

第七章 连分数
2015年06月08日



信息安全数学基础

陈恭亮 教授 博士生导师

上海交通大学信息安全工程学院

chengl@sjtu.edu.cn

[访问主页](#)

[标题页](#)

[目录页](#)

[◀](#) [▶](#)

[◀](#) [▶](#)

第 1 页 共 57 页

[返回](#)

[全屏显示](#)

[关闭](#)

[退出](#)



上海交通大学
SHANGHAI JIAO TONG UNIVERSITY
信息安全工程学院





1. 连分数的定义.
2. 简单连分数的定义.
3. 实数的连分数构造.
4. 最佳逼近.
5. 连分数的应用.

[访问主页](#)[标题页](#)[目录页](#)[◀◀](#) [▶▶](#)[◀](#) [▶](#)[第 2 页 共 57 页](#)[返 回](#)[全屏显示](#)[关 闭](#)[退 出](#)

上海交通大学
SHANGHAI JIAO TONG UNIVERSITY
信息安全工程学院





§7.1.1 连分数

对于实数 $\sqrt{2}$, 如何计算其值呢? 我们可以采用如下方法, 即用有理数来近似.

首先, 作展开式

$$\begin{aligned}\sqrt{2} &= 1 + (\sqrt{2} - 1) \\ &= 1 + \frac{1}{\sqrt{2} + 1} \\ &= 1 + \frac{1}{2 + \frac{1}{\sqrt{2} + 1}} \\ &= 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{\sqrt{2} + 1}}} \\ &= 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2 + \frac{1}{\sqrt{2} + 1}}}} \\ &= 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2 + \frac{1}{\sqrt{2} + 1}}}}}.\end{aligned}$$

[访问主页](#)[标题页](#)[目录页](#)[◀](#) [▶](#)[◀](#) [▶](#)[第3页共57页](#)[返回](#)[全屏显示](#)[关闭](#)[退出](#)



其次, 可用有理分数来近似. 例如,

$$1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2}}}} = 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2}}} = 1 + \frac{1}{2 + \frac{5}{12}}$$

$$= 1 + \frac{12}{29} = \frac{41}{29} = 1.413793103$$

最后, 列出 $\sqrt{2}$ (取10位十进制) 与10 个有理数间的误差.

i	a_i	P_i/Q_i	$\sqrt{2} - P_i/Q_i$	i	a_i	P_i/Q_i	$\sqrt{2} - P_i/Q_i$
0	1	1/1	0.414213562	5	2	99/70	-0.000072152
1	2	3/2	-0.085786438	6	2	239/169	0.000012379
2	2	7/5	0.014213562	7	2	577/408	-0.000002124
3	2	17/12	-0.002453105	8	2	1393/985	0.000000364
4	2	41/29	0.000420459	9	2	3363/2378	-0.000000063

[访问主页](#)
[标题页](#)
[目录页](#)
[<<](#)
[>>](#)
[<](#)
[>](#)

第 4 页 共 57 页

[返回](#)
[全屏显示](#)
[关闭](#)
[退出](#)




我们将对 $\sqrt{2}$ 的有理分数近似计算推广到任意的实数.

简单连分数构造

给定一个实数 x , 我们构造 x 的简单连分数(见定义11)如下:

(0) 令 $a_0 = [x]$, $x_0 = x - a_0$. a_0 是 x 的整数部分, 即 a_0 是不大于 x 的最大整数, $0 \leq x_0 < 1$.

(1) 如果 $x_0 = 0$, 则终止. 否则, 令 $a_1 = \left[\frac{1}{x_0} \right]$, $x_1 = \frac{1}{x_0} - a_1$.

(2) 如果 $x_1 = 0$, 则终止. 否则, 令 $a_2 = \left[\frac{1}{x_1} \right]$, $x_2 = \frac{1}{x_1} - a_2$.

如此继续下去....., 得到 a_k, x_k .

(k+1) 如果 $x_k = 0$, 则终止. 否则, 令 $a_{k+1} = \left[\frac{1}{x_k} \right]$, $x_{k+1} = \frac{1}{x_k} - a_{k+1}$.

.....

[访问主页](#)[标题页](#)[目录页](#)[◀](#) [▶](#)[◀](#) [▶](#)

第5页共57页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)

由此得到 x 的简单连分数为

$$x = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \dots + \frac{1}{a_{n-1} + \frac{1}{a_n + \dots}}}}. \quad (1)$$

以及

$$x = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \dots + \frac{1}{a_{n-1} + \frac{1}{a_n}}}}. \quad (2)$$

无限简单连分数记作 $[a_0, a_1, a_2, \dots]$,

有限简单连分数记作 $[a_0, a_1, a_2, \dots, a_{n-1}, a_n]$.

设 $k \geq 0$ (有限简单连分数时, $k \leq n$), 我们将有限连分数

$$[a_0, a_1, \dots, a_k] = \frac{P_k}{Q_k} \quad (3)$$

叫做简单连分数(1)和(2)的第 k 个**渐近分数**, 将 a_k 叫做它的第 k 个**部分商**.



访问主页

标题页

目录页

◀

▶

◀

▶

第 6 页 共 57 页

返回

全屏显示

关闭

退出





特别地, 当 x 为有理分数 $\frac{u_{-2}}{u_{-1}}$, $u_{-1} \geq 1$ 时, 我们所构造的 x 的简单连分数

$$[a_0, a_1, a_2, \dots, a_n]$$

的部分商 a_k , ($0 \leq k \leq n$) 满足如下关系式:

$$(0) \quad u_{-2} = a_0 \cdot u_{-1} + u_0, \quad 0 < u_0 = x_0 u_{-1} < u_{-1}.$$

$$(1) \quad u_{-1} = a_1 \cdot u_0 + u_1, \quad 0 < u_1 = x_1 u_0 < u_0.$$

$$(2) \quad u_0 = a_2 \cdot u_1 + u_2, \quad 0 < u_2 = x_2 u_1 < u_1.$$

.....

$$(n-1) \quad u_{n-3} = a_{n-1} \cdot u_{n-2} + u_{n-1}, \quad 0 < u_{n-1} = x_{n-1} u_{n-2} < u_{n-2}.$$

$$(n) \quad u_n = a_n \cdot u_{n-1} + u_n, \quad 0 = u_n = x_n u_{n-1} < u_{n-1}.$$

[访问主页](#)
[标题页](#)
[目录页](#)
[◀](#)
[▶](#)
[◀](#)
[▶](#)

第 7 页 共 57 页

[返回](#)
[全屏显示](#)
[关闭](#)
[退出](#)




因为 $\{u_k\}_{k \geq -2}$ 是关于 k 的严格递减的非负整数列, 所以使得 $u_n = 0$ 的 n 是存在的. 因此, $x_n = 0$. 有理分数 $x = \frac{u_{-2}}{u_{-1}}$ 有有限简单连分数

$$x = [a_0, a_1, a_2, \dots, a_n].$$

当 $a_n \geq 2$ 时, 我们也有

$$x = [a_0, a_1, a_2, \dots, a_n] = [a_0, a_1, a_2, \dots, a_n - 1, 1].$$

这就是说, 有理分数有两种连分数表示式. 是否存在其它形式的表示式呢? 答案是否定的. 我们有如下定理(证明见§7.3).

[访问主页](#)[标题页](#)[目录页](#)[<<](#)[>>](#)[<](#)[>](#)[第 8 页 共 57 页](#)[返回](#)[全屏显示](#)[关闭](#)[退出](#)



定理7.1.1 设 $[a_0, a_1, a_2, \dots, a_n]$ 和 $[b_0, b_1, b_2, \dots, b_m]$ 是两个有限简单连分数, $a_n \geq 2, b_m \geq 2$. 如果

$$[a_0, a_1, a_2, \dots, a_n] = [b_0, b_1, b_2, \dots, b_m],$$

则 $n = m, a_i = b_i, i = 0, \dots, n$.

