ROY WILHELM PROBST

NÚMEROS PRIMOS

Trabalho de Conclusão de Curso apresentado para avaliação na disciplina de Estágio Supervisionado do Curso de Bacharelado em Matemática do Centro de Ciências Exatas e Naturais da Universidade Regional de Blumenau.

Professor Orientador: Cláudio Loesch

Professor Coordenador: Nelson Hein

BLUMENAU

2003

SUMÁRIO

RESUMO

O propósito deste trabalho é apresentar uma categoria especial de números: os números primos. Será apresentada uma retrospectiva histórica, citando os resultados mais importantes e/ou interessantes obtidos ao longo dos anos. Em seguida, a maioria destes resultados será formalmente enunciada com proposições e suas respectivas demonstrações. Finalmente será apresentada uma das mais importantes aplicações envolvendo números primos, a criptografia de chave pública, além de algumas curiosidades envolvendo números primos.

INTRODUÇÃO

Origem do Trabalho

Os números primos são uma das mais fascinantes partes da matemática. Eles vêm intrigando os matemáticos desde a época dos antigos filósofos gregos, a mais de dois milênios atrás. A área da Matemática que estuda os números inteiros e suas propriedades é chamada Teoria dos Números. Atualmente, os números primos ocupam um papel reduzido nos primeiros capítulos dos livros de Teoria dos Números e Álgebra Moderna. Isto chega a ser uma injustiça, pelo papel fundamental que os números primos exercem hoje, em áreas aplicadas como a criptografia. Este trabalho tem o propósito de apresentar os números primos não como uma introdução às Estruturas Algébricas, mas como uma disciplina independente, capaz de despertar o interesse por suas aplicações.

Objetivo do Trabalho

Este trabalho tem como objetivo geral organizar de modo sistemático os mais destacados avanços dentro da Teoria dos Números, no que se refere aos números primos. Além disso, este trabalho possui os seguintes objetivos específicos:

- Elaborar uma retrospectiva histórica dos números primos;
- Enumerar alguns resultados importantes na área;

- Apresentar os recentes avanços na área da criptografia, auxiliada pela teoria dos números primos.

Importância do Trabalho

Como mencionado anteriormente, os números primos já são conhecidos e estudados a mais de 2.000 anos. Mas isto não significa que este seja um assunto velho: novos números primos e algoritmos para achá-los foram descobertos recentemente, principalmente nos últimos 50 anos, com o advento dos computadores. E ainda existem muitas questões em aberto. Este trabalho pretende fornecer uma visão geral do que foi conquistado no passado sobre o assunto e quais são as próximas metas.

A importância deste trabalho reside no fato de que os recentes avanços na área ainda se encontram em língua estrangeira. Este trabalho trará para o leitor interessado menos familiarizado, principalmente com a língua inglesa, matéria para eventuais pesquisas.

Estrutura do Trabalho

O corpo do trabalho está dividido em três capítulos:

- Retrospectiva Histórica dos Números Primos. Esta primeira parte irá contar a história dos números primos, desde a antiguidade até a atualidade. Não serão apresentadas definições formais ou demonstrações de teoremas, mas um desencadeamento de fatos importantes em ordem cronológica.

- Resultados Importantes. As teorias apresentadas na primeira parte serão agora fundamentadas. Serão apresentados definições, propriedades, proposições e teoremas. O rigor matemático será preocupação constante e sempre que possível os resultados virão acompanhados de suas demonstrações. Os resultados importantes cujas demonstrações ou são enfadonhas ou ultrapassam o escopo deste trabalho serão enunciados sem demonstração. Embora esta seja a parte que mais se assemelha a um livro texto, serão inseridos notas históricas e comentários para tornar o texto mais atrativo.
- Criptografia de chave pública e Curiosidades. O interesse pelos números primos cresceu recentemente graças à suas aplicações na criptografia. Será apresentado o método RSA, que reúne os melhores esforços de Euclides, Fermat, Euler, Gauss e outros. Também serão apresentadas algumas curiosidades envolvendo números primos.

O primeiro e o segundo capítulos são praticamente complementares. Já o terceiro pode ser lido separadamente.

Limitações do Trabalho

Este trabalho não pretende esgotar os assuntos abordados, tornando sua abordagem superficial. Além disso, não é possível cobrir todos os campos envolvendo números primos, pois senão o trabalho se estenderia muito além de seus objetivos.

1. RETROSPECTIVA HISTÓRICA DOS NÚMEROS PRIMOS

"A Matemática é a rainha das Ciências e a Teoria dos Números é a rainha das Matemáticas".

K. F. Gauss

Já nos primeiros anos acadêmicos, entramos em contato com o conceito de números primos: um número inteiro maior que um é primo se os seus únicos divisores são um e ele mesmo. Assim, por exemplo, 2, 3, 5, 7 e 11 são os primeiros números primos. O número 6 não é primo, pois é divisível por 2 e 3, além de ser divisível pela unidade e por ele mesmo. Apesar da simplicidade de sua definição e da facilidade de compreensão, jamais poderíamos imaginar a complexidade que este conceito envolve. Os números primos têm este nome devido aos gregos, que dividiam os números em primeiros ou indecomponíveis e secundários ou compostos. Os compostos são secundários, pois são formados a partir dos primeiros. Daí os romanos traduziram a palavra grega para primeiro, que em latim é *primus*.

Os números primos vem sendo estudados pelos matemáticos desde 500 a.C., aproximadamente. Entre os matemáticos gregos, os pitagóricos (aprox. 500 – 300 a.C.) foram os primeiros a se interessarem pelas propriedades "místicas" dos números. Apesar de conhecer os números primos, eles estavam realmente interessados nos números perfeitos e nos números amigáveis. Um número n é perfeito se a soma de seus divisores é igual a $2n$. Os

quatro primeiro números perfeitos são 6, 28, 496 e 8.128. Dois números se dizem amigáveis se o primeiro é a soma dos divisores próprios do segundo e vice-versa. O menor par de números amigáveis é 220 e 284.

1.1. Euclides e Eratóstenes

Quando Euclides de Alexandria publicou *Os Elementos*, cerca de 300 a.C., já haviam sido provados vários resultados importantes sobre números primos. A demonstração de que existem infinitos números primos aparece no livro IX de *Os Elementos* e é uma das primeiras provas conhecidas que se utiliza a demonstração por redução ao absurdo. Euclides também forneceu a prova para o Teorema Fundamental da Aritmética. Aliás, os livros VII, VIII e IX de *Os Elementos* são quase que exclusivamente dedicados à Teoria dos Números, área da Matemática que estuda os número inteiros e suas propriedades.

Cerca de 200 a.C. o grego Eratóstenes de Cirene (aprox. 276 – 194 a.C.) desenvolveu um algoritmo para calcular números primos, conhecido como Crivo de Eratóstenes. Este algoritmo ainda é a forma mais eficiente de achar todos os números primos não muito grandes. Ele consiste em dispor os números naturais até um determinado valor e eliminar desta lista os múltiplos dos números primos já conhecidos.

1.2 Fermat e Mersenne

Depois de alguns séculos sem qualquer descoberta importante, surge Pierre de Fermat (1.601 – 1.665) no início do século XVII. Ele provou o que ficou conhecido como o Pequeno Teorema de Fermat, que afirma que se p é um número primo, então para todo número inteiro a é válido que $a^p - a$ é divisível por p. Este resultado já era conhecido para o caso particular $a = 2$ cerca de 2.000 anos antes e era conhecido como a Hipótese Chinesa. Ela afirmava também que a recíproca era verdadeira. Além de generalizar para qualquer valor inteiro de a, Fermat mostrou que a recíproca é falsa ($2^{341} - 2$ é divisível por 341, embora 341 = 31 x 11 não seja primo). O Pequeno Teorema de Fermat é a base de muitos outros trabalhos na Teoria dos Números e ainda hoje é utilizado em testes de primalidade.

Em uma carta enviada a Mersenne, Fermat afirma ter descoberto uma fórmula para achar números primos: para todo $n \in \mathrm{N}$, $F_n = 2^{2^n} + 1$ é primo. Embora não tivesse conseguido provar este resultado, a fórmula funcionava para $n = 0, 1, 2, 3$ e 4. Os números da forma $2^{2^n} + 1$ ficaram conhecidos como números de Fermat, mas mais de 100 anos depois Euler provou que $F_5 = 2^{2^5} + 1 = 2^{32} + 1 = 4.294.967.297$ é divisível por 641 e portanto composto.

Os números da forma $M_n = 2^n - 1$ são conhecidos como números de Mersenne. Os números de Mersenne estão diretamente ligados aos números perfeitos, aqueles cuja soma dos seus divisores é igual a duas vezes o próprio número. Já na época de Euclides sabia-se que, se $2^n - 1$ é primo, então $2^{n-1}(2^n - 1)$ é perfeito. Sabe-se hoje que todos os números perfeitos pares são deste tipo, mas não se sabe se existem números perfeitos ímpares. Marin Mersenne (1.588 – 1.648) sabia que, se n é composto, então M_n também será composto. Mas se n é primo, M_n

nem sempre é primo ($2^{11} - 1 = 2.047 = 23 \times 89$ é composto). Em 1.644 Mersenne afirmou (sem provar) que M_n era primo para n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127 e 257 e composto para os outros primos menores que 257. Como na época só havia tábuas de números primos e técnicas para verificar até M_{19}, Mersenne jamais soube se estava certo.

