Primos de Mersenne
(e outros primos muito grandes)

Textuniversitários 12

Carlos Gustavo T. A. Moreira
Nicolau C. Saldanha

Primos de Mersenne
(e outros primos muito grandes)

Editora Livraria da Física
São Paulo – 2021

4a. Edição

Editor: José Roberto Marinho
Projeto gráfico e diagramação: Thiago Augusto Silva Dourado
Capa: Fabrício Ribeiro

Texto em conformidade com as novas regras ortográficas do Acordo da Língua Portuguesa.

Dados Internacionais de Catalogação na Publicação (CIP)
(Câmara Brasileira do Livro, SP, Brasil)

Moreira, Carlos Gustavo T. A.
Primos de Mersenne : e outros primos muito grandes / Carlos Gustavo T. A. Moreira, Nicolau C. Saldanha. – 4. ed. – São Paulo : Livraria da Física, 2021. – (Textuniversitários ; 12)

Bibliografia.
ISBN 978-65-5563-123-4

1. Matemática 2. Matemática - Estudo e ensino 3. Números primos 4. Teoria dos números I. Saldanha, Nicolau C. II. Título III. Série.

21-74420 CDD-512.7

Índices para catálogo sistemático:

1. Teoria dos números : Matemática 512.7

Maria Alice Ferreira - Bibliotecária - CRB-8/7964

ISBN 978-65-5563-123-4

Impresso no Brasil
Printed in Brazil

LF EDITORIAL
Editora Livraria da Física
Tel./Fax: +55 11 3459-4327 / 3936-3413
www.livrariadafísica.com.br

Prefácio à Quarta Edição

Esta nova edição deste livro é a primeira publicada na Livraria da Física da USP, a cujo Comitê Editorial agradecemos o interesse. Gostaríamos de agradecer particularmente a nosso amigo Thiago Dourado, um dos editores desta coleção, pelo estímulo e pelas ótimas sugestões de tópicos adicionais que incluímos nesta edição. Uma das principais modificações em relação às edições anteriores, publicadas pelo IMPA, foi a inclusão de uma discussão mais detalhada sobre o algoritmo (polinomial e determinístico) AKS para testar primalidade de inteiros positivos quaisquer, contendo em particular uma prova de que o algoritmo funciona. Esse material foi essencialmente retirado do nosso livro "Teoria dos Números — um passeio pelo mundo inteiro com primos e outros números familiares", em coautoria com Fabio Brochero e Eduardo Tengan. Agradecemos ao Fabio e ao Tengan por autorizarem a utilização desse material.

Atualizamos também a Seção 1.7 — "Outros Resultados e Conjecturas sobre Primos", mencionando alguns importantes resultados recentes, e também atualizamos diversas tabelas de primos grandes. Desde a publicação da segunda edição, foram descobertos mais 7 primos de Mersenne*:

$$2^{82589933}-1,\quad 2^{77232917}-1,\quad 2^{74207281}-1,\quad 2^{57885161}-1,$$
$$2^{43112609}-1,\quad 2^{42643801}-1\quad \text{e}\quad 2^{37156667}-1,$$

que atualmente são os 7 maiores primos conhecidos.

Este livro foi publicado originalmente como texto de um curso que demos no 22º Colóquio Brasileiro de Matemática, em 1999, e influenciou fortemente os livros de Teoria dos Números de que fomos coautores posteriormente, como o livro em colaboração com o Fabio e o Tengan que mencionamos acima, publicado pela coleção Projeto Euclides, do IMPA, e o livro "Tópicos de Teoria dos Números", da coleção PROFMAT da SBM, em colaboração com o Fabio.

Carlos Gustavo T. de A. Moreira
IMPA, Estr. D. Castorina 110
Rio de Janeiro, RJ 22460-320
gugu@impa.br, http://www.impa.br/~gugu

Nicolau C. Saldanha
Depto. de Matemática, PUC–Rio
R. Mq. de S. Vicente 225
Rio de Janeiro, RJ 22453-900
nicolau@mat.puc-rio.br, http://www.mat.puc-rio.br/~nicolau

* Veja www.mersenne.org ou https://primes.utm.edu/largest.html.

Prefácio à Terceira Edição

Desde a publicação da segunda edição, foram descobertos mais 5 primos de Mersenne*:

$$2^{32582657}-1, \quad 2^{30402457}-1, \quad 2^{25964951}-1,$$
$$2^{24036583}-1 \quad \text{e} \quad 2^{20996011}-1,$$

que atualmente são os 5 maiores primos conhecidos.

