連分数と二次体の整数論

寺杣　友秀

1. 初めに

高校の数学から行列の計算が消え去り、複素数が復活して、ユークリッドの互除法が新しい範囲としてはいりました。数学は少しづつでもいろいろなことを知っていると、その応用範囲がぐっと広まり、それらをうまく組み合わせることにより、解ける問題のバリエーションも豊かなものとなります。いろいろな分野が高校から切り離される理由として、多くのことをやると未消化になってしまう、というのが切り離す方の言い分ですが、たくさんある分野の一部を切り捨ててしまうことにより、いろんな視点から問題を考えることがしにくくなり、立体的に数学を考える事がしにくくなるのではないでしょうか？今日は行列とユークリッドの互除法の両方を用いて論じることのできる、美しい２次体の理論について話をしましょう。

2. ユークリッドの互除法と連分数展開

ユークリッドの互除法は二つの自然数 A, B の最大公約数を求めるアルゴリズムです。A, B の最大公約数を GCD(greatest common divisor) を $GCD(A, B)$ あるいは単に (A, B) と書きます。また二つの自然数 A, B に対して A が B で割れるときに $B \mid A$ と書きます。

定理 2.1. A, B, m を自然数とすると、$GCD(A, B) = GCD(A, mA + B)$ となる。

証明. $d = GCD(A, B)$ とすると $A = da, B = db$ となる自然数 a, b がある。従って $A = da$, $mA + B = mda + db = d(ma + b)$ なので、$A, mA + B$ の両方を d は割ることになり、$d \mid GCD(A, mA + B)$ となる。従って $GCD(A, B) \mid GCD(A, mA + B)$ である。また、$d' = GCD(A, mA + B)$ とおくと、$A = d'a', mA + B = d'b'$ なる a', b' があるので、$B = d'b' - md'a' = d'(b' - ma')$ となり、d' は A, B の双方をわるので $GCD(A, mA + B) \mid GCD(A, B)$ となる。したがって $GCD(A, B) = GCD(A, mA + B)$ がいえる。 □

これを用いると、次の系が得られます。

系 2.2. $A > B$ を自然数として、A を B で割った余りを C とすると、

$$GCD(A, B) = GCD(B, C)$$

が成りたつ。

Date: 11 月 16 日.

この定理を用いれば二つの自然数の最大公約数を求めるユークリッドのアルゴリズムが得られます。

例 2.3. 105 と 28 の最大公約数を求めてみましょう。

$$105 \div 28 = 3 \cdots 21$$
$$28 \div 21 = 1 \cdots 7$$
$$21 \div 7 = 3 \cdots 0$$

なので

$$GCD(105, 28) = GCD(28, 21) = GCD(21, 7) = 7$$

となります。最後は割りきれたところで終わりになります。

ところで、105 と 28 の最大公約数の 7 求めることができれば、分数 $\frac{105}{28}$ の分母分子を 7 で割って、最初の分数を既約分数 $\frac{15}{4}$ にすることができます。逆に既約分数したもの $\frac{15}{4}$ がわかれば、最大公約数 7 も簡単にわかるので、最大公約数を求める問題は分数を既約分数にする問題であるとも言い換えるられます。ユークリッドの互除法は分数の形でいえば、次のような一連の計算でも表せます。

$$\frac{105}{28} = 3\frac{21}{28}$$
$$\frac{28}{21} = 1\frac{7}{21}$$
$$\frac{21}{7} = 3$$

ここで 1 行目から 2 行目への移行は分数部分の逆数をとる操作です。これを分数の中に分数がはいっている、連分数の形で書くと、

$$\frac{105}{28} = 3 + \frac{21}{28} = 3 + \frac{1}{\frac{28}{21}} = 3 + \frac{1}{1 + \frac{7}{21}} = 3 + \frac{1}{1 + \frac{1}{\frac{21}{7}}}$$
$$= 3 + \frac{1}{1 + \frac{1}{3}}$$

