Universidade Federal de Goiás
Instituto de Matemática e Estatística
Programa de Mestrado Profissional em Matemática em Rede Nacional

Números Primos

Pequenos Tópicos

GLAUBER CRISTO ALVES DE CARVALHO

Goiânia
2013

sistema de bibliotecas ufg

UFG

TERMO DE CIÊNCIA E DE AUTORIZAÇÃO PARA DISPONIBILIZAR AS TESES E DISSERTAÇÕES ELETRÔNICAS (TEDE) NA BIBLIOTECA DIGITAL DA UFG

Na qualidade de titular dos direitos de autor, autorizo a Universidade Federal de Goiás (UFG) a disponibilizar, gratuitamente, por meio da Biblioteca Digital de Teses e Dissertações (BDTD/UFG), sem ressarcimento dos direitos autorais, de acordo com a Lei nº 9610/98, o documento conforme permissões assinaladas abaixo, para fins de leitura, impressão e/ou *download*, a título de divulgação da produção científica brasileira, a partir desta data.

1. Identificação do material bibliográfico: **Trabalho de Conclusão de Curso de Mestrado Profissional**

2. Identificação da Tese ou Dissertação

Autor (a):	Glauber Cristo Alves de Carvalho						
E-mail:	glaubercristo@bol.com.br						
Seu e-mail pode ser disponibilizado na página? [x]Sim [ ] Não							
Vínculo empregatício do autor							
Agência de fomento:		Coordenação de Aperfeiçoamento de Pessoal de Nível Superior			Sigla:	CAPES	
País:	Brasil	UF:	DF	CNPJ:	00.889.834/0001-08		
Título:	Números Primos – Pequenos Tópicos						
Palavras-chave:	Números primos, Primos de Mersene, Primos de Fermat, Outros tipos de números primos, Fórmulas para os números primos						
Título em outra língua:	Prime Numbers - Small Topics						
Palavras-chave em outra língua:	Primes, Mersenne primes, Fermat primes, Other types of primes, Formulas for primes						
Área de concentração:	Teoria dos números						
Data defesa: (15/03/2012)							
Programa de Pós-Graduação:	PROGRAMA DE MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL						
Orientador (a):	Dr. Maurílio Márcio Melo						
E-mail:							
Co-orientador(a):*	Jesus Carlos da Mota						
E-mail:							

*Necessita do CPF quando não constar no SisPG

3. Informações de acesso ao documento:

Concorda com a liberação total do documento [x] SIM [ ] NÃO[1]

Havendo concordância com a disponibilização eletrônica, torna-se imprescindível o envio do(s) arquivo(s) em formato digital PDF ou DOC da tese ou dissertação.

O sistema da Biblioteca Digital de Teses e Dissertações garante aos autores, que os arquivos contendo eletronicamente as teses e ou dissertações, antes de sua disponibilização, receberão procedimentos de segurança, criptografia (para não permitir cópia e extração de conteúdo, permitindo apenas impressão fraca) usando o padrão do Acrobat.

Glauber Cristo Alves de Carvalho

Assinatura do (a) autor (a)

Data: 15 / 03 / 2013

[1] Neste caso o documento será embargado por até um ano a partir da data de defesa. A extensão deste prazo suscita justificativa junto à coordenação do curso. Os dados do documento não serão disponibilizados durante o período de embargo.

GLAUBER CRISTO ALVES DE CARVALHO

Números Primos

Pequenos Tópicos

Trabalho de Conclusão de Curso apresentado ao Programa de Pós–Graduação do Instituto de Matemática e Estatística da Universidade Federal de Goiás, como requisito parcial para obtenção do título de Mestre em matemática

Área de concentração: Teoria dos números.

Orientador: Prof. Dr. Maurílio Márcio Melo

Goiânia
2013

Dados Internacionais de Catalogação na Publicação (CIP)
GPT/BC/UFG

C331n

Carvalho, Glauber Cristo Alves de.
Números primos [manuscrito] : pequenos tópicos / Glauber Cristo Alves de Carvalho. - 2013.
38 f. : tabs.

Orientador: Prof. Dr. Maurílio Marcio Melo.
Trabalho de conclusão de curso (Mestrado) – Universidade Federal de Goiás, Instituto de Matemática e Estatística, 2013.
Bibliografia.
Inclui lista de tabelas.

1. Números primos. 2. Mersene, Números primos de. 3. Fermat, Números primos de. I. Título.

CDU: 511.313

Glauber Cristo Alves de Carvalho

Números Primos: Pequenos Tópicos

Trabalho de Conclusão de Curso defendido no Programa de Mestrado Profissional em Matemática em Rede Nacional – PROFMAT/UFG, do Instituto de Matemática e Estatística da Universidade Federal de Goiás, como requisito parcial para obtenção do título de Mestre em Matemática, área de concentração Matemática do Ensino Básico, aprovado no dia 15 de março de 2013, pela Banca Examinadora constituída pelos professores:

Prof. Dr. Maurílio Márcio Melo
Instituto de Matemática e Estatística-UFG
Presidente da Banca

Prof. Dr. Ary Vasconcelos Medino
Membro/UnB

Prof. Dr. José Hilário da Cruz
Instituto de Matemática e Estatística-UFG

Glauber Cristo Alves de Carvalho

Licenciado em matemática na Universidade Estadual de Goiás (UEG). Durante a gradução foi monitor no departamento de matemática na disciplina de Cálculo Diferencial e Integral III. Foi professor na rede pública (Estadual e Municipal) de ensino do município de Formosa-GO. Atualmente Professor na rede pública de ensino do Distrito Federal e na Universidade Estadual de Goiás.

Dedico este trabalho a todas as pessoas que me ajudaram de forma direta e/ou indireta a alcançar esta conquista. Em especial aos professores que tive durante a minha vida acadêmica.

Agradecimentos

Fazer agradecimentos não é algo fácil, pois podemos esquecer pessoas importantes.

Pelas minhas crenças, tenho de agradecer ao criador do universo, que em sua infinita misericórdia nos mostra um caminho a seguir.

Agradecer aos meus país, Juari e Dhione, pelo auxílio dado nestes 23 anos que eu vivo.

Agradecer aos meus irmãos, Dayanne, Samara e Marcos que não criaram situações que atrapalhasse a construção deste trabalho.

Agradecer aos professores que tive na educação básica. Estes sempre incentivaram, as turmas que estive, a buscar felicidade. Um caminho caminho árduo, mas gratificante.

Agradecer aos professores da graduação, donde encontrei uma nova forma de analisar certas situações. Em especial ao professor Rógerio Cesar, que me inspirou com sua paciéncia e didática.

Aos professores do PROFMAT. Cada um com seu jeito de ensinar, puderam transmitir valores inestimáveis.

Aos colegas da graduação e do PROFMAT que de uma forma ou outra me ajudaram a esclarecer muito do que eu procurava.

Agradecer as escolas que trabalhei, donde pude obter uma nova visão de mundo e muito "stress"em determinadas.

Ao meu orientador. Com seu auxílio, muitos conceitos ficaram mais claros e uma nova "aprendizagem de vida"foi adquirida.

Agradeço a CAPES pelo suporte financeiro.

Pois, quando sou fraco, então sou forte.

Paulo de Tarso,
2º Carta aos Romanos.

A paciência tudo alcança...

Teresa D'Ávila,
Poemas.

Resumo

CARVALHO, Glauber Cristo Alves de. **Números Primos**. Goiânia, 2013. 41p. Trabalho de conclusão de curso. Instituto de Matemática e Estatística, Universidade Federal de Goiás.

Neste trabalho é apresentado um breve histórico sobre os números. Após, algumas definições importantes para compreensão dos textos. Seguindo, nos deparamos com o universo dos números primos. Nesta parte é apresentado algumas propriedades importantes, descobertas e problemas em aberto. O estudo sobre estes números já conseguiu encontrar algumas fórmulas para gerá-los, que são apresentadas no decorrer do texto. Apresenta-se alguns números especias, como os primos de Fermat, Mersene, Shopie German e outros. Por fim, temos uma aplicação que utiliza muitas propriedades apresentadas.