A principal novidade neste período na lista dos maiores primos conhecidos foi o aparecimento dos primos encontrados pelo projeto Seventeen or Bust — há 4 deles dentre os 10 maiores primos conhecidos. Este projeto, iniciado em 2002, almeja provar que 78557 é o menor número de Sierpinski — veja a Nota ao final do Capítulo 1 para mais detalhes.

Desde a segunda edição foram provados alguns teoremas muito importantes sobre números primos, que resolvem questões há muito tempo em aberto. Ben Green e Terence Tao demonstraram em [33] que existem progressões aritméticas arbitrariamente grandes formadas exclusivamente por números primos. Além disso, Goldston, Pintz e Yıldırım provaram em [28] que a diferença entre primos consecutivos

* Veja `www.mersenne.org` ou `www.utm.edu/research/primes/largest.html`.

pode ser menor que qualquer múltiplo constante da diferença média. Veja a Seção 1.7 para enunciados mais precisos e outros comentários sobre esses resultados.

Prefácio à Segunda Edição

Desde a publicação da primeira edição, foi descoberto mais um primo de Mersenne*:

$$2^{13466917} - 1,$$

que é atualmente o maior primo conhecido. Além disso, aparecem hoje na lista dos 100 maiores primos conhecidos um grande número de primos de Fermat generalizados, isto é, números primos da forma $a^{2^n} + 1$ (com a relativamente pequeno), o que se deve principalmente ao esforço computacional coordenado por Yves Gallot, que desenvolveu um programa eficiente para testar a primalidade de tais números (usando os critérios descritos na Seção 3.2). Veja a página `http://perso.wanadoo.fr/yves.gallot/primes/gfn.html`.

Por outro lado, a novidade mais importante deste período sobre números primos e testes de primalidade foi, sem dúvida, a descoberta de um teste de primalidade polinomial e determinístico, por Manindra Agrawal, Neeraj Kayal e Nitin Saxena, em agosto de 2002 (ver [2]). Descreveremos rapidamente (sem demonstração) esse algoritmo no Capítulo 3.

---

* Veja `www.mersenne.org`.

Sumário

Introdução

Nosso objetivo neste livro é descrever o processo utilizado para encontrar os maiores números primos conhecidos. Em abril de 2021, os oito maiores primos conhecidos são da forma $M_p = 2^p - 1$ para $p = 82589933$, 77232917, 74207281, 57885161, 43112609, 42643801, 37156667 e 32582657. Estes são os únicos primos conhecidos com mais de $9\,500\,000$ algarismos.

Primos da forma $2^p - 1$, com p primo, têm sido estudados há séculos e são conhecidos como *primos de Mersenne*; não é difícil demonstrar que $2^p - 1$ só pode ser primo quando p é primo. Parte do interesse em primos de Mersenne deve-se à sua estreita ligação com números perfeitos. Um número perfeito é um inteiro positivo que é igual à soma de seus divisores próprios (como $6 = 1+2+3$ e $28 = 1+2+4+7+14$); os números perfeitos pares são precisamente os números da forma $2^{p-1}(2^p - 1)$ onde $2^p - 1$ é primo (um primo de Mersenne).

Talvez o primeiro resultado não trivial sobre primos de Mersenne seja devido a Hudalricus Regius que em 1536 mostrou que $2^p - 1$ não precisa ser primo sempre que p for primo: $2^{11} - 1 = 2047 = 23 \cdot 89$. Em 1603, Pietro Cataldi tinha corretamente verificado a primalidade de $2^{17} - 1$ e $2^{19} - 1$ e afirmou (incorretamente) que $2^p - 1$ também era primo para $p = 23$, 29, 31 e 37. Em 1640, Fermat mostrou que $2^{23} - 1$ e $2^{37} - 1$ são compostos. Em 1644, o monge Marin Mersenne (1588–1648) afirmou por sua vez (também incorretamente) que $2^p - 1$ era primo para

$$p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127 \text{ e } 257$$

e composto para os demais valores de $p \leq 257$. Esta afirmação demoraria séculos para ser completamente corrigida.

