

## Prefácio à terceira edição

Desde a publicação da segunda edição, foram descobertos mais 5 primos de Mersenne:  $2^{32582657}-1$ ,  $2^{30402457}-1$ ,  $2^{25964951}-1$ ,  $2^{24036583}-1$  e  $2^{20996011}-1$  (veja [www.mersenne.org](http://www.mersenne.org) ou [www.utm.edu/research/primelargest.html](http://www.utm.edu/research/primelargest.html)), que atualmente são os 5 maiores primos conhecidos.

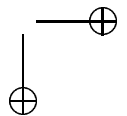
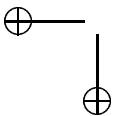
A principal novidade neste período na lista dos maiores primos conhecidos foi o aparecimento dos primos encontrados pelo projeto Seventeen or Bust - há 4 deles dentre os 10 maiores primos conhecidos. Este projeto, iniciado em 2002, almeja provar que 78557 é o menor número de Sierpinski - veja a Nota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

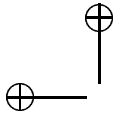
Desde a segunda edição foram provados alguns teoremas muito importantes sobre números primos, que resolvem questões há muito tempo em aberto. Ben Green e Terence Tao demonstraram em [GT] que existem progressões aritméticas arbitrariamente grandes formadas exclusivamente por números primos. Além disso, Goldston, Pintz e Yıldırım provaram em [GPY1] que a diferença entre primos consecutivos 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:  $2^{13466917}-1$  (veja [www.mersenne.org](http://www.mersenne.org)), 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/primel/gfn.html>.

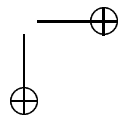
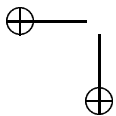
Por outro lado, a novidade mais importante deste período sobre números primos e testes de primalidade foi, sem dúvida, a descoberta de um teste de primalidade polinomial e determinístico, por Manindra Agrawal, Neeraj Kayal e Nitin Saxena, em agosto de 2002 (ver [AKS]). Descreveremos rapidamente (sem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

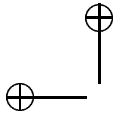




# Conteúdo

<b>Introdução</b> .....	<b>1</b>
<b>Capítulo 1: Divisibilidade e congruências</b> .....	<b>5</b>
1.1 Divisão euclidiana e o teorema fundamental da aritmética .....	5
1.2 Congruências .....	8
1.3 A função de Euler e o pequeno teorema de Fermat .....	11
1.4 A função de Möbius .....	14
1.5 Bases .....	17
1.6 Sobre a distribuição dos números primos .....	19
1.7 Outros resultados e conjecturas sobre primos .....	23
<b>Capítulo 2: Corpos finitos e reciprocidade quadrática</b> .....	<b>28</b>
2.1 Corpos e polinômios .....	28
2.2 Ordens e raízes primitivas .....	33
2.3 Raízes primitivas em $\mathbb{Z}/(n)$ .....	35
2.4 A lei da reciprocidade quadrática .....	37
2.5 Extensões quadráticas de corpos finitos .....	40
<b>Capítulo 3: Primos de Mersenne e testes de primalidade</b> .....	<b>41</b>
3.1 Fórmulas para primos e testes de primalidade .....	42
Apêndice: O algoritmo de Agrawal-Kayal-Saxena .....	48
3.2 Testes baseados em fatorações de $n - 1$ .....	50
3.3 Primos de Mersenne .....	51
3.4 Testes baseados em fatorações $n + 1$ .....	55





<b>Capítulo 4: Aspectos computacionais</b> .....	<b>63</b>
4.1 Primeiras tentativas .....	64
4.2 Alguns programas usando a biblioteca gmp .....	64
4.3 O algoritmo de multiplicação de Karatsuba .....	66
4.4 Multiplicação de polinômios usando FFT .....	67
4.5 Multiplicação de inteiros usando FFT .....	71
4.6 A complexidade das operações aritméticas .....	74
4.7 Tabelas: .....	76
– Os dez maiores primos conhecidos .....	76
– Os dez maiores pares de primos gêmeos conhecidos .....	77
– Os dez maiores primos multifatoriais e primoriais conhecidos .....	78
– Os dez maiores primos de Sophie Germain conhecidos .....	79
– O maior primo conhecido ao longo da história .....	80
– Os cem maiores primos conhecidos .....	82
<b>Referências</b> .....	<b>85</b>

