROFMAT) do Centro de Ciências e Tecnologia (CCT) da Universidade Estadual do Ceará, como requisito parcial para a obtenção do Título de Mestre em Matemática, Área de Concentração Matemática.

Aprovada em: 24/03/2014.

BANCA EXAMINADORA

Prof. Dr. João Marques Pereira
Orientador e Presidente da Banca Examinadora
Universidade Estadual do Ceará – UECE/PROFMAT

Prof.Dr. José Robério Rogério
Universidade Federal do Ceará – UFC

Prof. Dr. João Montenegro de Miranda
Universidade Estadual do Ceará – UECE/PROFMAT

Epígrafe

“O homem é formado por corpo, mente e imaginação. O corpo é defeituoso, a mente mentirosa, mas a imaginação fez dele um ser notável”.

John Masefield (1878 -1967)

AGRADECIMENTOS

A Deus em primeiro lugar.

A minha esposa Carla por dar todo o apoio que precisei ao longo dessa jornada, na qual presenciamos um milagre de Deus que é o nosso lindo filho Rafael, que nasceu de 5 meses durante o processo de desenvolvimento deste trabalho. Amo muito vocês.

Aos meus pais, Moacir e Eleusina, pelo amor, carinho e compreensão; aos meus irmãos, Andréa e Daniel, pelo apoio e torcida. Vocês fazem parte dessa conquista; a minha sogra Nazaré, que me apoiou e acolheu como um filho durante toda essa jornada.

Ao meu grande amigo Pedro Gurgel, que foi de fundamental importância no desenvolvimento deste trabalho.

Aos meus colegas de trabalho, que compreenderam as minhas ausências para concluir este trabalho.

Aos meus colegas da primeira turma do Profmat, que sabem qual é o real valor dessa conquista.

Ao meu orientador Prof. João Marques, que sempre me atendeu prontamente.

Ao nosso querido coordenador local do Profmat, Prof. Guilherme Ellery, que abraçou a causa do curso.

Aos demais professores do nosso mestrado, em especial, João Montenegro, Cleiton Vasconcelos e Othor Lopes.

A todos que fazem parte de minha vida e que contribuíram direta, ou indiretamente, a chegar tão longe, o meu muito obrigado.

RESUMO

Neste trabalho é feito um estudo sobre os números primos, citando parte da sua história, alguns dos problemas sem soluções deste tópico, teoremas e resultados importantes a eles relacionados. Também faremos uma introdução ao estudo da criptografia, apresentando a relação entre criptografia e números primos. Temos então o sistema de criptografia RSA, um dos mais importantes sistemas utilizados nas aplicações comerciais em todo mundo. Concluindo com uma reflexão sobre a instrução desse tópico nos diversos níveis de ensino.

Palavra chave: Números primos, Historia dos números primos, Teoremas, Criptografia RSA, Ensino dos números primos.

ABSTRACT

This paper made a study of prime numbers, citing part of their history, some of the problems without solutions in this topic, important theorems and results related to them. We will also do an introduction to the study of cryptography, showing the relationship between prime numbers and encryption. We have then the RSA encryption system, one of the most important systems used in commercial applications worldwide. Concluding with a reflection on the instruction of this topic in different levels of education.

Keyword: Prime numbers, History of prime numbers, theorems, RSA encryption, School of primes.

LISTA DE TABELA

LISTA DE FIGURAS

SUMÁRIO

INTRODUÇÃO

Ao estudarmos os números primos nos anos iniciais da educação básica, na maioria das vezes, somos apresentados a esse Tópico da Matemática por sua definição: *Um número inteiro n, maior do que um, cujos os únicos divisores positivos são o próprio n e a unidade é chamado de número primo. Se o inteiro n maior do que um não é primo, diremos que ele é composto.* Raramente recebemos, durante as aulas, indagações que nos levem ao entendimento de como surgiu o estudo dos números primos, suas curiosidades e os pensadores por trás dessas questões. O estudo dos números primos nos anos iniciais da educação básica se restringe ao cálculo de MMC (mínimo múltiplo comum) e MDC (máximo diviso comum). Deixando de lado, assim, o fato de que os números primos tem um papel significativo na História da Matemática, bem como possuem grande importância na matemática escolar do ensino fundamental, no sentido de orientar os alunos a compreender que os questionamentos adequados podem nos levar a descobertas fascinantes ou ao desenvolvimento de raciocínios notáveis, que é um dos principais papéis do ensino de matemática na educação básica (PCN).

Questões envolvendo os números primos surgiram na Matemática, desde o tempo de Pitágoras, passando por Euclides e chegando aos nossos dias com muitas perguntas que ainda não foram respondidas (conjecturas).

Segundo [BOYER, 1996], durante parte da história, grandes matemáticos, como Euclides de Alexandria (360 a.C. - 295 a.C.), Pierre de Fermat (1601 - 1665), Leonhard Euler (1707 - 1783), Carl Friedrich Gauss (1777 - 1855) e Georg Friedrich Bernhard Riemann (1826 - 1866), entre outros, desenvolveram pesquisas envolvendo teorias dos números, particularmente os números primos. E seus trabalhos acabaram por estruturar esse ramo da matemática e por influenciar várias outras áreas, como por exemplo, a matemática computacional.

A segurança de informações via internet, utiliza um sistema fortemente baseado nos números primos, como veremos ao estudarmos criptografia RSA.

A estrutura deste trabalho está assim distribuída.

No capítulo 1 apresentaremos um pouco da história dos números primos a partir da ideia de Pitágoras, passando por Euclides, Euler, Fermat, entre outros matemáticos, até os dias atuais. No capítulo 2 serão discutidos alguns teoremas que

envolvem os números primos, como a infinitude dos números primos, o Pequeno teorema de Fermat e os testes de primalidade como o Crivo de Erastóstenes, teorema de Wilson entre outros. No capítulo 3 apresentaremos quatro conjecturas sobre números primos. No capítulo 4 mostraremos como os números primos são usados na criptografia RSA e porque ela é segura. E no capítulo 5 faremos uma reflexão sobre o ensino da matemática na educação, em particular os números primos.

OBJETIVO

OBJETIVO GERAL

Fazer um estudo sobre os números primos no contexto da sua história, teoria, conjecturas e aplicações.

Sugerir uma metodologia para trabalhar os números primos no ensino fundamental e médio.

OBJETIVO ESPECIFICO

Para alcançar o objetivo geral, o trabalho foi dividido nos seguintes tópicos:

i) Um pouco sobre a história dos números primos;

ii) Alguns fatos e conjecturas sobre os números primos e apresentar uma de suas aplicações;

iii) Uma reflexão sobre o ensino dos números primos.

CAPÍTULO 1 – FATOS IMPORTANTES SOBRE OS NÚMEROS PRIMOS

1.1 O número primo na Grécia Antiga

Ao longo da história da humanidade, pode-se perceber a clara evolução das ideias e pensamentos, desde conceitos sobre as coisas concretas (descobertas pela observação e pelo empirismo), até formalizações mais abstratas (descobertas vindas da capacidade de projetar o imaginário). Entre as ideias abstratas, destaca-se a criação dos números, em especial dos números inteiros.

Os registros dos estudos dos números inteiros e suas propriedades mostram que este tópico é discutido desde as civilizações mais antigas, conforme [BOYER, p 42]. Devido a grande importância dos números primos na composição dos números inteiros, os números primos foram objetos de estudos por renomados matemáticos.

É possível que os primeiros estudos sobre os números primos venha da Escola Pitagórica por volta de 530 a.C. que já compreendia a ideia de primalidade e estudava os números perfeitos (a soma dos divisores de determinado número com exceção dele mesmo, é o próprio número) e os números amigáveis (são dois números onde cada um deles é a soma dos divisores positivos do outro). Os números primos eram chamados por eles de lineares, por serem representados por pontos agrupados em linha. Já os números não-primos poderiam ser representados por pontos formando retângulos, dando a ideia de que os números lineares (primos) seriam os geradores desses outros. Outro fato chamativo era que para os pitagóricos [BOYER, p 42] o número dois não era considerado um número primo. Para eles o número um e o número dois não seriam números verdadeiros, mas geradores de números ímpares e pares.

Embora acredite-se que os números primos inicialmente foram estudados por Pitágoras, é impossível ter completa segurança sobre esses fatos, já que Pitágoras não deixou registros escritos sobre seus trabalhos, os documentos mais antigos que falam a respeito de suas ideias, vêm de fragmentos de textos de muitas

gerações depois dele, mas, embora raros, tais fragmentos são unanimes em atribuir a Pitágoras os primeiros estudos sobre os números primos.

Os gregos antigos tinham conhecimentos relevantes acerca dos números primos. Foi com Euclides que alguns desses conceitos tomaram a forma que até hoje são encontradas nos livros didáticos.

Dentre os fatos da teoria dos números que os gregos já conheciam, podemos citar:

- o cálculo do máximo divisor comum entre dois números;
- a determinação dos números primos menores que um inteiro dado;
- a infinitude dos números primos.

Estes problemas são registrados num dos mais famosos trabalhos da Grécia antiga, os *Elementos* de Euclides. Euclides viveu em Alexandria por volta de 300 a.C.. e sua obra "Os Elementos" é composta por treze livros, e são nos livros VII, VIII e IX, que encontramos questões com teoria dos números. No livro VII encontramos as definições de números primos, como: **"protós arithmós estin monadi mone metroymenos".** Ou seja: Número primo é todo aquele que só pode ser medido através da unidade. Nesse livro encontramos, ainda, um dos principais teoremas dessa área, hoje conhecido como "Algoritmo de Euclides" (método para achar o máximo divisor comum entre dois números). O livro VIII fala principalmente das propriedades das progressões geométricas. Já no livro IX, BOYER [p 79] nos diz que:

> *"O Livro IX, o último dos três sobre teoria dos números, contêm vários teoremas interessantes. Desses, o mais célebre é a Proposição 20: 'Números primos são mais do que qualquer quantidade fixada de números primos. ' Isto é, Euclides dá aqui a prova elementar bem conhecida do fato de que há infinitos números primos. A prova é indireta, pois mostra-se que a hipótese de haver somente um número finito de primos leva a uma contradição".*

Apresentaremos essa demonstração no segundo capítulo deste trabalho.

Outro grego que trabalhou com os números primos, foi Eratóstenes de Alexandria, no século III a.C.. Ele foi o primeiro a criar uma tabela de números

primos: o crivo de Eratóstenes. O motivo desse nome era porque seu método consistia em montar uma tabela com os números de dois até N, onde N era um número natural qualquer. Como o 2 (dois) era o menor número primo (o número 1 (um) não satisfazia as definições de primos), tinha-se que todos os múltiplos de 2 (dois), exceto o próprio 2 (dois), eram furados, ou seja, “crivados” na tabela, o próximo número que não tinha sido “crivado” era o 3 (três), que é primo, logo todos os múltiplos de 3 (três) eram “crivados”, com exceção do próprio 3 (três). O próximo número não crivado era o 5 (cinco), que também é primo. Continuando nessa sequencia, todos os números compostos eram “crivados” sobrando somente os números primos finitos até o número N.

A seguir mostramos uma imagem do crivo de Eratóstenes, em que os números amarelos representam números primos.

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

Figura 1. Imagem do Crivo de Eratóstenes

Vale ressaltar que essa metodologia é utilizada ainda nos dias de hoje por muitos. Quando se quer determinar a quantidade de números primos, em um intervalo de números inteiros de 1 a n, com n grande.