Em 1738, Euler mostrou que $2^{29} - 1$ é composto e em 1750, verificou que $2^{31} - 1$ é primo. Lucas desenvolveu um algoritmo para testar a primalidade de números de Mersenne e em 1876 verificou que $2^{127} - 1$ é primo; este número permaneceria por muito tempo como o maior primo conhecido (ver [43]). Só em 1947 a lista dos primos até 257 foi varrida: os valores de p nesta faixa para os quais $2^p - 1$ é primo são

$$p = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107 \text{ e } 127.$$

O algoritmo de Lucas foi posteriormente melhorado por Lehmer para dar o seguinte critério: sejam

$$\begin{aligned} S_0 &= 4, \\ S_1 &= 4^2 - 2 = 14, \\ &\dots\dots\dots\dots\dots\dots\dots, \\ S_{k+1} &= S_k^2 - 2; \end{aligned}$$

dado $p > 2$, $2^p - 1$ é primo se e somente se S_{p-2} é múltiplo de $2^p - 1$. Esta sequência cresce muito rápido, mas basta fazer as contas módulo $2^p - 1$: temos assim o chamado critério de Lucas–Lehmer (ver [41]).

Em 1951, computadores eletrônicos começaram a ser usados para procurar grandes números primos. Desde então foram encontrados os seguintes valores de p para os quais M_p é primo: 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11213, 19937, 21701, 23209, 44497, 86243, 110503, 132049, 216091, 756839, 859433, 1257787, 1398269, 2976221, 3021377, 6972593, 13466917, 20996011, 24036583, 25964951, 30402457, 32582657, 37156667, 42643801, 43112609, 57885161, 74207281, 77232917 e 82589933. Em todos os casos foi usado o critério de Lucas–Lehmer. Os últimos 17 foram encontrados com a ajuda de computadores pessoais: se você tem um computador você também pode participar da busca do próximo número de Mersenne (veja as instruções em `www.mersenne.org`).

Note que um número de Mersenne M_p é escrito na base 2 como $111\ldots111$, com p algarismos. Uma generalização natural seriam os números escritos como $111\ldots111$ em outra base, isto é, números da forma $(B^p-1)/(B-1)$, onde B é a base. É fácil ver que um tal número só pode ser primo se p for primo. No caso $B=10$ estes números são conhecidos como *repunits*. Não se conhece um critério análogo ao de Lucas–Lehmer para testar a primalidade de números deste tipo quando $B>2$. O maior primo conhecido desta forma é $(7176^{24691}-1)/7175$, que tem 95202 algarismos. Os únicos repunits (comprovadamente) primos conhecidos são para $p=2,19,23,317,1031$. Recentemente (entre 1999 e 2007), foram descobertos os seguintes valores de p para os quais os repunits correspondentes são *provavelmente* primos, *i.e.* passam por diversos testes probabilísticos de primalidade (veja o Capítulo 3 para uma discussão sobre testes determinísticos e probabilísticos de primalidade): 49081, 86453, 109297 e 270343. De acordo com os testes já realizados, qualquer outro repunit primo deve ter mais de 2 500 000 dígitos.

No primeiro capítulo veremos algumas ideias básicas de teoria dos números. Inicialmente apresentaremos a definição e as propriedades mais importantes do mdc e demonstraremos o teorema fundamental da aritmética. Depois apresentaremos a linguagem de congruências, o teorema chinês dos restos e os teoremas de Fermat, Euler e Wilson. Estudaremos a função φ de Euler, fórmula de inversão de Möbius e bases de numeração. Veremos o teorema dos números primos (com demonstração de uma versão fraca) e comentaremos vários resultados e problemas em aberto famosos sobre primos.

O segundo capítulo, um pouco mais avançado que o primeiro, começa com um pouco de álgebra: falamos sobre corpos e polinômios. Estaremos especialmente interessados em corpos finitos e demonstraremos que em todo corpo finito existe uma raiz primitiva. Depois discutiremos a existência de soluções para a congruência $X^2 \equiv a \pmod{n}$ e reciprocidade quadrática.

O terceiro capítulo é de certa forma o mais importante do livro: nele discutiremos como gerar grandes primos ou testar a primalidade de grandes inteiros. Faremos inicialmente algumas considerações gerais e depois discutiremos testes de primalidade para n quando é conhecida uma fatoração de $n-1$ ou de $n+1$. Primos de Mersenne são um caso muito particular desta segunda situação. Daremos neste capítulo duas demonstrações para o critério de Lucas–Lehmer.

No quarto capítulo discutiremos aspectos computacionais de implementações de testes de primalidade, especialmente do teste de Lucas–Lehmer. Uma questão importantíssima para garantir a rapidez de uma implementação é a multiplicação rápida de inteiros grandes; discutiremos brevemente dois algoritmos: o de Karatsuba e FFT (fast Fourier transform).

