Frações contínuas e distribuição de números primos

Prof. Dr. Vinícius Wasques

Universidade Estadual Paulista "Júlio de Mesquita Filho" - Campus Rio Claro

27 de julho de 2020

Nas inclusões $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$, a passagem de $\mathbb{Q}$ para $\mathbb{R}$ é a que exige conceitos e ferramentas mais elaboradas.

Todo número real pode ser bem aproximado por números racionais, por meio de representações decimais.

Uma outra maneira de representar números reais é através de representações por *frações contínuas*, que sempre fornece aproximações racionais surpreendentemente boas e conceitualmente simples.

Definimos recursivamente:

$$\alpha_0 = x \quad \text{e} \quad a_n = \lfloor \alpha_n \rfloor$$

e se $\alpha_n \notin \mathbb{Z}$, então tomamos para todo $n \in \mathbb{N}$

$$\alpha_{n+1} = \frac{1}{\alpha_n - a_n}.$$

Frações contínuas

Se para algum n, $\alpha_n = a_n$, temos então

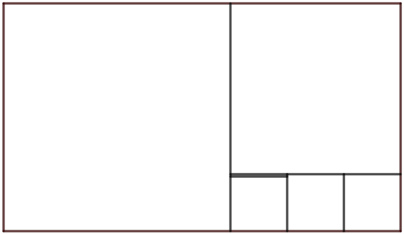
$$x = \alpha_0 = [a_0; a_1, \dots, a_n] = a_0 \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\ddots + \frac{1}{a_n}}}}$$

Caso contrário, denotamos

$$x = [a_0; a_1, \dots, a_n] = a_0 \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\ddots}}}$$

Tal representação é chamada de representação por *frações contínuas* de x.

Uma interpretação geométrica para esta representação é a seguinte:



Enchemos um retângulo com quadrados de forma a preencher o maior espaço, isto é, colocando o maior quadrado possível dentro do espaço ainda livre.

Observação:

1) Se a representação por frações contínuas de x for finita então x é racional.

2) Se $x \in \mathbb{Q}$, sua representação será finita, e seus coeficientes a_n são obtidos do algoritmo de Euclides: se $x = \frac{p}{q}$, com $q > 0$, temos

$$
\begin{aligned}
p &= a_0 q + r_1 & \qquad & 0 \leq r_1 < q \\
q &= a_1 r_1 + r_2 & & 0 \leq r_2 < r_1 \\
r_1 &= a_2 r_2 + r_3 & & 0 \leq r_3 < r_2 \\
&\vdots & & \vdots \\
r_{n-1} &= a_n r_n & &
\end{aligned}
$$

Temos então:

$$x = \frac{p}{q} = a_0 + \frac{r_1}{q} = a_0 + \cfrac{1}{a_1 + \frac{r_2}{r_1}} = \ldots = a_0 \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \frac{1}{a_n}}}}$$

Portanto, $x = [a_0; a_1, \ldots, a_n]$.

Isso mostra uma das vatagens dessa abordagem em relação a decomposição decimal, isto é, não é necessário escolhas artificiais de base.

Teorema

Dada uma sequência (finita ou infinita) $t_0, t_1, t_2, \ldots$ em $\mathbb{R}$ tal que $t_k > 0$, para todo $k \geq 1$, definimos as sequências (x_m) e (y_m) por

$$x_0 = t_0, y_0 = 1, x_1 = t_0 t_1 + 1, y_1 = t_1,$$

$$x_{m+2} = t_{m+2} x_{m+1} + x_m, y_{m+2} = t_{m+2} y_{m+1} + y_m,$$

para todo $m \geq 0$.

Temos então

$$[t_0; t_1, t_2, \ldots, t_n] = t_0 \frac{1}{t_1 + \frac{1}{t_2 + \frac{1}{\ddots + \frac{1}{t_n}}}} = \frac{x_n}{y_n}, \quad \forall n \geq 0.$$

Além disso, $x_{n+1} y_n - x_n y_{n+1} = (-1)^n$, para todo $n \geq 0$.

3) Frações contínuas podem ser utilizadas para estimar/aproximar números irracionais (Teoremas de Hurwitz, Markov e Dirichlet).

Sugestões de leitura:

[1] C. G. Moreira, Geometric properties of the Markov and Lagrange spectra. Preprint-IMPA-2009
`https://arxiv.org/pdf/1612.05782.pdf`

[2] J. C. Paixão. Sucessões e Frações Contínuas. Gazeta de Matemática, Escola ES/3 de Maria Lamas
`http://gazeta.spm.pt/getArtigo?gid=358`

[3] J. C. Paixão Fracções Contínuas no Ensino Pré-universitário. Dissertação de mestrado (2011)
`https://core.ac.uk/download/pdf/12427417.pdf`

Distribuição de números primos

Já vimos que existem infinitos primos.

O teorema dos números primos dá uma estimativa de quantos primos existem até um inteiro x, ou seja, descreve a distribuição dos primos.

