〔論　説〕

連立１次ディオファントス方程式

有　澤　健　治†

Abstract

Another solution to a system of linear Diophantine equations is presented. The idea stands on the work of Gilbert and Pathria eliminating some defects in their solution.

1　はじめに

ディオファントス方程式とは、整数係数の方程式において整数解を求める方程式である。例えば $x^2+y^2=z^2$ を満たす整数 x,y,z を求める問題もディオファントス方程式に含まれる。しかし、ここでは次の連立１次ディオファントス方程式だけを考える:

$$\left.\begin{array}{rcl} a_{1,1}x_1+a_{1,2}x_2+\cdots+a_{1,n}x_n &=& b_1 \\ a_{2,1}x_1+a_{2,2}x_2+\cdots+a_{2,n}x_n &=& b_2 \\ \cdots &=& \cdots \\ a_{m,1}x_1+a_{m,2}x_2+\cdots+a_{m,n}x_n &=& b_m \end{array}\right\} \quad (1)$$

ここに $a_{i,j}$ や b_i たちは全て整数であり、その下で整数解 $x_1,...,x_n$ を求めるのが目標である。不定方程式なので、多くの場合 $m<n$ として問題が与えられているだろう[1]。

連立ではない場合、すなわち $m=1$ の場合には、初等整数論のテキストや、ネット上に多数の解説が見つかる。しかし $m>1$ の場合の解説を見つ

†Kenji Arisawa, Aichi University, Nagoya, Japan, arisawa@aichi-u.ac.jp

[1]似て非なる問題に整数線形計画法がある。それはジャンルの異なる難しい問題である

けるのが難しい[2]。筆者はようやく Gilbert-Pathria による解説を見つけた[7]。彼らの解説を読むと、連立 1 次ディオファントス方程式は易しい問題であることが分かる。計算量も少ない、うまい初等的な解法が紹介されているのである[3]。ここでは彼らのアイデアに沿いながら、彼らのいくつかの欠点については修正を加えて解法を紹介する。修正点については本文の中で説明する。

この記事で使用する記法を簡単にまとめておく:

- $(M)_{i,j}$: 行列 M の i,j 要素
- $\lfloor \alpha \rfloor$: 床関数 (実数 α を超えない最大の整数)
- $a \mid b$: a は b の約数である ($ak = b$ となる整数 k が存在する)
- $a \bmod b$: a を b $(b > 0)$ で割った剰余 ($a = bq + r$ $(0 \leq r < b)$ となる r)

剰余については多少の注釈が必要であろう。標準的な整数論のテキストでは剰余計算を $b > 0$ の場合に限定している[4]。$b < 0$ についても剰余を定義できなくはないが、不必要な複雑さを招くからだと思える。ここでも $b > 0$ の場合にだけ mod を使っている。

2 解法

まずは簡単な問題から始める。

$$\begin{aligned} a_{1,1}x_1 + 0x_2 + 0x_3 + 0x_4 &= b_1 \\ 0x_1 + a_{2,2}x_2 + 0x_3 + 0x_4 &= b_2 \end{aligned} \tag{2}$$

この方程式の解は自明で、解を持つためには $a_{1,1} \mid b_1,\ a_{2,2} \mid b_2$ の条件が必要であり、その下で $x_1 = b_1/a_{1,1},\ x_2 = b_2/a_{2,2}$ で、x_3, x_4 は任意の整数である。

式 (1) で与えられた問題を、簡単な問題、つまり対角行列での問題に変形できれば問題が解けることが分かる。行列 M が対角行列であるとは、$(M)_{i,j} = 0$ $(i \neq j)$ である行列を言う。

問題を一般的に扱うために、最初に整数行列 (整数を要素とする行列) の性質を調べる。整数行列 M に次の変形規則を導入する。

[2] 高木 [2] の補遺に $m = 2$ の解法例が載っているが、素朴である
[3] 学生にも分かる解法であることが強調されている
[4] 例えば文献 [1, 2, 3, 4] など

