

连分数中的矩阵运算

朱林¹, 王冰^{2*}

¹上海理工大学, 理学院, 上海

²上海立信会计金融学院, 统计与数学学院, 上海

收稿日期: 2023年4月1日; 录用日期: 2023年5月2日; 发布日期: 2023年5月9日

摘要

本文旨在探究矩阵运算在连分数中的应用。本文通过欧几里得算法自然地引出连分数的概念, 探究了矩阵运算在连分数中的若干应用, 利用矩阵运算技巧证明了连分数的部分性质, 通过实例展示矩阵在连分数中的巧妙应用。矩阵运算在连分数中有着广泛而深入的应用, 为我们深入理解和研究连分数提供了新的视角和工具。

关键词

欧几里得算法, 连分数, 矩阵

Matrix Operations in Continued Fractions

Lin Zhu¹, Bing Wang^{2*}

¹College of Science, University of Shanghai for Science and Technology, Shanghai

²School of Statistics and Mathematics, Shanghai Lixin University of Accounting and Finance, Shanghai

Received: Apr. 1st, 2023; accepted: May 2nd, 2023; published: May 9th, 2023

Abstract

This article aims to explore the application of matrix operations in continued fractions. This article naturally introduces the concept of continued fractions through Euclidean algorithm, explores several applications of matrix operations in continued fractions, proves some properties of continued fractions using matrix operation techniques, and demonstrates the ingenious application of matrices in continued fractions through examples. Matrix operations have extensive and in-depth applications in continued fractions, providing us with new perspectives and tools for in-depth understanding and research of continued fractions.

*通讯作者。

文章引用: 朱林, 王冰. 连分数中的矩阵运算[J]. 理论数学, 2023, 13(5): 1151-1156.

DOI: 10.12677/pm.2023.135120

Keywords

Euclidean Algorithm, Continued Fractions, Matrices

Copyright © 2023 by author(s) and Hans Publishers Inc.

This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

1. 引言

连分数是数学领域中一个重要的概念,它在数论、代数、数值分析、密码学、数字图像处理、天文、历法、乐律等方面都有广泛的应用。在数论中,连分数被用于解决无理数的最佳有理逼近、二次无理数和求解不定方程等问题(参见[1])。在数值计算中,连分数被用于连分式插值与逼近理论,以及微分方程数值解的研究(参见[2])。在信息安全领域,连分数在攻击 RSA 密码系统中发挥着重要作用(参见[3] [4])。

随着现代数学的发展,连分数的研究得到了广泛的关注和不断深入的拓展。目前,学者们在连分数的理论研究、计算机数值计算及其他领域中的应用进行了不断的探索和研究。文献[5]提出并研究了一种可以在任意虚二次环中实现的广义连分数算法,且不限于欧几里得的情形,经典连分数的许多标志性特性被证明是可以保留的。文献[6]研究了 p -adic 域中的一族拟周期 p -adic Ruban 连分数。这些新的理论成果的发现,进一步推动了连分数理论的发展和应用的广泛化。

在实际应用中,我们通常要对连分数进行计算和处理,因此需要寻找一些有效的计算方法和工具。欧几里得算法是一种古老的算法,它可以用于寻找两个数的最大公约数。通过欧几里得算法,我们可以很自然地引出连分数的概念。矩阵是数学中的重要工具,它可以用于描述线性变换和解决一些代数和几何问题。本文的主题是探究矩阵运算在连分数中的应用,本文研究的方法和结果在数学理论和应用领域都具有广泛的应用价值。

本文的结构如下:首先介绍扩展的欧几里得算法,用矩阵技巧处理扩展的欧几里得算法中的迭代关系式;然后,由欧几里得算法自然地引出连分数的概念,并探究矩阵运算在连分数中的应用。在此基础上,利用矩阵运算技巧证明连分数的渐近分数的一些性质,并通过实例展示矩阵运算在连分数中的巧妙应用。最后,对本文的结论进行总结和展望。

