多項式環と Diophantus 方程式 I
—$\mathbb{Z}[X]$ 上の Pell 方程式と連分数展開—

Mc-1315 / あおいの
http://mc.yukigaya-8.net/extra/files/mn/pd-1.pdf

2024 年 6 月

はじめに

本稿は，2021 年 3 月・2022 年 3 月に行ったセミナー講演を 1 本の記事の形に再編したものです．15 分 2 コマで実施した内容のほか，予備・補足事項も併せて以下のトピックについて取扱います：

- Diophantus 方程式の定義と例，係数環の $\mathbb{Z}[X]$ への拡張
- $\mathbb{Z}$ または $\mathbb{Z}[X]$ 上の Pell 方程式と連分数展開

本稿は趣味製作物としての形で存在していますが，その根本で支えてくださった方は決して少なくありません．特に筑波大学計算機数学グループ「Team SNAC Tsukuba」の皆様には，講演の機会を設けていただいたのみならず，質問・議論を通じて深い理解に導いていただきました．この場を借りて感謝申上げます．

参考文献

[1] 桂利行（2007）『代数学 II　環上の加群』（大学数学の入門 2）：東京大学出版会．
[2] 雪江明彦（2013）『整数論 1　初等整数論から p 進数へ』：日本評論社．
[3] T. Andreescu，D. Andrica，I. Cucurezeanu（2010）『An Introduction to Diophantine Equations: A Problem-Based Approach』：Springer Science+Business Media．
[4] G. H. Hardy，E. M. Wright〈著〉，示野信一，矢神毅〈訳〉（2022）『数論入門 I【原書 6 版】』（数学クラシックス 8）：丸善出版．
[5] A. M. S. Ramasamy（1994）『Polynomial solutions for the Pell's equation』：Indian Journal of Pure and Applied Mathematics，25(6)，577-581．
[6] 亀井高孝，三上次男，林健太郎，堀米庸三〈編〉（1995）『世界史年表・地図』：吉川弘文館．

1　Diophantus 方程式

Diophantus は 3 世紀の中頃，ローマ帝国時代にあって地中海沿岸のエジプトの都市 Alexandria で活躍した数学者である．Diophantus は方程式の整数解に関する研究をはじめとした功績により「代数学の父」と呼ばれており，とりわけ Pythagoras 数を一般化する次の命題の証明を与えたことでも有名である：

命題 1　$a,b\in\mathbb{Z}$ は互いに素な偶数と奇数の組で，$a>b>0$ であるとする．このとき $x=2ab, y=a^2-b^2, z=a^2+b^2$ とすると，この (x,y,z) は方程式 $x^2+y^2=z^2$ の整数解を網羅する．□

このような背景の下，現代では整数係数不定方程式であり，特に整数解（・有理数解）を求めるものを一般に Diophantus 方程式と呼んでいる．

定義 2　$f(X_1,\ldots,X_n)\in\mathbb{Z}[X_1,\ldots,X_n]$ によって $f(X_1,\ldots,X_n)=0$ の形で表される不定方程式を Diophantus 方程式と呼ぶ．□

簡単な例を紹介する．

例 3　$a,b,c\in\mathbb{Z}$ とし，$d=\gcd(a,b)$ とする．このとき，(x_1,x_2) が $aX_1+bX_2+c=0$ の整数解であれば，$t\in\mathbb{Z}$ により $\left(x_1+\frac{bt}{d}, x_2-\frac{at}{d}\right)$ もその整数解となる．□

この方程式 $aX_1+bX_2+c=0$ が解を持つ条件について少し考えてみる．引続き $d=\gcd(a,b)$ とすれば，$a=a'd, b=b'd$ となるような $a',b'\in\mathbb{Z}$ があり，方程式は $d(a'X_1+b'X_2)+c=0$ と変形できる．この形から明らかな考察を含め，最終的には以下の結論を得る：

命題 4　$a,b,c\in\mathbb{Z}$ とし，$d=\gcd(a,b)$ とすると，以下は同値である：

- $aX_1+bX_2+c=0$ の整数解が存在する．
- c は d の倍数である．□

これは一般化すると単項イデアル整域におけるイデアルの和 $(a)+(b)=(d)$ と本質的に同じ議論をしていることが分かる．一方で，一意分解整域においてはこの議論は成立しない．$\mathbb{Z}[X]$ 上における方程式 $(X+1)f_1(X)+(X-1)f_2(X)=1$ を考えると，$\gcd(X+1,X-1)=1$ であるが，実際にはこれをみたす $f_1(X), f_2(X)$ が存在しない．