(a) M の任意の行 i に、i と異なる任意の行の整数倍を加えてもよい。列についても同様である

(b) M の任意の行、あるいは任意の列は符号を反転してもよい

(c) M の任意の 2 つの行、あるいは任意の 2 つの列は、交換可能である

これらの規則は行列式の変形規則でもある。ただし行列式は値を持っており、上記の (b) および (c) では行列式の符号が反転する可能性があるが、ここでは M は値を考えない。

これらの規則は可逆な変形規則である。(b) と (c) が可逆であることは自明である。(a) が可逆であることは次のように分かる: i 行目と j 行目を各々 v_i および v_j とすると、操作 (a) によって j 行目に i 行目の k 倍を加えると j 行目は $v_j + kv_i$ となる。その結果に i 行目の $-k$ 倍を加えると元に戻る。列についても同様である。

(c) は (a) と (b) の組み合わせて実現できることに注意しよう。なぜなら

状態	i 行目	j 行目	説明
S0	v_i	v_j	初期状態
S1	v_i	$v_i + v_j$	状態 S0 の j 行目に i 行目を加える
S2	$-v_j$	$v_i + v_j$	状態 S1 の i 行目から j 行目を引く
S3	$-v_j$	v_i	状態 S2 の j 行目に i 行目を加える
S4	v_j	v_i	状態 S3 の i 行目の符号を反転する

となるからである。列についても同様である。

M がこれらの変形規則によって M' を生成する場合、M は M' に変形可能であると言うこととし、記号的に $M \sim M'$ と書こう。

行列の変形について、よく知られた定理を、次の補題 1 と補題 1 の系として示しておく。

補題 1. 零行列 (全ての要素が 0 の行列) ではない $m \times n$ の整数行列 M は、

$$a'_{1,1} \neq 0, \quad a'_{1,j} = 0 \ (j = 2, ..., n), \quad a'_{i,1} = 0 \ (i = 2, ..., m)$$

となるように変形可能である。ここに $a'_{i,j} = (M')_{i,j}$ である。

証明: 証明に当たって、次の用語と記法を定義しておく:

- 零行 : 全ての要素が 0 の行
- ":=" : 代入

以下では $a_{i,j} = (M)_{i,j}$ とする。M の中の零行ではない要素を一つを選び[5]、先頭行に移動する。行の入れ替えを行えばよい。そして、以下の STEP を繰り返す。

STEP1: $a_{1,k}$ $(k = 1, ..., n)$ の中に負の要素があれば、その列の符号を反転しておく。$a_{1,k}$ $(k = 1, ..., n)$ の中の、0 ではない最小の要素を $a_{1,i}$ とする。列 1 を列 i と入れ替える。その結果 $a_{1,k}$ $(k = 2, ..., n)$ が全て 0 であれば STEP2 へ行く。そうでなければ次の計算をする:

$$n_k := \lfloor a_{1,k}/a_{1,1} \rfloor, \quad a'_{i,k} = a_{i,k} - n_k a_{i,1} \qquad (k = 2, ..., n)$$

ここに a の添字の i は $1, ..., m$ を表す。すると $a'_{1,k} = a_{1,k} \bmod a_{1,1}$ となっている。この操作の結果得られた行列 M' を再び M として、STEP1 へ行く。$a_{1,1}$ の値が減少することに注意。

STEP2: $i = 2, ..., m$ について $a_{i,1} \bmod a_{1,1}$ を調べる。$a_{i,1} \bmod a_{1,1} \neq 0$ となる i を見つけて $a_{i,1} := a_{i,1} \bmod a_{1,1}$ とし、1 行目と i 行目を入れ替えて、STEP1 へ行く。$a_{1,1}$ の値が減少することに注意。$a_{i,1} \bmod a_{1,1} \neq 0$ となる i が存在しなければ STEP3 へ行く。

