高校生のための現代数学講座　　東京大学
「連分数」　　玉原国際セミナーハウス
講義 (4)　斉藤　義久　　2015 年 7 月 25 日

「ユークリッドの互除法と連分数」

- 講義 (4) では，後に続く講義 (5)・(6) のための準備を行います．そのためのキーワードは “行列” と “一次分数変換” です．

1. ユークリッドの互除法

『ユークリッドの互除法』とは，与えられた 2 つの整数に対して，その最大公約数を求める方法（アルゴリズム）です[1]．やり方は至って簡単で，

ある数をある数で割って，商と余りを求める

という操作を，繰り返し行うだけです．以下，例で詳しく見てみましょう．

例 1. $a = 572, b = 231$ として，互除法で最小公倍数を求めてみます．

1 回目の操作：a を b で割る．

$$572 \div 231 = \text{商 } 2 \ldots \text{ 余り } 110$$

2 回目の操作：1 回目の割る数 (= 231) を 1 回目の余り (= 110) で割る．

$$231 \div 110 = \text{商 } 2 \ldots \text{ 余り } 11$$

3 回目の操作：2 回目の割る数 (= 110) を 2 回目の余り (= 11) で割る．

$$110 \div 11 = \text{商 } 10 \ldots \text{ 余り } 0$$

そして，同様の操作を余りが 0 になるまで続けます．今の場合は 3 回目で余りが 0 になったので，これで手続きは終了です．

このとき，最終操作での割る数（今の場合は 11）が，最初に与えた $a = 572$ と $b = 231$ の最大公約数です．実際，

$$572 = 2^2 \times 11 \times 13, \qquad 231 = 3 \times 7 \times 11$$

ですので，確かに 11 は 572 と 231 の最小公倍数になっています．以上のような最大公約数の求め方を**（ユークリッドの）互除法**といいます[2]．

[1] その歴史は古く，紀元前 3 世紀に古代ギリシャの数学者ユークリッド (Euclid) によって編纂された『原論』という本のなかに登場します．人類が考案した最も古いアルゴリズムであると言われています．

[2] 『どうして互除法で最大公約数が求められるのか？』については，何も説明していません．これは高校の『数学 A』で学ぶことになっていますので，まだ習っていない人は後で高校の数学の先生に聞いてみて下さい．もちろん，我々に聞いて下さっても OK です．

演習問題 2. 572 と 221 の最小公倍数を，互除法によって求めよ.

以下，互除法がどんな操作なのか，詳しく分析してみましょう．互除法の操作の過程では，いろいろな数が次々に現れます．話を一般化するためには現れる数を文字で表したいわけですが，このような場合『**どのように文字をおいたら，一番わかり易いか？**』を考えなくてはなりません．実は，この点が非常に大事です.

まず，最初に与える整数 a, b を，

$$a = u_0, \qquad b = u_1$$

と書きます．１回目の操作では，u_0 を u_1 で割って商 c_1 と余り u_2 を計算します.

$$u_0 \div u_1 = c_1 \ldots u_2 \quad \Leftrightarrow \quad u_0 = c_1 u_1 + u_2$$

２回目の操作でも同様のことを繰り返すわけですが，ただし

割られる数を u_0 から u_1 に，割る数を u_1 から u_2 に取り替えて，

操作を行います.

$$u_1 \div u_2 = c_2 \ldots u_3 \quad \Leftrightarrow \quad u_1 = c_2 u_2 + u_3$$

後はこの繰り返しです．k 回目の操作では，既知のデータ u_{k-1}, u_k に対して，

$$u_{k-1} \div u_k = c_k \ldots u_{k+1} \quad \Leftrightarrow \quad u_{k-1} = c_k u_k + u_{u+1} \tag{1.1}$$

によって，c_k と u_{k+1} を順次決めて行くわけです.

$$\cdots \longrightarrow \boxed{\begin{array}{c} c_{k-2} \text{ と } u_{k-1} \\ \text{が決まる} \end{array}} \xrightarrow{k-1 \text{ 回目の操作}} \boxed{\begin{array}{c} c_{k-1} \text{ と } u_k \\ \text{が決まる} \end{array}} \xrightarrow{k \text{ 回目の操作}} \boxed{\begin{array}{c} c_k \text{ と } u_{k+1} \\ \text{が決まる} \end{array}} \longrightarrow \cdots$$

そして，n 回目の操作終了時に $u_{n+1} = 0$ になっていたら，手続きは終了です.