となります。つまり、(1) 整数部分と小数部分に分ける。(2) 小数部分の逆数をとる。(3) (1) の操作に戻る。という操作繰り返しています。最後の式はより経済的に

$$3 + \frac{1}{1 + \frac{1}{3}}$$

と書きます。

3. 無理数の連分数

上にあげた連分数のアルゴリズムは実数を有理数で近似する方法にも用いられます。有理数の場合は上のアルゴリズムを有限回繰り返すことにより終わるのですが、無理数の場合は小数部分もその逆数も無理数なので有限回では終わりません。たとえば、よく知っている無理数 $\sqrt{7}$ についてこの操作を繰り返すと、どんなことが起こるでしょうか？以下の計算の最右辺の和は整数部分と小数部分に分けたものです。

$$\begin{aligned}\sqrt{7} =& 2+(\sqrt{7}-2)\\ \frac{1}{\sqrt{7}-2} =& \frac{\sqrt{7}+2}{3} = 1+(\frac{\sqrt{7}-1}{3})\\ \frac{3}{\sqrt{7}-1} =& \frac{\sqrt{7}+1}{2} = 1+(\frac{\sqrt{7}-1}{2})\\ \frac{2}{\sqrt{7}-1} =& \frac{\sqrt{7}+1}{3} = 1+(\frac{\sqrt{7}-2}{3})\\ \frac{3}{\sqrt{7}-2} =& \frac{\sqrt{7}+2}{1} = 4+(\frac{\sqrt{7}-2}{1})\end{aligned}$$

で以降は一行目と同じになり繰り返しとなります。したがって連分数表示すると、

$$\sqrt{7} = 2+\underbrace{\frac{1}{1}+\frac{1}{1}+\frac{1}{1}+\frac{1}{4}}+\underbrace{\frac{1}{1}+\frac{1}{1}+\frac{1}{1}+\frac{1}{4}}+\underbrace{\frac{1}{1}+\frac{1}{1}+\frac{1}{1}+\frac{1}{4}}+\frac{1}{1}+\frac{1}{1}+\cdots$$

というふうになり、循環する形になります。この操作を途中でやめると、たとえば

$$2+\underbrace{\frac{1}{1}+\frac{1}{1}+\frac{1}{1}+\frac{1}{4}}+\frac{1}{1}+\frac{1}{1} = \frac{82}{31}$$

とすると $\sqrt{7}$ の近似がえられます。実際、双方を小数であらわすと、

$$\begin{aligned}\sqrt{7} =& 2.6457513110\cdots\\ \frac{82}{31} =& 2.6451612903\cdots\end{aligned}$$

となります。$\sqrt{7}$ の連分数表示に現れる形の連分数を循環連分数といいます。実は次のことが成り立ちます。

定理 3.1. a, b を有理数、$D > 1$ を 1 より大きい整数の 2 乗で割りきれない自然数（このような自然数を平方因子を含まない自然数という。）とする。$a+b\sqrt{D}$ を連分数表示すると必ずいつかは循環する。

問題 3.2. $\sqrt{3}$ を連分数展開しなさい。

定義 3.3. $a+b\sqrt{D}$ の形の数を *2* 次数という。D を固定して、この形の元全体を 2 次体という。

4. 連分数と行列

この章では行列の計算を使います。行列は掛け算の算法が独特です。まず 1 より大きい有理数でない実数 x_0 から連分数のアルゴリズムを始めるとしましょう。x_0 の整数部分を k_0, 小数部分の逆数を x_1 とします。式で書くと、

$$x_0 = k_0 + \frac{1}{x_1}$$

となります。x_1 についてこの操作を施し、さらに同様に繰り返すので、

$$x_1 = k_1 + \frac{1}{x_2}, x_2 = k_2 + \frac{1}{x_3}, \ldots, x_i = k_i + \frac{1}{x_{i+1}}, \ldots$$

