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` ou `www.utm.edu/research/primes/largest.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`), 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 [AKS]). Descreveremos rapidamente (sem demonstração) esse algoritmo no Capítulo 3.

Conteúdo