STEP3: この段階で条件を満たす M' が得られている。 □

補題 1 の系 $m \times n$ の整数行列 M は、対角行列 M' に変形可能である。

証明: 補題 1 によって M は

$$\begin{pmatrix} a'_{1,1} & 0 & 0 & \cdots & 0 \\ 0 & * & * & \cdots & * \\ 0 & * & * & \cdots & * \\ 0 & * & * & \cdots & * \end{pmatrix}$$

の形に変形できる。ここに $*$ は何かの整数である。変形規則を M の (2 行目、2 列目以降の) 小行列に適用すると 2 行目まで対角化できる。そして、3 行目、4 行目へとこのプロセスを繰り返せばよい。 □

[5]一般的に言えば、絶対値が (0 ではない) 最小の要素が収束が速い

補注 1: 我々の目的には対角化されれば十分である。しかし、もっと強い主張が成り立つ。すなわち整数行列の対角化された対角要素を $e_1, e_2, ...$ とすると $e_i | e_{i+1}$ $(i = 1, 2, ...)$ になるように対角化可能である。このことは、補題 1 のアルゴリズムに多少の修正を加えることで証明できる。アーベル群論における対応する定理は、単因子定理と呼ばれる [6]。Kurosh によると、「有限個の生成元を持つアーベル群の全理論が、本質的にはこの定理 (単因子定理) に基づいている [7]」。それほど重要な定理なのである。

補注 2: Gilbert-Pathria は行列の変形目標を三角行列に置いている。そのことが変形後の処理を複雑にし、解の存否の判定にさらに計算を要する原因になっている。

問題 1. 行列 $\begin{pmatrix} 5 & 6 & 8 \\ 6 & -11 & 7 \end{pmatrix}$ を対角化せよ。

答: 行列の変形規則を基に、変形の結果を 1 ステップごとに書いて行くと次のようになる:

$$\begin{pmatrix} 5 & 6 & 8 \\ 6 & -11 & 7 \end{pmatrix} \sim \begin{pmatrix} 5 & 6 & 8 \\ 1 & -17 & -1 \end{pmatrix} \sim \begin{pmatrix} 0 & 91 & 13 \\ 1 & -17 & -1 \end{pmatrix}$$
$$\sim \begin{pmatrix} 0 & 91 & 13 \\ 1 & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} 0 & 0 & 13 \\ 1 & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 13 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 13 & 0 \end{pmatrix}$$

行われた操作は順に、行:(a), 行:(a), 列:(a), 列:(a), 行:(c), 列:(c) である。ここに (例えば)「行:(a)」は、行列の行に変形規則 (a) を適用したという意味である。 □

行列に対する変形操作が正方行列で表現できることを示しておく。E を単位行列、$I_{i,j}$ を行列要素 i, j が 1 で残りの全てが 0 の正方行列とする。すると $I_{i,j}$ は

$$I_{i,i}^2 = I_{i,i}, \quad I_{i,j}^2 = \mathbf{0} \ (i \neq j)$$

を満たす。ここに $\mathbf{0}$ は零行列である。

[6] Waerden [6] p.148
[7] Kurosh [5] p.121

$MI_{i,j}$ は M と同じサイズの行列であり、j 列目を除き全て 0 で、j 列目には M の i 列目が現れる。従って、行列 M の i 列目の k 倍を j 列目に加える操作は $M(E+kI_{i,j})$ で表される。$E+kI_{i,j}$ の逆行列は逆操作でもあり、$E-kI_{i,j}$ である。実際

$$(E+kI_{i,j})(E-kI_{i,j}) = E^2 + kI_{i,j} - kI_{i,j} + k^2 I_{i,j}^2 = E$$

である。

M の i 列目の符号を反転する行列は $E-2I_{i,i}$ である。この逆行列が $E-2I_{i,i}$ であることは自明であるが、計算によっても確認できる:

$$(E-2I_{i,i})(E-2I_{i,i}) = E - 4I_{i,i} + 4I_{i,i}^2 = E$$

M の 2 つの列を入れ替える操作 (c) は、(a) と (b) の組み合わせであるから、正方行列で表現でき、また逆行列も存在することになる。

行に対する操作は、M に左から正方行列を掛けることによって、列と同様に扱える。

問題 1 の答では

$$\begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 5 & 6 & 8 \\ 6 & -11 & 7 \end{pmatrix} = \begin{pmatrix} 5 & 6 & 8 \\ 1 & -17 & -1 \end{pmatrix}$$