Essa parte da matemática foi estudada também por outros gregos, como Diofanto de Alexandria (200 d.C. – 298 d.C.). A Aritmética deste tratava principalmente da solução de equações indeterminadas com coeficientes inteiros. No entanto, foi só por volta do ano 500 d.C. que os números primos começam a sair da Grécia e ganha o mundo. Tendo como marco, o primeiro livro que foi escrito em latim sobre teoria dos números, que é o *De Institutione Arithmetica*, do romano Boethius.

É neste livro de Boethius que aparece, pela primeira vez, a expressão '*numerus primus*' como tradução do tradicional '*protós arithmós'*, encontrada nos Elementos de Euclides. Esse foi, durante aproximadamente seiscentos anos, a única fonte de pesquisa sobre Teoria dos Números disponível na Idade Média. No inicio do renascimento científico e matemático pela Europa, cerca de 1200 d.C. é que começam a surgir obras árabes e a tradução das obras gregas preservadas no Mundo Islamita. É dessa época (1200 d.C.) um dos mais influentes livros da Matemática: *o Liber Abacci*, de Fibonacci. Esse grande matemático, que havia estudado entre os muçulmanos do Norte da África, diz que acha melhor dizer primus em vez do incomposto preferido pelos árabes. Ficou assim, definitivamente, consagrada a denominação "número primo" na Europa.

1.2. Os estudos dos números primos na Europa

Em 1621, Bachet publicou o texto original, em grego, da Aritmética de Diofanto, traduzindo também para o latim, língua usada pelos estudiosos europeus da época. Em posse de uma dessas cópias, um magistrado da corte de Toulouse, o francês Pierre de Fermat (que não era matemático de profissão), em suas horas vagas leu o texto de Diofanto, o que o despertou para o aprofundamento e desenvolvimento de muitos resultados, levando-o a se tornar o fundador da moderna teoria dos números. [BOYER, p 258]

Embora algumas das suas conjecturas tenham se mostrado falsas, como a afirmação de que todo número na forma $2^{2^n}+1$ seria um número primo, que ficou conhecido como "números de Fermat" onde tínhamos $F_0 = 3, F_1 = 5, F_2 = 17 e F_4 = 65.537$ como números primos e que, posteriormente, Euler demonstrou ser uma afirmação falsa. Segundo [HEFEZ, p 98], "Em 1732, Leonhard Euler mostrou que

$F_5 = 2^{2^5} + 1 = 4.294.967.297 = 641x6.700.417$, portanto, composto, contradizendo assim a afirmação de Fermat". Essa conjectura foi tão explorada que hoje os matemáticos se inclinam em afirmar que existem somente esses cinco números de Fermat que são primos.

[BOYER, p 259] chega a colocar que "Fermat foi verdadeiramente, 'o príncipe dos amadores' em matemática". Referindo-se às descobertas e contribuições que ele fez, quando nenhum matemático de profissão contribuiu tanto quanto Fermat para o desenvolvimento desse assunto naquela época. Entretanto, Fermat fez poucas publicações, contentando-se em escrever a Mersenne, o que levou a associar o nome de Mersenne aos "Números de Mersenne" (números primos na forma $2^p - 1$).

Outro estudo desenvolvido por Fermat, foi o que hoje conhecemos por "Pequeno Teorema de Fermat", que mostrou-se verdadeiro e diz que se p é primo, e a e p são primos entre si (dois números são ditos primos entre si, quando o único divisor positivo comum é 1) , então $a^{p-1} - 1$ é divisível por p.

Esse teorema também será discutido no próximo capítulo.

Foi Euler que primeiro mostrou que esse teorema era verdadeiro, e a partir dele, percebeu um teorema mais geral: "se a e m são números naturais maiores do que 1, primos entre si, então $a^{\varphi\ m} - 1$ é divisível por m (onde φ é a função fi de Euler, isto é, $\varphi\ m$ é a quantidade de números naturais entre 0 e m – 1 que são primos com m)".

É importante pontuar que, Euler, apesar de suas contribuições, como esta supracitada, não publicou nenhum livro tratando desse assunto, tendo escrito, no entanto, muitas cartas e artigos sobre muitos aspectos da teoria dos números.

Outra questão a ser lembrada é que muitos teoremas propostos por matemáticos, ficaram sem suas demonstrações, e muitos deles viraram objeto de desejo de especialistas em teoria dos números, que buscam por fama e dinheiro, posto que, para algumas dessas proposições, são oferecidos prêmios em dinheiro para quem as demonstrar. Uma dessas proposições afamadas é determinar uma função que determine todos os números primos, assim várias fórmulas apareceram.

Um exemplo de proposição que surgiu foi a função f(n) = n² - n + 41, onde n é um número inteiro positivo. Função que, para $1 \leq n \leq 40$, fornece 40 números primos maiores ou iguais a 41, mas, como para n = 41 temos f(41) = 41² - 41 + 41 = 41², que é um número composto, isto é, o valor f(n) nem sempre é um número primo. Semelhantemente a função f(n) = n² - 79n + 1601, apresenta valores primos para n < 80.

Provavelmente um dos resultados mais surpreendentes a respeito da quantidade de números primos que são menores que um dado número inteiro positivo n muito grande, é o chamado "teorema dos números primos". Como explica [EVES, p 624]:

> *"Indiquemos por A_n o numero de primos abaixo de n. O teorema dos números primos assegura que $A_n \log_e^n n$ se aproxima de 1 conforme n cresce indefinidamente. Em outras palavras, A_n n, chamada densidade dos primos entre os primeiros n inteiros, aproxima-se de $1 \log_e^n$, tanto mais quanto maior for n. Esse teorema, que fora conjeturado por Gauss após o exame de uma grande tábua de números primos, foi provado independentemente, em 1896 pelo francês J. Hadamard e pelo belga C. J. de la Vallee Poussim".*

Esse teorema será discutido no capítulo 2.

1.3. Em busca do maior número primo.

Na procura de uma fórmula lógica que expressasse ou os números primos ou a quantidade de números com precisão, muitos matemáticos escreveram tábuas extensas desses números. Em 1659 o inglês J. H. Rahn (1622 – 1676) publicou como apêndice de um livro de álgebra uma tábua com números primos até 24.000 e em 1668 o também inglês John Pell estendeu essa tábua até 100.000. Já no século XIX, em um trabalho conjunto, os matemáticos Chernac, Burckhardt, Crelle, Glaisher e o "calculador relâmpago" Dase, montaram um tábua que cobriam todos os números até 10.100.000, publicado em dez livros. Mas a realização mais expressiva foi a tábua calculada por J. P. Kulik (1773 – 1863) da universidade de praga, seu trabalho que ainda não foi publicado é fruto de um passa tempo de 20 anos e cobre números até 100.000.000.

Por outro lado, com o desenvolvimento dos computadores modernos, o trabalho de verificar se um número é primo e de construir tábuas de primos especiais ficou cada fez mais fácil. Em novembro de 1980, a revista *Crux mathematicorum* publicou todos os números primos palíndromos de 5, 7 e 9 dígitos (um palíndromo é um número, do tipo 3.417.143, que quando lido de traz para frente é o mesmo número). Esses números foram calculados por um computador PDP-11/45 da Universidade de Waterloo e o tempo gasto nesse trabalho foi um pouco maior que um minuto.

Nos dias atuais, já é possível encontrar números primos com até 17 milhões de dígitos. Com o aumento desses números, os custos e o tempo gasto para determina-los ficaram muito grandes, visto que até mesmo um computador de altíssimo desempenho pode demorar semanas para rodar um algoritmo de busca desses primos com muitas casas decimais. O maior número primo conhecido até essa data é $2^{57.885.161} - 1$ calculado pelo projeto GIMPS.

Os números primos foram e ainda serão o objeto de trabalho de muitos matemáticos, por muito tempo, pois, como disse [SAUTOY. 2007, p.13]: “os primos são as pérolas que adornam a vastidão infinita do universo de números que os matemáticos explorarão ao longo dos séculos”.

CAPÍTULO 2 - Números primos: Teoremas e Testes

Conforme vimos no capítulo anterior, existem vários resultados acerca dos números primos que tem fundamental importância no desenvolvimento da Teoria dos Números. Neste capítulo mostraremos alguns desses resultados.

2.1. A infinitude dos números primo

Teorema 1*: Existem infinitos números primos*.

Antes de demonstrarmos a infinitude dos números primos, apresentaremos um lema.

Lema 1: O menor divisor inteiro positivo de um número natural maior do que 1 é um número primo.

Demonstração: Sejam $N \in \mathbb{N}$, N > 1 e $A = \{n \in \mathbb{N}\ n > 1\ e\ n\ N\}$. Temos

$A \neq \emptyset$, pois $N \in A$.

Pelo Principio da Boa Ordenação, o conjunto A possui um menor elemento p. O número p é um número primo, caso contraio p = ab, onde b > a > 1, dai $a\ p$, logo $a\ N$, contrariando o fato de que p é o elemento de A.

Demonstração 1 (Euclides): Suponhamos que exista um número finito de números primos, a saber, $p_1, p_2, \ldots, p_r$. Consideremos agora o número $N = p_1.p_2.p_3 \ldots p_r + 1$. Como N > 1, existe um primo p que divide N, portanto $p = p_i$ para algum i, então $p\ N = p_1.p_2.p_3 \ldots p_r + 1$, logo p divide 1 que é um absurdo.

Outra demonstração da infinitude dos números primos foi feita por Christian Goldbach (1690 - 1764) em uma carta escrita para Euler. Em sua demonstração Goldbach apresenta uma sequencia infinita $a_1 < a_2 < a_3 < \ldots$ de números naturais, sendo eles dois a dois primos entre si (ou seja, o MDC de dois números quaisquer dessa sequencia é igual a um).

Para esta demonstração, apresentaremos, antes, dois lemas a respeito dos números de Fermat.

Um número de Fermat é um número inteiro positivo na forma: $F_n = 2^{2^n} + 1$, sendo n um número inteiro positivo.

Lema 2: *Se F_m é o m-ésimo (m ≥ 1) número de Fermat, então $F_m - 2 = F_0F_1 \dots F_{m-1}$.*

Demonstração: Se F_m é um número de Fermat, então $F_m = 2^{2^m} + 1$. Logo,

$$F_m - 2 = F_0F_1 \dots F_{m-1} \Leftrightarrow 2^{2^m} - 1 = \ 2^{2^0} + 1 \ \ 2^{2^1} + 1 \ \dots \ 2^{2^{m-1}} + 1 \ .$$

Usaremos indução sobre m.

Demostraremos que:

$$2^{2^m} - 1 = \ 2^{2^0} + 1 \ \ 2^{2^1} + 1 \ \dots \ 2^{2^{m-1}} + 1$$

i) A igualdade é válida para m = 1, pois $2^{2^1} - 1 = 2^{2^0} + 1$.

ii) Supondo que a igualdade é válida para m, iremos mostrar a validade para m+1 > 1. Multiplicando os dois membros da expressão,

$2^{2^m} - 1 = \ 2^{2^0} + 1 \ \ 2^{2^1} + 1 \ \dots \ 2^{2^{m-1}} + 1$ por $2^{2^m} + 1$, temos:

$$F_0F_1 \dots F_m = \ 2^{2^0} + 1 \ \ 2^{2^1} + 1 \ \dots \ 2^{2^{m-1}} + 1 \ \ 2^{2^m} + 1 \ = \ 2^{2^m} - 1 \ \ 2^{2^m} + 1$$
$$= 2^{2^{m+1}} - 1 = F_{m+1} - 2$$

Logo, a igualdade é válido para todo $m \in N$.