となります。ここで $k_0, k_1, \ldots$ はすべて自然数です。上の関係式を用いれば、x_0 は $k_0, k_1, \ldots, k_{i-1}$ と x_i を用いてあらわすことができます。小数部分 $\frac{1}{x_i}$ は次の段階の小数部分 $\frac{1}{x_{i+1}}$ を用いて

$$\frac{1}{x_i} = \frac{1}{k_i + \frac{1}{x_{i+1}}} = \frac{0 \cdot \frac{1}{x_{i+1}} + 1}{1 \cdot \frac{1}{x_{i+1}} + k_i}$$

と表すことができます。上の式につぎの関係式

$$\frac{1}{x_{i+1}} = \frac{0 \cdot \frac{1}{x_{i+2}} + 1}{1 \cdot \frac{1}{x_{i+2}} + k_{i+1}}$$

を代入すると $\frac{1}{x_i}$ は $\frac{1}{x_{i+2}}$ の式で表せることになります。これを繰り返して代入すれば、x_0 を x_i で表すことができるのですが、この計算は行列を用いると見やすくなります。もう少し一般的に

$$x = \frac{ay + b}{cy + d}, \quad y = \frac{pz + q}{rz + s}$$

という関係式があったとしましょう。このような関係式で結ばれているとき、x は y の一次分数関数であるといわれます。これから x を z で表すと、

$$x = \frac{a\frac{pz+q}{rz+s} + b}{c\frac{pz+q}{rz+s} + d} = \frac{a(pz+q) + b(rz+s)}{c(pz+q) + d(rz+s)} = \frac{(ap+br)z + (aq+bs)}{(cp+dr)z + (aq+ds)}$$

となり x は z の一次分数関数であることがわかります。他方

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

となるので、一次分数関数に一次分数関数を代入すると、また一次分数関数となるのですが、そこの係数は行列の積で計算できることになります。従って、$\frac{1}{x_0}$ を $\frac{1}{x_3}$ で表したかったら、

$$\begin{pmatrix} 0 & 1 \\ 1 & k_0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & k_1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & k_2 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

と計算しておけば、

$$\frac{1}{x_0} = \frac{a\frac{1}{x_3} + b}{c\frac{1}{x_3} + d},$$

となることがわかります。

例 4.1.

$$\begin{pmatrix}0 & 1\\ 1 & 1\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 1\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 1\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 4\end{pmatrix}=\begin{pmatrix}2 & 9\\ 3 & 14\end{pmatrix}$$

なので

$$\sqrt{7}-2=\frac{2(\sqrt{7}-2)+9}{3(\sqrt{7}-2)+14}(=\frac{2\sqrt{7}+5}{3\sqrt{7}+8})$$

となる。

5. Pell 方程式

さて、θ が 2 次の数で、初めから循環節が始まっている循環連分数（とくに無理数）になるとしましょう。上の行列の計算を使って、

$$\theta=\frac{a\theta+b}{c\theta+d}$$

なる整数 a,b,c,d が存在することがわかります。以下、D はこれまでの通り、平方因子を含まないとします。

定理 5.1. 上の状況で、$(c\theta+d)^n=s_n+t_n\sqrt{D}$ と書いたとき、$2s_n, 2t_n$ は整数になる。また $s_n^2-Dt_n^2=\pm 1$ となる。また n が偶数であれば、その符号は $+$ となる。

注意 5.2. 大学で数学をやると、行列の固有値というものを勉強します。固有値の言葉を用いれば、$c\theta+d$ は行列 $\begin{pmatrix}a & b\\ c & d\end{pmatrix}$ の固有値になることがわかります。

系 5.3. $S^2-DT^2=4$ を満たす整数解は無限にたくさんある。

例 5.4. 上の例で言えば、$c\theta+d=3(\sqrt{7}-2)+14=8+3\sqrt{7}$ となる。従って、２倍する必要はない。

$$(8+3\sqrt{7})^2=127+48\sqrt{7},\quad (8+3\sqrt{7})^3=2024+765\sqrt{7},$$
$$(8+3\sqrt{7})^3=32257+12192\sqrt{7},$$

