代数学と探求過程

– 無理数について –

平成16年度　前期

中川 仁

目標　循環小数，連分数，代数的数，超越数について基本事項を解説し，無理数についての理解を深める．

記号　$\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ をそれぞれ自然数全体の集合，整数全体の集合，有理数全体の集合，実数全体の集合，複素数全体の集合とする．

目 次

1　ユークリッドの互除法

自然数 a, b の**最大公約数**を $\gcd(a, b)$ で表す．$\gcd(a, b) = 1$ のとき，a と b は**互いに素**であるという．

補題 1.1. 自然数 a, b に対して，a を b で割ったときの余りを r とすれば，$\gcd(a, b) = \gcd(b, r)$ が成り立つ．

[証明]　$m = \gcd(a, b)$, $n = \gcd(b, r)$ とおく．a を b で割ったときの商を q とすれば，$a = bq + r$．$a = ma'$, $b = mb'$, a', b' は整数とかける．そのとき，$r = a - bq = ma' - mb'q = m(a' - b'q)$．よって，$m$ は b と r の公約数である．したがって，$n \geq m$．同様に，$b = nb''$, $r = nr''$, b'', r'' は整数とかける．そのとき，$a = bq + r = nb''q + nr'' = n(b''q + r'')$．よって，$n$ は a と b の公約数である．したがって，$m \geq n$．ゆえに，$m = n$．　□

定理 1.2 (Euclid の互除法). 自然数 a, b に対して，

$$\begin{aligned} a &= bq_0 + r_1, \quad 0 < r_1 < b, \\ b &= r_1 q_1 + r_2, \quad 0 < r_2 < r_1, \\ r_1 &= r_2 q_2 + r_3, \quad 0 < r_3 < r_2, \\ &\cdots\cdots\cdots \\ r_{n-2} &= r_{n-1} q_{n-1} + r_n, \quad 0 < r_n < r_{n-1}, \\ r_{n-1} &= r_n q_n \end{aligned}$$

であるとすると，$\gcd(a, b) = r_n$.

[証明]　補題 1.1 によって，$\gcd(a, b) = \gcd(b, r_1)$ である．これを繰り返せば，

$$\gcd(a, b) = \gcd(b, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_{n-1}, r_n) = r_n. \quad \square$$

例 1.3. 1995 と 1029 の最大公約数を求める．

$$\begin{aligned} 1995 &= 1029 \times 1 + 966, \\ 1029 &= 966 \times 1 + 63, \\ 966 &= 63 \times 15 + 21, \\ 63 &= 21 \times 3. \end{aligned}$$

したがって，$\gcd(1995, 1029) = 21$ である．

練習問題 1. 2003 と 417 の最大公約数 d を求めよ．さらに，$2003x + 417y = d$ を満たす整数 x, y を一組求めよ．

$$\begin{aligned} 2003 &= 417 \times 4 + 335, \\ 417 &= 335 \times 1 + 82, \\ 335 &= 82 \times 4 + 7, \\ 82 &= 7 \times 11 + 5, \\ 7 &= 5 \times 1 + 2, \\ 5 &= 2 \times 2 + 1. \end{aligned}$$

したがって，$\gcd(2003, 417) = 1$ である．$x = -178$, $y = 855$.

2　1 次不定方程式

整数 a, b が与えられたとき，$d = \gcd(a, b)$ とすると，

$$ax + by = d \tag{2.1}$$

を満たすような整数 x, y を見つけることがユークリッドの互除法を応用することによってできる．これを具体例で説明する．

例 2.1. 197 と 41 の最大公約数を求める．

$$\begin{aligned} 197 &= 41 \times 4 + 33, \\ 41 &= 33 \times 1 + 8, \\ 33 &= 8 \times 4 + 1, \\ 8 &= 1 \times 8. \end{aligned}$$

これから，$\gcd(197, 41) = 1$ となる．この計算を利用して，

$$197x + 41y = 1$$

を満たす整数 x, y をすべて求めることができる．

$$\begin{aligned} 1 &= 33 - 8 \times 4 \\ &= 33 - (41 - 33 \times 1) \times 4 = 33 \times 5 - 41 \times 4 \\ &= (197 - 41 \times 4) \times 5 - 41 \times 4 = 197 \times 5 - 41 \times 24. \end{aligned}$$

したがって，$197 \times 5 + 41 \times (-24) = 1$ を得る．

上の例をもっと一般的に述べれば，次の定理になる．

定理 2.2. a, b を互いに素な整数とすれば，$ax + by = 1$ を満たす整数 x, y が (無数に) 存在する．特に，p を素数とし，a を p で割り切れない整数とすれば，$ax + py = 1$ を満たす整数 x, y が存在する．

命題 2.3. m を自然数とし，a を m と互いに素な整数, b を整数とする．そのとき，ab が m で割り切れるならば，b は m で割り切れる．

[証明]　$ab = mk$ とかく．定理 2.2 より，$ax + my = 1$ を満たす整数 x, y が存在する．

$$b = b \cdot 1 = b(ax + my) = abx + mby = mkx + mby = m(kx + by).$$

よって，b は m で割り切れる．　□

命題 2.4. p を素数とし，a, b を整数とする．そのとき，ab が p で割り切れるならば，a または b は p で割り切れる．

[証明]　ab は p で割り切れるが，a は p で割り切れないとする．$\gcd(a, p)$ は素数 p の約数だから，1 または p である．a は p で割り切れないから，$\gcd(a, p) = 1$，すなわち，a は p と互いに素である．そのとき，命題 2.3 で $m = p$ とすれば，b は p で割り切れる．　□