Palavras–chave

Números primos, Primos de Mersene, Primos de Fermat, Outros tipos de números primos, Fórmulas para os números primos

Abstract

CARVALHO, Glauber Cristo Alves de. **Prime numbers**. Goiânia, 2013. 41p. Completion of course work. Instituto de Matemática e Estatística, Universidade Federal de Goiás.

This paper presents a brief history about the numbers. After some important definitions to understand the texts. Following, we encounter the world of prime numbers. This part is presented some important properties, findings and open problems. The study of these figures have managed to find some formulas to generate them, which are presented throughout the text. It presents some numbers especias such as Fermat primes, Mersene, Shopie German and others. Finally, we have an application that uses many properties presented.

Keywords

Primes, Mersenne primes, Fermat primes, Other types of primes, Formulas for primes

Sumário

Lista de Tabelas

Introdução

Durante a minha vida acadêmica uma das disciplinas que mais me encantou foi a teoria dos números. Disciplina a qual tive o prazer de conhecê-la no primeiro ano da graduação e no segundo semestre do mestrado. Dentro desta disciplina escolhi redigir este material apresentando alguns tópicos sobre os números primos.

Tendo em vista os objetivos do Mestrado Profissional em Matemática em Rede Nacional (PROFMAT), escolhi apresentar este assunto de maneira suave. De certa forma um bom estudante do ensino médio ou um acadêmico que estiver iniciando seus estudos em algumas das ciências exatas possa compreender e/ou se encantar com a grandiosidade destes números.

No primeiro capítulo há informações históricas e algumas definições e explicações sobre a noção de número. Conceito este não muito refletido entre a sociedade, mas sua história pode fascinar a muitos. Relembra-se algumas características dos números e agrupamos estes a partir destas características para melhor estudá-los e compreendê-los. Ao fim, temos certas informações sobre os números ao qual este trabalho destina descrever.

No segundo capítulo é colocado algumas definições seguidas de um exemplo, definições estas que são utilizadas nos capítulos posteriores. Caso o leitor fique em dúvida sobre alguma notação, este pode recorrer a este capítulo para melhor clareza dos textos. Para um leitor já acostumado com a simbologia empregada, pode-se ir diretamente ao terceiro capítulo.

No terceiro capítulo é descrito alguns tópicos sobre os números primos. Para a redação deste foi buscado artigos, textos e outros materiais a fim de apresentar alguns fatos interessantes. O leitor perceberá que este é o capítulo mais extenso deste trabalho, por isso o conteúdo foi organizado em seções e subseções. Assim pode-se buscar qualquer tópico de forma rápida.

Cada pessoa possui uma noção do que é interessante, por isso a seleção de informações foi feita a partir de uma organização lógica: Primeiro temos de lembrar a noção de número e uma maneira de organizá-los(Capítulo 1), posteriormente relembrar alguns conceitos (Capítulo 2). Feito isso, podemos de fato, observar as características dos números primos (Capítulo 3). Neste último partiremos de fatos muito antigos até chegarmos

muitas vezes em problemas em aberto, nos quais ninguém conseguiu demostrar com as ferramentas que a matemática possui atualmente.

Para finalizar mostraremos uma aplicação muito utilizada nos dias atuais (Capítulo 4). A utilização desta forma dos números primos decorre de um problema que parece ser muito simples, mas em termos práticos não é. Perceberás que no decorrer do texto do trabalho como um todo, muitos tópicos são tratados em vista da criptografia RSA, sendo assim importante mostrar como ela funciona e um pouco da aplicação de muitos conceitos apresentados para resolver vários problemas decorrentes.

Aos leitores deste, espero que as informações aqui contidas possam contribuir de alguma forma para um novo olhar sobre os números primos.

CAPÍTULO 1

Números

Em nosso dia a dia lidamos com números a todo momento. Os números transmitem vários tipos de mensagens: Momento de acordar, estar no trabalho, sair, almoçar, dormir, encontrar-se com alguém, etc. Eles também podem indicar medidas: quantidade de remédios a ser tomada, distância entre cidades, espaço existente em nossas casas, quanto de mercadorias podemos adquirir através de nosso salário, dentre outras coisas.

Apesar de tanta familiaridade que temos com eles, uma pergunta que não passa na cabeça de muitas pessoas e também não será respondida pelas mesmas, caso perguntemos, é esta: *"O que são números?"*

Ao buscar a resposta em um dicionário[4] obtemos a seguinte definição:

> **Número**: s.m. Expressão de quantidade; unidade; coleção de unidades ou de partes da unidade; série; conta; porção; abundância; cada um dos exemplares de uma publicação; cada um dos quadros ou cenas de uma peça teatral ou de um espetáculo de variedades; [Gram] flexão nominal ou verbal indicativa de um ou mais objetos ou pessoas; - atômico: numeração característica de cada elemento químico em ordem de seus pesos atômicos e que corresponde ao número total de cargas do seu núcleo ou ao número total de elétrons planetários do átomo elemento em causa; - fracionário: o que é constituído por fração da unidade, o mesmo que o número quebrado; - ímpar: aquele que termina em 1, 3, 5, 7 ou 9; - inteiro: aquele que contém a unidade por certo número de vezes; - par: o que termina em zero, 2, 4, 6, 8; - perfeito: assim se denomina um número igual à soma de seus divisores, excetuando ele próprio; - racional: o que pode ser expresso pelo quociente de dois números inteiros; -s primos entre si: os que só têm por divisor comum a unidade; ser um -: ser muito engraçado. **nú.me.ro**

O dicionário traz uma definição formal e várias informações extras. Mas podemos compreender este conceito de outro modo.

O ser humano no decorrer de sua evolução pôde perceber que havia alguns padrões no mundo que o cercava. Em um bando de lobos na floresta havia um padrão diferente de um lobo sozinho, ter um único filho era diferente de ter dois ou mais, mas ter um lobo ou um filho era um padrão comum.

Através da observação deste tipo de padrão, o ser humano começou a desenvolver sons que indicavam quantidades diferentes. A partir da invenção da escrita foi necessário a criação de símbolos para representar estes sons. Estes símbolos sofreram modificações até chegar ao formato que conhecemos atualmente.

Podemos afirmar que números são símbolos e sons que utilizamos para representar e diferenciar padrões quantitativos.

1.1 Tipos de números

No decorrer de nossa vida escolar nos deparamos com vários tipos de números. Estes são separados em grupos para melhor serem estudados.

Números naturais, inteiros, racionais, irracionais, reais e complexos. Uma pessoa que conclui a educação básica no Brasil nos dias atuais teve contato com esta organização dos números.

Se olharmos para a história da humanidade, cada grupo foi surgindo conforme uma necessidade da humanidade. Precisávamos saber quantos animais tínhamos domesticados, se os rebanhos estavam crescendo ou diminuindo, quantas pessoas havia na tribo, etc, para isso criamos números para contar, **os naturais**.

Com o desenvolver do comércio, precisamos de representação para as nossas posses e nossas dívidas, criamos **os inteiros**.

Os reis cobravam impostos sobre as terras, precisamos de ter noção da distância entre dois lugares, altura de muitos objetos, profundidade e área ocupada em determinado espaço, então criamos **os racionais**.

Algumas figuras possuíam padrões, mas os números conhecidos não conseguiam descrever estes padrões, assim enxergamos **os irracionais**, muito discutido dentro da geometria durante a descoberta dos incomensuráveis.

Precisamos formalizar e estruturar muitas descobertas e definições, para isso juntamos todos estes e denominamos eles como **reais**

Mas ainda haviam problemas que não podiam ser resolvidos, pois nosso números, apesar de serem infinitos, pareciam estar incompletos. Assim podemos enxergar **os complexos**.