2. 欧几里得算法

欧几里得算法与连分数关系密切。利用欧几里得算法(参见[1])可以快速地求整数 a, b 的最大公因子 (a, b) 。设整数 $a \geq b > 0$, 令 $r_0 = a, r_1 = b$ 。如果连续做带余除法得到 $r_j = r_{j+1}a_{j+1} + r_{j+2}, 0 < r_{j+2} < r_{j+1}, 0 \leq j \leq n-2$ 且有 $r_{n+1} = 0$, 那么 $(a, b) = r_n$, 即最后一个非零余数 r_n 为 a, b 的最大公因子。若沿着欧几里得算法的反方向递推,最终可将 (a, b) 表示成 $r_0 = a, r_1 = b$ 的线性组合,即得 Bezout 定理的构造性证明。

定理 1 (Bezout 定理) 如果 a, b 均为整数,那么存在整数 k, l 使得 $ka + lb = (a, b)$ 。

方程 $ka + lb = (a, b)$ 称为 Bezout 等式, k, l 称为 Bezout 系数。下面用矩阵运算的技巧给出 $d := (a, b)$ 表示成 a, b 的线性组合的解释(参见[7])。将行向量 (a, b) 作为矩阵的第一行,下面写一个 2 阶单位矩阵,构成 3 行 2 列整数矩阵 A 。只对 A 进行第三类初等列变换(且所乘系数均为整数),当 A 的第一行变成 $(d, 0)$ 或 $(0, d)$ 时,得到矩阵 B 或 B' , 其中 k, l, u, v 为整数。

$$A = \begin{pmatrix} a & b \\ 1 & 0 \\ 0 & 1 \end{pmatrix} \xrightarrow[\text{初等列变换}]{a, b \text{ 辗转相除}} B = \begin{pmatrix} d & 0 \\ k & u \\ l & v \end{pmatrix} \text{ 或 } B' = \begin{pmatrix} 0 & d \\ u & k \\ v & l \end{pmatrix}.$$

由此得到的 k, l 满足 Bezout 等式 $ka + lb = (a, b)$ 。Bezout 系数不是唯一的, 可以递归地求出。下面定理给出了另一种计算 Bezout 系数的方法(参见[3])。

定理 2 (扩展的欧几里得算法) 令 a, b 是正整数, 那么

$$(a, b) = s_n a + t_n b,$$

其中 s_n, t_n 是下面定义的递归序列的第 n 项,

$$s_0 = 1, t_0 = 0, s_1 = 0, t_1 = 1,$$

且

$$s_j = s_{j-2} - a_{j-1} s_{j-1}, t_j = t_{j-2} - a_{j-1} t_{j-1}.$$

其中 $2 \leq j \leq n+1$, a_j 是欧几里得算法 $r_j = r_{j+1} a_{j+1} + r_{j+2}$, $0 < r_{j+2} < r_{j+1}$ 中每一步的商。

在扩展的欧几里得算法中, 由递推序列有

$$\begin{pmatrix} s_j & t_j \\ s_{j-1} & t_{j-1} \end{pmatrix} = \begin{pmatrix} -a_{j-1} & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} -a_{j-2} & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} -a_1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad (1)$$

$$\begin{pmatrix} r_j \\ r_{j-1} \end{pmatrix} = \begin{pmatrix} s_j & t_j \\ s_{j-1} & t_{j-1} \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} \quad (2)$$

计算 s_n, t_n , 即可得到关于 a, b 的 Bezout 等式 $(a, b) = s_n a + t_n b$ 。利用(2)式可将任一余数 r_j 表示为 a, b 的线性组合。反之, a, b 也可由任意一对相邻的余数线性表示:

$$\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_2 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_j & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} r_j \\ r_{j+1} \end{pmatrix}, 1 \leq j \leq n.$$

命题 3 在扩展的欧几里得算法中, 系数 s_n, t_n 满足如下性质:

$$s_j t_{j-1} - s_{j-1} t_j = (-1)^j, \quad s_j t_{j-2} - s_{j-2} t_j = (-1)^{j-1} a_{j-1};$$