例 2.5. x, y が $31x + 7y = 1$ を満たす整数を動くとき，$|x + y|$ の最小値を求めよ．

$$\begin{aligned} 31 &= 7 \times 4 + 3, \\ 7 &= 3 \times 2 + 1. \end{aligned}$$

$$\begin{aligned} 1 &= 7 - 3 \times 2 \\ &= 7 - (31 - 7 \times 4) \times 2 \\ &= 7 \times 9 - 31 \times 2. \end{aligned}$$

よって，$x = -2$, $y = 9$ は $31x + 7y = 1$ を満たす．

$$\begin{aligned} 31x + 7y &= 1, \\ 31 \times (-2) + 7 \times 9 &= 1, \\ 31(x + 2) + 7(y - 9) &= 0, \\ 31(x + 2) &= -7(y - 9). \end{aligned}$$

左辺は 31 の倍数だから，右辺の $-7(y-9)$ も 31 の倍数である．7 は 31 と素であるから，命題 2.3 より，$y - 9$ は 31 で割り切れるから，$y - 9 = 31t$, t は整数，とかける．そのとき，$31(x+2) = -7 \times 31t$ より，$x + 2 = -7t$, $x = -2 - 7t$. $y = 9 + 31t$ だから，

$$|x + y| = |-2 - 7t + 9 + 31t| = |24t + 7|.$$

これが最小になるのは，$t = 0$ のとき，$x = -2$, $y = 9$ のときで，最小値は 7 である．

3 合同式

m を自然数とする．整数 a, b の差 $a - b$ が m で割り切れるとき，

$$a \equiv b \pmod{m}$$

とかき，a と b は m を**法として合同**であるという．次のことが成り立つ．

命題 3.1. $a \equiv b \pmod{m}$ かつ $c \equiv d \pmod{m}$ ならば，$a \pm c \equiv b \pm d \pmod{m}$, $ac \equiv bd \pmod{m}$.

[証明] $a - b = ms$, $c - d = mt$, s, t は整数とかける．そのとき，

$$(a + c) - (b + d) = m(s + t), \quad (a - c) - (b - d) = m(s - t)$$

であるから，

$$a + c \equiv b + d \pmod{m}, \quad a - c \equiv b - d \pmod{m}.$$

$a = b + ms$, $c = d + mt$ より，

$$\begin{aligned} ac &= (b+ms)(d+mt) \\ &= bd + mbt + mds + m^2st \\ &= bd + m(bt + ds + mst), \\ ac - bd &= m(bt + ds + mst). \end{aligned}$$

よって，$ac \equiv bd \pmod{m}$. □

p を素数とし，a を p で割り切れない整数とする．そのとき，定理 2.2 より，$ax + py = 1$ を満たす整数 x, y が存在する．よって，合同式

$$ax \equiv 1 \pmod{p}$$

を満たす整数 x が存在する．x_1 を x を p で割った余りとすれば，$0 \leq x_1 < p$, $x = pk + x_1$ とかけるから，$x_1 \equiv x \pmod{p}$, $ax_1 \equiv ax \equiv 1 \pmod{p}$ である．明らかに，$x_1 \neq 0$ である．x を x_1 で置き換えれば，

$$ax \equiv 1 \pmod{p}$$

を満たす整数 x で，$1 \leq x \leq p-1$ を満たすものが存在する．

定理 3.2 (フェルマーの小定理). p を素数とし，a を p で割り切れない整数とする．そのとき，

$$a^{p-1} \equiv 1 \pmod{p}$$

が成り立つ．

[証明] まず，$ax \equiv ay \pmod{p}$ ならば，$x \equiv y \pmod{p}$ であることを示す．$ax \equiv ay \pmod{p}$ とすると，$a(x-y) \equiv 0 \pmod{p}$，すなわち，$a(x-y)$ は素数 p で割り切れる．a は p で割り切れないとしたから，命題 2.4 より，$x - y$ が p で割り切れる．よって，$x \equiv y \pmod{p}$ である．この対偶をとって，$x \not\equiv y \pmod{p}$ ならば，$ax \not\equiv ay \pmod{p}$ である．したがって，x が $1, 2, \ldots, p-1$ を動くとき，ax の値は p を法として，0 でなく，また互いに合同ではない．よって，ax の値は p を法として，$1, 2, \ldots, p-1$ をすべて丁度 1 回ずつとる．したがって，

$$\begin{aligned} &(a \cdot 1)(a \cdot 2) \cdots (a \cdot (p-1)) \equiv 1 \cdot 2 \cdots (p-1) \pmod{p}, \\ &a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}, \\ &(p-1)!(a^{p-1} - 1) \equiv 0 \pmod{p}. \end{aligned}$$

すなわち，$(p-1)!(a^{p-1}-1)$ は素数 p で割り切れる．$(p-1)!$ は p で割り切れないから，命題 2.4 より，$a^{p-1} - 1$ が p で割り切れなければならない． □