2. 連分数展開と互除法

例 3. 例１と同じように，$a = 572, b = 231$ とします．このとき，

$$\begin{aligned} \frac{572}{231} &= 2 + \frac{110}{231} && (\Leftrightarrow\ 572 \div 231 = 2 \ldots 110) \\ &= 2 + \frac{1}{\frac{231}{110}} = 2 + \frac{1}{2 + \frac{11}{110}} && (\Leftrightarrow\ 231 \div 110 = 2 \ldots 11) \\ &= 2 + \frac{1}{2 + \frac{1}{\frac{110}{11}}} = 2 + \frac{1}{2 + \frac{1}{10}} && (\Leftrightarrow\ 110 \div 11 = 10 \ldots 0) \end{aligned}$$

最後の式を $\dfrac{572}{231}$ の**連分数展開**といい，これを $[2,2,10]$ と表記します．この例からもわかるように，連分数展開と互除法は実質的に同じ計算をしています．

一般に有理数 $\dfrac{a}{b}$ を連分数展開すると，

$$\frac{a}{b} = [c_1, c_2, \cdots, c_n]$$

となります[3]．ここに，$c_1, c_2, \cdots, c_n$ は，k 回目の互除法の操作で得られた商 c_k を，出てくる順番に並べたものです．念のため確認しておきましょう．

$$\frac{a}{b} = \frac{u_0}{u_1} = \frac{c_1u_1 + u_2}{u_1} = c_1 + \frac{u_2}{u_1} \qquad (1\text{回目})$$

$$= c_1 + \frac{1}{\dfrac{u_1}{u_2}} = c_1 + \frac{1}{\dfrac{c_2u_2 + u_3}{u_2}} = c_1 + \frac{1}{c_2 + \dfrac{u_3}{u_2}} \qquad (2\text{回目})$$

$$\vdots$$

$$= c_1 + \cfrac{1}{c_2 + \cfrac{1}{\ddots \quad c_{n-1} + \cfrac{1}{\dfrac{u_{n-1}}{u_n}}}} = c_1 + \cfrac{1}{c_2 + \cfrac{1}{\ddots \quad c_{n-1} + \cfrac{1}{c_n + \dfrac{0}{u_n}}}} \qquad (n\text{回目})$$

$$= c_1 + \cfrac{1}{c_2 + \cfrac{1}{\ddots \quad c_{n-1} + \cfrac{1}{c_n}}} = [c_1, c_2, \cdots, c_n].$$

最後に現れた連分数 $[c_1, c_2, \cdots, c_n]$ を計算すれば，有理数 a/b を $c_1, c_2, \cdots, c_n$ の有理式の形に書くことが出来るはずです．しかし，それは非常に複雑な式になってしまうので，このままでは具体的に書くのは困難です．この講義の目的は，

この計算の仕組み（アルゴリズム）を，系統的に理解して，
a/b を $c_1, c_2, \cdots, c_n$ を使って書く式を具体的に与えよう

というものです．次節では，そのために“**行列**”と“**一次分数変換**”という道具を導入します．その前に，式の具体形がどれぐらい複雑になるか，試してみて下さい．

演習問題 4. 連分数展開が $n = 3$ で終了するとき，a/b を c_1, c_2, c_3 の有理式の形で表せ．

[3]一般の実数 α に対しても，連分数展開を考えることが出来ますが，α が有理数であることと，連分数展開が有限で止まることは同値です．なぜだか分かりますか？

3. 行列と一次分数変換

定義 5. (1) ４つの実数 a,b,c,d を $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ のように並べたものを**行列**という.

(2) ２つの行列 $A=\begin{pmatrix} a & b \\ c & d \end{pmatrix}, B=\begin{pmatrix} p & q \\ r & s \end{pmatrix}$ に対して，新しい行列 AB を

$$AB=\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} p & q \\ r & s \end{pmatrix}=\begin{pmatrix} ap+br & aq+bs \\ cp+dr & cq+ds \end{pmatrix}$$

と定める．AB を**行列 A と行列 B の積**という.