Este processo não ocorreu da noite para o dia e nem foi feito por uma única pessoa. Tudo demorou mais de três mil anos, contou com a dedicação e esforço de muitas pessoas.

Para este trabalho iremos nos preocupar com o conjunto dos números naturais, mais especificamente com certo padrão de números existente neste que impressiona e encanta muitos matemáticos em mais de dois mil e quinhentos anos, **os números primos**

1.2 Os números primos

Durante a 5^a série/ 6^o ano[1] o estudante tem contato com determinados números naturais, classificados como **números primos**. Vários conceitos e algoritmos são aprendidos a partir destes, mas, em muitos casos, não é transmitido aos estudantes o porque da nomenclatura.

Para melhor compreensão devemos voltar para aproximadamente 400 A.C., época em que ciência e religião eram uma só. Para os matemáticos da época os números possuíam propriedades divinas, estudá-los era estudar os deuses. Alguns filósofos defendiam a ideia de que existia o mundo dos homens e o mundo das ideias, onde a matemática pertencia a este segundo mundo. Aprender matemática era adentrar na luz deste novo mundo e assim iluminado poderíamos iluminar outros. Daí surge a ideia tradicional de aluno (a-luno: o que não tem a luz).

Para os gregos, em especial os pitagóricos, o número um era supremo (a unidade) e todos os demais números eram gerados a partir de quantidades dele. Assim se tinha a unidade e os números. Mas percebeu-se que alguns podiam ser gerados - via multiplicação - por números diferentes de um, como o caso do 6 que pode ser gerado a partir do produto de 3 por 2. Enquanto que outros números não seguiam esta regra. Com isso os números ficaram divididos em três grupos: a unidade, os imcompostos (primários ou primos) e os compostos (ou secundários). Durante o estudo da matemática na idade média e a partir da tradução dos textos gregos para o latim na Europa, a nomenclatura *números primos* foi consagrada por Fibonacci, que a preferia em vez da palavra imcomposto.

[1] O ensino fundamental em 9 anos ainda está sendo implantado no Brasil, algumas escolas ainda utilizam a nomenclatura do ensino em 8 anos

CAPÍTULO 2

Algumas definições

Para melhor compreensão dos tópicos que serão apresentados nos capítulos posteriores, faz-se necessário algumas definições.

Tendo em vista uma melhor organização dos dados aqui apresentados, o texto ficará dividido em duas seções. A primeira terá definições e a segunda será composta de teoremas. As informações serão apresentadas na ordem que aparecem no texto do capítulo 3.

2.1 Definições

Como apresentado no capítulo anterior, podemos agrupar os números. Trabalharemos apenas com o grupo dos **números naturais** e este grupo será representado por $\mathbb{N}$, caso o menor número deste conjunto for o zero e por $\mathbb{N}^*$ caso o menor for um, ou seja,

$$\mathbb{N} = \{0, 1, 2, 3, 4, ...\}$$

,

$$\mathbb{N}^* = \{1, 2, 3, 4, ...\}$$

.

Definição 2.1 *Divisibilidade: Dados dois números a e b temos:*

O número a divide o número b se, e somente se, existir $k \in \mathbb{N}$ de modo que $b = k \cdot a$.

***Notação**: $a \mid b \iff \exists\ k$ tal que $b = k \cdot a$.*

O número a não divide o número b se, e somente se, não existe $k \in \mathbb{N}$ de modo que $b = k \cdot a$.

***Notação**: $a \nmid b \iff \nexists\ k$ tal que $b = k \cdot a$.*

Exemplo: Escolhendo os números naturais $5, 10$ e 12 temos que:

$5 \mid 10$ pois $\exists\ 2 \in \mathbb{N}$ tal que $10 = 2 \cdot 5$.
$5 \nmid 12$ pois $\nexists\ k \in \mathbb{N}$ tal que $10 = k \cdot 5$ seja satisfeita.

Definição 2.2 *Algoritmo de Euclides: Dados dois números a e b, com $a > 0$, temos que exitem q e r, $0 \leq r < a$, tais que $b = q \cdot a + r$.*

Exemplo: Tendo $b = 16$ e $a = 5$ temos que existe 3 e 1 tal que $16 = 3 \cdot 5 + 1$ sendo $1 < 5$.

Definição 2.3 *Conguência: Seja m um número natural diferente de zero. Diremos que dois números a e b são congruentes módulo m se os restos de sua divisão euclidiana por m são iguais. Quando os inteiros a e b são congruentes módulo m, escreve-se:*

$$a \equiv b\ mod(m).$$

Exemplo: Temos que $21 \equiv 13\ mod(2)$, já que os restos da divisão de 21 e de 13 por 2 são iguais a 1.

Definição 2.4 *Máximo divisor comum (Mdc): Dados dois números $a \neq 0$ e $b \neq 0$, a cada número podemos associar um conjunto de divisores, D_a e D_b. A intersecção não é vazia, pois 1 pertence a ambos. Ela é finita, pois o maior elemento de D_a é menor que a e o mesmo ocorre com D_b. O Máximo divisor comum de a e b (denotado como $Mdc(a,b)$) será o maior elemento desta intersecção.*

Exemplo: Tomemos os números 36 e 54, temos que os conjuntos de divisores dos respectivos números são $D_{36} = \{1,2,3,4,6,9,12,18,36\}$ e $D_{54} = \{1,2,3,6,9,18,27,54\}$. A intersecção é $D_{36} \cap D_{54} = \{1,2,3,6,9,18\}$. Logo o $Mdc(36,54) = 18$.

Definição 2.5 *Números primos entre si: Dados dois números $a \neq 0$ e $b \neq 0$, estes são ditos primos entre si quando $Mdc(a,b) = 1$.*

Definição 2.6 *Número primo: é todo número maior que 1 e divisível apenas por 1 e por ele mesmo.*

Exemplo: Temos que os divisores de 5 dentro do conjunto dos naturais são $\{1,5\}$ logo 5 é número primo. Por outro lado os divisores de 6 são $\{1,2,3,6\}$, portanto 6 não é primo.

Definição 2.7 *Número composto: é todo número maior que 1 e que pode ser escrito como produto de dois números, sendo ambos diferente de 1.*

Exemplo: Como no exemplo anterior 6 não é primo, logo ele é composto.

Definição 2.8 *Primorial: Dado um número primo p, o primorial de p (representado por p#) é o produto de todos os números primos menores ou iguais a p.*

Exemplo: (primorial de sete) $7\# = 2 \cdot 3 \cdot 5 \cdot 7 = 210$.

Definição 2.9 *Pseudoprimos: Números compostos que satisfazem o pequeno teorema de Fermat (Ver teorema 2.15 abaixo).*

Exemplo: $341 = 11 \cdot 31$ logo é composto, mas $341 \nmid 2$ e $2^{341-1} \equiv 1 \ mod(341)$

Definição 2.10 *Número de Fermat: Todo número da forma $F_n = 2^{2^n} + 1$, com $n \in \mathbb{N}$*

Definição 2.11 *Número de Mersene*[1] *Todo número da forma $M_q = 2^q - 1$ com q sendo um número primo.*

Definição 2.12 *Função de Möbius:*

Definimos a função de Möbius, $\mu(n) : \mathbb{N}^* \to \mathbb{Z}$, por

$$\mu(n) = \begin{cases} 1 & se \quad n = 1, \\ 0 & se \quad a^2 | n \ \ para \ algum \ \ a > 1, \\ (-1)^k & se \quad n \ é \ produto \ de \ k \ primos \ distintos. \end{cases}$$

[1] Esta definição foi retirada de [7]

2.2 Teoremas

Teorema 2.13 (Teorema Fundamental da Aritmética) *Todo número natural maior do que 1 ou é primo ou se escreve de modo único (a menos da ordem dos fatores) como produto de números primos.*

Exemplo: Podemos escrever o 18 como sendo $2 \cdot 3^2$.