例 3.3. $p=7$, $a=3$ とすると，

$$\begin{aligned}
3\cdot 1 &\equiv 3 \pmod 7,\\
3\cdot 2 &\equiv 6 \pmod 7,\\
3\cdot 3 &\equiv 2 \pmod 7,\\
3\cdot 4 &\equiv 5 \pmod 7,\\
3\cdot 5 &\equiv 1 \pmod 7,\\
3\cdot 6 &\equiv 4 \pmod 7.
\end{aligned}$$

これから，

$$\begin{aligned}
(3\cdot 1)(3\cdot 2)(3\cdot 3)(3\cdot 4)(3\cdot 5)(3\cdot 6) &\equiv 3\cdot 6\cdot 2\cdot 5\cdot 1\cdot 4 \pmod 7,\\
3^6 6! &\equiv 6! \pmod 7,\\
6!(3^6-1) &\equiv 0 \pmod 7.
\end{aligned}$$

$6!$ は素数 7 で割り切れないから，3^6-1 は 7 で割り切れる．実際，$3^6-1=728=7\times 104$.

例 3.4. $p=7$ のとき，$2^6-1=63=7\times 9$, $5^6-1=15624=7\times 2232$. $2^{10}-1=1023=11\times 93$, $3^{10}-1=59048=11\times 5368$.

練習問題 2. 2^{1000} を 7 で割ったときの余りはいくつか.

4 有理数

有理数は有限小数かまたは循環小数として表せる．これは次のようにして，簡単に証明できる．有理数を既約分数として，$\frac{a}{b}$ とかく．もし，これが有限小数にならないとすれば，小数に直す過程において，割り算の余りとして現れるのは 1 以上 $b-1$ 以下の整数であるから，b 回以上割り算をすれば，必ず前にでた余りと同じ余りが現れ，そこから先の割り算は全く同じことの繰り返しになって，循環小数になる．

それでは，p を 2, 5 以外の素数として，有理数 $\frac{a}{p}$, $a=1,\dots,p-1$ を循環小数として表すとき，何か規則性があるだろうか？特に，循環節の長さはどうなっているだろうか？

フェルマーの小定理により，$10^{p-1}\equiv 1 \pmod p$ である．今，s を $10^s\equiv 1 \pmod p$ を満たす最小の自然数とする．そのとき，$p-1$ を s で割ったときの商を q，余りを r とすると，$p-1=sq+r$, $0\le r<s$ であり，

$$1\equiv 10^{p-1}\equiv 10^{sq+r}\equiv (10^s)^q 10^r\equiv 10^r \pmod p.$$

s の最小性から，$r = 0$ でなければならない．したがって，$p - 1 = sq$ である．すなわち，s は $p - 1$ の約数である．

$$10^s - 1 = pb$$

とかける．ここで，b は s 桁以下の自然数である．この両辺に $\frac{a}{p}$ をかければ，

$$\frac{a}{p} \times 10^s - \frac{a}{p} = ab.$$

これは，$\frac{a}{p} \times 10^s$ と $\frac{a}{p}$ の小数部分が等しいことを意味している．したがって，$\frac{a}{p}$ を循環小数で表せば，s 桁ずつ同じ数字が繰り返されている．逆に，$\frac{a}{p}$ が循環節の長さ t の循環小数であるとする．そのとき，

$$\begin{aligned} \frac{a}{p} \times 10^t - \frac{a}{p} &= \frac{c}{10^k}, \quad \text{(有限小数)} \\ 10^k a(10^t - 1) &= pc, \\ 10^t - 1 &\equiv 0 \pmod{p}, \\ 10^t &\equiv 1 \pmod{p}. \end{aligned}$$

$p - 1$ が s の倍数であることと同様にして，t は s の倍数であることがわかる．特に，$t \geq s$ である．以上によって，$\frac{a}{p}$ を循環小数で表したときの循環節の長さは丁度 s であり，それは $p - 1$ の約数である．

例 4.1. $p = 7$ のとき，

$$\begin{aligned} 10 &\equiv 3 \pmod{7}, \\ 10^2 &\equiv 2 \pmod{7}, \\ 10^3 &\equiv 6 \pmod{7}, \\ 10^4 &\equiv 4 \pmod{7}, \\ 10^5 &\equiv 5 \pmod{7}, \\ 10^6 &\equiv 1 \pmod{7}. \end{aligned}$$

であるから，循環節の長さは 6 である．実際，$\frac{1}{7} = 0.\dot{1}42857\dot{}$.

この両辺を 10 倍して，整数部分を引けば，6 個の有理数 $\frac{a}{7}$, $a = 1, 2, 3, 4, 5, 6$ はすべて現れる．

$$\begin{aligned} &\frac{1}{7} = 0.\dot{1}42857\dot{}\,, \quad \frac{3}{7} = 0.\dot{4}28571\dot{}\,, \quad \frac{2}{7} = 0.\dot{2}85714\dot{}\,, \\ &\frac{6}{7} = 0.\dot{8}57142\dot{}\,, \quad \frac{4}{7} = 0.\dot{5}71428\dot{}\,, \quad \frac{5}{7} = 0.\dot{7}14285\dot{}\,. \end{aligned}$$