ちょっと複雑な定義ですが[4]，行列の積は以下の著しい性質を持っています.

定理 6. A,B,C を３つの行列とするとき，$(AB)C=A(BC)$ が成り立つ.

この性質を**結合律（結合法則）**といいます．数の掛け算なら当たり前に成り立つ性質ですが，これが『行列同士の積についても成り立つ』というのが，この定理の主張です．証明は難しくないので，興味のある人は自分でやってみて下さい.

注意. (1) 結合律から『括弧はあってもなくても同じ』ですので，外しても構いません．この辺の事情は数の場合と同じなので，理解し易いかと思います.
(2) 他方，行列の積では**交換法則は成り立ちません**，つまり，一般には $AB\neq BA$ です．この点は数の掛け算と違うところなので，注意が必要です.
演習問題 7. $A=\begin{pmatrix} 1 & 3 \\ 2 & 1 \end{pmatrix}, B=\begin{pmatrix} 0 & 3 \\ 2 & 5 \end{pmatrix}$ のとき，$AB\neq BA$ を確かめよ.

定義 8. $A=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ とする．このとき，実数 x に対して，新しい実数 $A\circ x$ を

$$A\circ x=\frac{ax+b}{cx+d}$$

と定める．対応 $x\mapsto A\circ x$ を（行列 A に付随する）**一次分数変換**という[5].

命題 9. A,B を行列，x を実数とするとき，$A\circ(B\circ x)=(AB)\circ x$ が成り立つ.

つまり『一次分数変換についても括弧の位置は気にしなくて良い』というわけです.

[4]『なぜこんな定義をするのか？』については，いまここで説明することは出来ません．大学に入ると１年時に『線型代数』という科目で習うことになるはずです.
[5]記号 $A\circ x$ は，あまり一般的なものではありません．今回だけのものと思って下さい.

4. 連分数展開への応用

連分数展開の k 回目の操作で行っている計算を，変化するところだけ抜き出すと，

$$\frac{u_k}{u_{k-1}} = \frac{1}{\dfrac{u_{k-1}}{u_k}} = \frac{1}{\dfrac{c_k u_k + u_{k+1}}{u_k}} = \frac{1}{c_k + \dfrac{u_{k+1}}{u_k}} \tag{4.1}$$

です．そして，$k+1$ 回目では $\dfrac{u_{k+1}}{u_k}$ の部分に対して同じ操作を繰り返していきます．

この過程で注目すべきことは，

u_k たちは単独で現れるのではなく，常に比 $\dfrac{u_{k+1}}{u_k}$ の形で現れる

ということです．

$$\cdots \longrightarrow \boxed{\begin{array}{c} c_{k-2} \text{ と } \dfrac{u_{k-1}}{u_{k-2}} \\ \text{が決まる} \end{array}} \xrightarrow{k-1 \text{ 回目の操作}} \boxed{\begin{array}{c} c_{k-1} \text{ と } \dfrac{u_k}{u_{k-1}} \\ \text{が決まる} \end{array}} \xrightarrow{k \text{ 回目の操作}} \boxed{\begin{array}{c} c_k \text{ と } \dfrac{u_{k+1}}{u_k} \\ \text{が決まる} \end{array}} \longrightarrow \cdots$$

そこで，$x_k = \dfrac{u_{k+1}}{u_k}$ $(k = 0, 1, 2, \cdots)$ と書くことにしましょう．このとき，(4.1) 式は

$$x_{k-1} = \frac{1}{c_k + x_k} = \frac{0 \cdot x_k + 1}{1 \cdot x_k + c_k}$$

と書けます．したがって，$C_k = \begin{pmatrix} 0 & 1 \\ 1 & c_k \end{pmatrix}$ とおけば一次分数変換を用いて

$$x_{k-1} = C_k \circ x_k \tag{4.2}$$

と書くことが出来ます．さらに (4.2) を繰り返し用いれば，

$$x_0 = C_1 \circ x_1 = C_1 C_2 \circ x_2 = \cdots = C_1 C_2 \cdots C_k \circ x_k$$