Duas referências que foram muito usadas neste livro são o excelente livro de Paulo Ribenboim, *Nombres premiers, mystères et records* e a também excelente home page sobre primos de Chris Caldwell* onde, entre outras coisas, podem ser sempre encontradas as listas atualizadas dos maiores primos conhecidos.

* `http://www.utm.edu/research/primes`

1

Divisibilidade e Congruências

Neste primeiro capítulo veremos os tópicos básicos de teoria dos números, como divisibilidade, congruências e aritmética módulo n.

1.1 Divisão Euclidiana e o Teorema Fundamental da Aritmética

A divisão euclidiana, ou divisão com resto, é uma das quatro operações que toda criança aprende na escola. Sua formulação precisa é: dados $a \in \mathbb{Z}$, $b \in \mathbb{Z} \setminus \{0\}$ existem $q, r \in \mathbb{Z}$ com $0 \leq r < |b|$ e $a = bq + r$. Tais q e r estão unicamente determinados e são chamados o *quociente* e *resto* da divisão de a por b. Se $b > 0$ podemos definir $q = \lfloor \frac{a}{b} \rfloor$ e se $b < 0$, $q = \lceil \frac{a}{b} \rceil$; em qualquer caso, $r = a - bq$. O resto r é às vezes denotado por $a \bmod b$; definimos $a \bmod 0 = a$. Lembramos que $\lfloor x \rfloor$ denota o único inteiro k tal que $k \leq x < k + 1$ e $\lceil x \rceil$ o único inteiro k tal que $k - 1 < x \leq k$.

Dados dois inteiros a e b (em geral com $b \neq 0$) dizemos que b *divide* a, ou que a é um *múltiplo* de b, e escrevemos $b \mid a$, se existir $q \in \mathbb{Z}$ com $a = qb$. Se $a \neq 0$, também dizemos que b é um *divisor* de a. Assim, $b \mid a$ se e somente se $a \bmod b = 0$.

Proposição 1.1 *Dados $a, b \in \mathbb{Z}$ existe um único $d \in \mathbb{N}$ tal que $d \mid a$, $d \mid b$ e, para todo $c \in \mathbb{N}$, se $c \mid a$ e $c \mid b$ então $c \mid d$. Além disso existem $x, y \in \mathbb{Z}$ com $d = ax + by$.*

Esse natural d é chamado o *máximo divisor comum*, ou mdc, entre a e b. Escrevemos $d = \mathrm{mdc}\,(a, b)$ ou (se não houver possibilidade de confusão) $d = (a, b)$.

Demonstração: O caso $a = b = 0$ é trivial (temos $d = 0$). Nos outros casos, seja $I\,(a, b) = \{ax + by \mid x, y \in \mathbb{Z}\}$ e seja $d = ax_0 + by_0$ o menor elemento positivo de $I\,(a, b)$. Como $d \in \mathbb{N} \setminus \{0\}$, existem $q, r \in \mathbb{Z}$ com $a = dq + r$ e $0 \leq r < d$. Temos $r = a - dq = a\,(1 - qx_0) + b\,(-qy_0) \in I\,(a, b)$; como $r < d$ e d é o menor elemento positivo de $I\,(a, b)$, $r = 0$ e $d \mid a$. Analogamente, $d \mid b$. Suponha agora que $c \mid a$ e $c \mid b$; temos $c \mid ax + by$ para quaisquer valores de x e y donde, em particular, $c \mid d$. $\square$

O *algoritmo de Euclides* para calcular o mdc baseia-se nas seguintes observações simples. Se $a = bq + r$, $0 \leq r < b$, temos (com a notação da demonstração acima) $I(a, b) = I(b, r)$, donde $(a, b) = (b, r)$. Definindo $a_0 = a$, $a_1 = b$ e $a_n = a_{n+1}q_{n+2} + a_{n+2}$, $0 \leq a_{n+2} < a_{n+1}$ (ou seja, a_{n+2} é o resto da divisão de a_n por a_{n+1}) temos

$$(a, b) = (a_0, a_1) = (a_1, a_2) = (a_2, a_3) = \cdots = (a_n, a_{n+1})$$

para qualquer valor de n. Seja N o menor natural para o qual $a_{N+1} = 0$: temos $(a, b) = (a_N, 0) = a_N$.