練習問題 3. $p = 13$ のとき，$10^s \equiv 1 \pmod{13}$ を満たす最小の自然数 s を求めよ．また，そのとき，$10^s - 1$ を 13 で割った商を求めよ．さらに，$\dfrac{a}{13}$, $a = 1, \ldots, 12$ を効率よく循環小数に直せ．

s は 12 の約数であるから，$1, 2, 3, 4, 6, 12$ のいずれかである．

$$\begin{aligned} 10^2 &\equiv (-3)^2 \equiv 9 \pmod{13}, \\ 10^3 &\equiv 90 \equiv 12 \equiv -1 \pmod{13}, \\ 10^4 &\equiv (-4)^2 \equiv 3 \pmod{13}, \\ 10^6 &\equiv (-1)^2 \equiv 1 \pmod{13}. \end{aligned}$$

よって，$s = 6$ である．

$$10^6 - 1 = 13 \times 76923.$$

$\dfrac{1}{13} = 0.\dot{0}76923\dot{}$ であるから，循環節の長さは 6 である．12 個の有理数 $\dfrac{a}{13}$, $a = 1, \ldots, 12$ は 2 つのグループに分かれる．

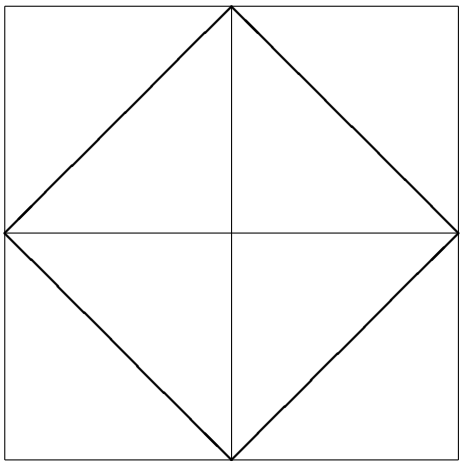
$$\begin{aligned} &\frac{1}{13} = 0.\dot{0}76923\dot{}\,, \quad \frac{10}{13} = 0.\dot{7}69230\dot{}\,, \quad \frac{9}{13} = 0.\dot{6}92307\dot{}\,, \\ &\frac{12}{13} = 0.\dot{9}23076\dot{}\,, \quad \frac{3}{13} = 0.\dot{2}30769\dot{}\,, \quad \frac{4}{13} = 0.\dot{3}07692\dot{}\,, \end{aligned}$$

$$\begin{aligned} &\frac{2}{13} = 0.\dot{1}53846\dot{}\,, \quad \frac{7}{13} = 0.\dot{5}38461\dot{}\,, \quad \frac{5}{13} = 0.\dot{3}84615\dot{}\,, \\ &\frac{11}{13} = 0.\dot{8}46153\dot{}\,, \quad \frac{6}{13} = 0.\dot{4}61538\dot{}\,, \quad \frac{8}{13} = 0.\dot{6}15384\dot{}\,. \end{aligned}$$

2 つ目のグループは，最初のグループの各有理数に，2 をかけたものから整数部分を引くことによって得られる．

5 無理数

一辺の長さが 1 の正方形を対角線によって 2 等分して，面積 1/2 の四つの直角二等辺三角形を組み合わせて正方形を作ると，その面積は 2 である．したがって，その一辺の長さを a とすれば，$a^2 = 2$ である．a を 2 の正の平方根といい，$a = \sqrt{2}$ と表す．



$\sqrt{2}$ は有理数ではないことを示そう．$\sqrt{2}$ が有理数であると仮定して矛盾を導く．$\sqrt{2} = \dfrac{n}{m}$, m, n は互いに素な自然数とかけたとする．$2 = \dfrac{n^2}{m^2}$, $2m^2 = n^2$．左辺は偶数であるから，右辺の n^2 も偶数である．したがって，n は偶数である．$n = 2k$ とかくと，$2m^2 = 4k^2$, $m^2 = 2k^2$ となる．この右辺は偶数であるから，左辺の m^2 も偶数である．したがって，m も偶数である．これは，m, n が互いに素であることに矛盾する．

$\sqrt{2}$ を少数に直せば，有理数でないことから，当然，無限小数になり，さらに，循環小数にもならない．

練習問題 4. 長さが 1 の正方形からなる格子を使って，一辺の長さが $\sqrt{5}$ の正方形を作れ．また，一辺の長さが $\sqrt{13}$ の正方形を作れ．

6 連分数

ユークリッドの互除法を見直してみる．$\gcd(31, 23)$ を求める．

$$\begin{aligned} 31 &= 23 \times 1 + 8, \\ 23 &= 8 \times 2 + 7, \\ 8 &= 7 \times 1 + 1. \end{aligned}$$

これから，$\gcd(31, 23) = 1$ を得る．この計算を書き直して，

$$\begin{aligned} \frac{31}{23} &= 1 + \frac{8}{23}, \\ \frac{23}{8} &= 2 + \frac{7}{8}, \\ \frac{8}{7} &= 1 + \frac{1}{7}. \end{aligned}$$

したがって,

$$\frac{37}{23} = 1 + \frac{8}{23} = 1 + \frac{1}{2 + \dfrac{7}{8}} = 1 + \frac{1}{2 + \dfrac{1}{1 + \dfrac{1}{7}}}.$$