Observação: A importância deste teorema será observada na sequência do trabalho. Por exemplo no capítulo 4.

Teorema 2.14 (Teorema de Wilson) *p é um número primo se, e somente se,*

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

Teorema 2.15 (Pequeno teorema de Fermat) *Dado um número primo p, tem-se que* $p|(a^p - a)$ *para todo* $a \in \mathbb{N}$.

Teorema 2.16 (Teorema Chinês dos Restos) *O sistema:*

$X \equiv c_1 mod(n_1)$

$X \equiv c_2 mod(n_2)$

...

$X \equiv c_r mod(n_r)$,

onde $MDC(n_i, n_j) = 1$, *para todo par* n_i, n_j *com* $i \neq j$, *possui uma única solução módulo* $N = n_1 n_2 ... n_r$. *Tal solução pode ser obtida como se segue:* $x = N_1 y_1 c_1 + ... + N_r y_r c_r$; *onde* $N_i = N/n_i$ *e* y_i *é solução de* $N_i Y \equiv 1\ mod(n_i)$, $i = 1, ..., r$.

A demostração deste teorema pode ser encontrada, por exemplo, em [7]

Exemplo: O matemático Sun-Tsu propôs o seguinte problema:

Qual é o número que deixa 2, 3 e 2 quando dividido respectivamente, por 3,5 e 7?

Este problema pode ser escrito na seguinte forma:

$X \equiv 2\ mod(3)$

$X \equiv 3\ mod(5)$

$X \equiv 2\ mod(7)$,

Tendo em vista o sistema formado, podemos utilizar o Teorema do resto chinês. Os cálculos ficaram da seguinte forma:

$N = 3 \times 5 \times 7 = 105$,

$N_1 = \frac{105}{3} = 35$, $N_2 = 21$ e $N_3 = 15$.

$N_1 y_1 \equiv 1 \ mod(n_1) \Rightarrow 35y_1 \equiv 1 \ mod(3) \Rightarrow y_1 = 2$ de modo análogo $y_2 = 21$ e $y_3 = 1$

Portanto $x = N_1 y_1 c_1 + N_2 y_2 c_2 + N_3 y_3 c_3 = 233$

Como $233 \equiv 23 \ mod(105)$ segue-se que 23 é uma solução para o problema de Sun-Tsu.

CAPÍTULO 3

Números primos

3.1 Finitos ou infinitos?

Ao separarmos os números naturais em três conjuntos ({0, 1}, {primos} e {compostos}) surge o questionamento: se os números primos existem em quantidade finita ou infinita?

Conforme **Euclides** temos:

Por volta de 2300 anos atrás esta questão foi respondida, de maneira magnífica na proposição 20 do livro 9 da obra de Euclides[5], da seguinte forma:

> *Os números primos são mais numerosos do que toda quantidade que tenha sido proposta de números primos.*
>
> Sejam os números primos que tenham sido propostos A,B, C; digo que os números primos sejam mais numerosos do que os A,B,C.
> Fique, pois, tomado o menor medido pelos A,B,C e seja o DE, e fique acrescida a unidade DF ao DE. Então, o EF ou é primo ou não. Primeiramente, seja primo; portanto, os números primos A,B,C, EF achados são mais numerosos do que os A,B,C.
> Mas, então, não seja primo o EF; portanto, é medido por algum número primo. Seja medido pelo primo G; digo que o G não é o mesmo que algum dos A,B,C. Pois, se possível, seja. Mas os A,B,C medem o DE; portanto, o G também medirá o DE. E também mede o EF; e o G, sendo um número, medirá a unidade DF restante; o que é absurdo. Portanto, o G não é o mesmo que algum dos A,B,C. E foi suposto primo. Portanto, os números primos achados, A,B,C, G são mais numerosos do que a quantidade que tenha sido proposta dos A,B,C; o que era preciso provar. (EUCLIDES, por volta de 400 a.c)

Nesta linguagem é um pouco trabalhoso compreender demostração, pois não estamos acostumados com a mesma. Podemos atualizar a escrita mantendo o raciocínio da seguinte forma:

Teorema 3.1 *Existem infinitos números primos.*

Prova.

Suponhamos que os números primos existam em quantidade finita, ou seja, que exista apenas n números primos. Organizemos eles da seguinte forma no conjunto B, $B = \{p_1, p_2, p_3, \cdots, p_n\}$.

Tomemos o número K sendo o sucessor do número composto formado pelos n números primos do conjunto B. $K = p_1 \cdot p_2 \cdot p_3 \cdot ... \cdot p_n + 1$.

Temos duas possibilidades: K é um número primo ou composto.

Se K for primo, K será maior que qualquer número pertencente ao conjunto B, contradizendo nossa suposição.

Se K for composto, logo existe um número primo p_k tal que $p_k|K$, mas se $p_k \in B$ e $p_k|K \Rightarrow p_k|(p_1 \cdot p_2 \cdot p_3 \cdot ... \cdot p_n + 1) \Rightarrow p_k \mid 1 \Rightarrow p_k = 1$ contradizendo mais uma vez nossa suposição.

Logo podemos afirmar que tendo uma quantidade finita de números primos, sempre é possível encontrar um novo número primo, mostrando assim que exitem infinitos números primos.

□

Com base no raciocínio de Euclides, temos algumas proposições interessantes:

Podemos montar um sequência de números a partir da recorrência $K_n = k_1 \cdot k_2 \cdot ... \cdot k_{n-1} + 1$ sendo k_1 um número primo.

Tomemos $k_1 = 2$, teremos:

$k_2 = 2 + 1 = 3$ é número primo

$k_3 = 2 \cdot 3 + 1 = 7$ é número primo

$k_4 = 2 \cdot 3 \cdot 7 + 1 = 43$ é número primo

Continuando a lista temos o conjunto $K = \{2, 3, 7, 43, 1807, 3263443, ...\}$, onde podemos observar que o número 1807 é composto e os demais são primos. Se continuarmos a lista surgiria outros números compostos? Estes seriam em quantidade finita ou infinita?

Para a noção de primorial, definida no segundo capítulo, as perguntas acima estão em aberto, conforme [11]

A infinidade dos números primos também foi demonstrada por outros matemáticos, tais como Goldbach e Euler.

Goldbach também demostrou:

Para demonstrar a infinidade dos números primos basta achar uma sequência infinita de números naturais crescente e primos entre si[1] dois a dois. Se tomarmos um fator primo de cada número, teremos uma sequência infinita de números primos.

[1] Primos entre si: Ver definição 2.5 no capítulo 2

Existem várias sequências donde os números que as compõe são primos estre si, dentre elas temos a sequência dos números de Fermat[2]

Outros matemáticos demostraram utilizando diversas ferramentas:

Euler demostrou utilizando soma de série geométrica. Thue, utiliza o teorema fundamental da álgebra e certa desigualdades. Perrot, utiliza o fato da série $\sum_{n=1}^{\infty} \frac{1}{n^2}$ ser convergente. Auric e Métrod, também demostram por contradição a partir da afirmação de que exista finitos números primos. Washington, provou a infinidade dos números primos utilizando Álgebra Comutativa em 1980. Furstenberg, demostrou com base em ideias topológicas em 1955.

Para leitor interessado nas demostrações acima, poderá consultar [11].

3.2 Como encontrar todos os números primos?

O resultado a seguir mostra a dificuldade de gerar todos os números primos.

Podemos encontrar um intervalo de números naturais consecutivos onde nenhum destes é um número primo. Para isto, dado um número natural k, basta calcular $(k+1)!$, o intervalo que inicia em $(k+1)!+2$ e termina em $(k+1)!+(k+1)$ terá somente números compostos.