O primeiro erro da lista foi descoberto em 1.886, por Pervusian e Seelhof: M_{61} era primo. Além de M_{61}, também são primos M_{89} e M_{107} e os números M_{67} e M_{257} são compostos. Os resultados foram obtidos pelo chamado Teste de Lucas. Usando seu teste, Lucas (1.842 – 1.891) demonstrou em 1.876 que M_{127} era primo e este número ficou sendo o maior número primo conhecido até 1.952.

Em 1.952 começava a era da computação. Robinson conseguiu mostrar que M_{521}, M_{607}, $M_{1.279}$, $M_{2.203}$ e $M_{2.281}$ são primos, por meio de computadores. Até hoje foram descobertos 39 números primos de Mersenne. O maior deles é $M_{13.466.917}$, possui 4.053.946 algarismos e foi descoberto por Michael Cameron, George Woltman e Scott Kurowski, entre outros, em 14 de novembro de 2.001. Os descobridores participam do GIMPS (Great Internet Mersenne Prime Search – Grande Busca pela Internet por Primos de Mersenne). O GIMPS foi lançado por Woltman em 1.996 e conta com cerca de 120.000 colaboradores espalhados pelo mundo.

1.3 Euler e Gauss

Após Fermat e Mersenne, um século se passou e Leonhard Euler (1.707 – 1.783) trouxe novos avanços à Teoria dos Números. Ele estendeu o Pequeno Teorema de Fermat e

demonstrou uma afirmação mais geral, que ficou conhecida como função φ de Euler. A função $\varphi(n)$ é definida como o número de naturais menores que n que são primos com n. Como mencionado anteriormente, ele fatorou o quinto número de Fermat e achou 60 pares de números amigos. Euler foi o primeiro matemático a usar as ferramentas da Análise Matemática na Teoria dos Números: provou que a série

$$\frac{1}{2}+\frac{1}{3}+\frac{1}{5}+\frac{1}{7}+\frac{1}{11}+\cdots,$$

formada pela soma dos inversos dos números primos, é divergente. Ao somarmos todos os inversos dos números primos já achados até hoje, com o computador mais potente conhecido, a soma seria aproximadamente 4, embora a série divirja para ∞.

Existem quantos números primos menores que um número dado? Esta pergunta vem perseguindo os matemáticos desde quando Euclides provou que existem infinitos números primos, há 2.300 anos atrás. A distribuição dos primos ao longo dos inteiros pode parecer "localmente" irregular, por exemplo, de 9.999.900 à 10.000.000 existem 9 primos enquanto que de 10.000.000 à 10.000.100 existem apenas 2. Mas em grandes escalas, ela se torna bastante regular. Se x é um número real positivo, definimos $\pi(x)$ como sendo a quantidade de números primos menor ou igual a x. Achar uma boa aproximação para a função $\pi(x)$ é um dos problemas mais importantes da Teoria dos Números. Karl Friedrich Gauss (1.777 – 1.855) foi o primeiro matemático a fazer alguns avanços neste sentido: ele estimou

$$\boldsymbol{p}(x) \cong \int_2^x \frac{1}{\ln t}\,dt\,.$$

Já Legendre (1.752 – 1.833) estimou

$$\boldsymbol{p}(x) \cong \frac{x}{\ln x - 1{,}08366}\,.$$

A constante 1,08366 era baseada na tábua de primos limitada que Legendre possuía. Na verdade, a melhor escolha seria

$$\pi(x) \cong \frac{x}{\ln x - 1}.$$

A fórmula de Gauss prevaleceria sobre as de Legendre e mostraria ser equivalente ao Teorema do Número Primo, que afirma que

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

Este teorema foi enunciado por Riemann (1.826 – 1.866), sem ser completamente provado. Somente em 1.896 ele foi provado independentemente por Hadamard e de la Vallé-Poussin.

1.4 Avanços Recentes e Questões Não Resolvidas

Ainda existem muitas conjecturas envolvendo números primos. As duas mais famosas são:

- Conjectura de Goldbach: todo número par ($n > 2$) pode ser escrito como a soma de dois primos.

Em 1.742, Goldbach (1.690 – 1.764) escreveu uma carta para Euler sugerindo que todo número par maior que dois é a soma de dois números primos. A conjectura continua em aberto e somente conseguiu-se provar versões mais fracas dela: todo número par maior que dois é a soma de no máximo seis primos ou números pares suficientemente grandes são a

soma de um primo com um número de no máximo dois fatores primos (P_2). Até 1.998, a conjectura havia sido verificada para todos os números até 4×10^{14}.

- Conjectura dos Primos Gêmeos: existem infinitos primos p tal que $p + 2$ também é primo.

Euler já havia provado que a soma dos inversos de todos os números primos é divergente. Já em 1.919, Brun provou que a soma dos inversos dos primos gêmeos converge. A soma

$$B = \left(\frac{1}{3} + \frac{1}{5}\right) + \left(\frac{1}{5} + \frac{1}{7}\right) + \left(\frac{1}{11} + \frac{1}{13}\right) + \left(\frac{1}{17} + \frac{1}{19}\right) + \cdots \cong 1{,}9021605778$$

é conhecida como constante de Brun. Caso a série divergisse, a conjectura dos primos gêmeos estaria provada. O maior par de primos gêmeos conhecido é $33.218.925 \times 2^{169.690} - 1$ e seu ímpar consecutivo.

Podem ser citadas ainda outras questões não resolvidas:

- Existem infinitos primos da forma $n^2 + 1$?
- Existe sempre um número primo entre n^2 e $(n + 1)^2$?
- Existem infinitos primos de Fermat? Aliás, existe algum maior que F_4?
- Existem infinitos primos da forma $n\# + 1$ ou $n\# - 1$?
- Existem infinitos primos da forma $n! + 1$ ou $n! - 1$?
- Existem infinitos primos na seqüência de Fibonacci?

Lembramos que $n\#$ significa o produto de todos os números primos menores ou iguais a n é denominado o primordial de n. Esta função já era utilizada por Euclides, embora não com esta simbologia. A função $n\#$ aparece na demonstração de que existem infinitos números primos.

São oferecidos prêmios para quem conseguir algum avanço na Teoria dos Números. A Eletronic Frontier Foundantion oferece um prêmio de cem mil dólares por um primo de Mersenne com dez milhões de algarismos. Já o Instituto Clay oferece um milhão de dólares para quem provar (ou refutar) a Hipótese de Riemann, um problema relacionado com a distribuição dos números primos ao longo dos naturais.

Um dos mais recentes avanços foi feito em 2.001 por Manindra Agrawal, Neeraj Kayal e Nitin Saxena, do Instituto Indiano de Tecnologia de Kanpur. Eles descobriram um algoritmo de maior eficiência computacional, para testar se um número é primo ou composto. O algoritmo não fornece os divisores do número caso ele seja composto: um alívio para os criptógrafos.

Aliás, os números primos só eram estudados por razões teóricas, até que a criptografia os colocou no papel central. O estudo das propriedades dos grupos de ordem prima possibilitou a criação de vários métodos na criptografia. O estudo de números primos é de grande interesse no mundo inteiro.

Além dessa introdução histórica, este trabalho tem como objetivo reunir os resultados importantes envolvendo números primos. Estes geralmente de encontram espalhados e desempenham um papel secundário em livros de Álgebra Abstrata e Teoria dos Números. Além da parte teórica, será apresentado o método RSA, um cripto-sistema de chave pública utilizado em softwares como o Netscape, um dos mais utilizados para acessar a Internet.

2. RESULTADOS IMPORTANTES

"O problema de distinguir os números primos dos números compostos e de exprimir estes últimos à custa de seus fatores primos deve ser considerado como um dos mais importantes e úteis em Aritmética. Ele tem envolvido o esforço e a sabedoria de antigos e atuais matemáticos em tal escala que seria inútil discutir o problema detalhadamente... Apesar disso, a própria dignidade da ciência requer que todos os meios possíveis sejam explorados para a resolução de um problema tão elegante e famoso".

K. F. Gauss

Neste capítulo serão apresentados os resultados mais importantes envolvendo os números primos. Serão assumidas como conhecidas as propriedades mais básicas dos conjuntos numéricos. O conjunto dos números naturais será denotado por $N = \{0, 1, 2, 3,...\}$ e o conjunto dos números inteiros por $Z = \{..., -2, -1, 0, 1, 2,...\}$.

2.1 Definições preliminares

Comecemos com as definições mais básicas.

Definição: Sejam $a, b, c \in \mathbb{Z}$. Dizemos que a é um divisor de c se existe b tal que $ab = c$. Notação: $a|c$ (lê-se a divide c).

Definição: Um número natural $p \neq 1$ é chamado número primo se os seus únicos divisores não negativos são 1 e p.

A própria definição de número primo pode gerar alguma polêmica. Alguns autores preferem estender a definição de número primo para todos os inteiros. Neste trabalho utilizaremos a definição acima, pois não há a necessidade de estender a discussão aos inteiros. Podemos considerar que um número é primo se seu oposto também o for. Em virtude desta correspondência, basta considerar os inteiros positivos.

2.2 Algoritmo Euclidiano

O primeiro resultado importante a ser apresentado é conhecido como Algoritmo da Divisão Inteira ou Algoritmo Euclidiano.

Teorema (Algoritmo da Divisão Inteira): Sejam $a, b \in \mathbb{Z}$, $b > 0$. Existem únicos inteiros q e r tais que $a = bq + r$ e $0 \leq r < b$.