Lema 3: *Os números de Fermat $F_n = 2^{2^n} + 1$ (para n ≥ 0) são, dois a dois primos entre si.*

Demonstração: Pelo Lema 2, $F_m - 2 = F_0F_1 \dots F_{m-1}$. Se $n \in N$, n < m, F_n divide $F_m - 2$. Se tivéssemos um número p primo que dividisse F_n e F_m, então p dividiria $F_m - 2$, portanto dividiria o 2, mas como p é primo, p = 2, que é um absurdo, já que todos os números de Fermat são ímpares.

Considerando o Lema 2, apresentaremos outra demonstração do Teorema 1.

Demonstração 2: Seja p_i o menor divisor positivo de F_i; i = 0, 1, 2, ... Então a sequência $p_0, p_1, p_2 \dots, p_r, \dots$ é formada por primos e é infinita, uma vez que $F_0, F_1, F_2, \dots, F_r, \dots$ são primos entre si, logo existem infinitos primos.

Outra demonstração interessante a respeito da infinidade dos números primos é que existem infinitos números primos da forma 6k+5.

Para a demonstração vamos usar a seguinte proposição e o teorema.

Proposição 1: Se a, b, c, m e n são inteiros, $c \ a$ e $c \ b$ então $c \ (ma + nb)$.

Demonstração: Se $c \ a \ e \ c \ b$ então $a = k_1 c$ e $b = k_2 c$. Multiplicando as duas equações por m e n respectivamente teremos $ma = mk_1 c$ e $nb = nk_2 c$. Somando as duas equações membro a membro obtemos $ma + nb = (mk_1 + nk_2)c$, o que nos diz que $c \quad ma + nb$.

Demonstração 3 (do teorema 1): Quando dividimos um número qualquer por 6, temos os possíveis restos: 0,1,2,3,4,5; ou seja, podemos escrever um inteiro da seguinte forma: 6k, 6k+1, 6k+2, 6k+3, 6k+4, 6k+5.

Se p é primo e diferente de 3, então p é da forma 6k+1 ou 6k+5. Vamos supor que exista uma quantidade finita de números primos da forma 6k+5, então $p_0 = 5, p_1, p_2, \dots, p_r$ números primos, considere $P = 6p_1 \dots p_r + 5$, pela proposição 1, temos que P não é divisível por nenhum p_i, para todo $i \in \{0, 1, \dots, r\}$, pois se $p_i \ P$, então $p_i \ 6p_1 \dots p_r + 5$, que é um absurdo, pois p_i teria que dividir 5. Portanto, P é primo e não se tem mais nada a provar ou P possui algum fator primo da forma 6k+5, pois se todos os fatores de p fossem da forma 6k+1 implicaria que o produto dos fatores continuaria 6k+1, que é uma contradição pela hipótese de P.

2.2. Teorema Fundamental da Aritmética

Esse teorema, um dos mais importantes da Teoria dos Números é encontrado nos Elementos de Euclides.

Teorema 2: *(Teorema Fundamental da Aritmética). Todo número natural maior do que 1 ou é primo ou se escreve de modo único (exceto pela ordem dos fatores) como um produto de números primos*.

Demonstração: Seja n $\in N$, se n for primo não há nada a ser demonstrado. Suponhamos que n seja composto. Tomemos p_1 (p_1 > 1) o menor divisor positivo de n; p_1 é primo, então $n = p_1.n_1$.

Se n_1 for primo a demonstração estará completa. Se não, tomemos p_2 como o menor fator inteiro positivo de n_1. Então p_2 é primo, logo n = $p_1.\ p_2.\ n_2$.

Aplicando o processo acima um número finito de vezes, obtemos n como o produto de primos. Como não necessariamente todos os fatores serão distintos, podemos ter fatores repetidos.

Para mostrar a unicidade, usaremos indução sobre n. Para n = 2 essa afirmação é verdadeira.

Agora suponha que para todos os números inteiros maiores que 1 e menores que n seja verdadeira a unicidade. Vamos provar que ela é verdadeira para n.

Se n for primo, já está provado.

Suponha, então, que n é composto, e que tenha duas formas de fatoração, ou seja, $n = p_1.p_2 \ldots p_r = q_1.q_2 \ldots q_s$.

Vamos mostra que r = s e que $p_i = q_j$. Como p_1 divide n, então divide $q_1.q_2 \ldots q_s$, e como todos q_j são primos, p_1 divide algum q_j.

Sem perda de generalidade podemos dizer que $p_1\ q_1$. Como os dois números são primos, temos que $p_1 = q_1$. Portanto $\frac{n}{p_1} = p_2 \ldots p_r = q_2 \ldots q_s$. Temos que 1 < $\frac{n}{p_1}$ < n, pela hipótese de indução as duas fatorações são idênticas, logo, s = r, portanto cada termo p_i é igual a q_i.

2.3. Pequeno Teorema de Fermat

Apresentaremos a demonstração do pequeno teorema de Fermat. Antes demonstraremos um lema.

Lema 4: *Se p um número primo, os números* $\binom{p}{i}$ *, onde 0 < i < p, todos divisíveis por p.*

Demonstração: Para a demonstração, basta usar a definição de $\binom{p}{i}$.

Temos, $\binom{p}{i} = \frac{p!}{i!\ p-i\ !} = \frac{p.\ p-1\ \ p-2\ \ldots\ p-i-1\ \ p-i\ !}{i!.\ p-i\ !} = p.\frac{p-1\ \ p-2\ \ldots\ p-i-1}{i!}$. E portanto $i!\ \binom{p}{i} = p.\ p-1\ \ p-2\ \ldots\ p-i-1$. Logo $p\ \ i!\ \binom{p}{i}$, com $1 \leq i \leq p-1$.

Temos que se $p\ \ i!\ \binom{p}{i}$, então $p\ i!$ ou $p\ \ \binom{p}{i}$, já que p é um número primo. p 1.2.3 … i, implica que $p\ j$ para algum j, onde $1 \leq j \leq i \leq p-1$, o que não acontece. Portanto p divide $p\ \ \binom{p}{i}$.

Teorema 3: *(Pequeno teorema de Fermat): Se p é um números primo, e se a um número natural, então , então* $a^p \equiv a\ mod\ p$. *Em particular se p não divide a, então* $a^{p-1} \equiv 1\ mod\ p$.

Demonstração: Usaremos indução sobre a.

i. Para a = 1 o resultado é valido.

ii. Supondo que o resultado é válido para a, vamos mostrar que também é válido para a + 1. Usando o desenvolvimento do binômio de newton,

$$a+1\ ^p - \ a+1\ = a^p - a + \binom{p}{1}\ a^{p-1} + \cdots + \binom{p}{p-1}\ a.$$

Pelo Lema 4 e pela hipótese de indução, o segundo membro da igualdade acima é divisível por p, logo o teorema é válido para todo $a \in N$. Portanto

$a^p \equiv a\ mod\ p$. Sendo $a^p \equiv a\ mod\ p$ tem se que $p\ a^p - a$. Como $a^p - a = a(a^{p-1} - 1)$ e p não divide a, então p divide $a^{p-1} - 1$. Isto é $a^{p-1} \equiv 1\ mod\ p$.

2.4. Crivo de Eratóstenes

O crivo de Eratóstenes, apresentado no capítulo um é um método eficaz para determinar quais números são primos dentro de um intervalo de 1 ate n, onde n é um número inteiro positivo. O próximo Teorema nos diz que para determinarmos

todos os primos de intervalo de 1 até n basta marcar (crivar) os múltiplos dos primos menores que $\overline{n}$.

Teorema 4: *Se n não é primo, então n possui, necessariamente, um fator primo menor que ou igual a* $\overline{n}$.

Demonstração: Se n é composto então $n = n_1.n_2$ onde $1 < n_1 \leq n_2 < n$. Portanto n_1 tem que ser menor ou igual a $\overline{n}$, caso contrario, $n = n_1.n_2 > \overline{n}.\ \overline{n} = n$. Portanto, pelo teorema fundamental da aritmética, n_1 possui algum fator primo p que deve ser menor ou igual a $\overline{n}$. Logo se p divide n_1, então divide n.

Na figura 1, no capítulo 1, temos todos os primos entre 1 e 100. Pelo teorema acima, bastaríamos excluir da tabela os números que são múltiplos dos primos menores que $\overline{100}$, ou seja, os primos menores que 10, que seriam os múltiplos de 2, 3, 5 e 7.

2.5. A distribuição dos números primos

Saber a localização exata dos números primos, ou descobrir uma fórmula que os determine, foi o objetivo de muitos matemáticos ao longo da história, estando entre eles o matemático alemão Johann Carl Friedrich Gauss. Porém, em vez de somente tentar localizar os números, ele começou a pensar em quantos primos existiam em um dado intervalo de números. Acredita-se que esse interesse surgiu após ele se deparar com um livro de logaritmo que continha, na contracapa, um tabela de números primos, onde ele percebeu uma possível regularidade nos intervalos de um primo para outro. BOYER [p 372].

Gauss estudou uma função, que posteriormente foi denotada de $\pi\ x$, definida como a quantidade de primos p, com p ≤ x. Assim, para x = 10, temos que $\pi\ 10\ = 4$; para x = 20, temos que $\pi\ 20\ = 7$; e para x = 100, $\pi\ 100\ = 25$ (Veja Crivo de Erastóstenes, figura 1, capítulo 1). Assim $\frac{\pi\ x}{x}$, é a probabilidade de um elemento do conjunto {1,2,3,...,x} ser primo.

Usando métodos computacionais é possível construir uma tabela que analise o comportamento dessa proporção, observe a tabela 1.

X	$\pi\ x$	$\frac{x}{\pi\ x}$
10	4	2,5
100	25	4,0
1.000	168	6,0
10.000	1.229	8,1
100.000	9.592	10,4
1.000.000	78.498	12,7
10.000.000	664.579	15,0
100.000.000	5.761.455	17,4
1.000.000.000	50.847.534	19,7
10.000.000.000	455.052.511	22,0

Tabela 1: proporção de primos até x

Uma tabela dessa foi desenvolvida por Gauss, mas em menor proporção, devida a dificuldade de trabalhar com números muito grandes. Foi percebido que na medida em que se multiplicava um número por dez, à proporção de primos era adicionado aproximadamente o valor de 2,3. Então, Gauss buscou trabalhar com uma função muito conhecida e fácil que transformasse multiplicação em soma, a função logarítmica. Logo, pensou em uma base *a* de modo que:

$\frac{x}{\pi\ x} = log_a^x \Leftrightarrow \frac{\pi\ x}{x} = \frac{1}{log_a^x}$Observando seus dados, concluiu que essa base poderia ser o número *e*, logo: $\frac{\pi\ x}{x} \approx \frac{1}{lnx} \Leftrightarrow \pi\ x\ \approx \frac{x}{lnx}$

Na figura 2, observamos um gráfico das duas funções e vemos que existe uma real semelhança no comportamento das duas funções no intervalo dado, embora exista diferença em relação à continuidade. Observa-se que, na estimativa feita por Gauss, na medida em que os valores aumentam, a curva da função $\frac{x}{lnx}$ vai ficando bem abaixo da função $\pi\ x$.