多項式係数に拡張した Diophantus 方程式の振舞いを見たが，少し視点を変えて整数係数のままの Diophantus 方程式において多項式解を探す意義を考えてみる．すると，少し考えるだけで以下の事実に到達する：

命題 5　$\mathbb{Z}$ 上に解を持たない Diophantus 方程式は，$\mathbb{Q}[X]$ 上でも解を持たない．□

この証明は至って簡単で，概略としては「仮に多項式解を持てば，その変数部分に適当な数値を代入することで整数解を得てしまい問題設定に反する」といったものである．

したがって，Diophantus 方程式の多項式の範囲への拡張は主に係数に対して行われるべきで，その目標は「自明でない解を持つか」「その解はどのように構成されるか」の 2 点に集約される．

2　Pell 方程式と連分数展開

Pell 方程式は Diophantus 方程式の一種であり，具体的には $d \in \mathbb{Z}_{>0}$ について $X_1^2 - dX_2^2 - 1 = 0$ の形で表される．なお，この形式の方程式について（近代数学史上）最初に取組んだのは Fermat，Brouncker，Wallis らであったが，後年に Euler が Pell による業績と誤認してしまい，以後現在に至るまで Pell 方程式の名で認知されている．もっとも，特殊解を求める営みは古くから行われており，4 世紀のインドでは Baudhayana が $X_1^2 - 2X_2^2 - 1 = 0$ の解として $(577, 408)$ を得ており，これにより $\sqrt{2}$ の近似値として $\frac{577}{408}$ を用いていたことが知られている．

なお，d が平方数である場合，すなわち $d'^2 = d$ となるような $d' \in \mathbb{Z}$ があるとすれば，Pell 方程式は $(X_1 + d'X_2)(X_1 - d'X_2) - 1 = 0$ の形に変形できる．これを満たす解は $(\pm 1, 0)$ しか存在しないため，基本的には d が平方数でないような問題を考察する．このような問題の解を網羅する方法は $\sqrt{d}$ を連分数に展開する過程で得られるが，ここでは天下り式にその手順を紹介する．

定義 6　$\alpha \in \mathbb{R}$ が $a_i \in \mathbb{N}$ により $\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots}}}$ と連分数の形で表されるとき，$\alpha = [a_0; a_1, a_2, a_3, \ldots]$ と書き，$[\alpha] = a_0$ を α の整数部分と呼ぶ．□

平方数でない d について $\sqrt{d}$ を連分数に展開すると，そこに現れる数は一定の周期で循環することが知られている．

定義 7　連分数 $\alpha = [a_0; a_1, a_2, a_3, \ldots]$ において，$n \geq k$ ならば $a_{n+l} = a_n$ となるような k, l が存在するとき，α は循環連分数であると言い，$\alpha = [a_0, a_1, \ldots, a_{k-1}, \dot{a_k}, a_{k+1}, \ldots, \dot{a_{k+l-1}}]$ と表す．□

例 8　$\sqrt{3}$ を連分数に展開すると，

$$\sqrt{3} = 1 + (\sqrt{3} - 1) = 1 + \frac{1}{\frac{\sqrt{3}+1}{2}}$$
$$\frac{\sqrt{3}+1}{2} = 1 + (\frac{\sqrt{3}-1}{2}) = 1 + \frac{1}{\sqrt{3}+1}$$
$$\sqrt{3} + 1 = 2 + (\sqrt{3} - 1) = 2 + \frac{1}{\frac{\sqrt{3}+1}{2}}$$

となって $\frac{\sqrt{3}+1}{2}$ が再度出現し，$\sqrt{3} = [1; \dot{1}, \dot{2}]$ と表される．□

連分数の展開が循環することを利用して，複数回出現する $\sqrt{3}+1$ そのものも展開してみると $\sqrt{3}+1 = 2 + \frac{1}{1+\frac{1}{\sqrt{3}+1}} = \frac{3\sqrt{3}+5}{\sqrt{3}+2}$，整理して $\sqrt{3} = \frac{2\sqrt{3}+3}{\sqrt{3}+2}$ となる．ここで分母に出現する数に着目すると，$2^2 - 3 \cdot 1^2 - 1 = 0$ となり，方程式 $X_1^2 - 3X_2^2 - 1 = 0$ の解 $(2, 1)$ が得られる．

ここで一般の $\sqrt{d} = \frac{p\sqrt{d}+q}{r\sqrt{d}+s}$ に対し，変換 $\pi \colon \mathbb{Z}\left(\sqrt{d}\right) \to \mathrm{M}(2, \mathbb{Z}) \colon \frac{p\sqrt{d}+q}{r\sqrt{d}+s} \mapsto \begin{pmatrix} p & q \\ r & s \end{pmatrix}$ を定めると，$a \in \mathbb{Z}$ として以下が成立する：