Lema 1.2 *Se $(a, b) = 1$ e $a \mid bc$ então $a \mid c$.*

Demonstração: Como $(a, b) = 1$, existem $x, y \in \mathbb{Z}$ com $ax + by = 1$, logo $a \mid c = acx + bcy$. $\square$

Quando $(a, b) = 1$ dizemos que a e b são *primos entre si*. Um natural $p > 1$ é chamado *primo* se os únicos divisores positivos de p

são 1 e p. Um natural $n > 1$ é chamado *composto* se admite outros divisores além de 1 e n.

Claramente, se p é primo e $p \nmid a$ temos $(p, a) = 1$. Usando o lema anterior e indução temos o seguinte resultado:

Corolário 1.3 *Sejam p um número primo e sejam $a_1, \dots a_m \in \mathbb{Z}$. Se $p \mid a_1 \cdots a_m$ então $p \mid a_i$ para algum i, $1 \le i \le n$.*

Estamos agora prontos para enunciar e provar o teorema que diz que todo inteiro admite fatoração única como produto de primos.

Teorema 1.4 (Teorema Fundamental da Aritmética) *Seja $n \ge 2$ um número natural. Podemos escrever n de uma única forma como um produto*

$$n = p_1 \cdots p_m$$

onde $m \ge 1$ é um natural e $p_1 \le \dots \le p_m$ são primos.

Demonstração: Mostramos a existência da fatoração por indução. Se n é primo não há o que provar (escrevemos $m = 1$, $p_1 = n$). Se n é composto podemos escrever $n = ab$, $a, b \in \mathbb{N}$, $1 < a < n$, $1 < b < n$. Por hipótese de indução, a e b se decompõem como produto de primos. Juntando as fatorações de a e b (e reordenando os fatores) obtemos uma fatoração de n.

Vamos agora mostrar a unicidade, também por indução. Suponha que

$$n = p_1 \cdots p_m = q_1 \cdots q_{m'},$$

com $p_1 \le \dots \le p_m$, $q_1 \le \dots \le q_{m'}$. Como $p_1 \mid q_1 \cdots q_{m'}$ temos $p_1 \mid q_i$ para algum valor de i, donde, como q_i é primo, $p_1 = q_i$ e $p_1 \ge q_1$. Analogamente temos $q_1 \le p_1$, donde $p_1 = q_1$. Mas por hipótese de indução

$$\frac{n}{p_1} = p_2 \cdots p_m = q_2 \cdots q_{m'}$$

admite uma única fatoração, donde $m = m'$ e $p_i = q_i$ para todo i. $\square$

Outra forma de escrever a fatoração é

$$n = p_1^{e_1} \cdots p_m^{e_m},$$

com $p_1 < \cdots < p_m$, $e_i > 0$. Ainda outra formulação é escrever

$$n = 2^{e_2} 3^{e_3} 5^{e_5} \cdots p^{e_p} \cdots$$

onde o produto é tomado sobre *todos* os primos mas apenas um número finito de expoentes é maior do que zero.

Segue deste teorema o outro algoritmo comum para calcular o mdc de dois números: fatoramos os dois números e tomamos os fatores comuns com os menores expoentes. Este algoritmo é bem menos eficiente do que o de Euclides para inteiros grandes (que em geral não sabemos fatorar) mas é instrutivo saber que os dois algoritmos dão o mesmo resultado.

Corolário 1.5 *Se* $(a, n) = (b, n) = 1$ *então* $(ab, n) = 1$.

Demonstração: Evidente a partir do algoritmo descrito acima. □

Teorema 1.6 (Euclides) *Existem infinitos números primos.*

Demonstração: Suponha por absurdo que $p_1, p_2, \ldots, p_m$ fossem *todos* os primos. O número $N = p_1 \cdot p_2 \cdots p_m + 1 > 1$ não seria divisível por nenhum primo, o que contradiz o teorema fundamental da aritmética. □

Observe que *não* provamos que $p_1 \cdot p_2 \cdots p_m + 1$ é primo para algum conjunto finito de primos (por exemplo, os m primeiros primos). Aliás, $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 \cdot 509$, $2 \cdot 3 \cdot 5 \cdot 7 - 1 = 209 = 11 \cdot 19$, $4! + 1 = 25 = 5^2$ e $8! - 1 = 40319 = 23 \cdot 1753$ não são primos. Não existe nenhuma fórmula simples conhecida que gere sempre números primos. Veja a Seção 3.1 (p. 62).