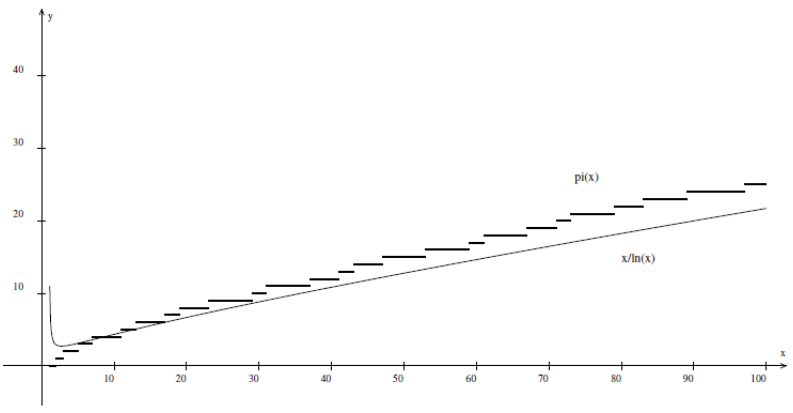

Figura 2: Gráfico conjunto de π(x) e x/lnx.

O matemático francês Jacques Hadamard (1865 – 1963) e o belga C. J. de la Vallé-Poussin (1866 – 1962), aproximadamente 1896, provaram que as curvas das funções $\pi\ x$ e $\frac{x}{lnx}$ são assintoticamente iguais, ou seja:

$$\lim_{x\to\infty} \frac{\pi\ x\ lnx}{x} = 1,$$

Este importante resultado ficou conhecido como Teorema dos Números Primos, que não será demonstrado neste trabalho devido a sua complexidade, mas se encontra no apêndice do livro *Teoria dos números: um passeio com primos e outros números familiares pelo mundo inteiro* do autor Fábio Brochero Martinez. A distribuição dos primos é discutida em detalhes nos livros Hardy e Wright 1994, Cap. XXII e Ingham 1932.

2.6. Teste de primalidade

Atualmente existem mais de uma centena de testes de primalidade, cada um deles com uma fundamentação teórica diferente. Um destes testes é o chamado "Teorema de Wilson". Esse teorema foi atribuído a John Wilson (1741 – 1793), mas foi provado, pela primeira vez pelo matemático italiano J. L. Lagrange (1736 – 1813).

Teorema 5: (Teorema de Wilson) *p é primo se, e somente se,* $p - 1\ ! \equiv p - 1\ mod\ p$.

Antes de demonstrarmos este teorema, apresentaremos uma proposição.

Proposição 2: Seja p > 2 um primo e seja 2 ≤ a ≤ (p−2). Então existe um único b ∈ {2, . . . , p−2} tal que $ab \equiv 1\ mod\ p$. Além disso, a ≠ b.

Demonstração: A congruência $ax \equiv 1\ mod\ p$ possui uma única solução $x = b \in \{1, 2, \dots, p - 2\}$. Necessariamente b ≠ 1 e b ≠ p – 1, pois $a \not\equiv 1\ mod\ p$. Portanto 2 ≤ b ≤ p – 2.

Agora vamos demonstrar o Teorema de Wilson.

Demonstração: Escrevemos o conjunto {2, 3,..., p – 2} sob os aspectos da proposição 2: Para todo $a \in \{2, \dots, p - 2\}$ existe um único $b \in \{2, \dots, p - 2\}$ com

$ab \equiv 1\, mod\, p$ e a ≠ b. podemos reordenar o conjunto {2, 3,..., p – 2} = $\{a_1, b_1, a_2, b_2, \dots, a_{\frac{p-3}{2}}, b_{\frac{p-3}{2}}\}$, onde $a_1 b_1 \equiv a_2 b_2 \equiv \cdots \equiv a_{\frac{p-3}{2}} b_{\frac{p-3}{2}} \equiv 1\, mod\, p$. Portanto

$p-1\,! = 1.2 \dots\ p-2\ \ p-1\ = 1.\ a_1 b_1\ \ a_2 b_2\ \dots\ a_{\frac{p-3}{2}} b_{\frac{p-3}{2}}\ \ p-1\ \equiv$

$1.1.1.1 \dots 1.\ p-1\ \equiv\ p-1\ mod\, p.$

Decorre do Teorema de Wilson, em que p é primo se, e somente se, $p-1\,! + 1 \equiv 0\, mod\, p$, pois:

$$p-1\,! \equiv p-1\ \equiv -1\, mod\, p \Rightarrow\ p-1\,! + 1 \equiv 0\, mod\, p.$$

2.7. Teste de Lucas-Lehmer

Outro teste, que é considerado um dos mais eficientes, segundo o Great Internet Mersenne Prime Search (GIMPS) (projeto que busca encontra o maior número primo), é o chamado “teste de Lucas-Lehmer”. Elaborado originalmente pelo matemático francês Édouard Lucas (1842 – 1891) que foi o criador do jogo matemático “Torre de Hanoi” e melhorado pelo matemático americano D. H. Lehmer (1905 -1991).

Antes de apresentarmos o teste de Lucas-Lehmer, precisamos definir o que é o número de Mersenne.

Um número da forma $\mathrm{M_q} = 2^{\mathrm{q}} - 1$, sendo q um número primo é chamado de número de Mersenne.

Outro fator importante para apresentarmos esse teste, é obtermos uma sequência de inteiros positivos $S_o, S_1, S_2, \dots$, definida recursivamente por $S_0 = 4$ e $S_{k+1} = S_k^2 - 2$.

Mostraremos, em primeiro lugar, que os inteiros dessa sequência podem ser escritos como potências de números irracionais.

Seja $\omega = 2 + \sqrt{3}$ e $\overline{\omega} = 2 - \sqrt{3}$. Vamos mostrar essa recorrência por indução em n que $\omega^{2^n} + \overline{\omega}^{2^n} = S_n$.

i. Para n = 0 o resultado é verdadeiro, pois $\omega + \overline{\omega} = S_0$;

ii. Supondo que para n – 1, seja verdade, vamos provar para n.

$$\omega^{2^{n-1}} + \overline{\omega}^{2^{n-1}} = S_{n-1}.$$

Elevando os dois membros ao quadrado, temos

$$\omega^{2^{n-1}} + \overline{\omega}^{2^{n-1}\ \ 2} = S_{n-1}^2$$

$$\omega^{2^n} + 2(\omega\overline{\omega})^{2^{n-1}} + \overline{\omega}^{2^n} = S_{n-1}^2.$$

Como $\omega\overline{\omega} = 1$, temos que

$$\omega^{2^n} + \overline{\omega}^{2^n} = S_{n-1}^2 - 2 = S_n.$$ (por definição)

Teste de Lucas-Lehmer: *Seja p um primo positivo. O número de Mersenne M(p) é primo se, e somente se,* $S_{p-2} \equiv 0 \ \ mod M_p$.

A demonstração desse teste não será apresentada neste trabalho, mas essa demonstração pode ser encontrada em [Bressoud 1989, Teorema 11.10, p. 175]. Contudo, iremos exemplificar o teste de Lucas.

Ex: Vamos testar a primalidade do número de Mersenne $M_5 = 31$.

Temos, $S_0 = 4, S_1 = 4^2 - 2 = 14, S_2 = 14^2 - 2 = 194$ e $S_3 = 194^2 - 2 = 37634$, portanto $37634 \equiv 0 \ \ mod M_5$, logo M_5 é primo.

Embora esse teste seja um pouco mais difícil de provar, ele é muito fácil de implementa e de usar. Como foi dito no inicio desta seção, esse teste é a base para o cálculo dos primos de Mersenne da GIMPS. Esse projeto não produz nenhum avanço conceitual em termos de números primos e em relação à teoria dos números, é uma mera curiosidade. Permite, porém, uma visão ampla sobre a distribuição dos números primos em termos dimensionais. Já para a computação algébrica é um avanço considerável, em termos conceituais e técnicos, com a utilização de computação distribuída, criando e desenvolvendo novas técnicas.

Para obter os programas do GIMPS, basta visitar o site (http://www.mersenne.org/) que oferece programas de graça (com código fonte) de modo que qualquer pessoa pode se juntar à busca por primos de Mersenne gigantescos.

CAPÍTULO 3 - NÚMEROS PRIMOS: CONJECTURAS

Não podemos encerra esta parte do estudo dos números primos sem tentar explicar o que a faz tão interessante que Gauss a chama de ‘rainha da matemática’. A história mostrou muitos fatos acerca dos Números Primos, muitos deles, como vimos no capítulo anterior, de fundamental importância para o desenvolvimento da Teoria dos Números. Algumas proposições apresentadas não puderam ser demonstradas, ou seja, não se sabe se são verdadeiras ou não. A estas chamamos de Conjecturas. Uma conjectura matemática é uma proposição que muitos matemáticos acham que deve ser verdadeira, porém, ainda não conseguiram prová-la.

Neste capítulo apresentaremos quatro afirmações. Duas conjecturas (1) e (4) e duas outras (2) e (3), antes conjecturas e, porque recentemente foram demonstradas, agora são teoremas.

(1) Conjetura de Goldbach: todo número inteiro par maior que 2 é a soma de dois primos;

(2) Conjectura de Catalan: não existem dois inteiros consecutivos, além de 8 e 9, que são potências de inteiros;

(3) Conjectura dos primos gêmeos: existem infinitos primos p para os quais $p + 2$ também é primo;

(4) Números de Fermat: todo número na forma $F_n = 2^{2^n} + 1$ são números primos.

3.1. Conjetura de Goldbach

A Conjectura de Goldbach diz que todo número inteiro par maior que 2 é igual a soma de dois números primos. Vários matemáticos já verificaram milhares de somas tendo essa hipótese verdadeira. Mas para que a conjectura vire um teorema é preciso que encontre uma prova que assegure que para qualquer número par pode ser escrito como soma de dois primos. A proposição é muito simples, mas, até hoje, ninguém conseguiu demonstrá-la.

Christian Goldbach nasceu em 1690 na cidade de Königsberg, na Prússia e viveu até 1764. Goldbach era membro da Academia Imperial de São Petersburgo,

onde atuou como professor de matemática e história. Foi ministro do Exterior na Rússia, em 1742.

Em matemática, estudou teoria dos números, teoria das curvas, séries infinitas e integração de equações diferenciais. Sua contribuição mais famosa foi exatamente a conjectura de Goldbach, que foi proposta em uma carta que escreveu a outro matemático que já discutimos, Leonhard Euler.

Muitos matemáticos apresentaram tentativas de se demonstrar essa conjectura. Iremos apresentar uma dessas tentativas e mostrar os erros ocorridos nesta demonstração.

"Demonstração: Vimos que, $a_n = 2n + 2, \ \ n \in \mathbb{N}$ *representa todos os números pares maiores que 2.*

$$a_n = 2n + 2 = n + 1 + n + 1 = \ n + 1 \ + \ n + 1 \ = \ n + 1 + m \ +$$

$n + 1 - m$ *. Com m < n+ 1, m par.* ***(1)***

*Note que n + 1 é impar ..****(2)****. Pois não nos interessa saber o resultado quando n + 1 é par. Isso quer dizer que existe* $m \in \mathbb{N}$ *tal que* $n + 1 + m$ *e* $n + 1 - m$ *são primos (VIDE PROVA ABAIXO), o que encerra a demonstração.*

PROPOSIÇÃO: Seja x um número composto impar. Então, existe , $k \in \mathbb{N}, k$ *par, tal que (x + k) e (x – k) são primos.*

DEMONSTRAÇÃO: Sabemos que $mmc\ a, b\ .mdc\ a, b\ = a\,.\,b$*.Não será diferente com os números (x + k) e (x – k). Então, temos:*

$$mmc\ x + k, x - k\ .mdc\ x + k, x - k\ = \ x + k \ \ x - k \ \Rightarrow$$

$$(\mathbf{3}) \ \Rightarrow \ x + k).(x - k\ .mdc\ x + k, x - k\ = \ x + k \ \ x - k \ \Rightarrow$$

$$\Rightarrow mdc\ x + k, x - k\ = 1$$

Logo, (x + k) e (x – k) são primos entre si. Mas eles são impares; então, temos o caso particular de serem primos ambos, quer dizer, existe k tal que (x + k) e (x – k) são primos".