など、多数の行の変形がある。列の変形としては

$$\begin{pmatrix} 0 & 91 & 13 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -7 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 13 \\ 1 & 0 & 0 \end{pmatrix}$$

などがある。

式 (1) を行列式 $A\boldsymbol{x} = \boldsymbol{b}$ で表そう。ここに A は $m \times n$ $(n > m)$ 行列で、$a_{i,j} = (A)_{i,j}$ とする。また $\boldsymbol{x}$ は $n \times 1$ の行列で $x_i = (\boldsymbol{x})_i$ であり、$\boldsymbol{b}$ は $m \times 1$ の行列で $b_i = (\boldsymbol{b})_i$ とする。目標は A, $\boldsymbol{x}$, $\boldsymbol{b}$ を変形して $\hat{A}\hat{\boldsymbol{x}} = \hat{\boldsymbol{b}}$ の形に持っていくことである。ここに $\hat{A}$ は対角行列である。

$A \sim \hat{A}$ 故 A と $\hat{A}$ は正方行列による変形操作で結ばれている:

$$\hat{A} = S_k S_{k-1} \cdots S_1 A T_1 T_2 \cdots T_l$$

ここに S_* $(*=1,...,k)$ は行に対する変形操作で $m\times m$ の行列である。また T_* $(*=1,...,l)$ は列に対する変形操作で $n\times n$ の行列である。

行列の掛け算の計算は行列の変形に比べてひどく煩わしく、極力避けたいものである。以下のことに気がつけば、それが可能であることが分かる:
方程式 $A\boldsymbol{x}=\boldsymbol{b}$ は

$$(S_kS_{k-1}\cdots S_1)A(T_1T_2\cdots T_l)(T_1T_2\cdots T_l)^{-1}\boldsymbol{x}=(S_kS_{k-1}\cdots S_1)\boldsymbol{b}$$

と変形できる。これと $\hat{A}\hat{\boldsymbol{x}}=\hat{\boldsymbol{b}}$ を比較して

$$\hat{\boldsymbol{x}}=(T_1T_2\cdots T_l)^{-1}\boldsymbol{x},\quad \hat{\boldsymbol{b}}=(S_kS_{k-1}\cdots S_1)\boldsymbol{b}$$

を得る。$\hat{\boldsymbol{b}}$ と、対角化された $\hat{A}$ が与えられれば、$\hat{\boldsymbol{x}}$ は容易に求まり、そして $\hat{\boldsymbol{x}}$ から $\boldsymbol{x}=T_1T_2\cdots T_l\hat{\boldsymbol{x}}$ によって $\boldsymbol{x}$ が得られる。計算を効率良く行うために、$n\times n$ の単位行列 E を導入すると $\boldsymbol{x}=ET_1T_2\cdots T_l\hat{\boldsymbol{x}}$ である [8]。

そこで

$$E^{(l)}=ET_1T_2\cdots T_l,\quad A^{(l)}=AT_1T_2\cdots T_l$$

と置くと、A から $A^{(l)}$ を得る操作も、E から $E^{(l)}$ を得る操作も、共に操作列 $T_1,T_2,...,T_l$ である [9]。また同様に A に対する行の操作は $\boldsymbol{b}$ に対する操作と共通である。従って A を対角化するついでに $\hat{\boldsymbol{x}}$ から $\boldsymbol{x}$ を求めるのに必要な行列 $\hat{E}$ を求め、さらにその上 $\boldsymbol{b}$ を $\hat{\boldsymbol{b}}$ に変形可能である。