Distribuição de números primos

Já vimos que existem infinitos primos.

O teorema dos números primos dá uma estimativa de quantos primos existem até um inteiro x, ou seja, descreve a distribuição dos primos.

Teorema dos Números Primos: Seja $\pi(x)$ o número de primos p, com $2 \leq p \leq x$. Então, $\pi(x)$ está entre $\frac{cx}{log(x)}$ e $\frac{Cx}{log(x)}$ para duas constantes $c < C$. Precisamente, temos

$$\lim_{x \to \infty} \frac{\pi(x)}{\frac{x}{log(x)}} = 1$$

Este resultado foi conjecturado por vários matemáticos, inclusive por Legendre e Gauss, mas a demonstração completa foi fornecida por de la Vallée Poussin e Hadamard (independentemente).
Uma aproximação mais precisa para $\pi(x)$ é dada por

$$L(x) = \int_0^x \frac{dt}{log(t)}$$

Primos gêmeos

Dois números p e q são chamados de primos gêmeos se p e q são primos e $|p - q| = 2$.

Conjectura: Existem inifinitos pares de primos gêmeos.

Demonstração ainda não fornecida!

São conhecidos pares de primos gêmeos bastante grandes $65516468355.2^6 \pm 1$, que possui 100355 dígitos cada.

Paralelo com o último teorema de Fermat.

Teorema de Sophie Germain

Se p e $2p+1$ são primos com $p>2$, então não existem inteiros x,y,z com $mdc(x,y,z)=1$ e $p \nmid xyz$ tais que $x^p+y^p+z^p=0$.

Fórmulas para primos

Não se conhece nenhuma fórmula simples para gerar primos arbitrariamente grandes.

Existem fórmulas que geram números primos, mas que são muito complicados e que também não ajudam a responder perguntas teóricas sobre a distribuição dos primos.

Por exemplo, a fórmula

$$p_n = \lfloor 10^{2^n} \rfloor - 10^{2^{n-1}} \lfloor 10^{2^{n-1}} c \rfloor$$

em que

$$c = \sum_{n=1}^{\infty} \frac{p_n}{10^{2^n}} = 0,0203000500000007\ldots$$

Teste de primalidade

Uma questão relacionada com a de gerar números primos é a de testar se um determinado número é primo.

Esse problema se tornou cada vez mais relevante por conta do uso intenso de números primos em criptografias.

Desenvolver algoritmos eficientes para testar a primalidade de um número se tornou um importante problema na área de Ciência da Computação.

Nesse sentido, duas coisas são requeridas:

1) certificar que o algoritmo realmente produz a resposta correta;

2) Uma medida da eficiência do algoritmo, isto é, avaliar o tempo ou número de passos executados, espaço ou memória utilizada para a obtenção da solução.

Existe um algoritmo bastante simples para testar se qualquer inteiro positivo n é primo:

Calcule o resto da divisão de n por cada inteiro m com $2 \leq m \leq \sqrt{n}$.

Se o resto for 0 em algum caso então n é composto e encontramos um divisor;

Se isto nunca ocorrer, então n é primo.

Problema: Algoritmo muito lento. Complexidade computacional $O(\sqrt{n})$, isto é, o algoritmo tem complexidade de tempo exponencial.

Exemplo:

Considere um número inteiro com 200 dígitos.

Para esse caso, seria necessário realizar aproximadamente 10^{100} divisões.

Em um passado não tão distante, efetuar essa quantidade de contas estaria fora do alcance de qualquer tecnologia plausível.

No entanto, computadores quânticos podem tornar possível a realização de tais contas.

Testes de primalidade em Teoria dos Números

Sugestão de leituras aprofundadas:

[1] H.W. Lenstra, Jr. Galois Theory and Primality Testing.
`http://pub.math.leidenuniv.nl/~lenstrahw/PUBLICATIONS/1984g/art.pdf`

[2] C. Pomerance. Primality testing: variations on a theme of Lucas.
`https://math.dartmouth.edu/~carlp/PDF/lucasprime2.pdf`

[3] H. W. Lenstra Jr. e C. Pomerance, Primality testing with Gaussian periods.
`https://math.dartmouth.edu/~carlp/aks102309.pdf`

Referências

MARTINEZ, F.E.B; MOREIRA, C.G.T; SALDANHA, N.,T.; TENGAN, E. Teoria dos Números. Um passeio com Primos e outros Números Familiares pelo Mundo Inteiro. IMPA, 2013.

GRAHAM, R. L., KNUTH, D. E., PATASHNIK, O Matemática Concreta. LTC, São Paulo, 1995

NIVEN, I. E.; ZUCKERMAN, N.S. An Introduction to the Theory of Numbers, NY, John Wiley & Sons, 1991.

Contato

Prof. Dr. Vinícius Wasques

email: viniciuswasques@gmail.com

Departamento de Matemática

site: `https://viniciuswasques.github.io/home/`