なので

$$127^2-7\cdot 48^2=1,\quad 2024^2-7\cdot 765^2=1,\quad 32257^2-7\cdot 12192^2=1$$

となります。

注意 5.5. 高木貞治著「初等整数論講義」には連分数と 2 次体の理論がくわしくのっています。

6. 定理 3.1 の証明

$a+b\sqrt{D}$ の形の連分数展開が必ず循環することを証明しましょう。まず連分数の作り方から、最初の項を $x_0 = a_0 + b_0\sqrt{D}$ とおいて x_i の整数部分を k_i, 小数部分を $\frac{1}{x_{i+1}}$ となるようにして $x_1, x_2, \dots$ を定めました。つまり式で書けば、

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

(ただし k_i は自然数、$0 < \frac{1}{x_{i+1}} < 1$) となるように定めました。この仕方で $x_i = a_i + b_i\sqrt{D}$ から分母の有理化をすることにより、x_{i+1} は $a_{i+1}+b_{i+1}\sqrt{D}$ という形に表されることがわかります。循環することを示すには、ある $n \geq 0, m \geq 1$ が存在して $x_n = x_{n+m}$ となることをいえば十分です。そのために

(1) $a+b\sqrt{D}$ なる元の判別式 Δ を定義し、
(2) $a+b\sqrt{D}$ が簡約的である、ということを定義する、

ことにします。さらに、それらが次の性質をもつ事を示します。

(1) x_i の判別式が Δ であれば、x_{i+1} の判別式も Δ である。
(2) x_i が簡約的であれば、x_{i+1} は簡約的である。
(3) x_i は簡約的となる i が存在する。
(4) 決められた Δ を判別式にもち、簡約的な 2 次数 $a+b\sqrt{D}$ は有限個である。

実際に上の性質が示されれば、ある番号 i_0 以上の i について、すべての x_i は簡約的であり、判別式 Δ はずっと変わらないので、i_0 以上の i については有限の可能性しかありえず、いつかは同じものがあらわれ、循環するという寸法です。

6.1. **判別式の定義.** まず、$a+b\sqrt{D}$ は整数係数 2 次方程式の解になっていることを示しましょう。実際 $x = a+b\sqrt{D}$ より $x-a = b\sqrt{D}, (x-a)^2 = b^2D$ を移項すれば有理数係数の方程式が得られるので、それを適当に整数倍します。さらに、係数の共通因数でわってその方程式は

$$Ax^2 + Bx + C = 0 \tag{6.1}$$

で A, B, C には共通因子はない、という形にできます。これを $a+b\sqrt{D}$ の**正規化された方程式**といいます。$a+b\sqrt{D}$ は有理数ではないので、上の方程式は整数の範囲で因数分解できず、もうひとつの解は $a-b\sqrt{D}$ となります。このとき $\Delta = B^2 - 4AC$ を**判別式**といいます。方程式 (6.1) の係数 (A, B, C) は共通因子がないという仮定のもとで、符号の差をのぞいて一意的に定まるので Δ は一意的に定まることがわかります。次のことから性質の (1) がいえます。

命題 6.1. (1) k を整数とするとき、$x = a+b\sqrt{D}$ の判別式と $x+k$ の判別式は等しい。
(2) $x = a+b\sqrt{D}$ の判別式と $\frac{1}{x}$ の判別式は等しい。

証明. $x' = x+k$ とおくと、x' に関する方程式は

$$A(x'-k)^2 + B(x'-k) + C = A(x')^2 + (-2kA+B)x' + (k^2A - kB + C)$$

となる。ここで (A, B, C) に共通因子がなければ、$(A, -2kA+B, k^2A-kB+C)$ にも共通因子がないことがわかる。したがってこれは x' の正規化された方程式