一般に,

$$\begin{aligned}
\frac{a}{b} &= k_0 + \frac{r_1}{b}, \quad 0 \le \frac{r_1}{b} < 1, \\
\frac{b}{r_1} &= k_1 + \frac{r_2}{r_1}, \quad 0 \le \frac{r_2}{r_1} < 1, \\
\frac{r_1}{r_2} &= k_2 + \frac{r_3}{r_2}, \quad 0 \le \frac{r_3}{r_2} < 1, \\
&\cdots\cdots\cdots \\
\frac{r_{n-2}}{r_{n-1}} &= k_{n-1} + \frac{r_n}{r_{n-1}}, \quad 0 \le \frac{r_n}{r_{n-1}} < 1, \\
\frac{r_{n-1}}{r_n} &= k_n.
\end{aligned}$$

これから,

$$\begin{aligned}
\frac{a}{b} &= k_0 + \frac{r_1}{b} = k_0 + \frac{1}{\dfrac{b}{r_1}} = k_0 + \frac{1}{k_1 + \dfrac{r_2}{r_1}} \\
&\cdots\cdots\cdots \\
&= k_0 + \cfrac{1}{k_1 + \cfrac{1}{k_2 + \cfrac{1}{\ddots \cfrac{1}{k_{n-1} + \cfrac{1}{k_n}}}}}
\end{aligned}$$

を得る．このような形の分数を**連分数**という．上の計算において，有理数 $x = \dfrac{a}{b}$ に対して，整数 k_i と有理数 $x_i = \dfrac{r_{i-1}}{r_i}$ は

$$x_0 = x, \quad k_i = [x_i], \quad x_{i+1} = \frac{1}{x_i - k_i} \tag{6.1}$$

によって定まる．したがって，x が無理数のときでも (6.1) によって，整数 k_i と実数 x_i を定めることができる．そのとき，x が無理数であることから，常に $0 < x_i - k_i < 1$ であり，この計算は無限に続く．

$$x_i = k_i + \frac{1}{x_{i+1}}$$

であるから,

$$x = k_0 + \cfrac{1}{k_1 + \cfrac{1}{k_2 + \cfrac{1}{\ddots \cfrac{1}{k_{n-1} + \cfrac{1}{x_n}}}}} \tag{6.2}$$

である．この右辺を記号 $[k_0, k_1, \ldots, k_{n-1}, x_n]$ で表す.

$$x_i = k_i + \frac{1}{x_{i+1}}$$

より,

$$\begin{aligned} x &= x_0 = k_0 + \frac{1}{x_1} = \frac{k_0 x_1 + 1}{x_1} \\ &= \frac{k_0\left(k_1 + \dfrac{1}{x_2}\right) + 1}{k_1 + \dfrac{1}{x_2}} = \frac{(k_0 k_1 + 1)x_2 + k_0}{k_1 x_2 + 1}. \end{aligned}$$

一般に,

$$x = \frac{p_n x_n + p_{n-1}}{q_n x_n + q_{n-1}} \tag{6.3}$$

の形にかけると予想される．(6.3) の右辺に，$x_n = k_n + \dfrac{1}{x_{n+1}}$ を代入すれば,

$$x = \frac{p_n\left(k_n + \dfrac{1}{x_{n+1}}\right) + p_{n-1}}{q_n\left(k_n + \dfrac{1}{x_{n+1}}\right) + q_{n-1}} = \frac{(k_n p_n + p_{n-1})x_{n+1} + p_n}{(k_n q_n + q_{n-1})x_{n+1} + q_n}.$$

したがって，数学的帰納法によって (6.3) は正しいことが証明された．さらに,

$$\begin{cases} p_{n+1} = k_n p_n + p_{n-1}, & p_1 = k_0,\ p_2 = k_0 k_1 + 1, \\ q_{n+1} = k_n q_n + q_{n-1}, & q_1 = 1,\ q_2 = k_1 \end{cases} \tag{6.4}$$

が成り立つことがわかった．等式 (6.4) より,

$$p_n q_{n-1} - p_{n-1} q_n = (-1)(p_{n-1} q_{n-2} - p_{n-2} q_{n-1})$$

がわかる．これを繰り返して用いれば,

$$p_n q_{n-1} - p_{n-1} q_n = (-1)^{n-2}(p_2 q_1 - p_1 q_2) = (-1)^n \tag{6.5}$$

を得る．さらに，(6.4), (6.5) から

$$p_nq_{n-2} - p_{n-2}q_n = k_{n-1}(p_{n-1}q_{n-2} - p_{n-2}q_{n-1}) = (-1)^{n-1}k_{n-1} \tag{6.6}$$

を得る．(6.2), (6.3) から，

$$\frac{p_nx_n + p_{n-1}}{q_nx_n + q_{n-1}} = k_0 + \cfrac{1}{k_1 + \cfrac{1}{k_2 + \cfrac{1}{\ddots \cfrac{1}{k_{n-1} + \cfrac{1}{x_n}}}}}.$$

これは，変数 x_n についての恒等式であるから，$x_n \longrightarrow \infty$ として，

$$\frac{p_n}{q_n} = k_0 + \cfrac{1}{k_1 + \cfrac{1}{k_2 + \cfrac{1}{\ddots \cfrac{1}{k_{n-2} + \cfrac{1}{k_{n-1}}}}}}$$