$(k+1)!+2, (k+1)!+3, \cdots, (k+1)!+(k+1)$

Pela definição de fatorial, temos que o primeiro termo da sequência é divisível por 2, o segundo por 3 e assim sucessivamente.

Como exemplo, vamos encontrar um intervalo que possui 15 números compostos consecutivos. Calculando $(15+1)!$ temos 1307674368000. Os números da sequência abaixo são todos compostos:

1307674368002, 1307674368003, 1307674368004, 1307674368005,
1307674368006, 1307674368007, 1307674368008, 1307674368009,
1307674368010, 1307674368011, 1307674368012, 1307674368013,
1307674368014, 1307674368015, 1307674368016.

3.2.1 Crivo de Eratóstenes

Por volta de 276 A.C., nasce o matemático Eratóstenes que em seus estudos propõem um método para encontrar todos os números primos em um determinado intervalo.

[2] Ver definição 2.10 no capítulo 2 e a secão 3.6.2 deste capítulo.

Consiste, este método, em colocar os números a partir do 2 em uma tabela, após grifar todos os múltiplos de 2, o seguinte número sem grifar será um primo, logo basta grifar os múltiplos dele e assim por diante.

Para encontrar todos os números primos no intervalo de 2 a 50 podemos proceder como na tabela 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**

Tabela 3.1: *Crivo de Eratóstenes*

Assim encontramos os seguintes números primos:
$2,3,5,7,11,13,17,19,23,29,31,37,41,43$ e 47

3.2.2 Fórmula para encontrar números primos

Muitas pessoas ainda transmitem a ideia de que não existe uma fórmula para encontrar todos os números primos. A professora Watanabe em seu artigo [16] mostra e demonstra que existe uma fórmula para **encontrar todos os números primos**.

Basta proceder da seguinte forma:

Escolha dois números naturais x e y, com $y \neq 0$. Em seguida, encontremos o número $a = x(y+1) - (y!+1)$. Por fim, apliquemos estes números na fórmula 3-1.

$$f(x,y) = \frac{y-1}{2}[\,|\,a^2-1\,|\,-(a^2-1)]+2. \tag{3-1}$$

Como **exemplo**, tomemos $x = 5$ e $y = 10$, obteremos $a = -3628746$, logo $f(5,10) = 2$ que é um número primo. Esta fórmula possui uma predileção pelo número 2, pois a mesma não é injetiva. É possível encontrar todos os números primos através desta, a demonstração da mesma encontra-se em [16].

Neste momento, pode-se surgir a curiosidade de conhecer a demostração desta fórmula. Assim segue abaixo a demostração, conforme publicação da professora Watanabe:

> A demonstração baseia-se no Teorema de Wilson que diz:
> p é primo $\Longleftrightarrow p \neq 1$ e p é um divisor de $(p-1)!+1$.
> Usando esse teorema:
> **a)** Vamos provar que $f(x,y)$ é sempre um número primo.
>
> - O número a é um número inteiro e, portanto, a^2 é inteiro. Há dois casos: $a^2 \geq 1$ ou $a^2 = 0$.
> - Se $a^2 \geq 1$, $\mid a^2 - 1 \mid = a^2 - 1$ e $f(x,y) = 0+2 = 2$.
> - Se $a^2 = 0$, $f(x,y) = \frac{y-1}{2} \times 2 + 2 = y - 1 + 2 = y + 1$.
>
> Neste caso, sendo $a = 0$, temos $x(y+1) = y! + 1$ e, portanto, $y+1$ é um número primo.
>
> **b)** $f(x,y)$ fornece **todos** os números primos.
> Seja p um número primo. Pelo Teorema de Wilson, $\frac{(p-1)!+1}{p}$ é um número natural e podemos calcular $f\left(\frac{(p-1)!+1}{p}, p-1\right)$.
> O valor de a é: $a = \frac{(p-1)!+1}{p} \times p - [(p-1)! + 1 = 0$. Seque-se que $f\left(\frac{(p-1)!+1}{p}, p-1\right) = p - 1 + 1 = p$.

Analisando esta demonstração é possível extrair uma forma de encontrar um par ordenado (x,y) que se associa ao um número primo já conhecido.

No livro do Professor Matinez [9] é apresentado as seguintes fórmulas para gerar números primos grandes:

$$p_n = \left\lfloor 1 - \frac{1}{log 2} log\left(-\frac{1}{2} + \sum_{d|P_{n-1}} \frac{\mu(d)}{2^d - 1}\right)\right\rfloor, \tag{3-2}$$

onde $P_{n-1} = p_1 p_2 \cdots p_{n-1}$ e $\mu(d)$ é a função de Möbius, conforme definição 2.12. A notação $\lfloor x \rfloor$ indica a parte inteira de x.

Outra fórmula é:

$$p_n = \lfloor 10^{2n} c \rfloor - 10^{2n-1} \lfloor 10^{2n} c \rfloor \quad onde \quad c = \sum_{n=1}^{\infty} \frac{p_n}{10^{2n}} = 0,0203000500000007... \tag{3-3}$$

Estas fórmulas não são úteis pois demoram muitos para serem aplicadas e não respondem perguntas teóricas sobre a distribuição dos números primos.

Mills provou, ver [11], que existem números reais A>1 tais que $\lfloor A^{3^n} \rfloor$ é primo para todo $n \in \mathbb{N}$.

O problema que temos na atualidade é encontrar uma forma de gerar todos o números primos de forma rápida e mais simples, tendo em vista que para números muito

grandes a aplicação destes métodos é muito demorado e em várias situações não é viável. Teremos esta noção no capítulo 4.

No livro do Doutor Ribenboim [11] ele apresenta três condições, citadas abaixo, que devem ser satisfeitas por uma fórmula para que esta produza números primos ou até mesmo todos eles.

1. $f(n) = p_n$ (o n-ésimo número primo).
2. $f(n)$ é sempre um número primo e, se $n \neq m$ então $f(n) \neq f(m)$.
3. O conjunto dos números primos é igual ao conjunto dos valores positivos da função.

3.3 Teste de Primariedade

Além de encontrar todos os números primos, outro problema existente é provar se um dado número é primo ou composto. Para números pequenos aprendemos que basta fatorar. Durante a educação básica é uma ideia que fica, mas com números muito grandes, que possuem 100 algarismos, por exemplo, é bem trabalhoso montar uma tabela do 2 até ele e retirar os compostos como no crivo de Eratóstenes ou mostrar se ele pertence a imagem de (3-1).

Eratóstenes mostrou que se tivermos um número e a raiz quadrada do mesmo, caso os números primos menores ou iguais a esta raiz não dividir o número este será primo.

De modo geral: Dado um número $N \in \mathbb{N}$, tomemos o conjunto finito $P_1, ..., P_n$ de números primos tais que $P_k < P_i$ para todo $k < i$ e $P_n \leq \sqrt{N}$. Se todos os $p_i \nmid N$, com $1 \leq i \leq n$, então N é primo.

Exemplo: Tomemos o número 123, temos que $\sqrt{123} \cong 11,09$. Basta testar os números $\{2,3,5,7,11\}$. Após os testes veremos que $3|123$, portanto 123 não é número primo.

Para números de 300 algarismos não seria tão rápido assim.

Durante séculos várias propriedades sobre os números primos foram descobertas, conjecturadas ou definidas.

Pelo teorema de Wilson temos que calcular $(n-1)!\ mod(n)$, com os métodos atuais não é rápido, pois o método que ainda temos é a definição de fatorial.

Uma outra maneira seria utilizar o pequeno Teorema de Fermat, dado um número n e um a tal que $n \nmid a$ temos que se n for primo então $a^n \equiv 1\ mod(n)$. O pequeno teorema de Fermat nos garante que os números primos possuem esta propriedade, mas existem números compostos que também satisfazem este teorema. A estes números compostos chamamos de pseudoprimos. Mas estes são muito escassos, logo ao encontrar um número pelo teorema a probabilidade dele não ser primo é muito pequena. Veremos mais sobre estes números na seção 3.4.

