原始 Eisenstein 数をつくる

やまなし　あきと
山梨　諒人

§0. はじめに

きっかけは，数研通信 19 号にて亀井喜久男先生が発表されていた原始 Pythagoras 数 (P.P.T.) をもれなく重複なく生成する初期値と 3 つの行列

$$\begin{pmatrix}3\\4\\5\end{pmatrix} と \begin{pmatrix}-1&2&2\\-2&1&2\\-2&2&3\end{pmatrix},\ \begin{pmatrix}1&2&2\\2&1&2\\2&2&3\end{pmatrix},\ \begin{pmatrix}1&-2&2\\2&-1&2\\2&-2&3\end{pmatrix}$$

の存在を知ったことでした。すべての P.P.T. が 1 と 2 と 3 で結びついていると知ったときの衝撃は今でも忘れられません。

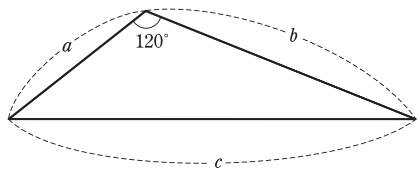
そこで，三平方の定理が余弦定理の特殊な場合であるわけだから，60° や 120° を内角にもつ整数辺三角形の 3 辺の長さの組をもれなく重複なく生成する行列もあるだろうと奮起したわけです。

§1. Eisenstein 数

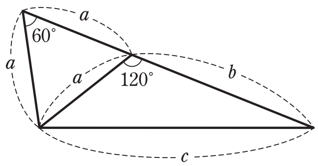
3 つの自然数 a，b，c が，等式

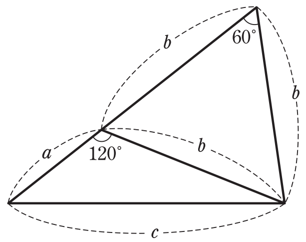
$$a^2+ab+b^2=c^2$$

を満たすとき，自然数の組 $(a,\ b,\ c)$ を Eisenstein 数 (E.T.) と呼びます。特に，a，b，c が互いに素のときは，原始 Eisenstein 数 (P.E.T.) と呼びます。$(a,\ b,\ c)$ が E.T. のとき，これは 120° を内角にもつ整数辺三角形の 3 辺の長さになります。余弦定理から明らかです。



余弦が有理数となる角度は 120° のほかに 60° があります。はじめは何となく鋭角である 60° について考察していたのですが，120° の三角形から容易に 60° の三角形が作られることに気づきました。





図のように，正三角形を 1 つ組み合わせるだけです。行列で表せば

$$\begin{pmatrix}1&0&0\\1&1&0\\0&0&1\end{pmatrix}\begin{pmatrix}a\\b\\c\end{pmatrix}=\begin{pmatrix}a\\a+b\\c\end{pmatrix},\quad \begin{pmatrix}0&1&0\\1&1&0\\0&0&1\end{pmatrix}\begin{pmatrix}a\\b\\c\end{pmatrix}=\begin{pmatrix}b\\a+b\\c\end{pmatrix}$$

といった具合です。逆に，60° を内角にもつ三角形が与えられたときに，どちらの行列から作られたかを判定するのは，2 辺の長さの大小関係によるため面倒です。そこで方針を変え，60° へ一方通行で進むことのできる 120° の整数辺三角形の 3 辺の長さの研究に没頭することにしました。

§2. Eisenstein 数をつくる

Pythagoras 数は，そもそも次の式で無数に生成することができました。

$$\begin{pmatrix}a\\b\\c\end{pmatrix}=\begin{pmatrix}m^2-n^2\\2mn\\m^2+n^2\end{pmatrix}$$

$(m,\ n$ は自然数で，$m>n)$　　……①

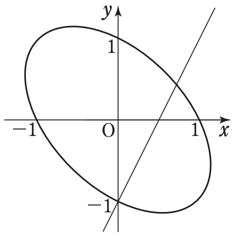
これが P.P.T. になるための必要十分条件は

『m，n が互いに素』かつ『$m\not\equiv n \pmod 2$』

……②

です。E.T. についても無数に生成する式を作りたいと思います。

座標平面上の曲線 $C: x^2+xy+y^2=1$ と，直線 $\ell: y=tx-1$ の交点のうち，$(0,\ -1)$ でない方の座標を求めます。



それほど多くない計算で，その座標は

$$\left(\frac{2t+1}{t^2+t+1},\ \frac{t^2-1}{t^2+t+1}\right)$$

とわかります。すなわち

$$\left(\frac{2t+1}{t^2+t+1}\right)^2+\frac{2t+1}{t^2+t+1}\cdot\frac{t^2-1}{t^2+t+1}+\left(\frac{t^2-1}{t^2+t+1}\right)^2=1$$