$\frac{s_j}{t_j}$, $2 \leq j \leq n+1$ 为既约分数;

$$\frac{a}{b} = -\frac{t_{n+1}}{s_{n+1}}, \quad |s_{n+1}| = \frac{b}{d}, \quad |t_{n+1}| = \frac{a}{d}.$$

证明 对(1)式左右两边同时取行列式即得 $s_j t_{j-1} - s_{j-1} t_j = (-1)^j$ 。对

$$\begin{pmatrix} s_j & t_j \\ s_{j-2} & t_{j-2} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & a_{j-1} \end{pmatrix} \begin{pmatrix} s_j & t_j \\ s_{j-1} & t_{j-1} \end{pmatrix}$$

左右两边同时取行列式即得 $s_j t_{j-2} - s_{j-2} t_j = (-1)^{j-1} a_{j-1}$ 。第 2 条性质 $\frac{s_j}{t_j}$ 为既约分数是第 1 条性质的直接推论。由(2)式知, $0 = r_{n+1} = s_{n+1} a + t_{n+1} b$, 则 $\frac{a}{b} = -\frac{t_{n+1}}{s_{n+1}}$ 。又 t_{n+1} 和 s_{n+1} 互素, 则 $|s_{n+1}| = \frac{b}{d}$, $|t_{n+1}| = \frac{a}{d}$, 证毕。

注意到, s_n, t_n 的这些性质与定理 6 中渐近分数的性质有相似之处。

3. 连分数中的矩阵技巧

连分数由欧几里得算法引入十分自然, 我们有时用数的整数部分近似代替这个数, 为了再精确一点,

就再给出小数部分的倒数的整数部分, 如此连续进行, 得到连分数。首先将欧几里得算法中的辗转相除法改写, 设 a, b 为正整数:

$$\frac{a}{b} = \frac{r_0}{r_1} = a_1 + \frac{r_2}{r_1}, \frac{r_j}{r_{j+1}} = a_{j+1} + \frac{r_{j+2}}{r_{j+1}} (0 \leq j \leq n-2), \frac{r_{n-1}}{r_n} = a_n.$$

依次将后式的倒数代入前式, 则

$$\frac{a}{b} = a_1 + \frac{r_2}{r_1} = a_1 + \frac{1}{\frac{r_1}{r_2}} = a_1 + \frac{1}{a_2 + \frac{r_3}{r_2}} = \cdots = a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \frac{1}{\ddots + \frac{1}{a_{n-1} + \frac{1}{a_n}}}}}$$

上述等式的最后一项就是 $\frac{a}{b}$ 的连分数展开式。

连分数是具有以下形式的表达式(记为 α):

$$a_0 + \frac{b_0}{a_1 + \frac{b_1}{a_2 + \cdots}}$$

其中 a_i, b_i 是任意数。如果 a_0 为整数, $a_k (k > 0)$ 为正整数, $b_i = 1 (i \geq 0)$, 则称表达式为简单连分数, 简记为 $[a_0, a_1, a_2, \dots]$ 。止于有限步时, 则为有限连分数, 记为

$$\alpha_n = [a_0, a_1, a_2, \dots, a_n] = \frac{p_n}{q_n},$$

这称为无限连分数 $[a_0, a_1, a_2, \dots]$ 的第 n 个渐近分数。

连分数的渐近分数在无理数的有理逼近中有非常重要的应用, 下面的定理 4 是关于渐近分数的基本结论(参见[1] [3] [8])。

定理 4 设正实数 α 展开连分数为 $[a_0, a_1, a_2, \dots]$, 则

渐近分数 $[a_0, a_1, a_2, \dots, a_n] = \frac{p_n}{q_n}$ 满足

$$\begin{cases} p_0 = a_0, & p_1 = a_0 a_1 + 1, & p_n = a_n p_{n-1} + p_{n-2}, \\ q_0 = 1, & q_1 = a_1, & q_n = a_n q_{n-1} + q_{n-2}. \end{cases}$$

事实上, 对任何 x , 有 $[a_0, a_1, \dots, a_{n-1}, x] = \frac{x p_{n-1} + p_{n-2}}{x q_{n-1} + q_{n-2}}$ 。