Prova: (Existência) Seja $S = \{a - bx \geq 0 \,/\, x \in \mathbb{Z}\}$. $S \neq \emptyset$, pois para $x = -|a|$, temos $a - bx = a + b|a| \geq a + |a| \geq 0$. Como S é limitado inferiormente, então existe $r = \min(S)$. Assim $r \geq 0$ e digamos $r = a - bq$, ou seja, $a = bq + r \in \mathbb{Z}$. Se, por absurdo, $b \geq r$, temos

$r = b + r'$, onde $r' \geq 0$ e como $b > 0$ teremos $r' < r$. Portanto $r' \notin$ S. Mas $r' = r - b =$ $= a - bq - b = a - b\,(q + 1)$, logo $r' \in$ S. Absurdo, logo $r < b$.

(Unicidade) Suponha $a = bq + r$ e $a = bq_1 + r_1$, com $0 \leq r < b$ e $0 \leq r_1 < b$. Assim $bq + r = bq_1 + r_1$ ou $r - r_1 = b(q_1 - q)$. Sem perda de generalidade, suponha $r > r_1$. Assim $q_1 - q$ ou $q_1 - q \geq 1$. Logo $r = r_1 + b\,(q_1 - q) \geq b$. Absurdo, logo $r_1 = r$ e conseqüentemente $q_1 = q$. ■

Definiremos a seguir o máximo divisor comum de dois números, que é o maior inteiro que os divide simultaneamente.

Definição: Sejam $a, b \in$ Z. Dizemos que $d \in$ Z é o máximo divisor comum entre a e b se:

(i) $d \geq 0$;

(ii) $d|a$ e $d|b$ e

(iii) se $d' \in$ Z tal que $d'|a$ e $d'|b$, então $d'|d$.

Notação: mdc (a,b).

A proposição a seguir pode ser considerada uma propriedade, e será utilizada nas próximas demonstrações.

Proposição: Sejam $a, b, c \in$ Z. Se $a|b$ e $a|c$, então $a|(bx + cy)$, para todo $x, y \in$ Z.

Prova: Por hipótese $b = ad_1$ e $c = ad_2$. Logo $bx = a(xd_1)$ e $cy = a(yd_2)$. Portanto $bx + cy = a(xd_1 + yd_2)$, o que mostra que $a|(bx + cy)$. ■

Proposição: Quaisquer que sejam $a, b \in Z$, existe $d \in Z$ tal que $d = \text{mdc}(a,b)$.

Prova: Sem perda de generalidade, vamos considerar $a > 0$ e $b > 0$. Seja $L = \{ax + by / x, y \in Z\}$. Evidentemente existem números positivos em L. Seja d o menor desses elementos. Mostraremos que d é o máximo divisor comum entre a e b.

(i) d é obviamente maior que zero;

(ii) Como $d \in L$, existem x_0 e $y_0 \in Z$ tal que $d = ax_0 + by_0$. Aplicando o algoritmo da divisão aos elementos a e d, temos $a = dq + r$ $(0 \leq r < d)$. Assim $a = (ax_0 + by_0)q + r$ ou $r = a(1 - qx_0) + b(-y_0q)$. Logo $r \in L$. Como $0 \leq r < d$ e d é o mínimo de L, então $r = 0$. Daí $a = dq$, ou seja, $d|a$. Analogamente se prova que $d|b$

(iii) Se $d'|a$ e $d'|b$, como $d = ax_0 + by_0$, pela primeira proposição então $d'|d$. ■

A próxima proposição é conhecida como Propriedade Fundamental dos Números Primos ou Lema de Euclides. Alguns autores a utilizam como definição de número primo.

Proposição (Lema de Euclides): Se p é primo e $p|ab$, então $p|a$ ou $p|b$.

Prova: Se $p|a$, então a proposição está provada. Caso $p \nmid a$, então os únicos divisores comuns de p e a são -1 e 1. Daí $\text{mdc}(p,a) = 1$. Pela demonstração da proposição anterior, existem $x_0, y_0 \in Z$ tal que $1 = ax_0 + py_0$. Portanto $b = (ax_0 + py_0)b = (ab)x_0 + p(by_0)$. Pela primeira proposição, como $p|ab$ e $p|p$ então $p|b$. ■

Generalizando, se p é primo e $p|a_1a_2...a_n$, então $p|a_i$, para algum $i = 1, 2, ..., n$.

2.3 Teorema Fundamental da Aritmética

No livro IX de *Os Elementos*, Euclides provou dois dos mais importantes resultados sobre números primos: haviam infinitos números primos e todo número inteiro podia ser fatorado de maneira única em número primos. Este último ficou conhecido como o Teorema Fundamental da Aritmética. A primeira demonstração conhecida para este teorema foi dada por Euclides, mas ele não enunciou a unicidade da decomposição em fatores primos. A seguir, serão apresentadas duas demonstrações distintas. A primeira, baseada nos conceitos de máximo divisor comum e números primos entre si, é devida a Gauss. A segunda é devida a Zermelo, e não utiliza os conceitos de mdc e primos entre si: estes conceitos passam a ser conseqüência do Teorema Fundamental da Aritmética. Já o teorema que afirma a infinidade de números primos tem um lugar de destaque, pois é um dos primeiros resultados demonstrado por redução ao absurdo na História da Matemática.

Teorema (Teorema Fundamental da Aritmética): Seja $n \in \mathrm{N}$, $n > 1$. Então existem únicos primos $p_1 \leq p_2 \leq ... \leq p_r$ tais que $n = p_1 ... p_r$.

Prova: (Existência) Por indução matemática.

1) Para $n = 2$ a afirmação é verdadeira, pois 2 é primo;
2) Considere o teorema verdadeiro para qualquer $n \geq 2$. Então $n + 1$:

   2.1) é primo, logo a afirmação é verdadeira;

   2.2) é composto, logo existe $a, b \in \mathrm{N} / n + 1 = ab$, $1 < a,b < n + 1$. Como $a,b \leq n$, o teorema é válido para a e b, logo também para $ab = n + 1$.

(Unicidade – Gauss) Suponha que n possua duas decomposições em fatores primos: $n = p_1...p_k = q_1...q_l = p_1(p_2...p_k)$. Então $p_1|q_1...q_l$, logo existe i, $1 \leq i \leq l$ tal que $p_1|q_i$, ou seja, $p_1 = q_i$. Reordenando os índices (se necessário) podemos supor $p_1 = q_1$. Aplicando a lei do cancelamento temos $p_2...p_k = q_2...q_l$ e prosseguindo com este raciocínio, temos $p_i = q_i$, com $i = 1, 2, ..., k$. Resta mostrar que $k = l$. Suponha, sem perda de generalidade, $l < k$. Logo podemos escrever $p_1...p_k = p_1...p_k q_{k+1}...q_l$, ou seja, $1 = q_{k+1}...q_l$. Isto é um absurdo, pois então q_l dividiria 1. Logo $k = l$ e a decomposição é única.

(Unicidade – Zermelo) Suponha que n possua uma decomposição em fatores primos: $n = p_1...p_s$. Se $n = q_1...q_t$ é uma outra decomposição em fatores primos, diremos que a primeira é diferente da segunda se, e somente se, existir um fator p_i ($1 \leq i \leq s$) tal que $p_i \neq q_j$, para $j = 1, 2, ..., t$. Consideremos então o conjunto S de todos os números inteiros $n > 1$ tais que n admite decomposições diferentes. Temos que provar que S = ∅. Suponha S ≠ ∅. Como S é limitado inferiormente, S tem um mínimo n. Logo $n = p_1p_2...p_s = q_1q_2...q_t$, onde existe um p_i ($1 \leq i \leq s$) tal que $p_i \neq q_j$, para $j = 1, 2, ..., t$. Podemos reordenar os índices de modo que $p_1 \leq p_2 \leq ... \leq p_s$ e $q_1 \leq q_2 \leq ... \leq q_t$. É obvio que $s > 1$ e $t > 1$ e vamos supor $p_1 \neq q_1$. De fato, se $p_1 = q_1$, poderíamos aplicar a lei do cancelamento, e o número inteiro $n' = p_2p_3...p_s = q_2q_3...q_t$ admitiria duas fatorações distintas. Assim $n' \in$ S, um absurdo, pois $n' < n$ e $n = \min$ (S). Suponha, sem perda de generalidade, $p_1 < q_1$. Então o número $m = n - p_1q_2...q_t =$ $= q_1q_2...q_t - p_1q_2...q_t = (q_1 - p_1)q_2...q_t$. Como $0 < m < n$, pois $0 < q_1 - p_1 < q_1$, então $m \notin$ S, logo m não possui fatorações distintas. Mas $m = n - p_1q_2...q_t = p_1p_2...p_s - p_1q_2...q_t =$ $= p_1(p_2...p_s - q_2...q_t)$. Logo p_1 é um fator primo de m e deveria aparecer também na decomposição $m = (q_1 - p_1)q_2...q_t$. Como $p_1 < q_1 \leq q_2 \leq ... \leq q_t$ concluímos que $p_1|(q_1 - p_1)$, ou

seja, $p_1|q_1$. Mas isto é uma contradição, pois q_1 é primo e $p_1 < q_1$. Portanto S = ∅, logo a fatoração é sempre única. ■

Teorema (Euclides): O conjunto P dos números primos é infinito.