ということです。特に t が有理数のときは，$t=\dfrac{m}{n}$ として x 座標，y 座標の分母を払うなどの変形で

$$(2mn+n^2)^2+(2mn+n^2)(m^2-n^2)+(m^2-n^2)^2 =(m^2+mn+n^2)^2$$

となり，E.T. を生成する式として

$$\begin{pmatrix}a\\b\\c\end{pmatrix}=\begin{pmatrix}m^2-n^2\\2mn+n^2\\m^2+mn+n^2\end{pmatrix}$$

があるということがわかります。a，b は P.P.T. との関連を考え逆にとりました。たとえば $m=2$，$n=1$ とすると，$\begin{pmatrix}a\\b\\c\end{pmatrix}=\begin{pmatrix}3\\5\\7\end{pmatrix}$ となりますが，

$$\frac{a^2+b^2-c^2}{2ab}=\frac{3^2+5^2-7^2}{2\cdot3\cdot5}=\frac{-15}{30}=-\frac{1}{2}$$

ですから，確かに 120° を内角にもつ整数辺三角形の 3 辺の長さであることがわかります。

さて，次はこれが P.E.T. となるための m，n の必要十分条件を調べます。いくつか具体例を試していると，$m=3$，$n=1$ のときの $(8,\ 7,\ 13)$ はともかく，$m=4$，$n=1$ で手が止まります。

$$m^2-n^2=15,\ 2mn+n^2=9,\ m^2+mn+n^2=21$$

となり，公約数 3 が出てきてしまいました。検証を続けていくと，ほかにも $(m,\ n)=(7,\ 1)$，$(10,\ 1)$，$(5,\ 2)$，$(8,\ 2)$ などで公約数 3 が出てきました。いずれも $m-n$ が 3 の倍数です。

このことから，P.E.T. が現れるための必要条件として，『m，n が互いに素』であることに加えて

『$m\not\equiv n \pmod 3$』 ……③

が予想されますが，$m-n=3k$，$m-n=3k+1$，$m-n=3k+2$ と場合分けすることによって簡単に証明ができ，これらが必要十分条件となります。P.P.T. と P.E.T. では法が 2 と 3 で変わるのが不思議です。

§3. 2×2 行列で表す

冒頭で紹介した 3 つの 3×3 行列は P.P.T. をもれなく重複なく生成するものですが，これを求めることと②を満たす m，n をもれなく重複なく生成する 2×2 行列を求めることは本質的に同じです。実際それは見つかっていて，次の 3 つです。

$$\begin{pmatrix}1&2\\0&1\end{pmatrix},\ \begin{pmatrix}2&1\\1&0\end{pmatrix},\ \begin{pmatrix}2&-1\\1&0\end{pmatrix}$$

初期値 $\begin{pmatrix}3\\4\\5\end{pmatrix}$ は①で $m=2$，$n=1$ とした場合ですが，この m と n を縦ベクトル $\begin{pmatrix}2\\1\end{pmatrix}$ としてとらえ，上記の 3 つの行列を左から次々にかけることで②の条件を満たす m，n をもれなく重複なく生成することができます(証明は省略します)。$\begin{pmatrix}1&2\\0&1\end{pmatrix}$ を例にすると，

$\begin{pmatrix}1&2\\0&1\end{pmatrix}\begin{pmatrix}m\\n\end{pmatrix}=\begin{pmatrix}m+2n\\n\end{pmatrix}$ であり，これを生成式に代入すると $\begin{pmatrix}a\\b\\c\end{pmatrix}=\begin{pmatrix}m^2+4mn+3n^2\\2mn+4n^2\\m^2+4mn+5n^2\end{pmatrix}$ となります。

そこで，

$$X\begin{pmatrix}m^2-n^2\\2mn+n^2\\m^2+mn+n^2\end{pmatrix}=\begin{pmatrix}m^2+4mn+3n^2\\2mn+4n^2\\m^2+4mn+5n^2\end{pmatrix}$$

が恒等式となるような 3×3 行列 X を求めたものが $\begin{pmatrix}-1&2&2\\-2&1&2\\-2&2&3\end{pmatrix}$ であったわけです。他の 2 つについても同様です。そこで，P.E.T. についてもこの 2×2 行列を求められないかと模索したところ，発見することができましたので，定理として紹介いたします。