渐近分数 $\frac{p_n}{q_n}$ 收敛于原实数 α , 而且是 α 的最佳逼近分数, 即分母不大于 q_n 的分数中, $\frac{p_n}{q_n}$ 与 α 最接

近, 且 $\frac{p_{2n}}{q_{2n}}$ 和 $\frac{p_{2n+1}}{q_{2n+1}}$ 分别单调递增和单调递减地趋于 α 。

命题 5 设正实数 α 展开连分数为 $[a_0, a_1, a_2, \dots]$, 则其渐近分数 $\frac{p_n}{q_n}$ 满足如下等式:

p_n, q_n 可以用行列式表达

$$\begin{aligned}
 p_n &= \begin{vmatrix} a_0 & -1 & & & & \\ 1 & a_1 & -1 & & & \\ & 1 & a_2 & -1 & & \\ & & \ddots & \ddots & \ddots & \\ & & & 1 & a_{n-1} & -1 \\ & & & & 1 & a_n \end{vmatrix}, q_n = \begin{vmatrix} 1 & 0 & & & & \\ 0 & a_1 & -1 & & & \\ & 1 & a_2 & -1 & & \\ & & \ddots & \ddots & \ddots & \\ & & & 1 & a_{n-1} & -1 \\ & & & & 1 & a_n \end{vmatrix}; \\
 \begin{pmatrix} p_n & q_n \\ p_{n-1} & q_{n-1} \end{pmatrix} &= \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_{n-1} & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix}; \\
 \begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix} &= \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix}.
 \end{aligned} \tag{3}$$

利用上述矩阵等式可以简洁地证明一些关于渐近分数的性质。

定理 6 设正实数 α 展开连分数为 $[a_0, a_1, a_2, \dots]$, 则其渐近分数 $\frac{p_n}{q_n}$ 满足如下性质:

$$p_n q_{n-1} - p_{n-1} q_n = (-1)^{n-1}, \quad p_n q_{n-2} - p_{n-2} q_n = (-1)^n a_n;$$

$\frac{p_n}{q_n}$ 为既约分数;

$[a_0, a_1, \dots, a_n]$ 和 $[a_n, a_{n-1}, \dots, a_0]$ 的第 n 个渐近分数的分子必相等。

证明 第 1、2 条性质与命题 3 中的证明类似。利用(3)式和行列式的性质即得第 3 条性质, 证毕。

利用渐近分数的矩阵等式还可以比较方便地计算连分数的渐近分数, 从而得到无理数的最佳有理逼近。

例 7 圆周率 π 的连分数为

$$\pi = [3, 7, 15, 1, 292, 1, 1, 1, 21, 31, 14, 2, 1, 1, 2, 2, \dots].$$

利用关于渐近分数的矩阵等式有

$$\begin{aligned}
 \begin{pmatrix} p_1 & p_0 \\ q_1 & q_0 \end{pmatrix} &= \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 22 & 3 \\ 7 & 1 \end{pmatrix}, \\
 \begin{pmatrix} p_3 & p_2 \\ q_3 & q_2 \end{pmatrix} &= \begin{pmatrix} 22 & 3 \\ 7 & 1 \end{pmatrix} \begin{pmatrix} 15 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 355 & 333 \\ 113 & 106 \end{pmatrix},
 \end{aligned}$$

则 π 的前几个渐近分数为

$$\frac{3}{1}, \frac{22}{7}, \frac{333}{106}, \frac{355}{113}, \frac{103993}{33102}, \frac{104348}{33215},$$

其中 $\frac{22}{7}$, $\frac{355}{113}$ 分别称为疏率和密率。密率是分子小于 16,604 的分数中最接近 π 的。

例 8 贵金属数是二次方程 $x^2 - mx - 1 = 0$ (整数 $m > 0$) 的正根

$$\frac{m + \sqrt{m^2 + 4}}{2}.$$

贵金属数的连分数表示是 $[m, m, m, \dots]$ 。利用命题 5 中关于渐近分数的矩阵等式有

$$\begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix} = A^{n+1}, \text{ 其中 } A = \begin{pmatrix} m & 1 \\ 1 & 0 \end{pmatrix}.$$