Com uma pequena variação no teorema de Fermat temos que:

Teorema 3.2 *O número p é primo* $\Longleftrightarrow a^{p-1} \equiv 1\ mod(p)$ *para todo* $1 \leq a < p$.

Lucas em 1876, com base no Pequeno Teorema de Fermat criou estes testes que seguem abaixo:

- Teste 1 - Seja $N > 1$. Supõe-se que exista um inteiro $a > 1$ tal que:

  (i) $a^{N-1} \equiv 1\ Mod(N)$ e
  (ii) $a^m \not\equiv 1\ Mod(N)$, para $m = 1, 2, ..., N-2$.
  Neste caso, N é primo.

- Teste 2 - Seja $N > 1$. Supõe-se que exista um inteiro $a > 1$, tal que:

  (i) $a^{N-1} \equiv 1\ Mod(N)$ e
  (ii) $a^m \not\equiv 1\ Mod(N)$ para todo divisor m de N-1.
  Neste caso, N é primo.

- Teste 3 - Seja $N > 1$. Supõe-se que, para todo fator primo q de N-1, exista um inteiro $a = a(q) > 1$, tal que:

  (i) $a^{N-1} \equiv 1\ Mod(N)$ e
  (ii) $a^{\frac{N-1}{q}} \not\equiv 1\ Mod(N)$.
  Neste caso, N é primo.

Também existem outros testes computacionais mais elaborados para realização deste tipo de teste baseados em conhecimentos matemáticos mais avançados.

3.4 Pseudoprimos

Chamaremos de pseudoprimos os números compostos que possuem propriedades esperadas para apenas os números primos. Um pouco sobre estes números é apresentado na seção 3.3.

Em [11] Ribenboim chama de "a congruência pseudo-chinesa sobre os pseudoprimos", por causa de um equivoco histórico, a seguinte congruência: $2^n \equiv 2\ mod(n)$, caso n satisfazer esta, n seria primo.

Todo número pseudoprimo é ímpar e satisfaz esta congruência. Temos que a recíproca também é verdadeira.

Como exemplo temos o número 561. Temos que $2^{561} \equiv 2\ mod(561)$. Pelo Pequeno Teorema de Fermat temos que $2^{561-1} \equiv 1\ mod(561)$. Mas $561 = 3 \cdot 11 \cdot 17$, logo ele é pseudoprimo.

Naturalmente surge as questões: Os pseudoprimos são finitos ou não? Como encontrar todos eles? Existe propriedades especificas para estes números?

Malo, em 1903 mostrou que se n é um pseudoprimo, então $n' = 2^n - 1$ também será. Por esta sucessão podemos notar que a lista de números pseudoprimos é infinita. Mas nem todos estarão nela.

Cipolla, ver [11], utilizou os números de Fermat para demonstrar a infinidade dos pseudoprimos. Lehmer, indicou um método para gerar uma infinidade destes números.

Podemos considerar a congruência $a^{n-1} \equiv 1\ mod(n)$, com $a > 2$. Se n é primo e $1 < a < n$, então a congruência acima é necessariamente satisfeita.

Uma aplicação seria: Se $2^{n-1} \equiv 1\ mod(n)$, mas $3^{n-1} \not\equiv 1\ mod(n)$, então n não é primo.

Assim estudaremos os números a-pseudoprimos. Em 1904 Cipolla indicou como obter estes tipos de números.

Na literatura, por exemplo em [11], encontramos os pseudoprimos de Euler, os fortes na base a, de Lucas, de Fibonacci dentre outros. Não apresentados neste trabalho, mas que podem ser objeto de pesquisa para o leitor interessado neste tipo de número.

3.5 Fatores primos de um número

Um outro grande problema é encontrar os fatores primos de um dado número. Utilizando a ideia de Eratóstenes podemos encontrar os fatores primos de um número dado, tendo em vista que estaremos fazendo vários testes de divisibilidade.

Durante o ensino fundamental, nas escola brasileiras, aprendemos o seguinte método:

> Para chegar à forma fatorada completa de um número natural, fazemos uma **decomposição em fatores primos** que consiste em:
>
> - Dividir o número dado por seu menor divisor primo;
> - Dividir o quociente obtido por seu menor divisor primo;
> - Repetir este procedimento até obter o quociente 1. (Junior 2009 [8])

Um exemplo para melhor compreensão do método:

É um bom método, mas para quem tentou aplicá-lo a números muito grande percebeu um certo trabalho em encontrar o menor divisor primo.

Existem métodos para fatorar números, como exemplo, crivo quadrático, as curvas elípticas, NFS, SNFS e o GNFS. Mas para números extremamente grandes, estes crivos e algoritmos dependem de demasiado tempo e de cáculos computacionais.

Por causa da dificuldade em se fatorar números o método de criptografia RSA é o mais utilizado. Conseguir um algoritmo rápido que possa encontrar estes fatores seria

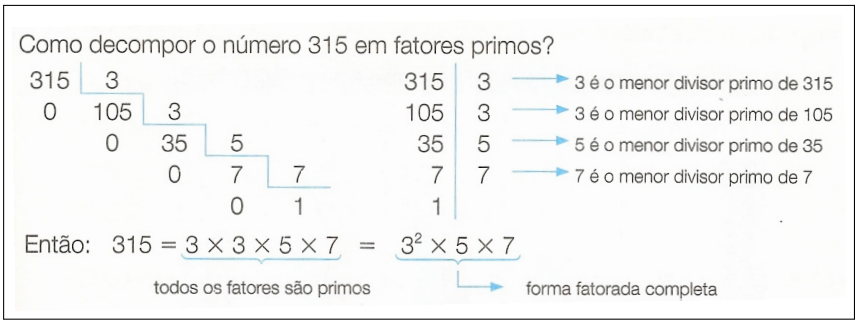

Tabela 3.2: *Exemplo de fatoração*

ao mesmo tempo encontrar uma forma de quebrar o RSA. No Capítulo 4 apresentaremos o método de criptografia RSA, como uma aplicação do conhecimento de números primos.

Atualmente o algoritmo mais rápido para fatorar um número é o de Schroppel, consegue fatorar números na velocidade descrita na tabela 4.1 no capítulo 4.

Muitos algoritmos estão sendo implementados para resolver este problema. Atualmente investimentos são feitos para a criação do computador quântico, onde este utilizaria o algoritmo de Shor, conseguindo quebrar os sistemas baseados em criptografia RSA em poucas horas. Assim a criptografia seria levada a um nível mais elevado: a criptografia quântica.

3.6 Números primos especiais

No decorrer do estudo de números primos que ocorreu desde a Grécia antiga até nossos dias atuais, muitos matemáticos descobriram várias propriedades e padrões dentro do conjunto dos números primos. Apresento aqui algumas delas.

3.6.1 Números primos de Mersene

Definição 3.3 *Um número M_q (ver definição 2.11) é dito primos de Mersene, quando este for primo.*

Para estes números o problema que se apresenta naturalmente é saber se um número de Mersene é primo ou composto e neste último quais fatores primos os compõe.

As demostrações dos resultados abaixo podem ser encontradas em [11].

Um resultado clássico que surgiu foi este:

Teorema 3.4 *Se q é um número primo e $q \equiv 3\ Mod(4)$, então $2q+1$ divide M_q se, e somente se, $2q+1$ é primo, neste caso, se $q > 3$, então M_q é composto.*

É mais fácil encontrar os fatores primos de um número de Mersene composto:

Teorema 3.5 *Se n divide M_q (onde $q > 2$), então $n \equiv \pm 1\ mod(8)$ e $n \equiv 1\ mod(q)$.*

Tomando a sequência definida da seguinte forma:

$$S_0 = 4, \quad S_{k+1} = S_k^2 - 2$$

.