以後，文脈に応じて，縦ベクトル $\begin{pmatrix}m\\n\end{pmatrix}$ とその成分を分数 $\dfrac{m}{n}$ の分子，分母とみなして説明することがあります。

定理

互いに素かつ $m \not\equiv n \pmod 3$ であるような任意の2つの自然数 $m>n$ は，$e_1=\begin{pmatrix}2\\1\end{pmatrix}$ または $e_2=\begin{pmatrix}3\\1\end{pmatrix}$ に次の5つの行列を左から次々に掛けたときの2つの成分として得られ，しかもその表し方は一意である。

$$A=\begin{pmatrix}1&3\\0&1\end{pmatrix},\ B=\begin{pmatrix}2&-1\\1&0\end{pmatrix},\ C=\begin{pmatrix}2&3\\1&1\end{pmatrix},$$

$$D=\begin{pmatrix}3&1\\1&0\end{pmatrix},\ E=\begin{pmatrix}3&2\\1&1\end{pmatrix}$$

証明

まずA，B，Cによる変換で，3を法として$m-n$の値が不変であることを示します。

$m-n=3k+\alpha$ として，例えばAで計算すると

$$\begin{pmatrix}1&3\\0&1\end{pmatrix}\begin{pmatrix}m\\n\end{pmatrix}=\begin{pmatrix}1&3\\0&1\end{pmatrix}\begin{pmatrix}n+3k+\alpha\\n\end{pmatrix}=\begin{pmatrix}4n+3k+\alpha\\n\end{pmatrix}$$

となりますが，

$$(4n+3k+\alpha)-n=3(n+k)+\alpha$$

ですから成り立ちます。B，Cについても同様です。D，Eについては，3を法とした$m-n$の値が1と2を巡回します。すると，逆行列はそれぞれ

$$A^{-1}=\begin{pmatrix}1&-3\\0&1\end{pmatrix},\quad B^{-1}=\begin{pmatrix}0&1\\-1&2\end{pmatrix},$$

$$C^{-1}=\begin{pmatrix}-1&3\\1&-2\end{pmatrix},\ D^{-1}=\begin{pmatrix}0&1\\1&-3\end{pmatrix},$$

$$E^{-1}=\begin{pmatrix}1&-2\\-1&3\end{pmatrix}$$

ですが，当然これらもその議論に従います。

さて，一意性を示します。ある2つの自然数 $M>N$ が，互いに素かつ $M\not\equiv N \pmod 3$ であると仮定し，5つの逆行列をそれぞれ掛けると，

$$A^{-1}\begin{pmatrix}M\\N\end{pmatrix}=\begin{pmatrix}M-3N\\N\end{pmatrix}\quad\cdots\cdots④$$

$$B^{-1}\begin{pmatrix}M\\N\end{pmatrix}=\begin{pmatrix}N\\-M+2N\end{pmatrix}\quad\cdots\cdots⑤$$

$$C^{-1}\begin{pmatrix}M\\N\end{pmatrix}=\begin{pmatrix}-M+3N\\M-2N\end{pmatrix}\quad\cdots\cdots⑥$$

$$D^{-1}\begin{pmatrix}M\\N\end{pmatrix}=\begin{pmatrix}N\\M-3N\end{pmatrix}\quad\cdots\cdots⑦$$

$$E^{-1}\begin{pmatrix}M\\N\end{pmatrix}=\begin{pmatrix}M-2N\\-M+3N\end{pmatrix}\quad\cdots\cdots⑧$$

となります。これらについて，

(i) 右辺の2つの成分は5つとも互いに素です。例えば④で$M-3N$とNが互いに素ではないと仮定すると，公約数 $d \geqq 2$ が存在して
$M-3N=pd$，$N=qd$ となりますが，
$M=(p+3q)d$ となるのでM，Nが互いに素であることに矛盾します。他も同様です。

(ii) 右辺について，分子＞分母 かつ 分子＞0 かつ 分母＞0 となるM，Nの値の範囲を求めると，

④は $4<\dfrac{M}{N}$，　⑤は $1<\dfrac{M}{N}<2$，

⑥は $2<\dfrac{M}{N}<\dfrac{5}{2}$，⑦は $3<\dfrac{M}{N}<4$，

⑧は $\dfrac{5}{2}<\dfrac{M}{N}<3$

となります。範囲として覆うことのできていない $\dfrac{M}{N}\leqq 1$ や $\dfrac{M}{N}=\dfrac{5}{2}$，4はそもそも仮定を満たしません。$\dfrac{M}{N}=2$，3は $(M,\ N)=(2,\ 1)$ または $(3,\ 1)$ のときのみ条件を満たしますが，これは初期値として採用するため問題ではありません。つまりこの5つの範囲は $\dfrac{M}{N}$ の存在範囲を重複なく覆っており，これは仮定を満たすM，Nが与えられたときに，掛けることのできる逆行列がただ1つだけ存在することを示しています。