根据简单连分数的构造以及定理7.1.1, 我们立即得到:

定理7.1.2 任一不是整数的有理分数 $x = \frac{u_{-2}}{u_{-1}}$ 有且仅有给出的两种有限简单连分数表示式

$$x = [a_0, a_1, a_2, \dots, a_n], \quad n \geq 1, a_n \geq 2$$

和

$$x = [a_0, a_1, a_2, \dots, a_n - 1, 1], \quad n \geq 1, a_n \geq 2.$$

[访问主页](#)[标题页](#)[目录页](#)[◀](#) [▶](#)[◀](#) [▶](#)[第9页共57页](#)[返回](#)[全屏显示](#)[关闭](#)[退出](#)

7.1.2 简单连分数的渐近分数

对于渐近分数(3)

$$[a_0, a_1, \dots, a_k] = \frac{P_k}{Q_k}$$

的计算, 有如下的定理(一般连分数的定理见定理7.2.2)

定理7.1.3 设 $[a_0, a_1, a_2, \dots]$ 是实数 α 的简单连分数. 再设

$$\begin{aligned} P_{-2} &= 0, \quad P_{-1} = 1, \quad P_n = a_n P_{n-1} + P_{n-2}, \quad n \geq 0, \\ Q_{-2} &= 1, \quad Q_{-1} = 0, \quad Q_n = a_n Q_{n-1} + Q_{n-2}, \quad n \geq 0. \end{aligned} \quad (4)$$

则我们有

$$[a_0, a_1, \dots, a_{n-1}, a_n] = \frac{a_n P_{n-1} + P_{n-2}}{a_n Q_{n-1} + Q_{n-2}} = \frac{P_n}{Q_n}, \quad n \geq 0, \quad (5)$$

$$P_n Q_{n-1} - P_{n-1} Q_n = (-1)^{n+1}, \quad n \geq -1, \quad (6)$$

$$P_n Q_{n-2} - P_{n-2} Q_n = (-1)^n a_n, \quad n \geq 0. \quad (7)$$

[访问主页](#)[标题页](#)[目录页](#)[◀](#) [▶](#)[◀](#) [▶](#)

第 10 页 共 57 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)



特别地, 我们有

$$\frac{P_0}{Q_0} < \dots < \frac{P_{2n-2}}{Q_{2n-2}} < \frac{P_{2n}}{Q_{2n}} < \dots < \alpha < \dots < \frac{P_{2n+1}}{Q_{2n+1}} < \frac{P_{2n-1}}{Q_{2n-1}} < \dots < \frac{P_1}{Q_1}, \quad (8)$$

$$[a_0, a_1, \dots, a_{n-1}, a_n] - [a_0, a_1, \dots, a_{n-1}] = \frac{(-1)^{n+1}}{Q_{n-1}Q_n}, \quad n \geq 1, \quad (9)$$

$$[a_0, a_1, \dots, a_{n-2}, a_{n-1}, a_n] - [a_0, a_1, \dots, a_{n-2}] = \frac{(-1)^n a_n}{Q_{n-2}Q_n}, \quad n \geq 2. \quad (10)$$

[访问主页](#)[标题页](#)[目录页](#)[◀](#) [▶](#)[◀](#) [▶](#)[第 11 页 共 57 页](#)[返回](#)[全屏显示](#)[关闭](#)[退出](#)



例7.1.1 求 $x = \frac{7700}{2145}$ 的有限简单连分数及它的各个渐近分数.

解 根据简单连分数的构造, 我们有

$$(0) a_0 = \left[\frac{7700}{2145} \right] = 3, \quad x_0 = x - a_0 = \frac{1265}{2145}.$$

$$(1) a_1 = \left[\frac{2145}{1265} \right] = 1, \quad x_1 = 1/x_0 - a_1 = \frac{880}{1265}.$$

$$(2) a_2 = \left[\frac{1265}{880} \right] = 1, \quad x_2 = 1/x_1 - a_2 = \frac{385}{880}.$$

$$(3) a_3 = \left[\frac{880}{385} \right] = 2, \quad x_3 = 1/x_2 - a_3 = \frac{110}{385}.$$

$$(4) a_4 = \left[\frac{385}{110} \right] = 3, \quad x_4 = 1/x_3 - a_4 = \frac{55}{110}.$$

$$(5) a_5 = \left[\frac{110}{55} \right] = 2, \quad x_5 = 1/x_4 - a_5 = 0.$$

因此, $\frac{7700}{2145} = [3, 1, 1, 2, 3, 2] = [3, 1, 1, 2, 3, 1, 1].$

i	a_i	x_i	P_i	Q_i	i	a_i	x_i	P_i	Q_i
0	3	$\frac{1265}{2145}$	3	1	3	2	$\frac{110}{385}$	18	5
1	1	$\frac{880}{1265}$	4	1	4	3	$\frac{55}{110}$	61	17
2	1	$\frac{385}{880}$	7	2	5	2	0	140	39

[访问主页](#)

[标题页](#)

[目录页](#)

◀

▶

◀

▶

第 12 页 共 57 页

[返回](#)

[全屏显示](#)

[关闭](#)

[退出](#)



例7.1.2 求 $\alpha = \frac{\sqrt{5}+1}{2}$ 的有限简单连分数及它的各个渐近分数.

解 根据简单连分数的构造, 并令 $\beta = \frac{\sqrt{5}-1}{2}$
我们有

$$\begin{aligned}
 \alpha = \frac{\sqrt{5}+1}{2} &= 1 + \frac{\sqrt{5}-1}{2} = 1 + \beta \\
 &= 1 + \frac{1}{\alpha} \\
 &= 1 + \frac{1}{1 + \frac{1}{\alpha}} \\
 &= 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{\alpha}}} \\
 &= 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{\alpha}}}}.
 \end{aligned}$$

因此, $\frac{\sqrt{5}+1}{2} = [1, 1, 1, 1, 1, 1, \dots]$.


[访问主页](#)
[标题页](#)
[目录页](#)
[◀](#)
[▶](#)
[◀](#)
[▶](#)

第 13 页 共 57 页

[返回](#)
[全屏显示](#)
[关闭](#)
[退出](#)




i	a_i	x_i	P_i	Q_i	i	a_i	x_i	P_i	Q_i
0	1	β	1	1	10	1	β	144	89
1	1	β	2	1	11	1	β	233	144
2	1	β	3	2	12	1	β	377	233
3	1	β	5	3	13	1	β	610	377
4	1	β	8	5	14	1	β	987	610
5	1	β	13	8	15	1	β	1597	987
6	1	β	21	13	16	1	β	2584	1597
7	1	β	34	21	17	1	β	4181	2584
8	1	β	55	34	18	1	β	6765	4181
9	1	β	89	55	19	1	β	10946	6765

[访问主页](#)[标题页](#)[目录页](#)[◀◀](#) [▶▶](#)[◀](#) [▶](#)

第 14 页 共 57 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)



7.1.3 重要常数 e , π , γ 的简单连分数

例7.1.3 分别求圆周率 $\pi = 3.141592654$ (取10 位十进制) 和
 $\pi = 3.1415926535897932385$ (取20 位十进制)的连分数展开式.

$$\pi_{10} = [3, 7, 15, 1, 293, 10, 3, 8, 2, 1, 3, 11, 1, 2, 1, 2, 1].$$

$$\pi_{20} = [3, 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, 1, 14, 2, 1, 1, 2].$$

i	a_i	P_i	Q_i	$\pi - P(i)/Q_i$	i	a_i	P_i	Q_i	$\pi - P(i)/Q_i$
0	3	3	1	0.141592654	0	3	3	1	0.1415926535897932385
1	7	22	7	-0.001264489	1	7	22	7	-0.0012644892673496186
2	15	333	106	0.000083220	2	15	333	106	0.0000832196275290876
3	1	355	113	-0.000000266	3	1	355	113	-0.0000002667641890624
4	293	104348	33215	0.0	4	292	103993	33102	0.0000000005778906344
5	11	1148183	365478	0.0	5	1	104348	33215	-0.0000000003316278062
6	1	1252531	398693	0.0	6	1	208341	66317	0.0000000001223565330
7	1	2400714	764171	0.0	7	1	312689	99532	$-2.91433849 \cdot 10^{-11}$
8	7	18057529	5747890	0.0	8	2	833719	265381	$8.7154673 \cdot 10^{-12}$
9	2	38515772	12259951	0.0	9	1	1146408	364913	$-1.6107400 \cdot 10^{-12}$
10	1	56573301	18007841	0.0	10	3	4272943	1360120	$4.040670 \cdot 10^{-13}$

[访问主页](#)
[标题页](#)
[目录页](#)
[◀](#) [▶](#)
[◀](#) [▶](#)

第 15 页 共 57 页

[返回](#)
[全屏显示](#)
[关闭](#)
[退出](#)