であることがわかる。この方程式の判別式は

$$(-2kA+B)^2-4A(k^2A-kB+C)=B^2-4AC$$

となり、x' の判別式も Δ と一致する。

(2) 等式 (6.1) を x^2 でわり、

$$A+B\frac{1}{x}+C(\frac{1}{x})^2=0$$

とすれば、これは $\frac{1}{x}$ の正規化された方程式で判別式は B^2-4CA となり判別式は変わらない。 □

6.2. **簡約的の定義と簡約理論.** $a+b\sqrt{D}$ (a,b は有理数) が**簡約的**であるとは

$$a+b\sqrt{D}>1, \tag{6.2}$$

$$-1<a-b\sqrt{D}<0 \tag{6.3}$$

という条件が成り立つこととして定めます。$a-b\sqrt{D}$ を $a+b\sqrt{D}$ の共役数といいます。次の命題は性質 (2) を言い換えたものです。

命題 6.2. $a+b\sqrt{D}$ が簡約的であるとして $k\geq 1$ をその整数部分とする。さらに $\dfrac{1}{a+b\sqrt{D}-k}$ の分母の有理をしたものを $a'+b'\sqrt{D}$ とおくと、これも簡約的である。

証明. 不等式 (6.2) は小数部分ということから明らかである。有理化するとときの操作を考えれば、上の a',b' を用いて、$\dfrac{1}{a-b\sqrt{D}-k}$ の分母の有理をしたものは $a'-b'\sqrt{D}$ となる。$k\geq 1$ であることと $a+b\sqrt{D}$ が簡約的であること考えると、

$$a-b\sqrt{D}-k<-1$$

となり、従って、

$$a'-b'\sqrt{D}=\frac{1}{a-b\sqrt{D}-k}$$

は $(-1,0)$ の元である。従って $a'+b'\sqrt{D}$ は簡約的であることがいえる。 □

6.3. **簡約的な元の個数の有限性.** 次に性質 (4) を見てみましょう。有限性をしめすのに簡約的の条件に出てくる符号が役に立ちます。

命題 6.3. Δ を正の整数としたとき、判別式が Δ となる簡約的な 2 次の数の個数は有限個である。

証明. $a+b\sqrt{D}$ を簡約的な 2 次の数として、その正規化された方程式を $Ax^2+Bx+C=0$ とする。この方程式のもう一つの解は $a-b\sqrt{D}$ なので、簡約的であるということから、二つの解 $a+b\sqrt{D}$ と $a-b\sqrt{D}$ は異符号となるので、解と係数の関係を用いると、$AC<0$ となる。上の方程式の判別式を Δ とすると、

$$\Delta=B^2-4AC>B^2$$

となる。Δ は初めに決まっているので、上の条件を満たす整数 B の可能性は有限通りである。そのそれぞれの B に対して $4AC=B^2-\Delta$ が定まるが、A,C は

整数なので、A, C の可能性は有限個である。従って、正規化された方程式の個数は有限個であり、その解となる簡約的な 2 次の数の個数も有限個である。 □

6.4. **連分数をとる操作でいつかは簡約的な元となること.** ここでは x_m が簡約的な元となる m があることを示しましょう。まず $x_0 = a + b\sqrt{D}$ の連分数展開を有限回で打ち切って、

$$x_0 = k_0 + \frac{1}{k_1} + \frac{1}{k_2} + \cdots + \frac{1}{k_m} + \frac{1}{x_m}$$

という形になったとします。まえにのべたように、右辺は $\frac{1}{x_m}$ の一次分数式で

$$x_0 = \frac{a_m(\frac{1}{x_m}) + b_m}{c_m(\frac{1}{x_m}) + d_m} \tag{6.4}$$

という形になります。またここに現れる a_m, b_m, c_m, d_m は正の整数となることがわかります。ここで $\frac{1}{x_m}$ は m 回近似をしたあとの小数部分だったので、区間 $(0, 1)$ にはいっていることになります。従って、x_{m-1} のところまで連分数展開してから、最後にの小数を切り下げて近似した有理数は式 (6.4) の $\dfrac{1}{x_m}$ に 0 を代入て得られる $\dfrac{b_m}{d_m}$ に等しくなります。従って m をどんどん大きくしていくと、これは x_0 に近づいていきます。（証明は省きます。）極限の記号を使えば、