Observe que inicialmente, em **(1)**, o autor da demonstração apenas cita que m é par não explicitando a que conjunto m pertence, mais ainda quando n = 1, temos n + 1 = 2 e como m < n + 1 e m par deveríamos ter um número par menor que 2.

No início da demonstração o n é tomado como qualquer $n \in \mathbb{N}$, em **(2)**, utiliza apenas a hipótese de que (n + 1) é impar, mas isso implica n ser sempre par, assim na demonstração apresentada estão excluídos os números pares da forma 2n + 2, com n ímpar.

Notemos que em **(3)**, é tomado que $mmc\ x+k, x-k\ =\ x+k\ \ x-k$, porém isso só ocorre quando esses números são primos entre si, o que é algo que deve ser mostrado.

Contudo fica evidente que existem erros de lógica matemática nesta demonstração, o que a torna inválida.

Goldbach propôs ainda outra conjectura, A conjectura fraca de Goldbach:

Todo número ímpar maior que 7 pode ser expresso como soma de três números primos ímpares.

Esta conjectura recebe o nome de "fraca", pois a conjectura de Goldbach que citamos acima, se demostrada, demonstraria automaticamente a conjectura fraca de Goldbach. Isto porque se cada número par maior ou igual a 4 é a soma de dois primos, é só somarmos 3 aos números pares maiores ou iguais a 4 para produzir os números ímpares maiores que 7.

Esta conjectura ainda não foi demostrada, mas se têm conseguido avanços importantes. Em 1923, Godfrey Harold Hardy e John Edensor Littlewood mostraram que, assumindo a Hipótese generalizada de Riemann, a conjectura fraca de Goldbach é verdadeira para todos números ímpares suficientemente grandes. Em 1937, o matemático Ivan Matvéyevich Vinogradov eliminou a dependência da hipótese de Riemann e provou diretamente que todos os números impares suficientemente grandes podem ser expressos como soma de três primos.

Atualmente, com o auxilio de computadores alguns matemáticos tentam verificar a veracidade da Conjectura de Goldbach para todos os números até 10^{23}. Com a tecnologia atual a previsão para terminar a verificação é de 20 anos.

3.2. Conjectura de Catalan

A Conjectura de Catalan diz que não existem dois inteiros consecutivos, além de 8 e 9, que são potências (de inteiros), ou seja, a equação $x^a - y^b = 1$, onde a e b são números inteiros maiores ou iguais a 2 e x e y inteiros positivos, possuem somente uma solução. Proposta em 1844 pelo matemático belga Eugène Charles Catalan (1814 – 1894).

Considere a sequência a seguir:

4, 8, 9, 16, 25, 27, 36, 49, 64, 81, 100, 121, 125, 128, ...

Catalan percebeu que nesta sequência de números inteiros maiores que 1, com quadrados, cubos e potências perfeitas, os únicos números consecutivos são o $8 = 2^3$ e $9 = 3^2$. As primeiras perguntas sugeridas foram: Existem outros pares de inteiros nesta sequência? Quantos? Finitos? Infinitos?

A conjectura afirma que 2^3 e 3^2 é o único par de potências consecutivas. Ou seja, que a única solução para os números naturais de

$x^a - y^b = 1$, para $x, a, y, b > 1$ **é** $x = 3$, $a = 2$, $y = 2$, $b = 3$.

Esta conjectura que por 153 anos permaneceu sem solução desafiando os melhores matemáticos, foi demonstrada em abril de 2002 pelo matemático romeno Preda V. Mihailescu (nascido em 23 de maio de 1955) e publicado no Jornal de Crelle em 2004. Portanto a conjectura teve que mudar de nome, passando a ser conhecida por Teorema de Mihailescu. A demonstração desse teorema está no livro European Congress of Mathematics: Stockholm, Junho 27-Julho 2, 2004.

3.3. Conjectura dos primos gêmeos

A conjectura dos primos gêmeos diz que existem infinitos primos p para os quais $p + 2$ também é primo, ou seja, x – y = 2, onde x e y são primos gêmeos. Por exemplo: 3 e 5, 5 e 7, 11 e 13, 17 e 19, 29 e 31, ...

Essa conjectura poderia ser provada através de uma fórmula que baseia-se no principio de que todo par maior que dois é a soma de dois primos (conjectura de Goldbach)

Considerando um número real, par, representado por 2x baseando-se na fórmula tem-se que $2x = p_1 + p_2$ onde p_1 e p_2 representam números primos quaisquer. Da fórmula temos que $x + x = p_1 + p_2$, reorganizando a equação temos que $x - p_1 = p_2 - x$.

Digamos que seja um número inteiro par igual a 12, para determinarmos outros números primos gêmeos, através dele teríamos que usar um primo gêmeo já conhecido como, por exemplo, o número 5, na formula ficaria da seguinte forma: $6 - 5 = p_2 - 6$ ou $6 + 1 = p_2$ obtendo como 7 um outro primo gêmeo.

Recentemente essa conjectura também teve que mudar de conjectura para teorema, pois a pesquisa de Yitang Zhang, chinês da Universidade de Hampshire, estudo publicado no Annals of Mathematics, provou que os números primos gêmeos são infinitos, como postulava a teoria de 1849 do francês Alphonse de Polignac.

3.4. Números de Fermat

Como vimos anteriormente número de Fermat é um número inteiro positivo na forma: $\mathrm{F_n} = 2^{2^n} + 1$.

Fermat lançou a conjectura, em uma carta escrita para Mersenne, que esses números eram primos. Mais tarde Leonard Euler provou que não era assim; para *n* = 5 obtinha-se um número composto:

$$F_5 = 2^{2^5} + 1 = 2^{32} + 1 = 4294967297 = 6414 \,.\, 6700417.$$

Até hoje só são conhecidos cinco números primos de Fermat, e não se sabe se há mais ou não.

$F_0 = 2^{2^0} + 1 = 3$
$F_1 = 2^{2^1} + 1 = 5$
$F_2 = 2^{2^2} + 1 = 17$
$F_3 = 2^{2^3} + 1 = 257$
$F_4 = 2^{2^4} + 1 = 65537$

Os números de Fermat de ordem 5 até 32, bem como, números enormes como F_{23288} e F_{23471} são comprovadamente compostos.

Algumas questões acerca dos números de Fermat continuam sem demonstrações, como:

- Serão infinitos os números primos de Fermat?
- Se são finitos, quanto serão?
- Se são infinitos, serão os números compostos finitos?

Muitos matemáticos ainda tentam provar essas conjecturas, com isso algumas propriedades foram desenvolvidas acerca dos números de Fermat:

- Todo número de Fermat composto pode ser decomposto em fatores primos na forma $k \,.\, 2^{n+1} + 1$, com *k* inteiro positivo;

- Apresentamos no Capítulo 2 que dois números de Fermat distintos são primos entre si;

- Se F_n é um número primo, então o polígono regular de F_n lados pode ser construído com régua e compasso;

- Um número de Fermat é igual ao produto de todos os anteriores mais 2.

  Vamos mostrar esta propriedade por indução:

  Vale para F_1, pois $F_1 = F_2 + 2$.

  Agora, se ele vale para $F_{(n-1)}$, então ele vale para F_n:

  $$F_0 \,.\, F_1 \,.\, \ldots \,.\, F_{n-2} \,.\, F_{n-1} + 2 = \; F_{n-1} - 2 \;.\, F_{n-1} + 2$$

  $$= \; 2^{2^{n-1}} + 1 - 2 \;\;.\;\; 2^{2^{n-1}} + 1 \;\; + 2$$

  $$= \; 2^{2^{n-1}} - 1 \;\;.\;\; 2^{2^{n-1}} + 1 \;\; + 2$$

  $$= \; 2^{2^{n-1}\;\;2} \;\; - 1 + 2 = 2^{2^n} + 1 = F_n.$$

Os números de Fermat ainda despertam muito interesse a vários matemáticos por varias razões. O “pedigree” destes números é uma delas. Eles têm uma longa história, e muitos matemáticos importantes já trabalharam no problema. Além disto, são uma boa fonte de exemplos de números grandes e difíceis de fatorar, ótimo para testar um novo algoritmo de fatoração.

CAPÍTULO 4 – Criptografia RSA

O nome criptografia vem do grego cryptos que significa oculto, secreto. A criptografia estuda os métodos para codificar uma mensagem de maneira que somente a pessoa de destino consiga interpretá-la. Essa técnica usada pelos antigos, desde o Egito, Palestina, passando por Roma, com o Imperador Júlio César, é utilizada hoje, em segurança de transações bancárias, trocas de informações pela internet, informações governamentais secretas, relatórios de espionagens, etc...

Existem vários métodos de criptografar uma mensagem ou informação. É desejável que o método empregado ofereça total segurança, para no caso da mensagem criptografada ser interceptada o interceptador não consiga decifra-la. Em tempo de guerra uma mensagem interceptada, se decifrada pelo inimigo poderá ocasionar efeitos catastróficos.

Neste capítulo apresentaremos um pouco da história dessa área, alguns dos métodos utilizados para codificar, a criptografia RSA e sua relação com os números primos.

Foi a partir da Primeira Guerra Mundial que a criptografia teve avanços mais significativos. Quando a base aliada conseguiu interceptar algumas mensagens criptografadas do exército alemão e, quebrando seus códigos, obteve informações que contribuíram decisivamente para sua vitória. Após a guerra, por volta 1918, foram criados vários sistemas de criptografia cada vez menos vulneráveis.

Os primeiros métodos matemáticos usados em criptografia começaram a ser desenvolvidos nesse período. Em 1929, surgiu um texto criptografado através de operações de matrizes. Nesse mesmo período aparecem as primeiras máquinas de enigmas, equipamentos usados para codificar e decodificar mensagens durante a Segunda Guerra Mundial.

Figura 3: Máquina de enigma (Fonte: http://users.telenet.be/d.rijmenants/en/enigma.htm)

Com o avanço da tecnologia e o advento dos computadores não se tinha como enviar mensagens privadas com segurança. Observava-se, até pouco mais da metade do século XX, as chaves criptográficas eram funções injetivas, e, para decodificar, bastava aplicar a função inversa da função inicial, o que poderia ser feito facilmente por um computador.

Apenas em 1976, é que Whitfied Diffie e Martin Hellman encontraram uma forma de poder ocorrer troca segura de chaves, sem as pessoas se encontrarem. Para isto foi usada aritmética modular e da cifra assimétrica, formada por uma chave publica e uma chave privada. A descrição dessa cifra será melhor desenvolvida na próxima seção. A idéia era usar uma chave para codificar a mensagem e outra para decodificar. Ronald Rivest, Adi Shamir, e Leonard Adleman, em Abril de 1978, criaram a cifra assimétrica RSA, que será apresentada na próxima seção.

4.1. Criptografia RSA

A criptografia RSA, que é o método mais conhecido de criptografia assimétrica (Criptografia assimétrica consiste em utilizar um par de chaves: uma chave privada e uma chave pública), foi desenvolvida em 1978 por R. L. Rivesst, A. Shamir e L. Adleman, três professores que trabalhavam no Massachussets Institute of Technology (M.I.T.). Esse método é identificado pelas siglas RSA, iniciais dos

nomes de seus criadores. Hoje ele é bastante usado em transações comerciais e em softwares de navegação da internet.