例7.1.4 分别求自然对数底 $e = 2.718281828$ (取10 位十进制) 和 $e = 2.7182818284590452354$ (取20 位十进制)的连分数展开式.

$$e_{10} = [2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1, 1, 3, 1, 1, 1, 2, 10, 1]$$

$$e_{20} = [2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1, 1, 10, 1, 1, 12, 1, 1, 14]$$

i	a_i	P_i	Q_i	$e - P(i)/Q_i$	i	a_i	P_i	Q_i	$e - P(i)/Q_i$
0	2	2	1	0.718281828	0	2	2	1	0.7182818284590452354
1	1	3	1	-0.281718172	1	1	3	1	-0.2817181715409547646
2	2	8	3	0.051615161	2	2	8	3	0.0516151617923785687
3	1	11	4	-0.031718172	3	1	11	4	-0.0317181715409547646
4	1	19	7	0.003996114	4	1	19	7	0.0039961141733309497
5	4	87	32	-0.000468172	5	4	87	32	-0.0004681715409547646
6	1	106	39	0.000333110	6	1	106	39	0.0003331105103272867
7	1	193	71	-0.000028031	7	1	193	71	-0.0000280306958843421
8	6	1264	465	0.000002258	8	6	1264	465	0.0000022585665721171
9	1	1457	536	-0.000001754	9	1	1457	536	-0.0000017536305070034
10	1	2721	1001	0.000000110	10	1	2721	1001	0.0000001101773269537
11	8	23225	8544	-0.000000007	11	8	23225	8544	-0.0000000067469472740
12	1	25946	9545	0.000000005	12	1	25946	9545	0.0000000055150955235
13	1	49171	18089	-0.000000001	13	1	49171	18089	-0.0000000002766504913
14	3	173459	63812	0.0	14	10	517656	190435	$1.36439174 \cdot 10^{-11}$
15	1	222630	81901	0.0	15	1	566827	208524	$-1.15384864 \cdot 10^{-11}$

[访问主页](#)[标题页](#)[目录页](#)[◀](#) [▶](#)[◀](#) [▶](#)

第 16 页 共 57 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)



例7.1.5 分别求欧拉常数 $\gamma = 0.5772156649$ (取10 位十进制) 和

$\gamma = 0.57721566490153286061$ (取20 位十进制)的连分数展开式.

$\gamma_{10} = [0, 1, 1, 2, 1, 2, 1, 4, 3, 13, 5, 1, 1, 9, 6, 5, 1, 2, 167, 151236069913024825412, 5]$

$\gamma_{20} = [0, 1, 1, 2, 1, 2, 1, 4, 3, 13, 5, 1, 1, 8, 1, 2, 4, 1, 1, 40, 1]$

i	a_i	P_i	Q_i	$\gamma - P(i)/Q_i$	i	a_i	P_i	Q_i	$\gamma - P(i)/Q_i$
0	0	0	1	0.5772156649	0	0	0	1	0.57721566490153286061
1	1	1	1	-0.4227843351	1	1	1	1	-0.42278433509846713939
2	1	1	2	0.0772156649	2	1	1	2	0.07721566490153286061
3	2	3	5	-0.0227843351	3	2	3	5	-0.02278433509846713939
4	1	4	7	0.0057870935	4	1	4	7	0.00578709347296143204
5	2	11	19	-0.0017317035	5	2	11	19	-0.00173170351951977097
6	1	15	26	0.0002925880	6	1	15	26	0.00029258797845593753
7	4	71	123	-0.0000201075	7	4	71	123	-0.00002010745619071663
8	3	228	395	0.0000004750	8	3	228	395	0.00000047502811513909
9	13	3035	5258	-0.0000000065	9	13	3035	5258	-0.00000000645639791155
10	5	15403	26685	0.0000000007	10	5	15403	26685	0.00000000067069156400
11	1	18438	31943	-0.0000000005	11	1	18438	31943	-0.00000000050246801595
12	1	33841	58628	0.0	12	1	33841	58628	$3.150488763 \cdot 10^{-11}$
13	9	323007	559595	0.0	13	8	289166	500967	$-2.54265734 \cdot 10^{-12}$
14	6	1971883	3416198	0.0	14	1	323007	559595	$1.02445721 \cdot 10^{-12}$
15	5	10182422	17640585	0.0	15	2	935180	1620157	$-7.852643 \cdot 10^{-14}$

[访问主页](#)[标题页](#)[目录页](#)[<<](#) [>>](#)[<](#) [>](#)

第 17 页 共 57 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)

上海交通大学
SHANGHAI JIAO TONG UNIVERSITY

信息安全工程学院





7.2 连分数

7.2.1 基本概念及性质

本节考虑连分数的定义及其性质. 简单连分数所考虑的部分商为整数.

定义7.2.1 设 x_0, x_1, x_2, \dots 是一个无穷实数列, $x_i > 0, i \geq 1$.

对于整数 $n \geq 0$, 我们将表示式

$$x_0 + \frac{1}{x_1 + \frac{1}{x_2 + \frac{1}{x_3 + \dots + \frac{1}{x_{n-1} + \frac{1}{x_n}}}}} \quad (11)$$

叫做 n 阶有限连分数, 它的值是一个实数. 当 x_0, x_1, \dots, x_n 都是整数时, 表示式(12) 叫做 n 阶有限简单连分数, 它的值是一个有理分数. 有理连分数也记作

$$[x_0, x_1, \dots, x_n]. \quad (12)$$

[访问主页](#)[标题页](#)[目录页](#)[<<](#)[>>](#)[<](#)[>](#)

第 18 页 共 57 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)

设 $0 \leq k \leq n$, 我们将有限连分数

$$[x_0, x_1, \dots, x_k] \quad (13)$$

叫做有限连分数(11)的第 k 个渐近分数. 当(12)是有限简单连分数时, 将 x_k 叫做它的第 k 个部分商.

当(11) (或(12))中的 $n \rightarrow \infty$ 时, 我们将表示式

$$x_0 + \frac{1}{x_1 + \frac{1}{x_2 + \frac{1}{x_3 + \dots}}} \quad (14)$$

或者简记为

$$[x_0, x_1, x_2, \dots]. \quad (15)$$

叫做无限连分数. 当 x_0, x_1, \dots 都是整数时, 表示式(14)叫做无限简单连分数.

设 $k \geq 0$, 我们将有限连分数

$$[x_0, x_1, x_2, \dots, x_k]$$

叫做无限连分数(14)的第 k 个渐近分数. 当(14)是无限简单连分数时, 将 x_k 叫做它的第 k 个部分商.

[访问主页](#)[标题页](#)[目录页](#)[<<](#)[>>](#)[<](#)[>](#)[第 19 页 共 57 页](#)[返回](#)[全屏显示](#)[关闭](#)[退出](#)



如果存在极限

$$\lim_{k \rightarrow \infty} [x_0, x_1, x_2, \dots, x_k] = \theta, \quad (16)$$

则称无限连分数(14)(或(15))是收敛的, θ 称为无限连分数(14)(或(15)) 的值, 记作

$$[x_0, x_1, x_2, \dots] = \theta.$$

如果极限(16)不存在, 则称无限连分数(14)(或(15))是发散的.

[访问主页](#)[标题页](#)[目录页](#)[◀](#) [▶](#)[◀](#) [▶](#)

第 20 页 共 57 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)



为了更清楚地讨论连分数的性质, 我们先给出几个引理:

引理7.2.1 设 a, b, c 是实数, $b \neq 0$. 设 $f(x) = a + \frac{b}{c+x}$. 则

(i) 当 $b > 0$ 时, $f(x)$ 在 $x > -c$ (或 $x < -c$) 上是单调递减函数, 即当 $-c < x < x'$ (或 $x < x' < -c$) 时, 有 $f(x) > f(x')$.

(ii) 当 $b < 0$ 时, $f(x)$ 在 $x > -c$ (或 $x < -c$) 上是单调递增函数, 即当 $-c < x < x'$ (或 $x < x' < -c$) 时, 有 $f(x) < f(x')$.