Prova: Suponha que P é finito, P = $\{p_1, ..., p_r\}$ e suponha que temos $p_1 < p_2 < ... < p_r$. Considere o número $u = p_1...p_r + 1$, que não pode ser primo, pois $u > p_r$. Então, pelo Teorema Fundamental da Aritmética, existe $p_i \in$ P, $1 \leq i \leq r$ tal que $p_i|u$. Logo existe $q \in$ Z tal que $u = p_1...p_r + 1 = p_iq$. Isto implica que $1 = p_iq - p_1...p_r = p_i (q - p_1...p_{i-1}p_{i+1}...p_r)$. Ou seja, $p_i|1$, um absurdo, pois a unidade não possui divisores primos. Logo P é infinito. ■

2.4 Crivo de Eratóstenes

Como mencionado anteriormente, Eratóstenes foi um matemático grego que viveu entre 284 a.C. a 250 a.C.. Ele desenvolveu um algoritmo bastante simples para achar números primos menores que um número dado, que não envolve nenhuma fórmula explícita. Embora se torne cada vez mais lento para números cada vez maiores, o Crivo de Eratóstenes ainda é bastante útil. Dos algoritmos apresentados neste capítulo, este será o único que virá acompanhado de exemplo. O motivo é simples: o Crivo de Eratóstenes é ideal para ser desenvolvido manualmente para números pequenos, enquanto que outros algoritmos só se tornam eficazes para números muito grandes.

O crivo na verdade é uma peneira, que separa os números primos dos compostos. Antes de mostrar o algoritmo, será provado uma proposição que irá melhorar o algoritmo.

Proposição: Seja $a \in \mathbb{Z}$, $a > 1$. Se a não é primo e d é o menor divisor de a, então $d^2 \leq a$.

Prova: Se $d|a$, então existe $q \in \mathbb{Z}$ tal que $a = dq$. Como d é o menor divisor de a, então $d \leq q$. Como $d > 1$, então $dd \leq dq$. Logo $d^2 \leq a$. ■

Para descobrir todos os números primos menores que um inteiro n, devemos inicialmente escrever o número 2 e todos os inteiros ímpares maiores que 2 e menores que n (os números pares maiores que 2 são compostos). Os passos do algoritmo são descritos a seguir:

1. O número 2 é primo. Como $2^2 = 4$, todos os números menores que 4 são primos. Assim 2 e 3 são primos. Risque todos os múltiplos de 3.
2. Como $3^2 = 9$, todos os números menores que 9 não riscados são primos. Logo 2, 3, 5 e 7 são primos. Risque os múltiplos de 5 e os múltiplos de 7.
3. Como $7^2 = 49$, todos os números menores que 49 não riscados são primos. Logo 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43 e 47 são primos. Risque os múltiplos de 11, 13, 17, 19, 23, 29, 31, 37, 41, 43 ou 47.
4. Repete-se este raciocínio até atingirmos um primo p tal que $p^2 > n$.

A garantia de que todos os números não riscados são primos é dada pela proposição provada anteriormente, pois cada número m não riscado não possui divisor primo p tal que $p^2 \leq m$.

Ao riscar os múltiplos de um certo primo p, aqueles múltiplos de p que são múltiplos de primos menores que p já foram riscados. Logo podemos começar a riscar a partir de menor múltiplo de p que não é múltiplo de um primo menor que p, ou seja, p^2.

O exemplo a seguir ilustra todas estas considerações.

Exemplo: Determine todos os números primos menores que 100 pelo Crivo de Eratóstenes.

Para iniciar, é necessário escrever o número 2 e todos os inteiros ímpares maiores que 2 e menores que 100.

2	3	5	7	9	11	13	15	17	19
21	23	25	27	29	31	33	35	37	39
41	43	45	47	49	51	53	55	57	59
61	63	65	67	69	71	73	75	77	79
81	83	85	87	89	91	93	95	97	99

Como 2 é primo e $2^2 = 4$, os números menores que 4 são primo: 2 e 3. Em seguida riscamos todos os múltiplos de 3. Podemos começar a riscar a partir de $3^2 = 9$, pois os números menores que 9 são primos.

2	3	5	7	~~9~~	11	13	~~15~~	17	19
~~21~~	23	25	~~27~~	29	31	~~33~~	35	37	~~39~~
41	43	~~45~~	47	49	~~51~~	53	55	~~57~~	59
61	~~63~~	65	67	~~69~~	71	73	~~75~~	77	79
~~81~~	83	85	~~87~~	89	91	~~93~~	95	97	~~99~~

Como 5 é primo e $5^2 = 25$, os números não riscados menores que 25 são primos. Podemos começar a riscar os múltiplos de 5 a partir de 25.

2	3	5	7	~~9~~	11	13	~~15~~	17	19
~~21~~	23	~~25~~	~~27~~	29	31	~~33~~	~~35~~	37	~~39~~
41	43	~~45~~	47	49	~~51~~	53	~~55~~	~~57~~	59
61	~~63~~	~~65~~	67	~~69~~	71	73	~~75~~	77	79
~~81~~	83	~~85~~	~~87~~	89	91	~~93~~	~~95~~	97	~~99~~

Como 7 é primo, e $7^2 = 49$, os números não riscados menores que 49 são primos. Podemos riscar os múltiplos de 7 a partir de 49.

2	3	5	7	~~9~~	11	13	~~15~~	17	19
~~21~~	23	~~25~~	~~27~~	29	31	~~33~~	~~35~~	37	~~39~~
41	43	~~45~~	47	~~49~~	~~51~~	53	~~55~~	~~57~~	59
61	~~63~~	~~65~~	67	~~69~~	71	73	~~75~~	~~77~~	79
~~81~~	83	~~85~~	~~87~~	89	~~91~~	~~93~~	~~95~~	97	~~99~~

Como 11 é primo e $11^2 = 121 > 100$, chegamos ao final do crivo. Os números primos menores que 100 são: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89 e 97.

Embora o algoritmo seja fácil de programar, computacionalmente ele é ruim, pois necessita de muita memória.

2.5 Fórmulas Polinomiais

Uma questão de grande interesse dos matemáticos é a busca por fórmulas que forneçam sempre números primos. A primeira tentativa foi através das funções polinomiais de Z em Z. Por exemplo, $f(n) = n^2 - n + 41$ é primo para $0 \leq n \leq 40$ e $f(n) = n^2 - 79n + 1601$ é primo para $0 \leq n \leq 79$. Não se sabe se estas fórmulas fornecem infinitos números primos, mas já foi provado que, para qualquer função polinomial $f(x) = a_n x^n + a^{n-1}x^{n-1} + ... + a_1 x + a_0$, onde $a_n, ..., a_0$ são inteiros, existem infinitos inteiros positivos m tal que $f(m)$ é composto. A proposição abaixo demonstra este fato para o caso $n = 2$.

Proposição: Seja $f(x) = ax^2 + bx + c$, com $a, b, c \in Z$. Existem infinitos inteiros positivos m tal que $f(m)$ é composto.

Prova: Podemos supor que $a > 0$, pois caso contrário raciocinaríamos com $-f(x)$. Se para todo inteiro m, $f(m)$ é composto, a afirmação está verificada. Seja m tal que $f(m) = p$, com p primo, e considere um inteiro positivo h tal que $aph > -b - 2am$. Temos que $f(m + ph) = a(m + ph)^2 + b(m + ph) + c = (am^2 + bm + c) + p(aph^2 + bh + 2amh) = p + p(aph^2 + bh + 2amh) = p(1 + aph^2 + bh + 2amh)$. Como $h > 0$ e $aph + b + 2am > 0$, temos $aph^2 + bh + 2amh > 0$ ou $1 + aph^2 + bh + 2amh > 1$ e, portanto, $f(m + ph)$ é o produto de um número primo por um número maior que 1, logo composto. Então $f(m + ph)$ é composto sempre que

$$h > \frac{-b - 2am}{ap}.$$

Como existem infinitos valores que h pode assumir, existem infinitos inteiros positivos x tal que $f(x)$ é composto. ■

Para valores maiores de n, seria necessário utilizar o binômio de Newton para calcular f ($m + ph$). Já para achar a cota inferior de h seria necessário extrair as raízes de um polinômio de grau $n - 1$.

A conclusão é que não existe uma fórmula polinomial deste tipo que gere sempre números primos. Porém, existem fórmulas de várias variáveis cujos valores positivos são sempre primos. Infelizmente estes polinômios têm grau muito alto, muitas variáveis e são complicados demais para terem alguma utilidade prática.

Abandonando as fórmulas polinomiais, os matemáticos se voltaram para as fórmulas exponenciais. Por razões históricas tentou-se achar primos da forma $2^n \pm 1$.

2.6 Números de Mersenne

Os números da forma $M_n = 2^n - 1$ são chamados números de Mersenne. Para que um número de Mersenne seja primo, é necessário que o expoente n seja primo. A proposição abaixo prova isto, mas observe que a recíproca não é verdadeira, pois $M_{11} = 2^{11} - 1 = 2047 = 23 \times 89$ é composto.

Proposição: Se n é composto, então M_n também é composto.

Prova: Seja $n = rs$. Então $M_n = 2^n - 1 = 2^{rs} - 1 = (2^r - 1)(2^{r(s-1)} + 2^{r(s-2)} + \ldots + 2^r + 1)$. Logo $M_r = 2^r - 1$ é um fator de M_n. ■

Os números de Mersenne receberam este nome em homenagem a Marin Mersenne (1588 – 1648), que afirmou que M_n é primo para n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127 e 257 e composto para os outros 44 valores primos de n menores que 257.