が得られます．k を大きくしていけば，その分連分数展開が進んで行くことになるわけですが，$k = n$ のときには $u_{n+1} = 0$ なので，$x_n = \dfrac{u_{n+1}}{u_n} = 0$ です．ゆえに，

$$x_0 = C_1 C_2 \cdots C_n \circ 0 = \begin{pmatrix} 0 & 1 \\ 1 & c_1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & c_2 \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & c_n \end{pmatrix} \circ 0 \tag{4.3}$$

が成り立ちます．ここで，もう一つ注意が必要です．我々が知りたいのは $\dfrac{a}{b}$ だったわけですが，$x_0 = \dfrac{u_1}{u_0} = \dfrac{b}{a}$ なので，(4.3) 式は我々が知りたいものの逆数を求めてしまっています．ところが，この点も一次分数変換を用いて解消することが出来ます．

実際，勝手な実数 x に対して，

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \circ x = \frac{0 \cdot x + 1}{1 \cdot x + 0} = \frac{1}{x}$$

です．したがって (4.3) の両辺に左から $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ を施せば，

$$\text{左辺} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \circ x_0 = \frac{1}{x_0} = \frac{a}{b}$$

となります．他方，右辺の方は結合律を用いることで

$$\text{右辺} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \left(\begin{pmatrix} 0 & 1 \\ 1 & c_1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & c_2 \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & c_n \end{pmatrix} \circ 0 \right) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & c_1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & c_2 \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & c_n \end{pmatrix} \circ 0$$

となります．以上，分かったことを定理の形でまとめておきましょう．

定理 10. 有理数 $\frac{a}{b}$ の連分数展開 $[c_1, c_2, \cdots, c_n]$ は，行列の積と一次分数変換を用いて

$$[c_1, c_2, \cdots, c_n] = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & c_1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & c_2 \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & c_n \end{pmatrix} \circ 0$$

と書ける．

定理 10 の意味について.

(1) 結合律から，最初の 2 つの行列の積 $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & c_1 \end{pmatrix} = \begin{pmatrix} 1 & c_1 \\ 0 & 1 \end{pmatrix}$ を先に計算して，

$$[c_1, c_2, \cdots, c_n] = \begin{pmatrix} 1 & c_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & c_2 \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & c_n \end{pmatrix} \circ 0$$

としても構いません．最初の行列 $\begin{pmatrix} 1 & c_1 \\ 0 & 1 \end{pmatrix}$ に付随する一分数変換は

$$x \mapsto \begin{pmatrix} 1 & c_1 \\ 0 & 1 \end{pmatrix} \circ x = \frac{1 \cdot x + c_1}{0 \cdot 1 + 1} = x + c_1$$

という操作，すなわち『x に c_1 を足す』という操作です．

(2) 後に続く $C_k = \begin{pmatrix} 0 & 1 \\ 1 & c_k \end{pmatrix}$ $(2 \leq k \leq n)$ については，わざと

$$\begin{pmatrix} 0 & 1 \\ 1 & c_k \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & c_k \\ 0 & 1 \end{pmatrix}$$

と積の形に書いた方が，意味がはっきりします．実際，一次分数変換としては，

$$\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\circ x = \frac{1}{x}\ \text{（}x\text{ の逆数を取る）}\qquad \begin{pmatrix}1 & c_k\\ 0 & 1\end{pmatrix}\circ x = x + c_k\ \text{（}x\text{ に }c_k\text{ を足す）}$$

ということでしたので,

$$\begin{pmatrix}0 & 1\\ 1 & c_k\end{pmatrix}\circ x = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\left(\begin{pmatrix}1 & c_k\\ 0 & 1\end{pmatrix}\circ x\right) = \frac{1}{x+c_k}\quad \left(\begin{array}{c} x\text{ に }c_k\text{ を足してから}\\ \text{全体の逆数を取る}\end{array}\right)$$

ということになります．これは (4.1) で書いた連分数展開の k 回目の操作

$$x_{k-1} = \frac{1}{c_k + x_k} \quad \Leftrightarrow \quad \left(x_k \mapsto c_k + x_k \mapsto \frac{1}{c_k + x_k}\right)$$