- $\pi\left(\sqrt{d}\right) = \pi\left(\frac{\sqrt{d}}{1}\right) = E_2$
- $\pi(a + \theta) = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \pi(\theta)$
- $\pi(a + \frac{1}{\theta}) = \begin{pmatrix} a & 1 \\ 1 & 0 \end{pmatrix} \pi(\theta)$

また，$\det\left(\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}\right) = 1, \det\left(\begin{pmatrix} a & 1 \\ 1 & 0 \end{pmatrix}\right) = -1$ であるから，上記の手法で得られる $\sqrt{d} = \frac{p\sqrt{d}+q}{r\sqrt{d}+s}$ に対して以下が成立する：

- $\pi\left(\frac{p\sqrt{d}+q}{r\sqrt{d}+s}\right)=ps-qr=\pm 1$
- $s\sqrt{d}+dr=p\sqrt{d}+q$

これらを整理することで，以下の結論に到達する：

命題 9　平方数でない $d\in\mathbb{Z}$ に対し，$\sqrt{d}$ を連分数に展開する過程で $\sqrt{d}=\frac{p\sqrt{d}+q}{r\sqrt{d}+s}$ を得ると，(s,r) は方程式 $X_1^2-dX_2^2\pm 1=0$ の解となる．　□

行列式の値から明らかなとおり，正負は連分数を 1 段階ずつ整理するごとに逆転する．したがって，実際には循環する周期が偶数か奇数か，奇数の場合は何段階整理したかで解となる方程式が入替わる．

ここまでの議論を $\mathbb{Z}[X]$ に拡張してみる．

定義 10　$\mathbb{Z}[X]$ に降冪辞書式順序 $\leq$ を導入し，$d(X)\in\mathbb{Z}[X]$ の次数が偶数であるとする．ここで $d'(X)^2\leq d(X)<(d'(X)+1)^2$ となるとき，$[\sqrt{d(X)}]=d'(X)$ とする．　□

このようにして「$\sqrt{d(X)}$ の整数部分」を形式的に定義することで，$\sqrt{d(X)}$ の連分数への展開を考えることができる．また，この連分数を $\mathbb{Z}$ 上での場合と同様に処理することで，方程式 $f_1(X)^2-d(X)f_2(X)^2-1=0$ の解を得られる場合がある．

例 11　$d(X)=X^2+2$ とすると，$X^2<X^2+2<X^2+2X+1=(X+1)^2$ より $[\sqrt{d(X)}]=X$ となって，

$$\sqrt{X^2+2}=X+\frac{1}{\frac{\sqrt{X^2+2}+X}{2}}$$
$$\frac{\sqrt{X^2+2}+X}{2}=X+\frac{1}{\sqrt{X^2+2}+X}$$

と展開できる．これを整理して

$$\sqrt{X^2+2}=X+\frac{1}{X+\frac{1}{\sqrt{X^2+2}+X}}$$
$$=\frac{(X^2+1)\sqrt{X^2+2}+X^3+2X}{X\sqrt{X^2+2}+(X^2+1)}$$

を得ると，実際に分母に出現する $\left(X^2+1,X\right)$ は方程式 $f_1(X)^2-d(X)f_2(X)^2-1=0$ の解となっている．　□

この手法は，仮に係数が $\mathbb{Z}[X]$ の範囲内であっても，その解までもが $\mathbb{Z}[X]$ の中にあることを保証しない．

例 12　$d(X)=X^2+3$ とすると，$X^2<X^2+3<X^2+2X+1=(X+1)^2$ より $[\sqrt{d(X)}]=X$ となって，

$$\sqrt{X^2+3}=X+\frac{1}{\frac{\sqrt{X^2+3}+X}{3}}$$
$$\frac{\sqrt{X^2+2}+X}{3}=\frac{2}{3}X+\frac{1}{\sqrt{X^2+3}+X}$$

と展開できる．これを整理して

$$\sqrt{X^2+3}=X+\frac{1}{\frac{2}{3}X+\frac{1}{\sqrt{X^2+3}+X}}$$
$$=\frac{(\frac{2}{3}X^2+1)\sqrt{X^2+3}+\frac{2}{3}X^3+2X}{\frac{2}{3}X\sqrt{X^2+3}+(\frac{2}{3}X^2+1)}$$

が得られ，実際に $\left(\frac{2}{3}X^2+1,\frac{2}{3}X\right)$ は方程式 $f_1(X)^2-d(X)f_2(X)^2-1=0$ の解となっている．　□