Fermat demonstrou que se um número primo q é fator de M_p então q é da forma $2kp + 1$, onde $k \geq 0$ é um número inteiro. Esta proposição simplifica bastante a verificação se um dado número M_p é primo ou não.

Proposição: Seja $p \neq 2$ um primo e q um fator primo de M_p. Então $q = 2kp + 1$ para algum inteiro positivo k.

Além disso, Mersenne sabia que se M_p for composto, então tem um fator $q \leq \sqrt{M_p}$. O problema é que na época de Mersenne a maior tábua de primos conhecida era a elaborada por Cataldi e continha todos os números primos até 750.

Portanto era possível verificar a primalidade de números menores que $750^2 = 562.500$. Voltando aos números Mersenne, era possível verificar a primalidade somente até M_{19}, pois $M_{19} = 2^{19} - 1 = 524.287$. Para números de Mersenne maiores que M_{19}, Mersenne contava com a sorte para que o fator primo de M_p fosse menor que 750. A lista de Mersenne carecia de credibilidade para verificação da maioria dos valores.

Em 1.732 Euler afirmou que M_{41} e M_{47} seriam primos. Estes números não estão na lista de Mersenne, mas neste caso, quem estava errado era Euler. O primeiro erro da lista foi descoberto 238 anos depois da morte de Mersenne. Em 1.886 Pervusian e Seelhof provaram que M_{61} era primo, embora não constasse na lista de Mersenne. Nos anos seguintes, foram encontrados mais 4 erros. Em 1.902 Cole provou que M_{67} é composto, em 1.911 Powers

provou que M_{89} é primo e em 1.914 que M_{107} é primo e finalmente em 1.926 Kraitchik demonstrou que M_{257} é composto, embora não se conheça nenhum fator primo deste número. Os erros acima foram achados utilizando o teste de Lucas, que será apresentado mais adiante.

A próxima proposição mostra que os primos de Mersenne estão diretamente ligados aos números perfeitos, aqueles cuja soma de seus divisores é igual a duas vezes o próprio número.

Proposição: Se $2^n - 1$ é primo, então $2^{n-1}(2^n - 1)$ é perfeito.

Prova: Suponha que $p = 2^n - 1$ é um número primo e seja $k = 2^{n-1}(2^n - 1)$. Para mostrar que k é perfeito precisamos provar que $\sigma(k) = 2k$, onde $\sigma(k)$ é a soma de todos os divisores positivos de k. Se p é um número primo, então $\sigma(p) = p + 1 = 2^n$. Além disso, a função σ é multiplicativa, ou seja, $\sigma(k) = \sigma(2^{n-1})\,\sigma(2^n - 1) = (2^n - 1)\,2^n = 2k$. Isto mostra que k é um número perfeito. ■

Sabe-se que todos os números perfeitos pares são desta forma, mas ainda permanece não respondida a questão se existem números perfeitos ímpares.

2.7 Números de Fermat

Outra fórmula exponencial bastante explorada foi tentar achar primos da forma $2^k + 1$. É possível provar que se $2^k + 1$ é primo, então k é uma potência de 2. Logo, estamos procurando primos da forma $2^{2^n} + 1$. Para provar esta propriedade seria necessário definir

muitos outros conceitos da Teoria dos Grupos, desviando o foco deste trabalho. Por este motivo esta proposição será deixada sem demonstração.

Proposição: Se $p = 2^k + 1$ é primo, então $k = 2^n$, para algum $n \in$ N.

Os números da forma $F_n = 2^{2^n} + 1$ são conhecidos como números de Fermat, pois Pierre de Fermat (1.601 – 1.665) os enunciou pela primeira vez. Em uma carta enviada a Mersenne, Fermat afirmou que esta fórmula fornecia sempre números primos. Realmente, para $0 \leq n \leq 4$, F_n é primo, mas Fermat jamais conseguiu demonstrar a veracidade da fórmula. E nem poderia, pois em 1.739, Euler provou que F_5 é divisível por 641, logo composto. Voltaremos aos números de Fermat após apresentar o Pequeno Teorema de Fermat.

A seguir será demonstrado o Pequeno Teorema de Fermat. Embora não o tenha demonstrado, Fermat enunciou este teorema em 1.640, em uma carta enviada para Frenicle. Este teorema é a base de muitos testes de primalidade que veremos mais adiante e pode ser considerado o resultado mais importante descoberto por Fermat. Euler publicou em 1.736 a primeira demonstração para este teorema, embora Leibniz tenha deixado praticamente a mesma demonstração em um manuscrito não publicado, datado de 1.683. Antes de enunciar o Pequeno Teorema de Fermat, será definido congruência.

Definição: Sejam $a, b, m \in$ Z. Dizemos que a é congruente a b módulo m se, e somente se, m divide $a - b$. Notação: $a \equiv b \pmod{m}$.

Teorema (Pequeno Teorema de Fermat): Se p é primo e $a \in Z$, então $a^p \equiv a \pmod{p}$. Em particular, se p não divide a, então $a^{p-1} \equiv 1 \pmod{p}$.

Prova: Sejam os primeiros $p - 1$ múltiplos positivos de a: a, $2a$, $3a$, ..., $(p - 1)a$. Suponha que ra e sa tenham o mesmo resíduo módulo p. Então $r \equiv s \pmod{p}$ e os $p - 1$ múltiplos de a são distintos e diferentes de zero, ou seja, eles devem ser congruentes a 1, 2, 3, ..., $p - 1$, em alguma ordem. Multiplicando todas as congruências temos $a.2a.3a \ldots (p - 1)a \equiv$ $\equiv 1.2.3....(p - 1) \pmod{p}$ ou ainda $a^{(p-1)}(p - 1)! \equiv (p - 1)! \pmod{p}$. Dividindo ambos os termos por $(p - 1)!$ a prova está completa. O caso mais geral segue praticamente como um corolário. Se p não divide a, então basta multiplicar ambos os lados da congruência por a para completar a prova. Se p divide a, então o resultado é trivial, pois ambos os termos são zero. ■

Embora os números de Fermat não sejam uma boa fonte de números primos, pode-se provar que existem infinitos números primos através deles. Isto segue da proposição abaixo.

Proposição: Se $m \neq n$, então mdc $(F_n, F_m) = 1$.

Prova: Vamos supor, sem perda de generalidade, que $n > m$. Então $n = m + x$, com $x > 0$. Como

$$2^{2^{n+1}} - 1 = \left(2^{2^n} - 1\right)\left(2^{2^n} + 1\right)$$

temos

$$\begin{aligned} 2^{2^{m+x}} - 1 &= \left(2^{2^{m+x-1}} + 1\right)\left(2^{2^{m+x-1}} - 1\right) \\ &= \left(2^{2^{m+x-1}} + 1\right)\left(2^{2^{m+x-2}} + 1\right)\left(2^{2^{m+x-2}} - 1\right) \\ &\vdots \\ &= \left(2^{2^{m+x-1}} + 1\right)\left(2^{2^{m+x-2}} + 1\right)\left(2^{2^{m+x-3}} + 1\right)\cdots\left(2^{2^m} + 1\right)\left(2^{2^m} - 1\right) \end{aligned}$$

Logo

$$2^{2^m}+1 \mid 2^{2^n}-1,$$

ou seja, existe q inteiro tal que

$$2^{2^n}-1=\left(2^{2^m}+1\right)q$$

e então

$$\left(2^{2^n}+1\right)-\left(2^{2^m}+1\right)q=2\,.$$

Seja d = mdc (F_n, F_m). Então $d|2$, ou seja, $d = 2$ ou $d = 1$. Como todos os números de Fermat são ímpares, $d = 1$. ■

A proposição acima mostra que dois números de Fermat quaisquer não possuem fatores primos em comum. Como o conjunto dos números de Fermat é infinito, o conjunto dos números primos tem que ser infinito também. Esta propriedade dos números de Fermat é apenas um caso específico de uma propriedade muito mais ampla. Por exemplo, se S_0 e a são primos entre si, com $S_0 > a$ 1, a sucessão definida pela fórmula de recorrência

$$S_n = a + S_{n-1}\,(S_{n-1} - a)$$

é composta de inteiros primos entre si, dois a dois. Assim, os números de Fermat, onde $S_0 = 3$ e $a = 2$ pode ser definida através da fórmula de recorrência

$$F_n = 2 + F_{n-1}\,(F_{n-1} - 2) = 1 + (F_{n-1} - 1)^2.$$

Aliás, qual é a probabilidade de mdc (m,n) = 1? Embora a probabilidade de um número ser primo diminua para valores maiores (Teorema do Número Primo), a probabilidade de dois números escolhidos aleatoriamente serem primos entre si é constante, aproximadamente 60,8%. Este resultado também será apresentado sem demonstração, pois seriam necessárias muitas ferramentas do Cálculo Diferencial e Integral.

Proposição: Sejam $m, n \in$ Z. Então $P[mdc(m,n)=1]=\frac{6}{p^2}\cong 60{,}8\%$.

Como mencionado anteriormente, Fermat acreditava que os números da forma $F_n = 2^{2^n}+1$ eram sempre primos, para $n \in$ N. Somente em 1.739 Euler mostrou que F_5 é composto. O método utilizado por ele pode ser resumido na proposição abaixo.

Proposição: Se p é um fator primo de F_n, então $p = 2^{n+2}k + 1$, para algum $k \in$ N.

A demonstração desta proposição não será apresentada, pois utiliza o símbolo de Legendre, que não será apresentado neste trabalho. Mas isto não nos impede de acompanhar o raciocínio de Euler para fatorar F_5.