证 对于 $-c < x < x'$ (或 $x < x' < -c$), 我们有

$$f(x') - f(x) = \left(a + \frac{b}{c+x'}\right) - \left(a + \frac{b}{c+x}\right) = \frac{-b(x' - x)}{(c+x')(c+x)}.$$

因为 $(c+x')(c+x) > 0$, 所以(i) 当 $b > 0$ 时, 有 $f(x') < f(x)$. 而(ii) 当 $b < 0$ 时, 有 $f(x') > f(x)$. 故结论成立. 证毕

[访问主页](#)[标题页](#)[目录页](#)[◀](#) [▶](#)[◀](#) [▶](#)

第 21 页 共 57 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)



定理7.2.1 设 x_0, x_1, \dots 是一个无穷实数列, $x_i > 0, i \geq 1$. 则

(i) 对任意整数 $n \geq 1, r \geq 1$, 我们有

$$\begin{aligned} & [x_0, x_1, \dots, x_{n-1}, x_n, \dots, x_{n+r}] \\ &= [x_0, x_1, \dots, x_{n-1}, [x_n, \dots, x_{n+r}]] \\ &= [x_0, x_1, \dots, x_{n-1}, x_n + \frac{1}{[x_{n+1}, \dots, x_{n+r}]}]. \end{aligned} \quad (17)$$

特别地, 我们有

$$[x_0, x_1, \dots, x_{n-1}, x_n, x_{n+1}] = [x_0, x_1, \dots, x_{n-1}, x_n + \frac{1}{x_{n+1}}]. \quad (18)$$

(ii) 对任意实数 $\eta > 0$ 和整数 $n \geq 0$,

(a) 当 n 是奇数时, 我们有

$$[x_0, x_1, \dots, x_{n-1}, x_n] > [x_0, x_1, \dots, x_{n-1}, x_n + \eta,] \quad (19)$$

(b) 当 n 是偶数时, 我们有

$$[x_0, x_1, \dots, x_{n-1}, x_n] < [x_0, x_1, \dots, x_{n-1}, x_n + \eta,] \quad (20)$$

[访问主页](#)

[标题页](#)

[目录页](#)

◀

▶

◀

▶

第 22 页 共 57 页

[返回](#)

[全屏显示](#)

[关闭](#)

[退出](#)





(iii) 对整数 $n \geq 0$, 令

$$\theta_n = [x_0, x_1, \dots, x_{n-1}, x_n],$$

(a) 对任意整数 $r \geq 1$, 我们有

$$\theta_{2n+1} > \theta_{2n+1+r},$$

(b) 对任意整数 $r \geq 1$, 我们有

$$\theta_{2n} < \theta_{2n+r},$$

(c)

$$\theta_1 > \theta_3 > \dots \theta_{2n-1} > \dots,$$

(d)

$$\theta_0 < \theta_2 < \dots \theta_{2n} < \dots,$$

(e) 对任意整数 $s \geq 1, t \geq 0$, 我们有

$$\theta_{2s-1} > \theta_{2t}.$$

[访问主页](#)[标题页](#)[目录页](#)[◀◀](#) [▶▶](#)[◀](#) [▶](#)

第 23 页 共 57 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)



证 (i) 根据连分数的定义, 我们有

$$\begin{aligned}
 x_0 + \frac{1}{x_1 + \dots + \frac{1}{x_{n-1} + \frac{1}{x_n + \dots + \frac{1}{x_{n+r}}}}} &= x_0 + \frac{1}{x_1 + \dots + \frac{1}{x_{n-1} + \frac{1}{[x_n, \dots, x_{n+r}]}}} \\
 &= [x_0, x_1, \dots, x_{n-1}, [x_n, \dots, x_{n+r}]] \\
 &= [x_0, x_1, \dots, x_{n-1}, x_n + \frac{1}{[x_{n+1}, \dots, x_{n+r}]}].
 \end{aligned}$$

特别地, 我们有

$$x_0 + \frac{1}{x_1 + \dots + \frac{1}{x_{n-1} + \frac{1}{x_n + \frac{1}{x_{n+1}}}}} = [x_0, x_1, \dots, x_{n-1}, x_n + \frac{1}{x_{n+1}}].$$

[访问主页](#)

[标题页](#)

[目录页](#)

◀

▶

◀

▶

第 24 页 共 57 页

[返回](#)

[全屏显示](#)

[关闭](#)

[退出](#)





(ii) 对任意实数 x_0 和 $x_1 > 0, x_2 > 0$, 由引理7.2.1, 我们有分数值 $x_0 + \frac{1}{x_1 + x}$ 随增大而减小, 分数值 $x_0 + \frac{1}{x_1 + \frac{1}{x_2 + x}}$ 随增大而增大.

应用这个事实, 可得到定理(ii)的结论.

[访问主页](#)[标题页](#)[目录页](#)[<<](#)[>>](#)[<](#)[>](#)

第 25 页 共 57 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)



(iii) 根据(i) 和(ii), 我们有

$$\begin{aligned} & [x_0, x_1, \dots, x_{2n}, x_{2n+1}, \dots, x_{2n+1+r}] \\ &= [x_0, x_1, \dots, x_{2n}, x_{2n+1} + \frac{1}{[x_{2n+2}, \dots, x_{2n+1+r}]}] \\ &< [x_0, x_1, \dots, x_{2n}, x_{2n+1}]. \end{aligned}$$

因此, 结论(a) 成立.

同理, 我们有

$$\begin{aligned} & [x_0, x_1, \dots, x_{2n-1}, x_{2n}, \dots, x_{2n+r}] \\ &= [x_0, x_1, \dots, x_{2n-1}, x_{2n} + \frac{1}{[x_{2n+1}, \dots, x_{2n+r}]}] \\ &> [x_0, x_1, \dots, x_{2n-1}, x_{2n}]. \end{aligned}$$

因此, 结论(b) 成立.

再从(a), (b), 立即得到(c), (d), (e).

证毕

访问主页

标题页

目录页

◀

▶

◀

▶

第 26 页 共 57 页

返回

全屏显示

关闭

退出





7.2.2 连分数的渐近分数

本节讨论连分数的渐近分数.

定理7.2.2 设 x_0, x_1, x_2, \dots 是无穷实数列, $x_j > 0, j \geq 1$. 再设

$$P_{-2} = 0, \quad P_{-1} = 1, \quad P_n = x_n P_{n-1} + P_{n-2}, \quad n \geq 0, \quad (21)$$

$$Q_{-2} = 1, \quad Q_{-1} = 0, \quad Q_n = x_n Q_{n-1} + Q_{n-2}, \quad n \geq 0. \quad (22)$$

则我们有

$$[x_0, x_1, \dots, x_{n-1}, x_n] = \frac{x_n P_{n-1} + P_{n-2}}{x_n Q_{n-1} + Q_{n-2}} = \frac{P_n}{Q_n}, \quad n \geq 0, \quad (23)$$

$$P_n Q_{n-1} - P_{n-1} Q_n = (-1)^{n+1}, \quad n \geq -1, \quad (24)$$

$$P_n Q_{n-2} - P_{n-2} Q_n = (-1)^n x_n, \quad n \geq 0. \quad (25)$$

[访问主页](#)[标题页](#)[目录页](#)[◀](#) [▶](#)[◀](#) [▶](#)[第 27 页 共 57 页](#)[返回](#)[全屏显示](#)[关闭](#)[退出](#)



特别地, 我们有

$$\frac{P_0}{Q_0} < \dots < \frac{P_{2n-2}}{Q_{2n-2}} < \frac{P_{2n}}{Q_{2n}} < \dots < \frac{P_{2n+1}}{Q_{2n+1}} < \frac{P_{2n-1}}{Q_{2n-1}} < \dots < \frac{P_1}{Q_1}, \quad (26)$$

$$[x_0, x_1, \dots, x_{n-1}, x_n] - [x_0, x_1, \dots, x_{n-1}] = \frac{(-1)^{n+1}}{Q_{n-1}Q_n}, \quad n \geq 1, \quad (27)$$

$$[x_0, x_1, \dots, x_{n-2}, x_{n-1}, x_n] - [x_0, x_1, \dots, x_{n-2}] = \frac{(-1)^n x_n}{Q_{n-2}Q_n}, \quad n \geq 2. \quad (28)$$

[访问主页](#)[标题页](#)[目录页](#)[◀](#) [▶](#)[◀](#) [▶](#)[第 28 页 共 57 页](#)[返回](#)[全屏显示](#)[关闭](#)[退出](#)



证 (i) 我们对 n 作数学归纳法来证明关系式(23).