Temos o seguinte resultado:

Teorema 3.6 *O número M_n é primo se, e somente se, M_n divide S_{n-2}.*

Atualmente 47 números primos de Mersene são conhecidos. O maior deles possui $q = 43112609$ e 12978189 algarismos e foi descoberto em 2008.

O maior número de Mersene composto conhecido é M_q, onde $q = 183027 \times 2^{265440} - 1$. Esse q é o maior primo de Shopie Germain conhecido.

As mesmas questões em aberto para os números de Fermat estão abertas também sobre os números de Mersene.

3.6.2 Números primos de Fermat

Definição 3.7 *O número F_n (ver definição 2.10) será um primo de Fermat quando F_n for um número primo.*

Temos que se $a^n + 1$ é primo então a é par e $n = 2^m$ com $a, m \in \mathbb{N}$.

Fermat achava que todos os números F_n eram primos, de fato $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537$ são primos mas $F_5 = 4.294.967.297$ é composto.

Além dos quatro primeiros, não se sabe se existem outros números primos de Fermat. Hardy e Wright conjecturaram que eles existem em número finito.

Temos também que $Mdc(F_n, F_m) = 1$ se $n \neq m$. Utilizando esta propriedade podemos também provar a infinidade dos números primos. Pois os números de Fermat são infinitos e todos possuem fatores primos distintos.

Como os números de Fermat crescem muito rápido é dificil fatorá-los completamente. O maior número de Fermat composto conhecido é $F_{2478782}$. Ele possui 746190 algarismos e o fator $3 \times 2^{2478785} + 1$

Sobre os números de Fermat temos alguns problemas em aberto, dentre eles:

- Existe uma infinidade de Números de Fermat primos?
  Esta pergunta pode ser respondida a partir da demonstração de Gauss, na qual ele mostra que se $n \geq 3$ é um inteiro, o polígono regular de n lados pode ser construído com régua e compasso se $n = 2^k p_1 p_2 \cdots p_n$, onde $k \geq 0$, $h \geq 0$ e $p_1 p_2 \cdots p_n$ são primos de Fermat.

- Existe uma infinidade de números de Fermat Compostos?
- É verdade que todo número de Fermat não possui fator quadrado?

O estudo dos números de Fermat e Mersene propôs uma especial atenção para os **números primos da forma** $kb^n \pm 1$, pois as propriedades destes são muito interessantes para a área da computação.

3.6.3 Números primos de Shopie Germain

Definição 3.8 *O número p é um primo de Sophie Germain se $2p+1$ também for um número primo.*

Atualmente conjectura-se que existam infinitos primos de Sophie Germain, mas ainda não conseguiu-se demostrar.

Um fato interessante sobre este tipo de número é que se p é um primo de Sophie Germain, então existem inteiros x, y e z, diferentes de zero, tais que $x^p + y^p = z^p$. Este é o primeiro caso para o último teorema de Fermat.

Como **exemplo** temos o 5 e o 11 como números primos de Shopie Germain.

3.6.4 Números primos de Wieferich

Definição 3.9 *O número p é um primo de Wieferich se p for número primo e*

$$2^{p-1} \equiv 1 \quad mod(p^2)$$

.

Como exemplo temos os números 1093 e 3511. Esta congruência é muito difícil de ser verificada.

3.6.5 Números primos de Wilson

Definição 3.10 *Com base no teorema de Wilson (Ver definição 2.14) temos que:*

$$W(p) = \frac{(p-1)!+1}{p}$$

é um inteiro. O número p será um primo de Wilson quando $W(p) \equiv 0\ mod(p^2)$.

Conhece-se apenas os números 5, 13 e 593 que podem ser classificados como primos de Wilson. Em 1997, Crandall, Dilcher e Pomerance fizeram cálculos até 5×10^8 e não encontraram nenhum outro. Não se sabe se estes primos são infinitos.

3.6.6 Números primos gêmeos

Definição 3.11 *Quando os números p e $p+2$ são números primos, estes são chamados primos gêmeos.*

Por exemplo temos os pares: $(3,5)$ e $(5,7)$.

Clement caracterizou em 1949 esses números da seguinte maneira:

Teorema 3.12 *Seja $n \geq 2$. Os inteiros n e $n+2$ são ambos primos se, e somente se,*

$$4[(n-1)!+1]+n \equiv 0 \quad mod(n(n+2))$$

.

Essa caracterização não possui praticidade para determinar primos gêmeos.

Os maiores primos gêmeos descobertos são $65516468355 \times 2^{333333} \pm 1$ que possuem 100355 algarismos. Foi descoberto em 2009 por P. Kaiser, K. Klahn, P. Jobling, J. Penné e PrimeGrid.

CAPÍTULO 4

Uma Aplicação: Criptografia RSA

Entende-se por criptografia os métodos inventados para esconder mensagens. Muito utilizados desde a antiguidade para comunicação entre generais nas guerras e famílias importantes de certa região. Estas pessoas precisavam se comunicar de maneira que se suas mensagens fossem interceptadas, estas não pudessem ser lidas.

Muitos métodos foram desenvolvidos, quanto mais a matemática avançava, mais métodos surgiam. Atualmente com o advento tecnológico precisamos enviar informações, como senha de contas, de cartões de crédito dentre outras pela rede mundial de computadores conhecida como Internet. Mas caso essas informações sejam interceptadas na transmissão de dados, o interceptador não deverá compreendê-la.

Como vimos no capítulo 3 encontrar os fatores primos de um número, com a tecnologia e o algoritmos atuais não é uma tarefa rápida, que dependendo do número pode-se demorar até séculos. Por conta deste fato, o método de criptografia RSA[1] é muito utilizado.

Podemos ter uma noção com a tabela 4.1 abaixo, se utilizando um computador capaz de realizar uma multiplicação em um microssegundo (10^{-6} seg) e utilizando o algoritmo de Schroeppel, demoraríamos:

nº de algarismos de n	tempo necessário para "quebrar"o RSA
50	3,9 horas
75	104 dias
100	74 anos
200	3,8 x 10^7 séculos
300	4,9 x 10^13 séculos
500	4,2 x 10^23 séculos

Tabela 4.1: *Tempo médio para "quebrar"o código.*

Vamos compreender como funciona este método. Precisamos de dois números primos, a partir destes números vamos encontrar dois outros conhecidos como *chave pública ou de codificação* e *chave de decodificação*. A chave de codificação pode ser

[1] Método inventado por Ronald **R**ivest, Adi **S**hamir e Leonard **A**dleman em 1977.

enviada junto da mensagem, como para decodificar a mensagem precisamos dos números primos que formaram a chave pública, basta fatorar o número. Mas se este número possuir 300 algarismos o processo de fatoração poderá demorar muito conforme tabela 4.1.

Na prática funciona assim: Primeiro devemos associar cada letra do alfabeto e símbolos que utilizaremos a números, de maneira que não haja ambiguidade.Vamos utilizar a seguinte tabela 4.2 para transformar uma mensagem em uma sequência de números. É importante não haver ambiguidades e para representar um espaço vazio utilizaremos 99.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Q	R	S	T	U	V	W	X	Y	Z	a	b	c	d	e	f
26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41
g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57
w	x	y	z	.	ç										
58	58	59	60	61	62	99									

Tabela 4.2: *Tabela de conversão*

Tomemos então a mensagem da epígrafe deste trabalho e transformemos em uma sequência de números.

A paciência tudo alcança...

10995136384440493844369955563950993647383649623661616 1

Feito isso podemos utilizar o método RSA. Para isso *precisamos de dois números primos x e y tais que quando divididos por 6 deixam resto 5*. Estes números são conhecidos como parâmetros. Para este exemplo tomemos os números $x = 23$ e $y = 29$. Tenha o leitor em vista que utilizamos números pequenos para facilitar os cálculos e o entendimento, no dia a dia estes números possuem mais de 100 algarismos.