Para o caso particular de F_5, Euler sabia que $p = 2^{5+2}k + 1 = 2^7 k + 1 = 128k + 1$, para algum $k \in$ N. Assim:

- Se $k = 0$ então $p = 1$ não é primo;
- Se $k = 1$ então $p = 129$ não é primo;
- Se $k = 2$ então $p = 257$ é primo, mas $2^{2^5} \equiv 1 \pmod{257}$;
- Se $k = 3$ então $p = 385$ não é primo;
- Se $k = 4$ então $p = 513$ não é primo;
- Se $k = 5$ então $p = 641$ é primo, e $2^{2^5} \equiv -1 \pmod{641}$.

Logo 641 é um fator primo de F_5. De fato

$$F_5 = 2^{2^5}+1 = 4.294.967.297 = 641 x\, 6.700.417 .$$

Note que se Euler tentasse determinar o outro fator primo de F_5 utilizando o seu método, ele teria que prosseguir até k = 52.347, pois 6.700.417 = 52.347 x 128 + 1. Na

verdade, como o valor de F_n cresce muito rapidamente, pois é duplamente exponencial, o método de Euler se torna rapidamente inútil. Observe que Euler contou com muita sorte no caso de F_5, pois um dos fatores primos é um número pequeno.

2.8 A Função j de Euler

Antes de abordar outros testes de primalidade, será apresentado a chamada função φ de Euler. Esta função é uma generalização do Pequeno Teorema de Fermat.

Definição: Seja $n \geq 1$, $n \in \mathbb{N}$. Então $\varphi(n)$ é a quantidade de inteiros a, $1 \leq a \leq n$, tais que mdc $(a,n) = 1$.

Assim, se p é primo então $\varphi(p) = p - 1$ e $\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p - 1)$. Esta fórmula se justifica pelo fato de existirem exatamente p^{k-1} inteiros positivos menores que p^k que são divisíveis por p. Além disso, φ é uma função multiplicativa, ou seja, se m, $n \geq 1$ e mdc$(m,n) = 1$, então $\varphi(mn) = \varphi(m)\varphi(n)$. Assim tem-se uma fórmula para calcular os valores da função de Euler para números compostos.

Dentro da Teoria dos Grupos, a função de Euler é interpretada como a quantidade de elementos que possuem inverso multiplicativo em Z_n.

O teorema abaixo também foi demonstrado pelo criador da função φ e é conhecido como Teorema de Euler.

Teorema (Teorema de Euler): Sejam $n > 0$, a, $n \in$ Z. Se mdc(a,n) = 1, então $a^{\varphi(n)} \equiv 1$ (mod n).

Prova: Seja $r = \varphi(n)$ e sejam b_1, b_2, ..., b_r inteiros, dois a dois, não côngruos módulo n, tais que mdc(b_i,n) = 1, para $i = 1, ..., r$. Têm-se então que ab_1, ab_2, ..., ab_r são ainda, dois a dois, não côngruos módulo n e mdc(ab_i,n) = 1, para $i = 1, ..., r$. Daí, os conjuntos $\{b_1 \bmod n, ..., b_r \bmod n\}$ e $\{ab_1 \bmod n, ..., ab_r \bmod n\}$ são iguais. Então

$$a^r \prod_{i=1}^{r} b_i \equiv \prod_{i=1}^{r} ab_i \equiv \prod_{i=1}^{r} b_i \pmod{n}$$

e daí

$$\left(a^r - 1\right) \prod_{i=1}^{r} b_i \equiv 0 \pmod{n}$$

donde resulta que $a^r \equiv 1$ (mod n). ■

O Teorema de Euler mostra porque a função φ é uma generalização do Pequeno Teorema de Fermat, pois possuí menos restrições. Enquanto que no teorema de Fermat é necessário que p seja primo e p não divida a para que $a^{p-1} \equiv 1$ (mod p), no teorema de Euler basta que a e n sejam primos entre si para que $a^{\varphi(n)} \equiv 1$ (mod n). Note que se $n = p$ for primo, então $\varphi(p) = p - 1$, como definido previamente.

2.9 Testes de Primalidade

Como visto anteriormente, a recíproca do Pequeno Teorema de Fermat não é verdadeira. Um exemplo utilizado pelo próprio Fermat e já apresentado no primeiro capítulo é

$2^{341} \equiv 1 \pmod{n}$, embora 341 = 11 x 31 seja composto. Este exemplo sugere uma nova categoria de números.

Definição: Sejam n, $a \in Z$, $n > a$, n composto. Se $a^{n-1} \equiv 1 \pmod{n}$, então n é pseudoprimo na base a.

No exemplo acima, 341 é pseudoprimo na base 2. Não existem números que sejam pseudoprimos em todas as bases. Isto é provado na próxima proposição.

Proposição: Seja n um número composto, com fator b. Então n não é pseudoprimo para a base b.

Prova: Se b é um fator de n, então $\text{mdc}(b^{n-1}, n) \neq 1$. Então b não possui inverso multiplicativo módulo n. Em particular, $b^{n-1} \not\equiv 1 \pmod{n}$.■

No entanto, um número composto n pode ser pseudoprimo para todas as bases a que são primas com n.

Definição: Sejam n, $a \in Z$, $n > a$, n composto. Se $a^{n-1} \equiv 1 \pmod{n}$ para todo a, $1 < a < n$, onde a é primo com n, então n é um número de Carmichael.

É interessante frisar que para um número ser de Carmichael é necessário que ele seja composto. Um número primo p também satisfaz a equação $a^{p-1} \equiv 1 \pmod{p}$, mas não é um número de Carmichael. O menor número de Carmichael é 561. Estes números são bastante

raros entre os números inteiros. Por exemplo, entre 1 e 1.000.000 existem apenas 43 números de Carmichael (contra 78.498 números primos). Uma pergunta natural é saber quantos números de Carmichael existem. Esta questão foi resolvida por Alford, Granville e Pomerance, em 1.994. Pelo grau de complexidade da demonstração e pelo enfoque introdutório dados aos números de Carmichael neste trabalho, a próxima proposição será apresentada sem demonstração.

Proposição: Existem infinitos números de Carmichael.

A discussão sobre os números de Carmichael serviu para mostrar que a recíproca do Pequeno Teorema de Fermat não pode ser utilizada como um teste de primalidade, pois existem números compostos que se comportam como os números primos. Porém, com algumas adaptações, Lucas elaborou em 1.876 um teste baseado no Pequeno Teorema de Fermat, conhecido como Teste de Lucas. Este teste se tornou a principal fonte de números primos da sua época.

Proposição (Teste de Lucas): Seja $n \in Z$, $n > 1$. Supõe-se que exista um inteiro $a > 1$ tal que $a^{n-1} \equiv 1 \pmod{n}$ e $a^m \not\equiv 1 \pmod{n}$, para $m = 1, ..., n-2$. Então n é primo.

Prova: Basta mostrar que todo inteiro m, $1 \leq m < n$ é primo com n, isto é, $\varphi(n) = n - 1$. Com este objetivo, basta mostrar que existe a, $1 \leq a < n$, $\text{mdc}(a,n) = 1$, tal que a ordem de a módulo n seja $n - 1$. Isto é exatamente o que exprime a hipótese. ■

Ao longo dos anos, outros matemáticos, inclusive o próprio Lucas, criaram versões mais flexíveis para o Teste de Lucas. Entretanto, todos os testes de primalidade baseados no Teste de Lucas têm o mesmo defeito: são necessárias muitas multiplicações sucessivas por a e muitas congruências para verificar que 1 não é resíduo módulo n.

Para encerrar a discussão sobre testes de primalidade, será apresentado o algoritmo descoberto pelos indianos Manindra Agrawal, Neeraj Kayal e Nitin Saxena, em 2.001. Embora a demonstração seja relativamente direta, ela é extremamente extensa e necessita de muitos outros resultados auxiliares, extrapolando o objetivo deste trabalho. Por isso ele será exibido sem demonstração.

Algoritmo (Algoritmo Indiano)

Entrada: inteiro $n > 1$

Algoritmo

1. Se n é da forma a^b, $b > 1$ retorne COMPOSTO;
2. $r = 2$;
3. Enquanto $r < n$ {
4. Se (mdc(n,r) $\neq 1$) retorne COMPOSTO;
5. Se (r é primo)
6. Seja q o maior fator primo de $r - 1$;
7. Se $q \geq 4\sqrt{r} \ln n$ e $n^{\frac{r-1}{q}} \not\equiv 1 \pmod{r}$
8. Pare;
9. $r \leftarrow r + 1$;
10. }
11. Para $a = 1$ até $2\sqrt{r} \ln n$
12. Se $(x-a)^n \not\equiv (x^n - a) (\mathrm{mod}\ x^r - 1, n)$ retorne COMPOSTO;
13. Senão retorne PRIMO.

2.10 Distribuição dos Números Primos

Outra questão de grande interesse para os matemáticos é a quantidade de números primos menores que um número dado. A função de contagem dos números primos é definida a seguir.

Definição: Seja $x > 0$. Então $\pi(x)$ é o número de primos p tais que $p \leq x$.