A criptografia RSA tem como base para construir a chave pública os números primos e, para podermos compreender esse método, utilizaremos algumas dos fatos sobre os números primos que apresentamos no Capítulo 2.

4.1.1. Pre-Codificação

Na criptografia RSA primeiramente deve ser definido qual tipo de chave privada a ser utilizada. A escolha dessa chave é fundamental para o desenvolvimento da chave pública e, por isso, essa chave é a cifra numérica de substituição. Explicaremos o processo de criptografia RSA com um exemplo simples.

Considere que pretendamos codificar a mensagem “MEU FILHO RAFAEL”. Usaremos a tabela abaixo para cifrar a mensagem. Lembrando que a escolha do cifrante ficará a critério das pessoas ou empresas que pretendem codificar as mensagens ou informações.

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

O espaço entre duas palavras será substituído pelo número 99.

Portanto, a mensagem a ser transmitida ficará:

22143099151821172499271015101421.

Observe que escolhemos números de dois algarismos. Essa escolha é feita porque se tivéssemos intercalado números de um algarismo com números de dois algarismos, alguns problemas poderiam surgir. Por exemplo: se começássemos com 1 representando a letra A, 2 o B e assim sucessivamente, o símbolo 25, tanto poderia representar BE, como Y, e não teríamos como saber qual escolha seria a correta.

Após a substituição das letras por números, escolheremos dois números p e q primos com os quais iremos determinar $n = pq$, que é a primeira parte da chave pública. Para garantir a maior dificuldade em decifrar o código, esses números

primos devem ser números muito grandes. Assim, o tamanho da chave poderá ser de 1024 bits, um número de aproximadamente 300 algarismos.

Para facilitar as contas em nosso exemplo iremos escolher dois números primos pequenos, *p = 11* e *q = 17*, logo *n = 11·17 = 187*. Agora vamos separar em blocos a sequência de números da nossa mensagem, de modo que cada bloco não seja maior que n e nenhum bloco comece com o algarismo 0, pois isso poderia causar erros na hora da decodificação. Temos:

22-14-30-99-151-82-11-72-49-92-7-101-5-101-42-1.

Observe que a escolha dos blocos poderia ser diferente, gerando outros números. Veja também que os blocos em que a mensagem foi quebrada não formam unidade de linguagem linguística, o que dificulta ainda mais a decodificação, impossibilitando a quebra por contagem de frequência.

4.1.2. Codificando e decodificando

Agora começamos a codificar a mensagem utilizando os números primos *p* e *q*. Conhecemos o número n que é o produto dos dois primos. Calcularemos $\boldsymbol{\phi\ n\ } = (\boldsymbol{p-1})(\boldsymbol{q-1})$ e determinaremos um número natural *e,* onde o $\boldsymbol{mdc\ \ e,\phi\ n\ } = \mathbf{1}$. Chamaremos o par (e, n) de chave de codificação do sistema RSA.

Para o nosso exemplo, onde p =11, q = 17 e n = 187, temos que:

$$\boldsymbol{\phi\ n\ } = \ \boldsymbol{p-1\ \ q-1\ } = (\mathbf{11-1})(\mathbf{17-1}) = \mathbf{10.16 = 160},$$

e, como precisamos de um número e, onde o $\boldsymbol{mdc\ \ e,\phi\ n\ } = \mathbf{1}$, podemos escolher esse número e = 3.

Portanto, a nossa chave de codificação será *(n, e)* = *(187, 3)*. Essa chave será aplicada em cada bloco b pertence ao conjunto dos blocos de codificação. No nosso caso, cada b ∈ {22, 14, 30, 99, 151, 82, 11, 72, 49, 92, 7, 101, 5, 101, 42, 1}, gera um bloco codificado C(b) dado em função da chave *(n, e)* por $\boldsymbol{C\ b\ } \equiv \boldsymbol{b^e\ mod\ n}$. Assim o bloco codificado C(b) é o resto da divisão de $\boldsymbol{b^e}$ por *n*. Com C(b) < n.

Em nosso exemplo temos:

$$C\ 22 \equiv 22^3\ mod\ 187 = 176$$
$$C\ 14 \equiv 14^3\ mod\ 187 = 126$$
$$C\ 30 \equiv 30^3\ mod\ 187 = 72$$
$$C\ 99 \equiv 99^3\ mod\ 187 = 143$$
$$C\ 151 \equiv 151^3\ mod\ 187 = 94$$
$$C\ 82 \equiv 82^3\ mod\ 187 = 92$$
$$C\ 11 \equiv 11^3\ mod\ 187 = 22$$
$$C\ 72 \equiv 72^3\ mod\ 187 = 183$$
$$C\ 49 \equiv 49^3\ mod\ 187 = 26$$
$$C\ 92 \equiv 92^3\ mod\ 187 = 20$$
$$C\ 7 \equiv 7^3\ mod\ 187 = 156$$
$$C\ 101 \equiv 101^3\ mod\ 187 = 118$$
$$C\ 5 \equiv 5^3\ mod\ 187 = 125$$
$$C\ 101 \equiv 101^3\ mod\ 187 = 118$$
$$C\ 42 \equiv 42^3\ mod\ 187 = 36$$
$$C\ 1 \equiv 1^3\ mod\ 187 = 1$$

Obtemos um novo bloco, que representa a mensagem codificada,

176-126-72-143-94-92-22-183-26-20-156-118-125-118-36-1,

essa será a informação transferida com segurança junto com a chave *(n, e) = (187, 3).*

Observe que essa nova sequência não pode ser unificada, isso faria com que a mensagem ficasse impossível de ser decodificada.

Feita a codificação, iremos apresentar a decodificação.

Agora as informações que precisamos para decodificar são dois números: o mesmo número $\boldsymbol{n}$ e o inverso do número *e* modulo $\boldsymbol{\phi\ n}$, que será um número que chamaremos de *d*. Portanto, a chave para a decodificação é *(n, d)*. De posse desses dois números e o conjunto dos blocos codificados, faremos a decodificação. Se a é um desses blocos codificados, isto é, a ∈ {176-126-72-143-94-92-22-183-26-20-156-118-125-118-36-1}, denote por *D(a)* o bloco a decodificado. Teremos:

$$\boldsymbol{D\ a \equiv a^d mod\ n,}$$

ou seja, *D(a)* é o resto da divisão de $\boldsymbol{a^d}$ por n. Com D(a) < n.

Verifica-se que a função D é a inversa de C, isto é *D(C(b)) = b*.

Para mostrar que *D(C(b))* = *b,* basta mostrar que $\boldsymbol{D\ C\ b} \equiv \boldsymbol{b\ mod\ n}$. Como tanto *D(C(b))*, como *b* estão no intervalo *1* e (*n – 1)*, a congruência acontece se, somente se, a igualdade é verdadeira. Observe a importância de termos escolhido os blocos *b* menores que *n*.

Pela definição temos:

$$\boldsymbol{D\ C\ b} \equiv \boldsymbol{b^{e\ d} \equiv b^{ed} mod\ n.}$$

Como d é o inverso de e modulo $\boldsymbol{\phi\ n}$, temos que $\boldsymbol{ed = 1 + k\phi\ n}$, onde $\boldsymbol{k} \in \mathbb{Z}$. Veja que, $\boldsymbol{e, d} \in \mathbb{Z}$, onde $\boldsymbol{e, d > 2}$ e $\boldsymbol{\phi\ n > 0}$, portanto k > 0. Podemos substituir *ed* por $\boldsymbol{1 + k\phi\ n}$.

$\boldsymbol{D\ C\ b} \equiv \boldsymbol{b^{e\ d} \equiv b^{ed} \equiv b^{1+k\phi\ n} \equiv b.b^{k\phi\ n}\ mod\ n}$, como $\boldsymbol{\phi\ n = (p-1)(q-1)}$, temos $\boldsymbol{b^{ed} \equiv b.b^{k\phi\ n} \equiv b.\ b^{p-1\ \ k(q-1)} mod\ n}$.

Temos que *n* = *pq*, onde *p* e *q* são números primos distintos. Portanto, faremos os cálculos em relação à *p* e *q*. Como os resultados são análogos, basta mostrar para *p*. Logo, queremos mostrar,

$$\boldsymbol{b^{ed} \equiv b.\ b^{p-1\ \ k\ q-1}\ mod\ p.}$$

Se p não divide b, então, pelo Pequeno Teorema de Fermat, $\boldsymbol{b^{p-1} \equiv 1\ mod\ p}$, logo $\boldsymbol{b^{ed} \equiv b\ mod\ p}$, e, se p divide b, temos que $\boldsymbol{b \equiv 0\ mod\ p}$, logo $\boldsymbol{b^{ed} \equiv b\ mod\ p}$ vale para qualquer valor de b.

Mostramos, deste modo, que $\boldsymbol{b^{ed} \equiv b\ mod\ p}$, por analogia a demonstração, também vale para *q*. Portanto $\boldsymbol{b^{ed} - b}$ é divisível, tanto por *p* como por *q*. Como *p* e *q* são primos, *pq* divide $\boldsymbol{b^{ed} - b}$, logo n divide $\boldsymbol{b^{ed} - b}$ para qualquer valor de $\boldsymbol{b} \in \mathbb{Z}$. Portanto *D(C(b)) = b.*

Para finalizar o método, vamos terminar a decodificação da nossa mensagem. Para isso, precisamos determinar o número d, que calculamos usando o algoritmo euclidiano estendido, dividindo $\boldsymbol{\phi\ n}$ por e, temos:

$$\boldsymbol{160 = 3.53 + 1 \Rightarrow 1 = 160 + \ -53\ .3,}$$

logo o inverso de 3 modulo 160 é – 53. Como precisamos que o número d seja positivo, temos que $-53 \equiv 107\ mod\ 160$, portanto d = 107. A chave de decodificação dessa mensagem é o par (187,107). Aplicando na função de decodificação temos:

$$D\ 176 \equiv 176^{107}\ mod\ 187 = 22$$
$$D\ 126 \equiv 126^{107}\ mod\ 187 = 14$$
$$D\ 72 \equiv 72^{107}\ mod\ 187 = 30$$
$$D\ 143 \equiv 143^{107}\ mod\ 187 = 99$$
$$D\ 94 \equiv 94^{107}\ mod\ 187 = 151$$
$$D\ 92 \equiv 92^{107}\ mod\ 187 = 82$$
$$D\ 22 \equiv 22^{107}\ mod\ 187 = 11$$
$$D\ 183 \equiv 183^{107}\ mod\ 187 = 72$$
$$D\ 26 \equiv 26^{107}\ mod\ 187 = 49$$
$$D\ 20 \equiv 20^{107}\ mod\ 187 = 92$$
$$D\ 156 \equiv 156^{107}\ mod\ 187 = 7$$
$$D\ 118 \equiv 118^{107}\ mod\ 187 = 101$$
$$D\ 125 \equiv 125^{107}\ mod\ 187 = 5$$
$$D\ 118 \equiv 118^{107}\ mod\ 187 = 101$$
$$D\ 36 \equiv 36^{107}\ mod\ 187 = 42$$
$$D\ 1 \equiv 1^{107}\ mod\ 187 = 1$$

Obtemos o bloco original, que representa a mensagem primaria,

22-14-30-99-151-82-11-72-49-92-7-101-5-101-42-1,

reagrupando os números, temos

22-14-30-99-15-18-21-17-24-99-27-10-15-10-14-21

voltando a mensagem de origem.