$$\lim_{m\to\infty} \frac{b_m}{d_m} = x_0 \tag{6.5}$$

となります。またもう一段階連分数展開をして x_0 を $\frac{1}{x_{m+1}}$ の一次分数式であらわすと、その係数は次の行列で計算できます。

$$\begin{pmatrix} a_{m+1} & b_{m+1} \\ c_{m+1} & d_{m+1} \end{pmatrix} = \begin{pmatrix} a_m & b_m \\ c_m & d_m \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & k_m \end{pmatrix} = \begin{pmatrix} b_m & a_m + k_m b_m \\ d_m & c_m + k_m d_m \end{pmatrix}$$

従って、$a_{m+1} = b_m, c_{m+1} = d_m$ となるので、

$$\lim_{m\to\infty} \frac{a_m}{c_m} = x_0 \tag{6.6}$$

なる等式も得られます。

以上の準備のもと、連分数展開の操作で $x_0, x_1, x_2, \ldots$ と続けていくといつかは簡約的になることを証明しましょう。まず、$x_1, x_2, \ldots$ は小数部分の逆数ですから、一つ目の条件である、1 より大きいことは明らかに満たされます。いま $x_i = a_i + b_i\sqrt{D}$ に対して、$a_i - b_i\sqrt{D}$ を $\overline{x_i}$ と書きます。このとき一次分数変換の式の係数 a_m, b_m, c_m, d_m は整数であること、および有理化する手順を考えると、

$$\overline{x_0} = \frac{a_m(\frac{1}{\overline{x_m}}) + b_m}{c_m(\frac{1}{\overline{x_m}}) + d_m} = \frac{a_m + b_m\overline{x_m}}{c_m + d_m\overline{x_m}}$$

となります。この式を $\overline{x_m}$ について解くと、

$$\overline{x_m} = \frac{c_m\overline{x_0} - a_m}{-d_m\overline{x_0} + b_m} = -\frac{c_m}{d_m}\frac{\overline{x_0} - \frac{a_m}{c_m}}{\overline{x_0} - \frac{b_m}{d_m}}$$

となります。極限の式 (6.5), (6.6) から $\dfrac{\overline{x_0}-\frac{a_m}{c_m}}{\overline{x_0}-\frac{b_m}{d_m}}$ は 1 に収束するので、すべての m について、$c_m, d_m > 0$ であることを考えると、十分大きな m について $\overline{x_m} < 0$ となります。したがってこのような m に対して、$k_m \geq 1$ であることを考慮にいれると、

$$\overline{x_{m+1}} = \frac{1}{\overline{x_m} - k_m}$$

が $(-1, 0)$ の範囲にあることがわかります。

7. 循環節と Pell 方程式

前に述べた様に、θ から循環節が始まっているとしましょう。一次分数式の合成と、循環することを使うと、次の関係式がなりたっていることがわかっていました。

$$\theta = \frac{a\theta + b}{c\theta + d} \tag{7.1}$$

ここで a, b, c, d はある整数の列 $k_1, \ldots, k_m$ を用いて、

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & k_1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & k_2 \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & k_m \end{pmatrix}$$

と表せていることもわかっていました。行列の計算については次の命題が成り立ちます。これらは大学の 1,2 年生で習うことです。

命題 7.1. (1) $ad - bc = (-1)^m$. この式の左辺は上の行列の行列式と呼ばれる。

(2) *(ケーリー・ハミルトンの定理)* 一般に行列

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \tag{7.2}$$

に対して

$$M^2 - (a+d)M + (ad - bc)I_2 = O$$

が成り立つ。ただし I_2 は単位行列と呼ばれる、次の行列である。

$$I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

証明. (1) m に関する帰納法で示す。$m = 1$ のときは $ad - bc = 0 \cdot k_1 - 1 \cdot 1 = -1$ となり成立する。$m = p$ のときに成立すると、