A *chave pública* é formada pelo produto dos números escolhidos, ou seja, $n = x * y$. Portanto nosso $n = 667$.

Devemos separar nosso número em blocos tais que cada bloco seja um número menor que a chave pública e não iniciados em zero.

$$109 - 95 - 136 - 384 - 440 - 493 - 84 - 436 - 99 - 555 - 639 - 509 - 93 - 647 - 383 - 649 - 623 - 661 - 616 - 1$$

Cada bloco deve ser *codificado*, representaremos por C(b) o bloco decodificado e b o bloco a ser codificado.. A regra é $C(b) =$ resto da divisão de b^3 por n.

Para codificar o primeiro bloco temos:

$109^3 \equiv 109^2 \cdot 109 \equiv 11881 \cdot 109 \equiv 542 \cdot 109 \equiv 59078 \equiv 382\ mod 667$

O primeiro bloco codificado será 382.

Fazendo os cálculos para os demais blocos teremos a seguinte sequência de blocos codificados:

$$382-622-233-444-62-118-346-377-382-62-311-277-490-62-181-8-181-64-302-355-355-343$$

Esta mensagem e a chave pública poderá ser enviada, veremos agora como *decodificar*, ou seja, voltar a mensagem para o seu estado normal.

Para isso precisamos de um par de números (n,d) chamados de chave de decodificação. o número n já temos, para encontrar o número d teremos de resolver a congruência:

$$3 \cdot d \equiv 1\ mod((x-1) \cdot (y-1)).$$

Para nosso caso temos:

$3d \equiv 1\ mod(22 \cdot 28) \Rightarrow 3d \equiv 1\ mod(616)$

Utilizando conhecimentos básicos de teoria dos números encontraremos $d = 411$. Nossa chave de decodificação será $(667, 411)$.

Sendo s um bloco codificado, para decodificar $(D(a))$ procede-se da seguinte forma: $D(a) =$ resto da divisão de a^d por n.

Sem ajuda computacional, precisaríamos do pequeno teorema de Fermat e o teorema do resto chinês para resolver esta situação, caso contrário seria impossível a solução.

$D(a) = x$ sendo $382^{411} \equiv x\ mod(667)$ e $x < 667$.

Como $667 = 23 \cdot 29$ temos de proceder da seguinte forma:

$a = 382$

$382 \equiv 14\ mod(23)$ e $382 \equiv 5\ mod(29)$.

Temos $382^{411} \equiv 14^{411}\ mod(23)$ e $382^{411} \equiv 5^{411}\ mod(29)$

$14^{411} \equiv 14^{22 \cdot 18+15} \equiv (14^{18})^{22} \cdot 14^{15} \equiv (14^3)^5 \equiv 7^5 \equiv 17\ mod(23)$

Fazendo o mesmo raciocínio na segunda congruência teremos:

$382^{411} \equiv 17\ mod(23)$

$382^{411} \equiv 22\ mod(29)$.

Basta achar a solução do sistema

$x \equiv 17\ mod(23)$

$x \equiv 22\ mod(29)$.

Utilizando o teorema do resto chinês teremos $x = 109$.

Procedendo assim teremos novamente os blocos antes da codificação e por fim utilizando a tabela poderemos ter a mensagem novamente.

Conclusão

Lembro-me de anos atrás ler um artigo, apesar de ter chamado atenção, não me lembro onde eu o encontrei. Mas o que ficou na minha memória foi a informação de que os estudantes que terminam o ensino médio no Brasil, não tem noção da matemática desenvolvida a partir do século XX.

Ao realizar a pesquisa deste trabalho, com a ideia de pesquisar a extensão dos estudos sobre os números primos, matéria esta que apresento aos alunos de 6^o ano/5^a série a mais de 4 anos e atualmente para alunos de graduação (de uma forma bem mais avançada) pude perceber o verdadeiro sentido de determinada afirmação. Esta afirmação ensina que muitos conceitos simples poderiam ter aplicação que os levassem a resolver ou propor problemas muito complexos.

Para leitores interessados este trabalho poderá ser apenas uma revisão de conceitos e conteúdos conhecidos, para outros poderá ser uma nova visão sobre o assunto e poderá haver pessoas que não enxergarão a profundidade dos problemas aqui apresentados. Mas a todos estes que de alguma forma tiveram acesso a este material, que este sirva para uma maior aprendizado sobre os números.

Esta organização dos tópicos apresentados perece-me ser bastante adequada. Primeiro começamos do mundo macro, a ideia de número. Depois fomos restringindo nosso estudo ao ponto de estarmos apenas no mundo dos números primos. Foi apresentado propriedades e em seguida apresenta-se os números primos especiais, tais como os de Fermat, Mersene, dentre outros, algumas propriedades importantes e curiosidades sobre estes. Durante todo este percurso sempre nos deparamos com situações-problema ainda não solucionadas.

Para não fugir aos objetivos deste trabalho, não foi apresentados conceitos muito avançados em matemática, como as curvas elíptica, teoremas baseados na teoria dos conjuntos (corpos, anéis, etc), dentre outros. Mas o leitor interessado poderá buscar estes nos materiais utilizados na pesquisa para este trabalho. Estes materiais são apresentados nas referencias bibliográficas.

Que este trabalho sirva para um novo olhar sobre os números primos em você, leitor. Com meus sinceros cumprimentos

Prof Glauber Cristo

.

Referências Bibliográficas

[1] ANDRADE, L. N. D. **Breve Introdução ao LATEX 2ε**. Universidade Federal da Paraíba, 2000.

[2] BENTLEY, P. **O Livro dos Números: Uma história ilustrada da matemática**. Rio de Janeiro: Jorge Zahar Ed., 2009.

[3] BOYER, C. B. **História da Matemática**. São Paulo: Edgard Blucher, 1996.

[4] BUENO, S. **Minidicionário da língua portuguesa**. São Paulo: FTD, 2000.

[5] EUCLIDES. **Os Elementos**. São Paulo: Editora UNESP, 2009.

[6] FREIRE, B. T. V. **Números primos: Os argumentos de euclides e aplicações**. *CD da Revista do Professor de Matemática (RPM)*, São Paulo: IME USP, 2012.

[7] HEFEZ, A. **Elementos de aritmética**. Rio de Janeiro: SBM, 2011.

[8] JÚNIOR, J. R. G.; CASTRUCCI, B. **A conquista da matemática,** 6^o **ano**. São Paulo: FTD, 2009.

[9] MARTINEZ, F. B.; [ET AL]. **Teria dos números: um passeio com primos e outros números familiares pelo mundo inteiro**. Rio de Janeiro: IMPA, 2011.

[10] RECKDAHL, K. **Using imported graphics in latex and pdflatex**. *Disponível em <ftp://ftp.tex.ac.uk/tex-archive/info/epslatex.pdf>*, Janeiro de, 2013.

[11] RIBENBOIM, P. **Números Primos: Velhos Mistérios e Novos Recordes**. Rio de Janeiro: IMPA, 2012.

[12] SANTOS, J. P. D. O. **Introdução à teoria dos números**. Rio de Janeiro: Impa, 2011.

[13] SILVEIRA, J. F. P. D. **POR QUE O NOME PRIMO PARA OS NÚMEROS PRIMOS?** Disponível em http://www.mat.ufrgs.br/ portosil/pqprimo.html, 15 de Dezembro de 2012.

[14] SOUZA, S. D. **Será que foi assim?** *CD da Revista do Professor de Matemática (RPM)*, São Paulo: IME USP, 2012.

[15] TERADA, R. **Criptografia e a importância das suas aplicações.** *CD da Revista do Professor de Matemática (RPM)*, São Paulo: IME USP, 2012.

[16] WATANABE, R. G. **Uma fórmula para os números primos**. *CD da Revista do Professor de Matemática (RPM)*, São Paulo: IME USP, 2012.