に他なりません．したがって，定理 10 の右辺は,

$$0 \xrightarrow{c_n\text{を足す}} c_n(+0) \xrightarrow{\text{逆数を取る}} \frac{1}{c_n}$$

$$\xrightarrow{c_{n-1}\text{を足す}} c_{n-1} + \frac{1}{c_n} \xrightarrow{\text{逆数を取る}} \frac{1}{c_{n-1} + \dfrac{1}{c_n}}$$

$$\vdots$$

$$\xrightarrow{c_2\text{を足す}} c_2 + \cfrac{1}{\ddots\ c_{n-1} + \dfrac{1}{c_n}} \xrightarrow{\text{逆数を取る}} \cfrac{1}{c_2 + \cfrac{1}{\ddots\ c_{n-1} + \dfrac{1}{c_n}}}$$

$$\xrightarrow{c_1\text{を足す}} c_1 + \cfrac{1}{c_2 + \cfrac{1}{\ddots\ c_{n-1} + \dfrac{1}{c_n}}}$$

という計算をしていることになるわけです．最終形が連分数展開そのものであることは，言うまでもないでしょう．つまり,

右辺の意味さえ分かってしまえば，定理 10 なんて当たり前！

ということになるのです.

このような考え方（一次分数変換の解釈）は，この後の講義でも用いられますので，覚えておいて下さい.

例 11. $n = 3$ の場合に定理 10 を別の方法で検証してみましょう．まず，

$$\begin{aligned}\text{定理の右辺} &= \begin{pmatrix}0&1\\1&0\end{pmatrix}\begin{pmatrix}0&1\\1&c_1\end{pmatrix}\begin{pmatrix}0&1\\1&c_2\end{pmatrix}\begin{pmatrix}0&1\\1&c_3\end{pmatrix}\circ 0 = \begin{pmatrix}0&1\\1&0\end{pmatrix}\begin{pmatrix}1&c_2\\c_1&c_1c_2+1\end{pmatrix}\begin{pmatrix}0&1\\1&c_3\end{pmatrix}\circ 0\\ &= \begin{pmatrix}0&1\\1&0\end{pmatrix}\begin{pmatrix}c_2&c_2c_3+1\\c_1c_2+1&c_1+(c_1c_2+1)c_3\end{pmatrix}\circ 0 = \begin{pmatrix}0&1\\1&0\end{pmatrix}\circ\frac{c_2c_3+1}{c_1+(c_1c_2+1)c_3}\\ &= \frac{c_1+(c_1c_2+1)c_3}{c_2c_3+1}\end{aligned}$$

です．この式の右辺をさらに計算すると

$$\begin{aligned}\frac{c_1+(c_1c_2+1)c_3}{c_2c_3+1} &= \frac{c_1(c_2c_3+1)+c_3}{c_2c_3+1} = c_1+\frac{c_3}{c_2c_3+1}\\ &= c_1+\frac{1}{\frac{c_2c_3+1}{c_3}} = c_1+\frac{1}{c_2+\frac{1}{c_3}}\end{aligned}$$

となり，確かに $[c_1, c_2, c_3]$ になっています．同時に，この計算は演習問題 4 の解答も与えています．

これを使って，例 3 の計算が復元できることも見ておきましょう．

$$\frac{a}{b} = \frac{572}{231} = [2, 2, 10]$$

なのでした．$c_1 = 2, c_2 = 2, c_3 = 10$ とすれば，

$$\begin{pmatrix}0&1\\1&0\end{pmatrix}\begin{pmatrix}0&1\\1&2\end{pmatrix}\begin{pmatrix}0&1\\1&2\end{pmatrix}\begin{pmatrix}0&1\\1&10\end{pmatrix}\circ 0 = \frac{2+(2\cdot 2+1)10}{2\cdot 10+1} = \frac{52}{21}$$

です．ここで，

$$572 = 2^2\cdot 11\cdot 13, \qquad 231 = 3\cdot 7\cdot 11$$

だったので，

$$\frac{572}{231} = \frac{2^2\cdot 11\cdot 13}{3\cdot 7\cdot 11} = \frac{2^2\cdot 13}{3\cdot 7} = \frac{52}{21} \quad \text{（最小公倍数は 11）}$$

です．今回紹介した『連分数展開 = 行列の積と一次分数変換の計算』は，この既約分数 $\frac{52}{21}$ を計算していることになる，というわけです．