を得る．$\dfrac{p_n}{q_n} = [k_0, k_1, \ldots, k_{n-1}]$ と表す．(6.5) から，$\dfrac{p_n}{q_n}$ は既約分数であることがわかる．さらに，

$$\lim_{n\longrightarrow\infty} \frac{p_n}{q_n} = x \tag{6.7}$$

であることが示される．これを x の**連分数展開**といい，

$$x = [k_0, k_1, k_2, \ldots]$$

とかく．(6.7) を証明しよう．$y_n = [k_0, k_1, \ldots, k_{n-1}] = \dfrac{p_n}{q_n}$ とおく．$n \geq 1$ について，k_n は自然数であるから，(6.4) から，$\{q_n\}$ は自然数からなる数列であり，

$$1 = q_1 < q_2 \cdots < q_{n-1} < q_n < \cdots$$

を満たすことがわかる．(6.6) より，

$$y_n - y_{n-2} = (-1)^{n-1}\frac{k_{n-1}}{q_nq_{n-2}}.$$

したがって，$y_{2n} - y_{2n-2} < 0$, $y_{2n+1} - y_{2n-1} > 0$ である．また，(6.5) より，

$$y_n - y_{n-1} = \frac{(-1)^n}{q_nq_{n-1}}.$$

したがって，$y_{2n} > y_{2n-1}$ である．以上によって，

$$y_1 < y_3 < \cdots < y_{2n-3} < y_{2n-1} < y_{2n} < y_{2n-2} < \cdots < y_4 < y_2,$$

$$\lim_{n\to\infty} |y_{2n} - y_{2n-1}| = 0$$

であることが示された (これから，$\lim_{n\to\infty} y_n$ が存在することもわかる)．最後に，$\lim_{n\to\infty} y_n = x$ であることを示そう．

$$x_n \geq [x_n] = k_n, \quad q_n x_n + q_{n-1} \geq k_n q_n + q_{n-1} = q_{n+1}$$

に注意すれば，

$$\begin{aligned} |y_n - x| &= \left| \frac{p_n}{q_n} - \frac{p_n x_n + p_{n-1}}{q_n x_n + q_{n-1}} \right| = \left| \frac{(-1)^n}{q_n(q_n x_n + q_{n-1})} \right| \\ &\leq \frac{1}{q_n q_{n+1}} < \frac{1}{q_n^2} \end{aligned} \tag{6.8}$$

であるから，$y_{2n} < x < y_{2n+1}$ であり，$\lim_{n\to\infty} y_n = x$ であることが示された． □

例 6.1. $x = \sqrt{2}$ とすれば，

$$\begin{aligned} x_0 &= \sqrt{2}, \quad k_0 = [\sqrt{2}] = 1, \\ x_1 &= \frac{1}{\sqrt{2}-1} = \sqrt{2}+1, \quad k_1 = [\sqrt{2}+1] = 2, \\ x_2 &= \frac{1}{\sqrt{2}+1-2} = \sqrt{2}+1, \quad k_2 = [\sqrt{2}+1] = 2, \\ \cdots &\quad \cdots \\ x_n &= \sqrt{2}+1, \quad k_n = 2. \end{aligned}$$

したがって，$\sqrt{2}$ は循環する連分数

$$\sqrt{2} = [1, 2, 2, \ldots] = [1, \dot{2}]$$

として表せる．有理数を連分数展開すれば，ユークリッドの互除法によって，有限連分数になる．$\sqrt{2}$ は循環する無限連分数に展開されたから，$\sqrt{2}$ は有理数ではなく，無理数である．(6.4) より，

$$\begin{aligned} p_{n+1} &= 2p_n + p_{n-1}, \quad p_2 = 3, p_1 = 1, \\ q_{n+1} &= 2q_n + q_{n-1}, \quad q_2 = 2, q_1 = 1. \end{aligned}$$

$$p_1 = 1,\ p_2 = 3,\ p_3 = 7,\ p_4 = 17,\ p_5 = 41,\ p_6 = 99, \ldots$$

$$q_1 = 1,\ q_2 = 2,\ q_3 = 5,\ q_4 = 12,\ q_5 = 29,\ q_6 = 70, \ldots$$

である．

$$\frac{1}{1} = 1,\ \frac{3}{2} = 1.5,\ \frac{7}{5} = 1.4,\ \frac{17}{12} = 1.416\cdots,\ \frac{41}{29} = 1.413\cdots,\ \frac{99}{70} = 1.4142\cdots\ \ldots$$

である．

練習問題 5. $x = \dfrac{1+\sqrt{5}}{2} = 1.6180\cdots$ の連分数展開を求めよ.

一般に，次の定理が成り立つ.

定理 6.2 (ラグランジュの定理). 2 次無理数は循環連分数で表せる．逆に，循環連分数で表せる実数は 2 次無理数である.

7　代数的数と超越数

定義 7.1. 複素数 α が有理数係数の方程式の解であるとき，**代数的数**であるという．代数的数の全体を $\bar{\mathbb{Q}}$ とかく．代数的数でないような複素数を**超越数**という.

例 7.2. $\sqrt{5}, \sqrt[3]{2}$ は代数的数である．円周率 π, 自然対数の底 e は超越数であることが知られている.

命題 7.3. 代数的数たちから四則演算によって得られる数は代数的数である.