$n = 0$ 时, 根据假设条件(21) 和(22), 我们有

$$P_0 = x_0 P_{-1} + P_{-2} = x_0 \cdot 1 + 0 = x_0, \quad Q_0 = x_0 Q_{-1} + Q_{-2} = x_0 \cdot 0 + 1 = 1,$$

从而

$$\frac{P_0}{Q_0} = x_0.$$

假设 $n = k$ 时, 命题成立, 即我们有

$$[x_0, x_1, \dots, x_{k-1}, x_k] = \frac{x_k P_{k-1} + P_{k-2}}{x_k Q_{k-1} + Q_{k-2}} = \frac{P_k}{Q_k}.$$

[访问主页](#)[标题页](#)[目录页](#)[◀](#) [▶](#)[◀](#) [▶](#)[第 29 页 共 57 页](#)[返 回](#)[全屏显示](#)[关 闭](#)[退 出](#)



对于 $n = k + 1$, 根据假设条件(21) 和(22) 和归纳假设, 以及关系式(18), 我们有

$$\begin{aligned} [x_0, x_1, \dots, x_{k-1}, x_k, x_{k+1}] &= [x_0, x_1, \dots, x_{k-1}, x_k + \frac{1}{x_{k+1}}] \\ &= \frac{(x_k + \frac{1}{x_{k+1}})P_{k-1} + P_{k-2}}{(x_k + \frac{1}{x_{k+1}})Q_{k-1} + Q_{k-2}} \\ &= \frac{x_{k+1}(x_k P_{k-1} + P_{k-2}) + P_{k-1}}{x_{k+1}(x_k Q_{k-1} + Q_{k-2}) + Q_{k-1}} \\ &= \frac{x_{k+1}P_k + P_{k-1}}{x_{k+1}Q_k + Q_{k-1}} \\ &= \frac{P_{k+1}}{Q_{k+1}}. \end{aligned}$$

因此, 关系式(23)成立.

[访问主页](#)[标题页](#)[目录页](#)[◀](#) [▶](#)[◀](#) [▶](#)[第 30 页 共 57 页](#)[返回](#)[全屏显示](#)[关闭](#)[退出](#)



(ii) 我们对 n 作数学归纳法来证明关系式(24).

$n = -1$ 时, 根据假设条件(21)和(22), 我们有

$$P_{-1}Q_{-2} - P_{-2}Q_{-1} = 1 \cdot 1 - 0 \cdot 0 = 1 = (-1)^0.$$

假设 $n = k$ 时, 命题成立, 即我们有

$$P_kQ_{k-1} - P_{k-1}Q_k = (-1)^{k+1}.$$

对于 $n = k + 1$, 从关系式(21) 和(22) 中消除 x_{k+1} , 并根据归纳假设, 我们有

$$P_{k+1}Q_k - P_kQ_{k+1} = -(P_kQ_{k-1} - P_{k-1}Q_k) = -(-1)^{k+2}.$$

因此, 关系式(24)成立.

(iii) 根据关系式(21) 和(22), 以及关系式(24), 我们得到

$$P_nQ_{n-2} - P_{n-2}Q_n = x_n(P_{n-1}Q_{n-2} - P_{n-2}Q_{n-1}) = (-1)^n x_n.$$

因此, 关系式(25)成立.

[访问主页](#)[标题页](#)[目录页](#)[◀](#) [▶](#)[◀](#) [▶](#)

第 31 页 共 57 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)



(iv) 运用关系式(24) 和(25), 我们得到

$$\frac{P_0}{Q_0} < \dots < \frac{P_{2n-2}}{Q_{2n-2}} < \frac{P_{2n}}{Q_{2n}} < \dots < \frac{P_{2n+1}}{Q_{2n+1}} < \frac{P_{2n-1}}{Q_{2n-1}} < \dots < \frac{P_1}{Q_1}.$$

(v) 运用关系式(23) 和(24), 我们得到

$$\begin{aligned} & [x_0, x_1, \dots, x_{n-1}, x_n] - [x_0, x_1, \dots, x_{n-1}] \\ &= \frac{P_n}{Q_n} - \frac{P_{n-1}}{Q_{n-1}} = \frac{P_n Q_{n-1} - P_{n-1} Q_n}{Q_{n-1} Q_n} = \frac{(-1)^{n+1}}{Q_{n-1} Q_n}. \end{aligned}$$

(vi) 运用关系式(23)和(25) 我们得到

$$\begin{aligned} & [x_0, x_1, \dots, x_{n-1}, x_n] - [x_0, x_1, \dots, x_{n-2}] \\ &= \frac{P_n}{Q_n} - \frac{P_{n-2}}{Q_{n-2}} = \frac{P_n Q_{n-2} - P_{n-2} Q_n}{Q_{n-2} Q_n} = \frac{(-1)^n x_n}{Q_{n-1} Q_n}. \end{aligned}$$

证毕

[访问主页](#)

[标题页](#)

[目录页](#)

[◀](#) [▶](#)

[◀](#) [▶](#)

第 32 页 共 57 页

[返回](#)

[全屏显示](#)

[关闭](#)

[退出](#)





在知道连分数的部分商的情况下, 定理7.2.2 给出了求渐近连分数的方法.
我们用列表的形式给出 $\sqrt{2} = [1, 2, 2, 2, \dots]$ 的渐近连分数:

k	x_k	P_k	Q_k	k	x_k	P_k	Q_k
-2		0	1	3	2	17	12
-1		1	0	4	2	41	29
0	1	1	1	5	2	99	70
1	2	3	2	6	2	239	169
2	2	7	5	7	2	577	408

由此得到

$$1.412011 < \frac{P_6}{Q_6} = \frac{239}{169} < \sqrt{2} < \frac{P_7}{Q_7} = \frac{577}{408} < 1.412157.$$

访问主页

标题页

目录页

◀

▶

◀

▶

第 33 页 共 57 页

返回

全屏显示

关闭

退出





关于 α 与其渐近连分数, 我们有更准确的公式.

定理7.2.3 设 $x_0, x_1, x_2, \dots, x_n$ 是实数列, $x_j > 0, j \geq 1$. 再设

$$\alpha = [x_0, x_1, x_2, \dots, x_n], \quad \alpha_{k+1} = [x_{k+1}, \dots, x_n] \quad (0 \leq k \leq n).$$

则

$$\alpha - \frac{P_k}{Q_k} = \frac{(-1)^k}{Q_k(\alpha_{k+1}Q_k + Q_{k-1})}. \quad (29)$$

证 根据定理7.2.1 (i) 及定理7.2.2, 我们有

$$\alpha = [x_0, x_1, x_2, \dots, x_k, x_{k+1}, \dots, x_n] = [x_0, x_1, x_2, \dots, x_k, \alpha_{k+1}]$$

以及

$$\alpha - \frac{P_k}{Q_k} = \frac{\alpha_{k+1}P_k + P_{k-1}}{\alpha_{k+1}Q_k + Q_{k-1}} - \frac{P_k}{Q_k} = \frac{-(P_kQ_{k-1} - P_{k-1}Q_k)}{Q_k(\alpha_{k+1}Q_k + Q_{k-1})} = \frac{(-1)^k}{Q_k(\alpha_{k+1}Q_k + Q_{k-1})}.$$

证毕

访问主页

标题页

目录页

◀

▶

◀

▶

第 34 页 共 57 页

返回

全屏显示

关闭

退出





定理7.2.4 设 α 是实数, $[a_0, a_1, a_2, \dots, a_n, \dots]$ 是其简单连分数. 则

$$\left| \alpha - \frac{P_k}{Q_k} \right| \leq \frac{1}{Q_k^2}. \quad (30)$$

证 根据定理7.2.3, 我们有

$$\left| \alpha - \frac{P_k}{Q_k} \right| = \frac{1}{Q_k(\alpha_{k+1}Q_k + Q_{k-1})} < \frac{1}{Q_k^2}.$$

证毕

访问主页

标题页

目录页

◀

▶

◀

▶

第 35 页 共 57 页

返回

全屏显示

关闭

退出





7.3 简单连分数的进一步性质

定理7.1.1 之证明

证 不妨设 $n \leq m$. 我们对 n 作数学归纳法.

$n = 0$ 时, 如果 $m \geq 1$, 根据定理7.2.1, 我们有 $a_0 = b_0 + \frac{1}{[b_1, b_2, \dots, b_m]}$.

但由 $b_m > 1$, 有 $[b_1, b_2, \dots, b_m] > 1$. 因此上式不能成立. 故 $m = 0$, $a_0 = b_0$.