4.1.3. Segurança do RSA

A segurança do método RSA não está nas operações matemáticas para codificar ou decodificar informações. Os números primos escolhidos é quem fazem a diferença, pois o método RSA utiliza números astronômicos, na ordem de 100 a 200 algarismos em cada um dos dois números, os quais não tem necessariamente mesmas quantidades de algarismos. O sistema então gera um número n maior ainda que os primos. Para quebrar o código seria preciso conhecer os dois números primos utilizados. Estes nunca são informados, e conhecidos apenas pelas pessoas que codificaram e as que iram decodificar.

A possibilidade de se descobrir os números primos seria fatorando o número n. Mesmo se conhecêssemos todos os números primos entre 1 e (n – 1), não existe método eficiente para se fazer essa fatoração com rapidez, o que garante a segurança da mensagem.

A tabela 2 mostra o número de operações necessárias para fatorar n e o tempo requerido em cada operação em um microssegundo para cada quantidade de dígitos decimais do número n.

Número de algarismos de n	Tempo necessário para quebra o RSA
50	3,9 horas
75	104 dias
100	74 anos
200	3,8 x $\mathbf{10^7}$anos
300	4,9 x $\mathbf{10^{13}}$anos
500	4,2 x $\mathbf{10^{23}}$anos

Tabela 2:Tempo para quebrar o RSA. Adaptada de: Criptografia e a importância das suas aplicações. RPM 12.

Mesmo tendo uma fórmula para determinar os números primos, nós nos deparamos com o problema de fazer operações rápidas com números astronômicos. Entretanto, a busca de um algoritmo tanto para fazer uma fatoração rápida, como para descobrir os números primos, continua sendo objeto de estudo por parte de vários pesquisadores no mundo inteiro.

Depois desta, outras cifras assimétricas foram criadas. Em 1984, Taher ELGamal cria uma baseado no Problema do Logaritmo Discreto. Em 1986, Miller introduz na criptografia as curvas elípticas.

CAPÍTULO 5 – REFLEXÕES SOBRE O ENSINO DOS NÚMEROS PRIMOS

Neste trabalho, apresentamos três aspectos acerca dos números primos: um pouco da história dos números primos; alguns fatos teóricos relacionadas aos números primos; e uma aplicação dos números primos. Três direções que podem conduzir o aluno do ensino básico a um maior interesse pelo estudo da matemática e em particular dos números primos. Os dados apresentado pelo IDEB indicam baixo índice de assimilação dos conteúdos pelos alunos do ensino fundamental e médio.

Anos Iniciais do Ensino Fundamental

	IDEB Observado				Metas				
	2005	2007	2009	2011	2007	2009	2011	2013	2021
Total	3.8	4.2	4.6	5.0	3.9	4.2	4.6	4.9	6.0

Anos Finais do Ensino Fundamental

	IDEB Observado				Metas				
	2005	2007	2009	2011	2007	2009	2011	2013	2021
Total	3.5	3.8	4.0	4.1	3.5	3.7	3.9	4.4	5.5

Ensino Médio

	IDEB Observado				Metas				
	2005	2007	2009	2011	2007	2009	2011	2013	2021
Total	3.4	3.5	3.6	3.7	3.4	3.5	3.7	3.9	5.2

Tabela 3: Tabela histórica dos dados do IDEB Fonte: Saeb e Censo Escolar.

As atuais tendências pedagógicas apontam para procedimentos didáticos interdisciplinares. Na maioria das vezes os conteúdos de duas disciplinas distintas se complementam e assim passam a ter mais sentido para o aluno, o que facilita a compreensão, e até mesmo desperta o interesse, do aluno pela matéria. Por outro lado, o conteúdo específico da disciplina não deve ser secundarizado pela interdisciplinaridade, isto é, deve ser apresentado e desenvolvido respeitando os aspectos da linguagem e rigor matemático.

Observa-se que frequentemente, os professores de Matemática apresentam os números primos em sua definição formal, sem antes ter alguma

preocupação em despertar o interesse dos estudantes, através da contextualização histórica, da apresentação das diferentes ideias que surgiram sobre o tema, das indagações e conjecturas sobre o assunto.

Os números primos são inicialmente apresentados para os alunos no 6º ano do ensino fundamental, com o objetivo único de usá-los na decomposição de números compostos, para o calculo do máximo divisor comum e mínimo múltiplo comum de números inteiros. Sendo estudados depois somente em algumas disciplinas da graduação. Assim, pouca importância é dada aos números primos, deixando passar uma oportunidade de construção e desenvolvimento que esse conteúdo encerra, pois inerente ao ensino de matemática está a construção de diversas formas de raciocínio, conforme [MACHADO et al. (2005) .

Apresentaremos neste capítulo uma proposta de metodologia para o ensino dos números primos na educação básica.

5.1. História da Matemática

O estudo da história da matemática pode fazer com que o aluno compreenda melhor a construção do assunto estudado, levando-o a compreender as dúvidas dos diversos matemáticos, bem como a descobrir suas estratégias para a solução dessas dúvidas. É uma área de estudo que vem sendo usada pelos professores para melhorar suas práticas pedagógicas. Baroni e Nobre (1999) destacam algumas destas teorias educacionais:

> *A Modelagem, a Etnomatemática, a Informática, dentre outros, são exemplos de importantes estudos teórico-educacionais que proporcionam avanços nas relações educacionais voltadas ao trabalho diário do professor de matemática. A história da matemática é um destes instrumentos que, nos últimos tempos, vem ganhando certo destaque no meio acadêmico-educacional (*Baroni e Nobre, 1999, *p.129).*

O ensino da história da matemática pode fazer com que o aluno busque reflexões a respeito da compreensão das ideias, através dos fatos e contextos que levaram alguns matemáticos a desenvolver teorias, conjecturas, teoremas e etc... Faz também uma aproximação da matemática, considerada uma ciência exata, com as ciências sociais e humanas, mostrando que a construção de um conhecimento

ocorre em um determinado contexto histórico e social. Farago (2003) comenta que conhecer a origem ajuda na compreensão do por que da construção dos conceitos matemáticos.

Os PCNs de matemática de 1997, considera a história da matemática, como uma entre várias ferramentas para alavancar o ensino da matemática no Brasil.

> *Ao revelar a Matemática como uma criação humana, ao mostrar necessidades e preocupações de diferentes culturas, em diferentes momentos históricos, ao estabelecer comparações entre os conceitos e processos matemáticos do passado e do presente, o professor tem a possibilidade de desenvolver atitudes e valores mais favoráveis do aluno diante do conhecimento matemático.*
>
> *Além disso, conceitos abordados em conexão com sua história constituem-se veículos de informação cultural, sociológica e antropológica de grande valor formativo. A História da Matemática é, nesse sentido, um instrumento de resgate da própria identidade cultural.*
>
> *Em muitas situações, o recurso à História da Matemática pode esclarecer ideias matemáticas que estão sendo construídas pelo aluno, especialmente para dar respostas a alguns "porquês" e, desse modo, contribuir para a constituição de um olhar mais crítico sobre os objetos de conhecimento. (Pcns - matemática 1997).*

No caso dos números primos tem-se material para trabalhar com alunos do ensino fundamental ao ensino superior, mostrando o surgimento da ideia de números primos, como a construção do "Crivo de Erastóstenes", a ideia de números lineares estudados por Pitágoras, até os teoremas e conjecturas hoje estudados pelos matemáticos.

Portanto, porque facilita a compreensão, desperta interesse e desenvolve a interdisciplinaridade, entendemos que o ensino da matemática deve ser apresentado de forma contextualizada na história.

5.2. Ensinando a teoria matemática

A construção do conhecimento matemático deve ser feita pelo aluno, tendo o professor como um facilitador. Em uma aula planejada, o professor pode,

após a proposta dos questionamentos, fazer com que o aluno pesquise, investigue e tire suas próprias conclusões, chegando à formalização do assunto, que pode ser apresentada pelo professor ou pelo próprio aluno.

No entanto, é bom enfatizar, que o estudo teórico deve ser feito de forma aprofundada e com rigor adequado, principalmente nos cursos de formação de professores. Isto propiciara ao futuro professor uma base teórica sólida evitando erros rotineiros que poderão ser passados para os alunos de forma imperceptível.

Parafraseando Lorenzato e Vila (1993, p. 46), “compete-nos ensinar matemática e linguística não somente por sua beleza ou pela consistência interna de suas teorias, mas também para que elas sejam úteis ao homem e à sociedade”.

5.3. As aplicações dos conteúdos estudados na disciplina de Matemática

É muito comum, durante as aulas, alguns alunos perguntarem: para que estudar esse assunto? Em que é que eu vou utilizar essa matéria na minha vida? As respostas para a primeira pergunta são muitas. Conforme as orientações apresentadas nos PCNs de matemática do ensino fundamental:

> *A constatação da sua importância apoia-se no fato de que a Matemática desempenha papel decisivo, pois permite resolver problemas da vida cotidiana, tem muitas aplicações no mundo do trabalho e funciona como instrumento essencial para a construção de conhecimentos em outras áreas curriculares. Do mesmo modo, interfere fortemente na formação de capacidades intelectuais, na estruturação do pensamento e na agilização do raciocínio dedutivo do aluno.*

A resposta para a segunda pergunta depende dos assuntos discutidos, visto que nem sempre tem aplicação cotidiana, o que não diminui a importância do conteúdo, que pode ter aplicação na própria matemática, bem como pode servir para aguçar o desenvolvimento do raciocínio lógico e dedutivo do estudante. Usando o caso dos números primos, percebemos que, como foi apresentado no capítulo anterior, este assunto tem papel fundamental para o processo da criptografia RSA. Fato que pode ser comentado no ensino básico, e estudado no ensino superior. Além disso, eles são necessários para o estudo do MMC e do MDC, que resolvem

problemas que podem ser descritos de forma aplicada no estudo básico da álgebra desenvolvida durante o 6º ano do ensino fundamental.

Encontramos muitas aplicações da matemática no dia a dia. Certamente algumas dessas aplicações interessará alguns alunos que têm afinidade com essas outras áreas, aproximando esses alunos da matemática e aproximando a matemática da realidade de outra área ou do aluno, mostrando que a matemática não só pode ser aplicável como é próxima deles, desenvolvendo, assim, uma aprendizagem significativa para o aluno. Transformando a matemática teórica em prática, ou, pelo menos, em uma matemática contextualizada.

Observe que as três abordagens do ensino de matemática que discutimos neste capítulo, não têm um desenvolvimento sólido se aplicadas separadamente, mas, interligadas, as três se complementam:

- História: facilita a construção do conhecimento, contextualiza o assunto na sociedade e pode fornecer ideias diferentes sobre o tópico;
- Teoria: formaliza a construção do conhecimento;
- Aplicação: torna palpável o conhecimento construído e contextualiza o conteúdo de forma prática.

Nas palavras de Paulo Freie: “A alegria não chega apenas no encontro do achado, mas faz parte do processo da busca. E ensinar e aprender não pode dar-se fora da procura, fora da boniteza e da alegria”.

5.4. Sugestão para uma aula sobre números primos

Partindo do que foi apresentado nesse trabalho, tecemos algumas propostas de abordagens desse assunto. Podemos apresentar os números primos a partir dos estudos desenvolvidos pelos pitagóricos.

Uma atividade sobre os números primos utilizando folhas quadriculadas e separando os alunos em grupos. Em que, para cada grupo, sejam distribuídos números que variam de 1 a 30.