(iii) 5つとも右辺の分子は計算前より小さくなります。④⑤⑦⑧は明らかで，⑥は $2<\dfrac{M}{N}<\dfrac{5}{2}$ のとき十分成り立ちます。

まず(i)(ii)から，M，Nに5つの逆行列を1つずつ次々に掛けることができることがわかります。さらに(iii)から，これを続けていくと 分子＞分母 を満たしながら分子が小さくなっていくわけですので，いつか $\dfrac{2}{1}$ または $\dfrac{3}{1}$ になります。これで一意性が証明されました。(**証明終**)

§4. 3×3 行列を求める

では，A，B，C，D，Eに対応する3×3行列を求めます。5つとも同様の手順で求められますので，Aのみ過程を記そうと思います。

$$\frac{2}{1}\xrightarrow{A}\frac{5}{1}\xrightarrow{A}\frac{8}{1}\xrightarrow{A}\frac{11}{1}$$

という計算で，これらに対応するP.E.T.である

$$\begin{pmatrix}3\\5\\7\end{pmatrix}\to\begin{pmatrix}24\\11\\31\end{pmatrix}\to\begin{pmatrix}63\\17\\73\end{pmatrix}\to\begin{pmatrix}120\\23\\133\end{pmatrix}$$

が得られます。したがって，求める 3×3 行列Xは

$$X\begin{pmatrix}3&24&63\\5&11&17\\7&31&73\end{pmatrix}=\begin{pmatrix}24&63&120\\11&17&23\\31&73&133\end{pmatrix}$$

を満たします。これを求め，その十分性(恒等式になること)を調べました。B，C，D，E も同様に計算し，求めた 3×3 行列を以下にまとめます。

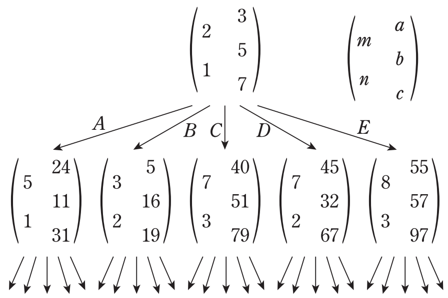
$$A\to\begin{pmatrix}-3&1&4\\-4&-1&4\\-6&0&7\end{pmatrix},\ B\to\begin{pmatrix}-1&-4&4\\1&-3&4\\0&-6&7\end{pmatrix},$$

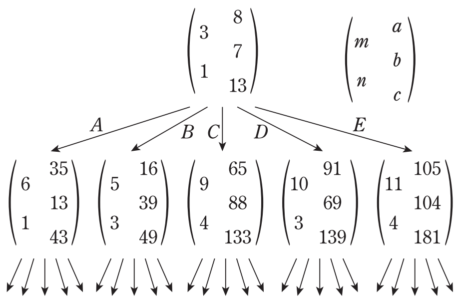
$$C\to\begin{pmatrix}-1&3&4\\1&4&4\\0&6&7\end{pmatrix},\quad D\to\begin{pmatrix}4&1&4\\3&-1&4\\6&0&7\end{pmatrix},$$

$$E\to\begin{pmatrix}4&3&4\\3&4&4\\6&6&7\end{pmatrix}$$

§5. 具体例

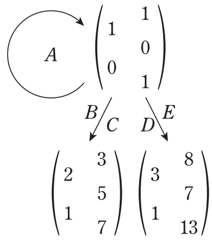
実際に計算した五分木は次のようになります。





いずれも 120° を内角にもつ整数辺三角形の 3 辺の長さになっています。また，§1. で述べたことから，このそれぞれから 60° を内角にもつ整数辺三角形の 3 辺の長さが 2 つずつ出てくると思うと，その広がり方は想像以上に膨大です。

また，2 つの五分木は全く独立というわけではなく，定義外ですが $(m,\ n)=(1,\ 0)$ に 5 つの作用を施すと，重複がありますが $(2,\ 1)$ と $(3,\ 1)$ が出てきます。A については恒等変換となります。