假设对 $n = k$ 时, 结论成立.

对于 $n = k + 1$, 根据假设条件和定理7.2.1, 我们有

$$a_0 + \frac{1}{[a_1, a_2, \dots, a_n]} = b_0 + \frac{1}{[b_1, b_2, \dots, b_m]}.$$

因为 $a_n > 1$, $b_m > 1$, 所以 $[a_1, a_2, \dots, a_n] > 1$, $[b_1, b_2, \dots, b_m] > 1$. 因此由上式可推出

$$a_0 = b_0, \quad [a_1, a_2, \dots, a_n] = [b_1, b_2, \dots, b_m].$$

根据归纳假设, 我们有 $n - 1 = m - 1$, $a_i = b_i$, $i = 1, \dots, n$. 从而, $n = m$, $a_i = b_i$, $i = 0, \dots, n$. 即结论对 $n = k + 1$ 成立. 根据数学归纳法原理, 定理对所有的 $n \geq 0$ 成立. 证毕

[访问主页](#)[标题页](#)[目录页](#)[◀](#) [▶](#)[◀](#) [▶](#)

第 36 页 共 57 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)



定理7.3.1 无限简单连分数 $[a_0, a_1, a_2, \dots]$ 是收敛的, 即存在实数 θ , 使得

$$\lim_{n \rightarrow +\infty} [a_0, a_1, a_2, \dots, a_n] = \theta.$$

证 对 $n \geq 0$, 记 $\theta_n = [a_0, a_1, a_2, \dots, a_n]$. θ_n 是有理分数. 根据定理7.2.1, 有

$$\theta_1 > \theta_3 > \dots > \theta_{2n-1} > \dots > \theta_0,$$

$$\theta_0 < \theta_2 < \dots < \theta_{2n} < \dots < \theta_1.$$

一方面, $\{\theta_{2n-1}\}_{n \geq 1}$ 单调递减有下界 θ_0 , 存在极限 $\lim_{n \rightarrow +\infty} \theta_{2n-1} = \theta'$.

另一方面, $\{\theta_{2n}\}_{n \geq 0}$ 单调递增有上界 θ_1 , 存在极限 $\lim_{n \rightarrow +\infty} \theta_{2n} = \theta''$.

因此, $\theta_0 < \theta_2 < \dots < \theta_{2n} < \dots < \theta' \leq \theta'' < \dots < \theta_{2n-1} < \dots < \theta_1$.

但根据定理7.2.2, 对任意 $n \geq 1$, 我们有

$$|\theta'' - \theta'| \leq |\theta_n - \theta_{n-1}| = \frac{1}{Q_{n-1}Q_n}.$$

因此, $\theta' = \theta'' = \theta$.

证毕

访问主页

标题页

目录页

◀ ▶

◀ ▶

第 37 页 共 57 页

返回

全屏显示

关闭

退出





定理7.3.2 设实数 $\theta > 1$ 的渐近分数为 $\frac{P_n}{Q_n}$. 则对任意 $n \geq 1$,

$$|\theta^2 Q_n^2 - P_n^2| < 2\theta.$$

证 从定理7.3.1之证明, 有 θ 介于两渐近分数 $\frac{P_n}{Q_n}$ 和 $\frac{P_{n+1}}{Q_{n+1}}$. 根据定理7.2.2,

$$|\theta^2 Q_n^2 - P_n^2| = Q_n^2 \left| \theta - \frac{P_n}{Q_n} \right| \left| \theta + \frac{P_n}{Q_n} \right| < Q_n^2 \frac{1}{Q_n Q_{n+1}} \left(\theta + \left(\theta + \frac{1}{Q_n Q_{n+1}} \right) \right).$$

但

$$2\theta \left(\frac{Q_n}{Q_{n+1}} + \frac{1}{2\theta Q_{n+1}^2} \right) - 2\theta < 2\theta \frac{Q_n + 1}{Q_{n+1}} - 2\theta \leq 2\theta \frac{Q_{n+1}}{Q_{n+1}} - 2\theta = 0,$$

故定理成立.

证毕

访问主页

标题页

目录页

◀

▶

◀

▶

第 38 页 共 57 页

返回

全屏显示

关闭

退出





7.4 最佳逼近

前面, 我们考虑了用有理数来逼近一个实数. 现在, 我们对逼近的效果给以定性描述.

对任意给定的正整数 Q , 记集合 S_Q 为

$$S_Q = \left\{ \frac{p}{q} \mid 1 \leq q \leq Q, p \in \mathbf{Z} \right\}$$

则我们有

$$\mathbf{Z} = S_1 \subset S_2 \subset \cdots \subset S_Q \subset \cdots$$

定义7.4.1 设 θ 是一个实数. 有理数 $\frac{p}{q}$ ($q > 0$) 称为 θ 的**最佳逼近**, 如果对所有的有理数 $\frac{p'}{q'} \neq \frac{p}{q}$, $0 < q' \leq q$, 有

$$\left| \theta - \frac{p}{q} \right| < \left| \theta - \frac{p'}{q'} \right|. \quad (31)$$

这说明, 在分母 $q' \leq q$ 的所有有理数 $\frac{p'}{q'}$ 中, $\frac{p}{q}$ 是距离 θ 最近的有理数 $\frac{p}{q}$.

[访问主页](#)[标题页](#)[目录页](#)[◀](#) [▶](#)[◀](#) [▶](#)[第 39 页 共 57 页](#)[返回](#)[全屏显示](#)[关闭](#)[退出](#)



在说明 θ 的连分数是 θ 的最佳逼近之前, 我们先给出如下定理:

定理7.4.1 设 θ 是无理实数. 设 $\frac{P_n}{Q_n}$ ($n \geq 1$) 是 θ 的第 n 个渐近分数时. 如果整数 p, q ($q > 0$) 使得

$$|q\theta - p| < |Q_n\theta - P_n| \quad (32)$$

则 $q \geq Q_{n+1}$.

证 反证法. 假设存在整数 p, q ($0 < q < Q_{n+1}$) 使得

$$|q\theta - p| < |Q_n\theta - P_n|. \quad (33)$$

首先, 线性方程组:

$$\begin{cases} \lambda P_{n+1} + \mu P_n = p, \\ \lambda Q_{n+1} + \mu Q_n = q. \end{cases} \quad (34)$$

有整数解 $\lambda \neq 0, \mu \neq 0$, 且 $\lambda \cdot \mu < 0$. 从而有

$$q\theta - p = (\lambda Q_{n+1} + \mu Q_n)\theta - (\lambda P_{n+1} + \mu P_n) = \lambda(Q_{n+1}\theta - P_{n+1}) + \mu(Q_n\theta - P_n). \quad (35)$$

[访问主页](#)[标题页](#)[目录页](#)[<<](#)[>>](#)[<](#)[>](#)

第 40 页 共 57 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)



事实上, 因为 $P_{n+1} Q_n - P_n Q_{n+1} = (-1)^{n+2} = (-1)^n$, 所以方程组(34)有整数解:

$$\begin{cases} \lambda = \frac{p Q_n - P_n q}{P_{n+1} Q_n - P_n Q_{n+1}} = (-1)^n (p Q_n - P_n q), \\ \mu = \frac{P_{n+1} q - p Q_{n+1}}{P_{n+1} Q_n - P_n Q_{n+1}} = (-1)^n (P_{n+1} q - p Q_{n+1}). \end{cases}$$

进一步, 我们有 $\lambda \neq 0, \mu \neq 0$.

- 如果 $\mu = 0$, 则 $P_{n+1} q - p Q_{n+1} = 0$. 因为 $(P_{n+1}, Q_{n+1}) = 1$, 所以 $Q_{n+1} \mid q$. 从而, $q \geq Q_{n+1}$. 这与假设 $0 < q < Q_{n+1}$ 矛盾.
- 如果 $\lambda = 0, \mu \neq 0$, 我们有 $p = \mu P_n$ 及 $q = \mu Q_n$, 从而

$$|q \theta - p| = |\mu| |Q_n \theta - P_n| \geq |Q_n \theta - P_n|.$$

这与(33)矛盾.

此外, λ 与 μ 互为异号, 这从 $0 < q < Q_{n+1}$ 和(34)第二个方程可推出.