$\alpha \in \bar{\mathbb{Q}}$ を実数の代数的数とする．α が満たす整数係数の方程式で次数が最小のものを

$$f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n, \quad a_i \in \mathbb{Z}, a_0 > 0$$

とする．$\gcd(a_0, \ldots, a_n) = 1$ としてよい．そのとき,

$$H(\alpha) = \max\{|a_0|, |a_1|, \ldots, |a_n|\}$$

とおく．$f(x)$ は α を根に持つ整数係数の多項式で次数が最小であることから，$f(x)$ は有理数係数の多項式として既約である (因数分解できない)．また，$f'(\alpha) \neq 0$ である．ここで，$n \geq 2$ とする．$f(x)$ は既約だから，任意の有理数 $\dfrac{p}{q}, q \geq 1$ に対して,

$$q^n f\left(\frac{p}{q}\right) = a_0p^n + \cdots + a_nq^n \neq 0$$

は 0 でない整数であり，したがって，その絶対値は 1 以上である．$f(\alpha) = 0$ であるから，平均値の定理によって,

$$f\left(\frac{p}{q}\right) = f\left(\frac{p}{q}\right) - f(\alpha) = \left(\frac{p}{q} - \alpha\right) f'(\xi), \quad |\xi - \alpha| < \left|\frac{p}{q} - \alpha\right|$$

を満たす実数 ξ が存在する．$\left|\dfrac{p}{q} - \alpha\right| < 1$ とすると，$|\xi - \alpha| < 1, |\xi| < |\alpha| + 1$ であ

る．したがって，

$$\begin{aligned} 1 &\leq \left|q^n f\left(\frac{p}{q}\right)\right| = q^n \left|\frac{p}{q}-\alpha\right| |f'(\xi)| \\ &\leq q^n \left|\frac{p}{q}-\alpha\right| \sum_{i=0}^{n-1}(n-i)|a_i||\xi|^{n-i-1} \\ &\leq q^n \left|\frac{p}{q}-\alpha\right| \sum_{i=0}^{n-1}(n-i)H(\alpha)(|\alpha|+1)^{n-i-1} \\ &\leq q^n \left|\frac{p}{q}-\alpha\right| \sum_{i=0}^{n-1}(n-i)H(\alpha)(|\alpha|+1)^{n-1} \\ &= q^n \left|\frac{p}{q}-\alpha\right| H(\alpha)(|\alpha|+1)^{n-1}\frac{n(n+1)}{2}. \end{aligned}$$

$M = \dfrac{1}{H(\alpha)(|\alpha|+1)^{n-1}\frac{n(n+1)}{2}}$ とおけば，

$$\left|\frac{p}{q}-\alpha\right| \geq \frac{M}{q^n}.$$

$\left|\dfrac{q}{p}-\alpha\right| \geq 1$ のときは，$M \leq 1$ より，

$$\left|\frac{p}{q}-\alpha\right| \geq 1 \geq \frac{1}{q^n} \geq \frac{M}{q^n}$$

であるから，つねに

$$\left|\frac{p}{q}-\alpha\right| \geq \frac{M}{q^n}.$$

$n = 1$ のときは，$\alpha = \dfrac{a}{b}$, $b > 0$ を既約分数とすると，$f(x) = bx - a$ であるから，$H(\alpha) = \max\{|a|, |b|\}$ である．$\dfrac{p}{q} \neq \alpha$ ならば，

$$\left|\frac{p}{q}-\alpha\right| = \frac{|pb-aq|}{bq} \geq \frac{1}{bq} \geq \frac{1}{H(\alpha)q}.$$

よって，$M = \dfrac{1}{H(\alpha)}$ とおけば，$\dfrac{p}{q} \neq \alpha$ ならば，

$$\left|\frac{p}{q}-\alpha\right| \geq \frac{M}{q}$$

が成り立つ．以上まとめて，

定理 7.4 (リュービルの定理). α を n 次の代数的数とすれば，任意の有理数 $\dfrac{p}{q} \neq \alpha$ に対して，

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{M}{q^n}$$

が成り立つ．ここで，M は α のみによって次のように定まる定数である．

$$M = \frac{1}{H(\alpha)(|\alpha|+1)^{n-1}\frac{n(n+1)}{2}}.$$

定理 7.5. $r \geq 2$ を自然数とし，

$$\alpha = \sum_{k=1}^{\infty} r^{-k!}$$

とおけば，α は超越数である．

[証明]　$S_m = \sum_{k=1}^{m} r^{-k!}$ とおけば，S_m は有理数である．$S_m = \dfrac{p_m}{q_m}$ と既約分数の形にかけば，明らかに，$q_m = r^{m!}$ である．α が代数的数だと仮定する．α の次数を n とする．定理 7.4 より，α のみで定まる定数 $M > 0$ が存在して，任意の有理数 $\dfrac{p}{q} \neq \alpha$ に対して，

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{M}{q^n}$$

が成り立つ．特に，$S_m \neq \alpha$ であるから，すべての $m = 1, 2, \ldots$ に対して，

$$\left|\alpha - \frac{p_m}{q_m}\right| \geq \frac{M}{(q_m)^n} = \frac{M}{r^{m!\,n}}.$$