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & k_1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & k_2 \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & k_p \end{pmatrix}$$

とおいたとき、$ad - bc = (-1)^p$ となる。さらに

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & k_{p+1} \end{pmatrix} = \begin{pmatrix} b & a + bk_{p+1} \\ d & c + dk_{p+1} \end{pmatrix}$$

の行列式を計算すると、

$$b(c + dk_{p+1}) - (a + bk_{p+1})d = bc - ad = (-1)^{p+1}$$

となり、帰納法により、すべての自然数 p について上の式が成り立つ。

(2) 定義にしたがって計算する。

$$M^2 = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a^2+bc & ab+bd \\ ca+dc & cb+d^2 \end{pmatrix}$$
$$(a+d)M = \begin{pmatrix} (a+d)a & (a+d)b \\ (a+d)c & (a+d)d \end{pmatrix}$$
$$(ad-bc)I_2 = \begin{pmatrix} ad-bc & 0 \\ 0 & ad-bc \end{pmatrix}$$

から命題の式が得られる。 □

それでは定理の証明に移りましょう。関係式 (7.1) をベクトルと行列の掛け算を使って、次の様に書き換えます。

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} \theta \\ 1 \end{pmatrix} = \begin{pmatrix} a\theta+b \\ c\theta+d \end{pmatrix} = (c\theta+d)\begin{pmatrix} \frac{a\theta+b}{c\theta+d} \\ 1 \end{pmatrix} = (c\theta+d)\begin{pmatrix} \theta \\ 1 \end{pmatrix}$$

$\alpha = c\theta+d$ とおき、M を (7.2) のように定めると

$$M\begin{pmatrix} \theta \\ 1 \end{pmatrix} = \alpha\begin{pmatrix} \theta \\ 1 \end{pmatrix}$$

と書けます。

命題 7.2. (1) α は整数係数方程式

$$x^2-(a+d)x+(ad-bc)=0$$

の解になっている。さらに $\alpha = s+t\sqrt{D}$ とかくと、$\beta = s-t\sqrt{D}$ は上の方程式のもう一つの解になっている。とくに $s^2-Dt^2 = (-1)^m$

(2) $2s, 2t$ は整数である。

証明. 行列の結合法則を使って、

$$M^2\begin{pmatrix} \theta \\ 1 \end{pmatrix} = MM\begin{pmatrix} \theta \\ 1 \end{pmatrix} = \alpha M\begin{pmatrix} \theta \\ 1 \end{pmatrix} = \alpha^2\begin{pmatrix} \theta \\ 1 \end{pmatrix}$$
$$-(a+d)M\begin{pmatrix} \theta \\ 1 \end{pmatrix} = -(a+d)\alpha\begin{pmatrix} \theta \\ 1 \end{pmatrix}$$
$$(ad-bc)I_2\begin{pmatrix} \theta \\ 1 \end{pmatrix} = (ad-bc)\begin{pmatrix} \theta \\ 1 \end{pmatrix}$$

となる。ここで左辺同志、右辺同志を加える。左辺を $\begin{pmatrix} \theta \\ 1 \end{pmatrix}$ でくくって、ケーリ・ハミルトンの定理を用いると左辺は 0 ベクトルとなる。右辺は

$$(\alpha^2-(a+d)\alpha+(ad-bc))\begin{pmatrix} \theta \\ 1 \end{pmatrix}$$

となり、これが 0 ベクトルであるということは、α が命題の方程式の解となっていることを意味する。また $\sqrt{D}$ は無理数なので、もう一つの解 β は $s-t\sqrt{D}$ となり、解と係数の関係から $(-1)^m = ad-bc = \alpha\beta = s^2-Dt^2$ となる。

(2) 解と係数の関係から $a+d=\alpha+\beta=2s$ は整数となる。従って (1) で示した式を用いて、$D(2t)^2=4Dt^2=4s^2-4(-1)^m$ も整数になる。D は平方因子を含まない整数なので $2t$ も整数となる。 □