访问主页

标题页

目录页

◀

▶

◀

▶

第 41 页 共 57 页

返回

全屏显示

关闭

退出





其次, 有 $\lambda(Q_n \theta - P_n)$ 与 $\mu(Q_{n+1} \theta - P_{n+1})$ 有相同的符号. 事实上, 根据定理7.2.2, 有 θ 介于 $\frac{P_n}{Q_n}$ 与 $\frac{P_{n+1}}{Q_{n+1}}$ 之间. 从而, $(Q_n \theta - P_n) \cdot (Q_{n+1} \theta - P_{n+1}) < 0$, 进而,

$$\lambda(Q_n \theta - P_n) \cdot \mu(Q_{n+1} \theta - P_{n+1}) > 0.$$

一方面, λ 与 μ 互为异号, 这从 $0 < q < Q_{k+1}$ 和第二个方程可推出.

另一方面, $Q_n \theta - P_n$ 与 $Q_{n+1} \theta - P_{n+1}$ 的互为异号. 因为根据定理7.2.2, 我们有 θ 介于 $\frac{P_n}{Q_n}$ 与 $\frac{P_{n+1}}{Q_{n+1}}$ 之间.

最后, 由(35) 得到

$$|q \theta - p| = |\lambda(Q_{n+1} \theta - P_{n+1})| + |\mu(Q_n \theta - P_n)| \geq |\mu(Q_n \theta - P_n)| \geq |Q_n \theta - P_n|$$

这与(33) 矛盾. 故定理成立.

证毕

访问主页

标题页

目录页

◀ ▶

◀ ▶

第 42 页 共 57 页

返回

全屏显示

关闭

退出





定理7.4.2 实数 θ 的渐近分数是 θ 的最佳逼近. 即当 $\frac{P_n}{Q_n}$, ($n \geq 1$), 是 θ 的第 n 个渐近分数时, 对所有的有理数 $\frac{p}{q} \neq \frac{P_n}{Q_n}$, $0 < q \leq Q_n$, 有

$$\left| \theta - \frac{P_n}{Q_n} \right| < \left| \theta - \frac{p}{q} \right|. \quad (36)$$

证 反证法. 假设存在有理数 $\frac{p}{q} \neq \frac{P_n}{Q_n}$, $0 < q \leq Q_n$, 使得

$$\left| \theta - \frac{p}{q} \right| < \left| \theta - \frac{P_n}{Q_n} \right|.$$

因为 $0 < q \leq Q_n$, 所以

$$q \left| \theta - \frac{p}{q} \right| < Q_n \left| \theta - \frac{P_n}{Q_n} \right|,$$

即

$$|q\theta - p| < |Q_n\theta - P_n|.$$

根据定理7.4.1, 我们有 $q \geq Q_{n+1} > Q_n$. 这与假设 $0 < q \leq Q_n$ 矛盾. 证毕

[访问主页](#)[标题页](#)[目录页](#)[◀](#) [▶](#)[◀](#) [▶](#)

第 43 页 共 57 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)



7.5 循环连分数

设实数 θ 是无限简单连分数 $[a_0, a_1, a_2, \dots]$. 如果存在整数 $m \geq 0$, 使得对于该整数 m , 存在整数 $k \geq 1$, 使得对于所有 $n \geq m$, 有

$$a_{n+k} = a_n, \quad (37)$$

那么, θ 叫做循环简单连分数, 简称循环连分数. 这时 θ 可写成

$$\theta = [a_0, a_1, \dots, a_{m-1}, \overline{a_m, \dots, a_{m+k-1}}].$$

例1 $\sqrt{2} = [1, 2, 2, \dots] = [1, \overline{2}]$ 是循环连分数.

如果 $m = 0$, 使得(1) 式成立, 则 θ 叫做纯循环简单连分数, 简称纯循环连分数

例7.5.1 $\frac{\sqrt{5}+1}{2} = [1, 1, 1, \dots] = [\overline{1}]$ 是纯循环连分数.

[访问主页](#)[标题页](#)[目录页](#)[◀](#) [▶](#)[◀](#) [▶](#)

第 44 页 共 57 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)



定理7.5.1 设 θ 是循环简单连分数, 则 θ 是二次无理数.

证 设 $\theta = [\overline{a_0, \dots, a_{k-1}}]$ 是纯循环连分数, 则根据定理7.2.2,

$$\theta = [a_0, a_1, \dots, a_{k-1}, \theta] = \frac{P_k}{Q_k} = \frac{\theta P_{k-1} + P_{k-2}}{\theta Q_{k-1} + Q_{k-2}},$$

其中 $P_{k-2}, P_{k-1}, Q_{k-2}, Q_{k-1}$ 是整数. 从而,

$$Q_{k-1} \theta^2 + (-P_{k-1} + Q_{k-2})\theta - P_{k-2} = 0.$$

这说明 θ 是二次无理数.

如果 $\theta = [a_0, a_1, \dots, a_{m-1}, \overline{a_m, \dots, a_{m+k-1}}]$ 是循环连分数,

则 $\theta_0 = [\overline{a_m, \dots, a_{m+k-1}}]$ 是纯循环连分数. 根据定理7.2.2,

$$\theta = [a_0, a_1, \dots, a_{k-1}, \theta_0] = \frac{P_k}{Q_k} = \frac{\theta_0 P_{k-1} + P_{k-2}}{\theta_0 Q_{k-1} + Q_{k-2}},$$

其中 $P_{k-2}, P_{k-1}, Q_{k-2}, Q_{k-1}$ 是整数. 因此, θ 是二次无理数.

定理7.5.2 设 θ 是二次无理数, 则 θ 是循环简单连分数.

[访问主页](#)[标题页](#)[目录页](#)[◀](#) [▶](#)[◀](#) [▶](#)

第 45 页 共 57 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)



7.6 \sqrt{n} 与因数分解

利用简单连分数, 我们可以对合数 n 作因数分解.

给定整数 n , 我们希望找到 x, y 使得

$$x^2 \equiv y^2 \pmod{n}, \quad \text{且} \quad n \nmid x - y, \quad n \nmid x + y$$

进而, 可找到 n 的真因数 $(x - y, n)$ 和 $(x + y, n)$. 例如, 分解 $n = p \cdot q$.

注意, 假设 $y^2 \leq n/2$, 则 $y \leq \sqrt{n/2} = \sqrt{2n}/2$. 这时 $x \geq \sqrt{n}/2$. 现在, 我们对 x 的上界作出规定, 要求 $|x| \leq n^2$, 以提高运算速度.

设 $\theta = \sqrt{n}$. 对 θ 作连分数展开和近似, 有

$$P_k^2 - n Q_k^2 = R_k, \quad k = 0, 1, \dots \quad (38)$$

根据定理7.3.2, 有 $|R_k| \leq 2\theta = 2\sqrt{n}$.

[访问主页](#)[标题页](#)[目录页](#)[◀](#) [▶](#)[◀](#) [▶](#)

第 46 页 共 57 页

[返回](#)[全屏显示](#)[关闭](#)[退出](#)



例7.6.1 利用简单连分数, 分解整数 $n = 47 \cdot 67 = 3149$.

解 对实数 $\sqrt{n} = 56.11595139$ 作简单连分数展开:

I) 计算 $P_k^2 \bmod n$ 时, 仅考虑最小非负余数.

k	P_k	$P_k^2 \bmod n$	k	P_k	$P_k^2 \bmod n$	k	P_k	$P_k^2 \bmod n$
0	56	$2^6 \cdot 7^2$	10	1676 **	$2^2 \cdot 17$	20	2112	$2^3 \cdot 3 \cdot 5 \cdot 13$
1	449*	$5 \cdot 13$	11	1227	307	21	309	$3 \cdot 337$
2	505	$3^3 \cdot 5 \cdot 23$	12	2903	$5 \cdot 137$	22	1126	$2 \cdot 23 \cdot 43$
3	954	$5 \cdot 11$	13	243	$3^2 \cdot 263$	23	1435	$2^4 \cdot 3 \cdot 61$
4	1459	$2 \cdot 1553$	14	969	$13 \cdot 43$	24	2561	2503
5	2413 **	$2^2 \cdot 17$	15	1212	$2 \cdot 5 \cdot 151$	25	847	$2 \cdot 3 \cdot 431$
6	723	$2^3 \cdot 3 \cdot 131$	16	2441	$3 \cdot 191$	26	2800	$3 \cdot 23 \cdot 31$
7	1851	89	17	504	$2^4 \cdot 131$	27	498	$2 \cdot 3 \cdot 397$
8	2574	$3 \cdot 7 \cdot 149$	18	804	$13 \cdot 67$	28	984	$17 \cdot 89$
9	2700*	$5 \cdot 13$	19	1308	$3 \cdot 11 \cdot 29$	29	1482	1471

[访问主页](#)

[标题页](#)

[目录页](#)

[◀](#) [▶](#)

[◀](#) [▶](#)

第 47 页 共 57 页

[返回](#)

[全屏显示](#)

[关闭](#)

[退出](#)





i) 将 P_1 与 P_9 作组合, 令 $x = P_1 \cdot P_9$, $y = 5 \cdot 13$, 有

$$x - y = 449 \cdot 2700 - 5 \cdot 13 = 1212235 = 5 \cdot 242447;$$

$$x + y = 449 \cdot 2700 + 5 \cdot 13 = 1212365 = 5 \cdot 7 \cdot 11 \cdot 47 \cdot 67;$$

这时, $(x + y, n) = n$. 无法对整数 n 进行分解.