Os matemáticos vêm tentando achar boas aproximações para $\pi(x)$ por funções contínuas. Em 1.792 Gauss conjecturou que $\pi(x)$ era assintoticamente aderente a função integral logarítmica, definida como

$$Li\,(x) = \int_2^x \frac{dt}{\ln t}.$$

Introduzindo a notação $f(x) \sim g(x)$ para f e g assintoticamente iguais quando x tende para o infinito, Gauss sabia que

$$Li(x) \sim \frac{x}{\ln x}.$$

Logo a conjectura poderia ser rescrita como

$$p(x) \sim \frac{x}{\ln x}.$$

Este fato só foi provado em 1.896, por Hadamard e de la Vallée Poussin e é conhecido como Teorema do Número Primo.

Teorema (Teorema do Número Primo): $\lim_{x\to\infty} \frac{p(x)\cdot \ln n}{x} = 1$

A aproximação de $\pi(x)$ por Li (x) é bem melhor que por

$$\frac{x}{\ln x},$$

mas existem outras funções ainda melhores, como será mostrado a seguir. Vale a pena frisar que quando Gauss conjecturou a aproximação de $\pi(x)$ pela função integral logarítmica ele contava com apenas 15 anos de idade.

Inspirado pelo Teorema do Número Primo, Legendre conjecturou em 1.798 que

$$\pi(x) \sim \frac{x}{\ln x - 1{,}08366}.$$

Quarenta anos mais tarde Tschebycheff mostrou que a conjectura era falsa.

A melhor aproximação conhecida de $\pi(x)$ é dada utilizando-se a Função de Riemann. Antes de apresentá-la, serão necessárias algumas observações adicionais. Serão apresentadas algumas fórmulas e resultados sem definição prévia, apenas com o objetivo de alcançar a Hipótese de Riemann.

Euler definiu a função zeta como

$$\zeta(x) = \sum_{n=1}^{\infty} \frac{1}{n^x},$$

para todo número real x tal que $x > 1$. Riemann teve a idéia de generalizá-la para o campo complexo, por

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s},$$

para todo número complexo s tal que Re (s) >1. Em 1.859 Riemann conseguiu uma equação que não restringia o valor de Re (s), intervindo a função $\Gamma(s)$:

$$\pi^{-\frac{s}{2}} \Gamma\left(\frac{s}{2}\right) \zeta(s) = \pi^{\frac{-(1-s)}{2}} \Gamma\left(\frac{1-s}{2}\right) \zeta(1-s).$$

Riemann observou que a sua função zeta possuía zeros triviais nos pontos –2, –4, –6, ... e zeros não triviais na reta

$$\mathrm{Re}(s) = \frac{1}{2}.$$

Riemann conjecturou que todos os zeros não triviais ρ da função zeta se encontram sobre esta reta crítica, isto é

$$\rho = \frac{1}{2} + it.$$

Esta é a Hipótese de Riemann, que nunca foi provada, embora se acredita que seja verdadeira. Uma suposta demonstração da Hipótese de Riemann foi apresentada pelos colombianos

Carlos Castro e Jorge Mahecha, no final de 2.002. Esta demonstração ainda está sendo verificada por outros matemáticos, antes de ser reconhecida como correta. Caso se confirme, a prova da Hipótese de Riemann será um dos mais importantes avanços da Matemática nos tempos atuais.

Caso a Hipótese de Riemann seja verdadeira, é possível definir a função de Riemann como

$$R(x) = \sum_{n=1}^{\infty} \frac{m(n)}{n} \cdot Li\left(x^{-n}\right),$$

onde $\mu(n)$ é a função de Möbius. Riemann indicou a seguinte fórmula, reunindo $\pi(x)$ e $R(x)$:

$$p(x) = R(x) - \sum_{r} R\left(x^{r}\right),$$

onde a soma é estendida a todos os zeros ρ não triviais da função zeta. Assim é possível aproximar $\pi(x)$ por $R(x)$. A tabela a seguir compara o valor de $\pi(x)$ com as funções

$$\frac{x}{\ln x},$$

Li (x) e $R(x)$.

Como $\pi(x)$ só assume valores naturais e as três funções citadas acima são contínuas, é necessário utilizar apenas a parte inteira de cada uma delas (isto é representado pelos colchetes).

x	$\pi(x)$	$\left[\frac{x}{\ln x}\right]-\pi(x)$	$[\mathrm{Li}\,(x)]-\pi(x)$	$[\mathrm{R}(x)]-\pi(x)$
10^8	5.761.455	–332.774	754	97
10^9	50.847.534	–2.592.592	1.701	–79
10^{10}	455.052.511	–20.758.030	3.104	–1.828
10^{11}	4.118.054.813	–169.923.160	11.588	–2.318
10^{12}	37.607.912.018	–1.416.705.193	38.263	–1.476
10^{13}	346.065.536.839	–11.992.858.452	108.971	–5.773
10^{14}	3.204.941.750.802	–102.838.308.636	314.890	–19.200
10^{15}	29.844.570.422.669	–891.604.962.453	1.052.619	73.218
10^{16}	279.238.341.033.925	–7.804.289.844.393	3.214.632	327.052
10^{17}	2.623.557.157.654.233	–68.883.734.693.929	7.956.589	–598.255
10^{18}	24.739.954.287.740.860	–612.483.070.893.537	21.949.555	–3.051.366
10^{19}	234.057.667.276.344.607	–5.481.624.169.369.961	99.877.775	23.884.333
10^{20}	2.220.819.602.560.918.840	–49.347.193.044.659.702	222.744.643	–4.891.825

Como sugere a tabela, Rosser e Schoenfeld provaram em 1.962, que se $x \geq 17$, então

$$\frac{x}{\ln x} \leq \pi(x).$$

A tabela também sugere que $\pi(x) < \mathrm{Li}\,(x)$, para x suficientemente grande. Embora Gauss e Riemann acreditassem nesta conjectura, Littlewood mostrou em 1.914 que a diferença $\mathrm{Li}\,(x) - \pi(x)$ muda de sinal infinitas vezes. Este episódio mostra que mesmo grandes matemáticos, como Gauss e Riemann, também erraram. Em 1.933 Skewes determinou um limite superior para a primeira mudança de sinal de $\mathrm{Li}\,(x) - \pi(x)$. O número $10^{10^{10^{34}}}$ ficou conhecido como número de Skewes e se tornou célebre, embora já seja possível determinar um limite superior bem menor.

Antes de terminar o capítulo, vale a pena lembrar que Euler foi o primeiro matemático a utilizar as séries, em especial a função zeta, em problemas que envolvem números primos. Ele mostrou que

$$1+\frac{1}{2^n}+\frac{1}{3^n}+\frac{1}{4^n}+\frac{1}{5^n}+\cdots=\frac{2^n}{2^n-1}\cdot\frac{3^n}{3^n-1}\cdot\frac{5^n}{5^n-1}\cdot\frac{7^n}{7^n-1}\cdots,$$

ou seja,

$$\zeta(s) = \prod_p \frac{1}{1 - p^{-s}}.$$

Em 1.737 Euler utilizou esta igualdade para demonstrar a infinidade de números primos. A última proposição deste capítulo ilustra isto, embora sua demonstração ultrapasse o escopo deste trabalho.

Proposição: A soma dos inversos dos números primos é divergente, isto é,

$$\sum_p \frac{1}{p} = \infty.$$

3. CRIPTOGRAFIA DE CHAVE PÚBLICA E CURIOSIDADES

"Na maior parte das ciências uma geração põe abaixo o que a outra construiu, e o que uma estabeleceu a outra desfaz. Somente na Matemática é que cada geração constrói um novo andar sobre a antiga estrutura".

H. Hankel

A criptografia é a arte de codificar e decodificar uma mensagem de modo que apenas o seu destinatário verdadeiro possa lê-la. Em grego, *cryptos* significa secreto, oculto. Um dos primeiros códigos a serem utilizados consiste em substituir cada letra por outra pré-determinada. Embora bastante simples este sistema possui duas falhas gravíssimas: saber codificar implica em saber também decodificar e o código pode ser facilmente quebrado por meio de contagem de freqüência das letras. Outros métodos foram criados para contornar este problema.

3.1 Criptografia de Chave Pública

Em 1.976, Diffie e Hellman propuseram um tipo de cripto-sistema de chave pública, no qual saber codificar não implica saber decodificar. O mais famoso e difundido método de criptografia de chave pública é conhecido como RSA. Este método foi idealizado em 1.978 por Rivest, Shamir e Adleman e é utilizado, por exemplo, no Netscape, um dos softwares

mais conhecidos para acesso à Internet. Este método será descrito a seguir, pois está diretamente fundamentado na teoria dos números primos e é uma das mais importantes aplicações envolvendo números primos.

Antes de iniciar a codificação é necessário que cada caractere da mensagem seja substituído por um número. Para simplificar, suporemos que a mensagem não contém números, símbolos ou sinais, apenas letras, e que a conversão será feita pelo *American Standard Code for Information Interchange (ASCII)*:

A	B	C	D	E	F	G	H	I	J	K	L	M
65	66	67	68	69	70	71	72	73	74	75	76	77

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
78	79	80	81	82	83	84	85	86	87	88	89	90

Assim, a palavra *MATEMÁTICA* é substituída por

77658469776584736765.

A chave de codificação, que é pública, consiste num par de inteiros (n, e), onde $n = pq$ é o produto de dois primos distintos p e q e e deve ser inversível módulo $\varphi(n)$, ou seja, $\text{mdc}(e, \varphi(n)) = 1$, onde φ é a função de Euler. Por exemplo, se $p = 53$ e $q = 137$, então $n = 53 \times 137 = 7.261$. Agora a mensagem deve ser separada em blocos, cada um menor que n. Assim, uma das formas possíveis para separá-la é:

776 – 5846 – 977 – 6584 – 736 – 765.