表し方の一意性が失われるため定理には含めませんでしたが，本質的には 2 つの五分木すらもつながっているものと私は捉えています。

少し大きい数値から逆算する例を紹介します。

$(M,\ N)=(528,\ 233)$ とすると，

$$\frac{528}{233}\xrightarrow{C^{-1}}\frac{171}{62}\xrightarrow{E^{-1}}\frac{47}{15}\xrightarrow{D^{-1}}\frac{15}{2}\xrightarrow{A^{-1}}\frac{9}{2}\xrightarrow{A^{-1}}\frac{3}{2}\xrightarrow{B^{-1}}\frac{2}{1}$$

となるので，$\begin{pmatrix}528\\233\end{pmatrix}=CEDAABe_1$ です。三角形の 3 辺の長さに直すと，

$$\begin{pmatrix}a\\b\\c\end{pmatrix}=\begin{pmatrix}528^2-233^2\\2\times528\times233+233^2\\528^2+528\times233+233^2\end{pmatrix}=\begin{pmatrix}224495\\300337\\456097\end{pmatrix}$$

となりますが，当然 $C=120°$ です。また，

$$\begin{pmatrix}a'\\b'\\c'\end{pmatrix}=\begin{pmatrix}1&0&0\\1&1&0\\0&0&1\end{pmatrix}\begin{pmatrix}224495\\300337\\456097\end{pmatrix}=\begin{pmatrix}224495\\524832\\456097\end{pmatrix}$$

$$\begin{pmatrix}a''\\b''\\c''\end{pmatrix}=\begin{pmatrix}0&1&0\\1&1&0\\0&0&1\end{pmatrix}\begin{pmatrix}224495\\300337\\456097\end{pmatrix}=\begin{pmatrix}300337\\524832\\456097\end{pmatrix}$$

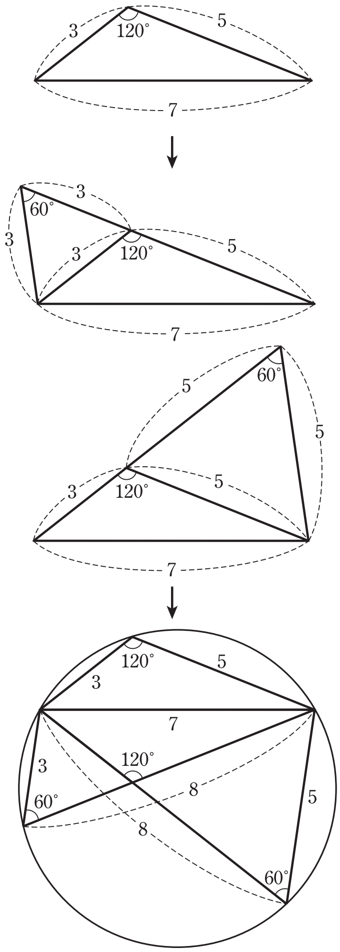
が $C=60°$ の整数辺三角形の 3 辺であることが従います。

§6. 中高数学への活用

Eisenstein 数に関連した入試問題は，2012 年の一橋大学で出題されていますが，図形の性質というよりかは，やはり整数の性質をうまく利用する問題であるように感じます。

また，Eisenstein 数は「友円数」と呼ばれることもあるようです。円に所縁のある三角形の 3 辺の長さの組という意味でしょうか。これに関連すると思いますが，§1. で述べた通り，120° を内角にもつ三角形に対して，1 辺を共有する形で 60° を内角にもつ三角形をつくることができます。これを利用する

と，右に示すように，図形の問題で頻出の，円に内接する整数辺三角形に関連した図を作ることができます。整数辺ばかりですので，中学数学でも十分出題が可能です。



§7. まとめ

個人的には，「原始 Eisenstein 数が」「もれなく」「重複なく」生成できることにこの上ない魅力を感じます。ある程度の行列の知識さえあれば高校生でも十分に理解できる難易度だと思いつつ，その内容の豊かさにただ驚きます。行列の有用性を改めて痛感した次第です。

今回紹介した通り，120° や 60° を内角にもつ整数辺三角形の 3 辺の長さの組は，それこそ無数にあるわけですが，右の図のような例もありますので，数値の小さい代表的なものは覚えておくと役に立つかもしれません。「七五三」「花見」「名古屋」なんて語呂合わせはいかがでしょうか。

《参考文献》

〔1〕 数研通信　数学　No.19　数研出版
〔2〕 数研通信　数学　No.49　数研出版
〔3〕 数研通信　数学　No.84　数研出版

（東京都　獨協中学・高等学校）