将 P_5 与 P_{10} 作组合, 令 $x = P_5 \cdot P_{10}$, $y = 4 \cdot 17$, 有

$$x - y = 2413 \cdot 1676 - 4 \cdot 17 = 4044120 = 2^3 \cdot 3 \cdot 5 \cdot 67 \cdot 503;$$

$$x + y = 2413 \cdot 1676 + 4 \cdot 17 = 4044256 = 2^5 \cdot 47 \cdot 2689;$$

这时, $(x - y, n) = 67$, $(x + y, n) = 47$. 可对整数 n 进行分解,
 $n = 47 \cdot 67$.

[访问主页](#)[标题页](#)[目录页](#)[◀](#) [▶](#)[◀](#) [▶](#)[第 48 页 共 57 页](#)[返回](#)[全屏显示](#)[关闭](#)[退出](#)

II) 计算 $P_k^2 \bmod n$ 时, 仅考虑绝对值最小余数.

k	P_k	$P_k^2 \bmod n$	k	P_k	$P_k^2 \bmod n$	k	P_k	$P_k^2 \bmod n$
0	56^{***}	$(-1) \cdot 13$	10	-1473	$2^2 \cdot 17$	20	-1037	$2^3 \cdot 3 \cdot 5 \cdot 13$
1	449	$5 \cdot 13$	11	1227	307	21	309	$3 \cdot 337$
2	505	$(-1) \cdot 2^2 \cdot 11$	12	-246	$5 \cdot 137$	22	1126	$(-1) \cdot 1171$
3	954	$5 \cdot 11$	13	243	$(-1) \cdot 2 \cdot 17 \cdot 23$	23	1435	$(-1) \cdot 13 \cdot 17$
4	1459^{***}	$(-1) \cdot 43$	14	969^{***}	$13 \cdot 43$	24	-588	$(-1) \cdot 2 \cdot 17 \cdot 19$
5	-736	$2^2 \cdot 17$	15	1212	$2 \cdot 5 \cdot 151$	25	847	$(-1) \cdot 563$
6	723	$(-1) \cdot 5$	16	-708	$3 \cdot 191$	26	-349	$(-1) \cdot 2 \cdot 5 \cdot 101$
7	-1298	89	17	504	$(-1) \cdot 3^4 \cdot 13$	27	498	$(-1) \cdot 13 \cdot 59$
8	-575	$(-1) \cdot 2^2 \cdot 5$	18	804	$13 \cdot 67$	28	984	$17 \cdot 89$
9	-449	$5 \cdot 13$	19	1308	$3 \cdot 11 \cdot 29$	29	1482	1471

将 P_0, P_4, P_{14} 作组合, 令 $x = P_0 \cdot P_4 \cdot P_{14}, y = 13 \cdot 43$, 有

$$x - y = 56 \cdot 1459 \cdot 969 - 13 \cdot 43 = 79170617 = 67 \cdot 73 \cdot 16187;$$

$$x + y = 56 \cdot 1459 \cdot 969 + 13 \cdot 43 = 79171735 = 5 \cdot 47 \cdot 336901;$$

这时, $(x - y, n) = 67, (x + y, n) = 47$. 可对整数 n 进行分解, $n = 47 \cdot 67$.


[访问主页](#)
[标题页](#)
[目录页](#)
[101](#)
[59](#)

第 49 页 共 57 页

[返回](#)
[全屏显示](#)
[关闭](#)
[退出](#)




例7.6.2 利用简单连分数, 分解整数 $167 \cdot 227 = 37909$.

解 对实数 $\sqrt{n} = 194.7023369$ 作简单连分数展开:

$\sqrt{n} = [194, 1, 2, 2, 1, 3, 1, 1, 2, 1, 1, 1, 11, 1, 1, 1, 1, 5, 1, 6, 1, 12, 2, 1, 1, 3, 1, 6, 1, 4, \dots]$

计算 $P_k^2 \bmod n$ 时, 仅考虑绝对值最小余数.

k	P_k	$P_k^2 \bmod n$	k	P_k	$P_k^2 \bmod n$	k	P_k	$P_k^2 \bmod n$
0	194	$(-1) \cdot 3 \cdot 7 \cdot 13$	10	-13650	$(-1) \cdot 5 \cdot 47$	20	-14823	$3^2 \cdot 5 \cdot 17$
1	195	$2^2 \cdot 29$	11	6657	$2^2 \cdot 7$	21	-17340	$(-1) \cdot 2^2 \cdot 3 \cdot 17 \cdot 49$
2	584	$(-1) \cdot 5^3$	12	-16241	$(-1) \cdot 3 \cdot 13 \cdot 19$	22	-11594	$(-1) \cdot 2 \cdot 2239$
3	1363	$2^2 \cdot 3 \cdot 19$	13	-9584	$(-1) \cdot 11 \cdot 41$	23	8975	$(-1) \cdot 2^4 \cdot 3 \cdot 5^3$
4	1947	$(-1) \cdot 7 \cdot 13$	14	12084	$(-1) \cdot 2^2 \cdot 3^2 \cdot 67$	24	-2619	$(-1) \cdot 2^6 \cdot 37$
5	7204	$3 \cdot 5 \cdot 13$	15	2500	$(-1) \cdot 5 \cdot 997$	25	1118	$(-1) \cdot 29 \cdot 37$
6	9151	$(-1) \cdot 2^2 \cdot 3^2 \cdot 5$	16	14584	$(-1) \cdot 3 \cdot 7 \cdot 683$	26	-1501	$2 \cdot 5 \cdot 1637$
7	16355	11^2	17	-398	$2^4 \cdot 3^2 \cdot 47$	27	-7888	$5^4 \cdot 19$
8	3952	$(-1) \cdot 2^2 \cdot 3 \cdot 17$	18	14186	$(-1) \cdot 5 \cdot 3257$	28	-9389	$2^4 \cdot 7^2 \cdot 19$
9	-17602	$3 \cdot 7^2$	19	8900	$3^2 \cdot 2011$	29	-7535	$(-1) \cdot 3^2 \cdot 19 \cdot 67$





i) 令 $x = P_7$, $y = 11$, 有

$$x - y = 16355 - 11 = 16344 = 2^3 \cdot 3^2 \cdot 227;$$

$$x + y = 16355 + 11 = 16366 = 2 \cdot 7^2 \cdot 167;$$

这时, $(x - y, n) = 227$, $(x + y, n) = 167$. 可对整数 n 进行分解,
 $n = 167 \cdot 227$.

ii) 将 P_2, P_6 作组合, 令 $x = P_2 \cdot P_6$, $y = 2 \cdot 3 \cdot 5^2$, 有

$$x - y = 584 \cdot 9151 + 2 \cdot 3 \cdot 5^2 = 5344034 = 2 \cdot 79 \cdot 149 \cdot 227;$$

$$x + y = 584 \cdot 9151 + 2 \cdot 3 \cdot 5^2 = 5344334 = 2 \cdot 167 \cdot 16001;$$

这时, $(x - y, n) = 227$, $(x + y, n) = 167$. 可对整数 n 进行分解,
 $n = 167 \cdot 227$.

[访问主页](#)[标题页](#)[目录页](#)[◀](#) [▶](#)[◀](#) [▶](#)[第 51 页 共 57 页](#)[返回](#)[全屏显示](#)[关闭](#)[退出](#)