A 的特征多项式 $\varphi_A(\lambda) = \lambda^2 - m\lambda - 1$ 有两个不相等的特征值

$$\lambda_1 = \frac{m + \sqrt{m^2 + 4}}{2}, \lambda_2 = \frac{m - \sqrt{m^2 + 4}}{2}.$$

分别解出属于特征值 λ_1, λ_2 的特征向量 $X_1 = (\lambda_1, 1)^T, X_2 = (\lambda_2, 1)^T$ 。依次以 X_1, X_2 为列向量组成可逆方阵 P , 则

$$A = P \begin{pmatrix} \lambda_1 & \\ & \lambda_2 \end{pmatrix} P^{-1},$$

$$A^{n+1} = \frac{1}{\lambda_1 - \lambda_2} \begin{pmatrix} \lambda_1 & \lambda_2 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} \lambda_1^{n+1} & \\ & \lambda_2^{n+1} \end{pmatrix} \begin{pmatrix} 1 & -\lambda_2 \\ -1 & \lambda_1 \end{pmatrix} = \frac{1}{\sqrt{m^2 + 4}} \begin{pmatrix} \lambda_1^{n+2} - \lambda_2^{n+2} & * \\ \lambda_1^{n+1} - \lambda_2^{n+1} & * \end{pmatrix}.$$

所以, 贵金属数的渐近分数为

$$\frac{p_n}{q_n} = \frac{\lambda_1^{n+2} - \lambda_2^{n+2}}{\lambda_1^{n+1} - \lambda_2^{n+1}}.$$

特别地, $m=1$ 时, $\frac{1+\sqrt{5}}{2}$ 是黄金分割数, 同时也是斐波那契数列相邻两项之比的极限。当 $m=2$ 时, $1+\sqrt{2}$ 是白银分割数, 同时也是佩尔数列相邻两项之比的极限。

4. 结论

矩阵运算在连分数中具有广泛而深入的应用, 为我们深入理解和研究连分数提供了很好的工具和有益的指导。本文利用矩阵运算技巧证明了连分数的一些性质, 通过实例展示了矩阵在求圆周率、贵金属数的渐近分数等问题时的巧妙应用。然而, 本文的研究范围存在一定的局限性, 未来的研究可以充分利用矩阵的强大性质, 深入探究矩阵在连分数的逼近理论、求解不定方程、数值分析等方面的应用。

基金项目

感谢国家自然科学基金(批准号 11901390), 上海高校青年教师培养资助计划(“互联网+”背景下课程思政融入《高等数学》的路径研究)的支持。

参考文献

- [1] 张贤科. 初等数论[M]. 北京: 高等教育出版社, 2016.
- [2] 檀结庆, 等. 连分式理论及其应用[M]. 北京: 科学出版社, 2007.
- [3] Rosen, K.H. (2011) *Elementary Number Theory and Its Applications*. 6th Edition, Pearson, Boston.
- [4] 江宝安. 一种基于连分数逼近 Legendre 定理的 RSA 攻击算法[J]. 信息安全研究, 2021, 7(11): 1037-1040.
- [5] Martin, D.E. (2023) Continued Fractions over Non-Euclidean Imaginary Quadratic Rings. *Journal of Number Theory*, **243**, 688-714. <https://doi.org/10.1016/j.jnt.2022.06.004>
- [6] Ammous, B., Ben Mahmoud, N. and Hbaib, M. (2022) On the Quasi-Periodic P-Adic Ruban Continued Fractions. *Czechoslovak Mathematical Journal*, **72**, 1157-1166. <https://doi.org/10.21136/CMJ.2022.0409-21>
- [7] 王琳. 关于最大公约数的问题[J]. 数学通报, 1992(1): 33-35.
- [8] Hardy, G.H. and Wright, E.M. (2008) *An Introduction to the Theory of Numbers*. Oxford University Press, Oxford.