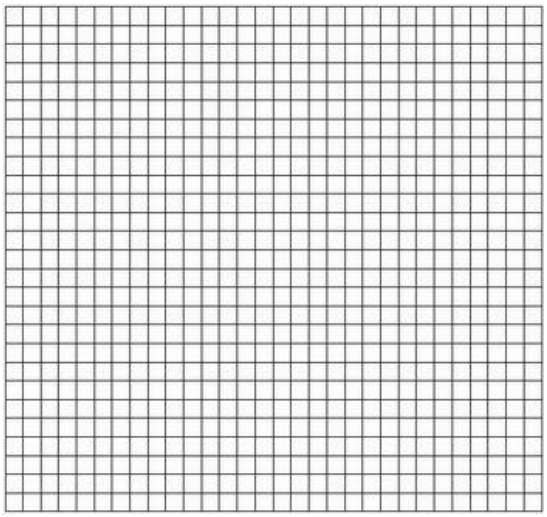

Figura 4:http://portaldoprofessor.mec.gov.br/fichaTecnicaAula.html?aula=52256

É bom lembrar que cada grupo deve ficar com um conjunto de números diferente dos outros grupos, para que, ao final, se possa construir a definição de números primos de forma coletiva.

De posse das folhas e dos números que foram distribuídos para os grupos, cada grupo deverá representar esses números na forma de retângulos, de quantas maneiras forem possíveis para cada número. Por exemplo, os números 6 e 7, poderiam ser representados da seguinte forma:

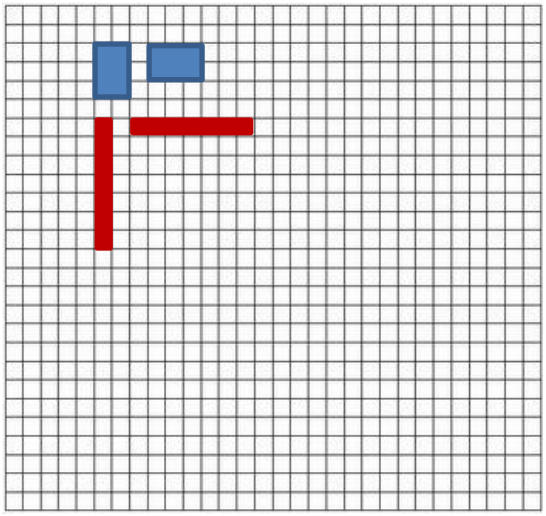

Figura 5:http://portaldoprofessor.mec.gov.br/fichaTecnicaAula.html?aula=52256

Com essa atividade, pretende-se que os alunos percebam os números que poderão ser representados apenas por uma linha vertical ou horizontal, momento em que o professor pode fazer um paralelo com a história de Pitágoras e a

ideia de números lineares, propondo questionamentos que indaguem sobre o que esses números têm de diferente dos demais.

Após esse momento pode-se apresentar o ‘Crivo de Erastóstenes’ para que os alunos marquem (crivem) em uma tabela os números de 1 a 30 que não são lineares, conduzindo, assim, os alunos para as definições de números primos e números compostos, fazendo um paralelo com a história desses números.

Após essa atividade, pode-se apresentar uma tabela, agora com números de 1 a 100 e traçar, junto com os alunos, uma estratégia para descobrir quem é primo (linear) e quem é composto (não linear), elaborando testes de primalidade.

Como atividade extra, o professor pode relacionar os números primos com a criptografia, contando sua história, apresentando alguns sistemas criptográficos mais simples.

Podemos para alunos do ensino médio, apresentar o modelo de criptografia associada à matrizes ou à funções invertíveis.

Dada a Tabela baixo.

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
1	2	3	4	5	6	7	8	9	10	11	12	13
N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**X**	**W**	**Y**	**Z**
14	15	16	17	18	19	20	21	22	23	24	25	26

Pretende-se criptografar a seguinte mensagem: “Matemática”.

Fazendo a substituição temos:

13 1 20 5 13 1 20 9 3 1

Seja a matriz $A = \begin{matrix} 1 & 3 \\ 2 & 1 \end{matrix}$ a matriz codificadora e $B = \begin{matrix} 13 & 1 & 20 & 5 & 13 \\ 1 & 20 & 9 & 3 & 1 \end{matrix}$, a matriz da mensagem, para completar a codificação, vai multiplicar uma matriz pela outra.

$$A.B = \begin{matrix} 1 & 3 \\ 2 & 1 \end{matrix} \cdot \begin{matrix} 13 & 1 & 20 & 5 & 13 \\ 1 & 20 & 9 & 3 & 1 \end{matrix} = \begin{matrix} 16 & 61 & 47 & 14 & 16 \\ 27 & 22 & 49 & 13 & 27 \end{matrix}$$

Logo, o código a ser transmitido será 16 61 47 14 16 27 22 49 13 27.

Para decodificar a mensagem basta calcular $A^{-1}.B$.

CONSIDERAÇÕES FINAIS

Neste trabalho apresentamos um pouco da história dos números primos, alguns fatos teóricos e uma de suas aplicações. Ao final sugerimos como trabalhar os números primos no ensino básico.

Apresentamos a historia dos números primos, com a finalidade de despertar ao leitor o instinto investigativo. Vimos como os pitagóricos tratavam os números primos e apresentamos alguns dos teoremas a eles associados. Observamos que estes tópicos podem ser apresentados desde o ensino básico ao ensino superior, respeitando, obviamente, os níveis de complexidade.

Como aplicação, apresentamos o sistema de criptografia RSA. A base deste sistema está vinculada fortemente aos números primos. Concluímos que a segurança do sistema de criptografia RSA depende essencialmente de alguns fatos teóricos sobre os números primos.

Acreditamos ser possível e necessária à diminuição da distância entre o aluno e a matemática. Observou-se a importância da exploração de várias metodologias que auxiliem no ensino da matemática. A história dos números primos pode facilitar a compreensão das definições e teoremas sobre estes números.

Enfim, esperamos que esse trabalho possa servir como material de apoio para o docente de matemática da educação básica, com vistas a sanar algumas dificuldades e omissões dos nossos livros didáticos. E, também, que possa servir de motivação e inspiração para que o mesmo busque aperfeiçoar sua prática pedagógica, apresentando novas aplicações em sala de aula.

APÊNDICE

Algoritmo euclidiano

Este algoritmo é descrito por Euclides nas proposições 1 e 2 do Livro 7 dos Elementos e será utilizado para fazer alguns cálculos no Capítulo 4.

O algoritmo euclidiano consiste em dividir dois números a e b inteiros positivos, onde $a \geq b$, dividindo a por b, teremos o resto r_1. Se r_1 for diferente de zero, dividiremos b por r_1, obtendo r_2. Se r_2 for diferente de zero, dividiremos r_1 por r_2, obtendo r_3. Assim por diante. O último resto diferente de zero desta sequência de divisões é o máximo divisor comum entre a e b.

Teorema 1: Se a e b inteiros e a = q.b + r onde q e r são inteiros, então MDC(a, b) = MDC(b, r).

Demonstração: Da relação a = q.b + r podemos concluir que todo divisor de b e r é divisor de a pela proposição 1 do capitulo 2. Esta mesma relação, escrita na forma r= a – qb, nos diz que todo divisor de a e b é um divisor de r. Logo o conjunto de divisores comuns de a e b é igual ao conjunto de divisores comuns de b e r, o que nos garante o resultado MDC(a, b) = MDC(b, r).

Se $r_0 = a$ e $r_1 = b$ inteiros não-negativos com $b \neq 0$. Se o algoritmo da divisão for aplicado sucessivamente para obter $r_i = r_{i+1}q_0 + r_{i+2}, 0 < r_{i+2} < r_{i+1}$, para i = 0, 1, 2, ..., n – 1 e $r_n = 0$ então $MDC\ a, b\ = r_n$, o último resto diferente de zero.

Demonstração do algoritmo euclidiano: Aplicando o algoritmo da divisão entre a e b, temos:

$$a = bq_0 + r_1 \qquad 0 < r_1 < b$$
$$b = r_1q_1 + r_2 \qquad 0 < r_2 < r_1$$
$$r_1 = r_2q_1 + r_3 \qquad 0 < r_3 < r_2$$
$$\vdots$$

Observamos que na sequencia dos restos uma é sempre menor que o seu anterior, mas todos são maiores que zero. Escrevendo as desigualdades dos restos uma em seguida à outra, $b > r_1 > r_2 > r_3 > \cdots \geq 0$.

Como entre b e 0 há uma quantidade finita de números inteiros, esta sequência não pode continuar indefinidamente. Por tanto,

$\vdots$

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

A partir deste último resultado e pelo teorema 1, temos que o máximo divisor comum de $r_n \; e \; r_{n-1}$é r_n. Da penúltima equação temos que $MDC\ r_{n-1}, r_{n-2} = r_n$, aplicando o mesmo teorema nos resultados anteriores, temos:

$$r_n = MDC\ r_{n-1}, r_{n-2} = MDC\ r_{n-2}, r_{n-3} = \cdots = MDC\ b, r_1 = MDC\ a, b\ .$$

Portanto o máximo divisor comum de a e b é o último resto não-nulo da sequência de divisões descrita.

A partir deste resultado podemos obter o Algoritmo euclidiano estendido. Das equações acima, fazendo algumas substituições dos restos, teremos que $\alpha . a + \beta . b = r_n$, onde $\alpha \; e \; \beta$ são números inteiros e que se $a \geq b$, então β sera um inteiro negativo.

BIBLIOGRAFIA

BARONI, R. L. S. e NOBRE, S. (1999). A Pesquisa em História da Matemática e Suas Relações com a Educação Matemática. In: BICUDO, M. A.(org.). Pesquisa em Educação Matemática: concepções e perspectivas. São Paulo: UNESP.

BOYER, Carl B. História da matemática, 2a. ed. - São Paulo: Edgard Blucher, 1996.

BRASIL. Secretaria de Educação Fundamental. Parâmetros Curriculares Nacionais: 3º e 4º ciclos do Ensino Fundamental na Matemática. Brasília: MEC/SEF, 1997.

COUTINHO, S. Números Inteiros e Criptografia RSA. 2 ed. Rio de Janeiro: IMPA, 2005.

CRIPTOGRAFIA. Disponível em: <http://www.numaboa.com.br/criptografia>. Acesso em: 20 jul. 2013.

Dados do IDEB. Disponível em: <http://ideb.inep.gov.br/resultado/resultado/resultadoBrasil.seam?cid=20399>. Acesso em 24 ago. 2013

EUCLIDES. Os Elementos. Tradução de Irineu Bicudo. São Paulo: Unesp, 2009.

EVES, Howard. Introdução _a história da matemática, tradução: Hygino H. Domingues. 5ª. ed. - Campinas, SP: Editora da UNICAMP, 2011.

FREIRE, P. Pedagogia do Oprimido. 8 ed. Rio de Janeiro: Paz & Terra, 1980.

GIMPS (2008). Mersenne prime search. Disponível em: <http://www.mersenne.org/>. Acesso em: 20 jul. 2013.

HEFEZ, A. Elementos de Aritmética. Sociedade Brasileira de Matemática, Textos Universitários, 2006.

LORENZATO, Sérgio, VILA, Maria do Carmo. Século XXI: qual a matemática recomendável? Zetetiké, vol. 1, nº 1, Campinas, Unicamp, 1993.

MACHADO, S. D. A.; MARANHAO, M.C.; COELHO, S. P. Como é utilizado o Teorema Fundamental da Aritmética por atores do Ensino Fundamental. In: Atas do V CIBEM. Porto, julho de 2005, v.1.

SANTOS, José Plínio de Oliveira. Introdução à teoria dos números, 3ª. ed. - Rio de Janeiro: IMPA, 2010.

SAUTOY, M. A Música dos Números Primos: a história de um problema não resolvido na matemática. Rio de Janeiro: Jorge Zahar, 2007.