Observe que cada bloco não corresponde a nenhuma unidade lingüística, o que torna a contagem de freqüência de letras impossível.

Para iniciar a codificação é necessário escolher o parâmetro e. Se $n = 53 \times 137 = 7.261$ então $\varphi(n) = (53 - 1)(137 - 1) = 7.072$. Assim, toma-se qualquer número e tal que mdc $(7.072, e) = 1$. O menor destes números é $e = 3$, logo a chave pública de codificação deste exemplo é (7.261, 3).

A codificação de cada bloco b é feita tomando-se o resto da divisão de b^e por n. Denotando o bloco codificado por C (b), onde $0 \leq C(b) < n$, temos

$$C(b) \equiv b^e \pmod{n}.$$

Codificando os blocos do exemplo:

$$C(776) \equiv 776^3 \equiv 6.921 \pmod{7.261}$$

$$C(5.846) \equiv 5.846^3 \equiv 6.693 \pmod{7.261}$$

$$C(977) \equiv 977^3 \equiv 1.037 \pmod{7.261}$$

$$C(6.584) \equiv 6.584^3 \equiv 2.841 \pmod{7.261}$$

$$C(736) \equiv 736^3 \equiv 1.268 \pmod{7.261}$$

$$C(765) \equiv 765^3 \equiv 5.648 \pmod{7.261}$$

Logo, a mensagem codificada é:

$$6921 - 6693 - 1037 - 2841 - 1268 - 5648.$$

A chave de decodificação, mantida em segredo, consiste num par de inteiros (n, d), onde d é o inverso de e em $Z_{\varphi(n)}$, ou seja, $ed \equiv 1 \pmod{\varphi(n)}$. É obvio que d existe, pois e foi escolhido de forma que mdc $(e, \varphi(n)) = 1$. No exemplo dado, $d = 4.715$, logo a chave de decodificação para este exemplo é (7.261, 4.715).

A decodificação de cada bloco a é feita tomando-se o resto da divisão de a^d por n. Denotando o bloco decodificado por D (a), onde $0 \leq D(a) < n$, temos

$$D(a) \equiv a^d \pmod{n}.$$

Assim, decodificando os blocos codificados anteriormente:

$$D\ (6.921) \equiv 6.921^{4.715} \equiv 776 \pmod{7.261}$$

$$D\ (6.693) \equiv 6.693^{4.715} \equiv 5.846 \pmod{7.261}$$

$$D\ (1.037) \equiv 1.037^{4.715} \equiv 977 \pmod{7.261}$$

$$D\ (2.841) \equiv 2.841^{4.715} \equiv 6.584 \pmod{7.261}$$

$$D\ (1.268) \equiv 1.268^{4.715} \equiv 736 \pmod{7.261}$$

$$D\ (5.648) \equiv 5.648^{4.715} \equiv 765 \pmod{7.261}$$

Embora não sejam apresentados neste trabalho, existem algoritmos bastante eficientes para a determinação de d (conhecido como algoritmo euclidiano estendido) e para a potenciação módulo n (através da expansão binária do expoente). Mas não existe nenhum algoritmo eficiente para fatorar n. A segurança do método RSA se baseia neste fato, pois mesmo que n e e sejam públicos, é necessário calcular o inverso de e módulo $\varphi(n)$. Como $\varphi(n) = (p - 1)(q - 1)$, é necessário conhecer p e q. Porém, se p e q são números primos muito grandes, a fatoração de n não pode ser efetuada em tempo razoável pelos métodos conhecidos hoje.

Antes de encerrar a discussão sobre o RSA será mostrado porque o método funciona, ou seja, porque $D \circ C(b) = b$. Por definição

$$D \circ C(b) = D(C(b)) = D(b^e) = (b^e)^d = b^{ed}.$$

Queremos mostrar que

$$b^{ed} \equiv b \pmod{n}.$$

Como d é o inverso de e módulo $\varphi(n)$, então

$$ed = 1 + k\varphi(n),$$

para algum inteiro k. Assim

$$ed = 1 + k\varphi(n) = 1 + k(p-1)\,(q-1).$$

Logo

$$b^{ed} \equiv b\,(b^{p-1})^{k(q-1)} \pmod{p}.$$

Pelo Pequeno Teorema de Fermat, se p não divide b, então

$$b^{p-1} \equiv 1 \pmod{p},$$

logo

$$b^{ed} \equiv b \pmod{p}.$$

Caso p divida b, então $b \equiv 0 \pmod{p}$ e a congruência é imediatamente verificada. Assim

$$b^{ed} \equiv b \pmod{p},$$

para qualquer valor de b. Analogamente mostra-se que

$$b^{ed} \equiv b \pmod{q}.$$

Como p e q são primos distintos, conclui-se que

$$b^{ed} \equiv b \pmod{pq},$$

ou seja,

$$b^{ed} \equiv b \pmod{n},$$

para qualquer valor de b.

3.2 Curiosidades

A seguir serão apresentadas algumas curiosidades envolvendo números primos:

- $p = 2$ é o único primo que pode ser expresso na forma $n^n + n$.
- $p = 3$ é o único primo tal que $p^2 + 2$ também é primo.

- $p = 61! - 60! + 59! - 58! + ... + 3! - 2! + 1!$ é primo.
- $p = 10^{39.026} + 4.538.354 \times 10^{19.510} + 1$ possui 39.027 dígitos, pode ser escrito na forma $p = 1000...0001$ e é o maior primo palíndromo conhecido.
- Os primeiros 16.208 dígitos de π formam um número primo.
- p = 353535 ... 535353 (4.157 dígitos) é o maior primo conhecido com apenas dois dígitos primos.
- A soma dos cem primeiros primos é 1.111.
- p = 6.173 é primo e continuará primo mesmo apagando qualquer de seus dígitos.
- O milênio de 13.893.290.219.204.000 a 13.893290.219.204.999 é o primeiro milênio sem nenhum número primo.
- $p = 6 \times 66 \times 666 \times 6.666 \times 66.666 \times 666.666 + 1$ é primo.
- $p = 2 \times 22 \times 222 \times 2.222 \times 22.222 \times 222.222 \times 2.222.222 \times 22.222.222 + 1$ é primo.
- p = 131.211.109.876.543.212.345.678.910.111.213 é primo (contagem regressiva e normal até treze).
- p = 71.828.182.828.182.817 é primo palíndromo formado por parte da dízima de *e*.
- p = 1.799.999.999.999.999.999 é primo e contém dezessete dígitos 9.
- p = 179.999.999.999.999.999.917 é primo e contém dezessete dígitos 9 cercados por 17.
- p = 19.666.666.666.666.666.666.619 é primo e contém dezenove dígitos 6.
- p = 11.111.117 e q = 71.111.111 são primos (7 antes ou depois de sete dígitos 1).
- p = 3.331.999 e seu reverso q = 9.991.333 são primos.
- O 81.839° número de Fibonacci contém 17.103 dígitos e é primo.

- p = 13579111315171921...513551375139 é primo e contém 9.725 dígitos (ímpares consecutivos até 5.139).

CONCLUSÃO

Na citação apresentada no início do segundo capítulo Gauss afirma que os problemas envolvendo números primos foram amplamente estudados e que seria inútil discuti-los detalhadamente. E Gauss está correto. Neste trabalho, que pretendia apresentar os números primos sob diferentes enfoques, foi necessário deixar muitos assuntos de fora. Como exemplo, podem ser citados: as demonstrações que existem infinitos números primos de Thue, Perrot, Auric, Méthod, Washington e Fürstenberg, o teorema de Wilson, o teorema chinês, resíduos quadráticos, raízes primitivas, sucessões de Lucas, pseudoprimos fortes, de Euler, de Fibonacci e de Lucas, espaçamento entre primos consecutivos, primos em progressão aritmética, primos regulares, de Sophie German, de Wieferich, de Cullen e de Woodall, o teste de Miller, além de resultados probabilísticos sobre números primos.

Mas o próprio Gauss, na mesma citação, afirma também que a própria dignidade da ciência exige que estes e outros problemas sejam estudados. Embora de forma superficial, muito dos principais e mais interessantes resultados foram aqui expostos. Longe de esgotar o assunto, este trabalho se propõe apenas a criar o interesse pelos números primos. Espera-se ter tido sucesso neste sentido.

BIBLIOGRAFIA

1 Boyer, C.B. **História da Matemática.** São Paulo: Edgard Blücher, 1974.

2 Caldwell, C. **The Prime Pages.** Disponível em: http://www.utm.edu/research/primes. Acesso em 10 jun. 2003.

3 Coutinho, S.C. **Números Inteiros e Criptografia RSA.** Rio de Janeiro: IMPA/SBM, 1997.

4 Domingues; H.,Iezzi, G. **Álgebra Moderna.** São Paulo: Atual, 1982.

5 Evaristo,J.; Perdigão,E. **Introdução à Álgebra Abstrata.** Maceió: Edufal, 2002.

6 Jacy Monteiro, L.H. **Elementos de Álgebra.** Rio de Janeiro: Ao Livro Técnico S.A., 1969.

7 Landau, E.**Teoria Elementar dos Números.** Rio de Janeiro: Ciência Moderna, 2002.

8 Ribenboim, P. **Números Primos: mistérios e recordes.** Rio de Janeiro, IMPA, 2001.

9 Shokranian, S. [et al.].**Teoria dos Números.** 2. ed. Brasília: UnB,1999.