一方，

$$\begin{aligned} 0 < \alpha - \frac{p_m}{q_m} &= \sum_{k=m+1}^{\infty} r^{-k!} \\ &< \sum_{N=(m+1)!}^{\infty} r^{-N} = r^{-(m+1)!}\sum_{k=0}^{\infty} r^{-k} \\ &= \frac{1}{1-r^{-1}}\frac{1}{r^{(m+1)!}}. \end{aligned}$$

よって，

$$\frac{M}{r^{m!\,n}} < \frac{1}{1-r^{-1}}\frac{1}{r^{(m+1)!}},$$

$$r^{(m+1-n)m!} < \frac{1}{M(1-r^{-1})}$$

がすべての m について成り立つことになる．しかし，この右辺は m によらない定数であり，左辺は，$m > n$ を大きくすればいくらでも大きくなるから矛盾である． □

最後に，α が無理数であるとき，有理数によってどれくらい近似できるかについて考えよう．無理数 α を連分数展開する．

$$\alpha = [k_0, k_1, \ldots].$$

$\dfrac{p_n}{q_n} = [k_0, k_1, \ldots, k_{n-1}]$ とおけば，(6.8) から

$$0 < \left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_n^2}, \quad \lim_{n\to\infty} \frac{p_n}{q_n} = \alpha$$

である．

8 円周率の無理数性

円周率 π が無理数であることを証明しよう．

$$f(x) = \frac{1}{n!}x^n(1-x)^n = \frac{1}{n!}\sum_{k=n}^{2n} c_k x^k$$

とおけば，$c_k \in \mathbb{Z}$ である．$0 < x < 1$ に対して，

$$0 < f(x) < \frac{1}{n!}, \quad f(0) = 0$$

である．$m < n$ または $m > 2n$ ならば，$f^{(m)}(0) = 0$ であり，$n \le m \le 2n$ ならば，

$$f^{(m)}(0) = \frac{m!}{n!}c_m = m(m-1)\cdots(n+1)c_m \in \mathbb{Z}$$

である． したがって，

$$f^{(m)}(0) \in \mathbb{Z} \quad (\forall m \in \mathbb{Z},\ m \ge 0). \tag{8.1}$$

$f(1-x) = f(x)$ であるから，

$$f^{(m)}(1) \in \mathbb{Z} \quad (\forall m \in \mathbb{Z},\ m \ge 0). \tag{8.2}$$

ここで，π^2 が有理数であると仮定する．$\pi^2 = \dfrac{a}{b}$, a, b は互いに素な自然数とかく．

$$G(x) = \sum_{m=0}^{n} (-1)^m b^n \pi^{2n-2m} f^{(2m)}(x)$$

とおく．$b^n\pi^{2n-2m} = b^n\left(\dfrac{a}{b}\right)^{n-m} = a^{n-m}b^m \in \mathbb{Z}$ と (8.1), (8.2) から，$G(0) \in \mathbb{Z}$, $G(1) \in \mathbb{Z}$ を得る．さらに，

$$\begin{aligned}
&\frac{d}{dx}\left\{G'(x)\sin\pi x - \pi G(x)\cos\pi x\right\} \\
&= G''(x)\sin\pi x + \pi G'(x)\cos\pi x - \pi G'(x)\cos\pi x + \pi^2 G(x)\sin\pi x \\
&= \left\{G''(x) + \pi^2 G(x)\right\}\sin\pi x.
\end{aligned}$$

ここで，

$$\begin{aligned}
G''(x) + \pi^2 G(x) &= b^n \sum_{m=0}^{n} (-1)^m \pi^{2n-2m} f^{(2m+2)}(x) \\
&\quad + b^n \sum_{m=0}^{n} (-1)^m \pi^{2n-2m+2} f^{(2m)}(x) \\
&= b^n \sum_{m'=1}^{n+1} (-1)^{m'-1} \pi^{2n-2(m'-1)} f^{(2m')}(x) \\
&\quad + b^n \sum_{m=0}^{n} (-1)^m \pi^{2n-2m+2} f^{(2m)}(x) \\
&= b^n \pi^{2n+2} f(x) \\
&= \pi^2 a^n f(x)
\end{aligned}$$

であるから，

$$\frac{d}{dx}\left\{G'(x)\sin\pi x - \pi G(x)\cos\pi x\right\} = \pi^2 a^n f(x)\sin\pi x.$$

したがって，

$$\begin{aligned}
\pi\int_0^1 a^n f(x)\sin\pi x\,dx &= \left[\frac{G'(x)\sin\pi x}{\pi} - G(x)\cos\pi x\right]_0^1 \\
&= G(1) + G(0) \in \mathbb{Z}.
\end{aligned}$$

しかし，

$$0 < \pi\int_0^1 a^n f(x)\sin\pi x\,dx < \pi\int_0^1 \frac{a^n}{n!}\,dx = \frac{\pi a^n}{n!}$$

であり，$\lim_{n\to\infty}\dfrac{\pi a^n}{n!} = 0$ であるから，n を十分大きくとれば，$\dfrac{\pi a^n}{n!} < 1$ にできる．よって，

$$0 < \pi\int_0^1 a^n f(x)\sin\pi x\,dx < 1$$

となるが，この積分の値は整数であったから矛盾である．したがって，π^2 は無理数である．よって，π も無理数である．