従って図 1 のような計算表を描くが良い。この図には変形目標が計算表によって示されている。ここに終状態の "$*$" は自然数であり、$\hat{A}$ の対角要素を表す。ここの最後の行 "$0\ 0\ \cdots\ 0$" は全てが 0 である必要はなく、一般的には対角要素がここまで伸びている。また $\hat{e}_{i,j}=(\hat{M})_{i,j}$ である。ここに $\hat{E}=E^{(l)}$ は $\boldsymbol{x}=\hat{E}\hat{\boldsymbol{x}}$ を満たす、我々が欲しかった行列である。

補注 3: Gilbert-Pathria は $b_1,...,b_m$ を表に加えない。対角化の意図がないからであろうが、方法の力を弱める原因になる。さらに A も E も行列を転置して表に書く [10]。そのために E を A の右隣に書いている。その結果、表と

[8] Gilbert-Pathria のうまさは、単位行列 E の導入にある。それによって、変数を引きずる計算から解放され、行列の計算だけでやって行けるようになるのである

[9] このことが理解しやすいように証明したから、ここでは自明なのであるが、そうでなければ、ここは気付きにくい箇所である。整数線形計画法ではよく知られたテクニックなのであろう

[10] この点について彼らも不自然であることを認めている。学生が列の操作よりも行の操作の方

図 1: 変形目標 (左: 始状態, 右: 終状態)

$$
\begin{array}{l|l}
a_{1,1}\ \cdots\ a_{1,n} & b_1 \\
a_{2,1}\ \cdots\ a_{2,n} & b_2 \\
\cdots & \cdots \\
a_{m,1}\ \cdots\ a_{m,n} & b_m \\
\hline
1\,0\ \cdots\ 0 & \\
0\,1\ \cdots\ 0 & \\
\cdots & \\
0\,0\ \cdots\ 1 &
\end{array}
\quad\Rightarrow\quad
\begin{array}{l|l}
*\,0\ \cdots\ 0 & \hat{b}_1 \\
0\,*\ \cdots\ 0 & \hat{b}_2 \\
\cdots & \cdots \\
0\,0\ \cdots\ 0 & \hat{b}_m \\
\hline
\hat{e}_{1,1}\ \cdots\ \hat{e}_{1,n} & \\
\hat{e}_{2,1}\ \cdots\ \hat{e}_{2,n} & \\
\cdots & \\
\hat{e}_{n,1}\ \cdots\ \hat{e}_{n,n} &
\end{array}
$$

式 (1) との対応が不自然になり、彼らの証明もまた分かり難くなるのである。

連立ディオファントス方程式

$$
\begin{aligned}
5x_1 + 6x_2 + 8x_3 &= 1 \\
6x_1 - 11x_2 + 7x_3 &= 9
\end{aligned}
\tag{3}
$$

を解く場合の計算表を図 2 に示す [11]。この計算表によって解は

$$x_1 = \hat{x}_1 + \hat{x}_2 + 10\hat{x}_3, \quad x_2 = \hat{x}_3, \quad x_3 = \hat{x}_2 - 7\hat{x}_3$$

として得られる。そして $\hat{x}_1 + 0\hat{x}_2 + 0\hat{x}_3 = 8,\ 0\hat{x}_1 + 13\hat{x}_2 + 0\hat{x}_3 = -39$ 故 $\hat{x}_1 = 8,\ \hat{x}_2 = -3$ であり、$\hat{x}_3$ は任意の整数である。従って k を任意の整数として

$$x_1 = 5 + 10k, \quad x_2 = k, \quad x_3 = -3 - 7k$$

を得る [12]。

に慣れているからだとか...

[11] 題材は Gilbert-Pathria から採った。彼の解法と比較するが良い

[12] 得られた解は Gilbert-Pathria の解 $x_1 = -5 + 10k,\ x_2 = -1 + k,\ x_3 = 4 - 7k$ とは (見かけ上) 異なるが、$k \to k + 1$ の置き換えで両者は一致するので実際は同じである

図 2: 式 (3) の計算表

$$
\begin{array}{cccc|c}
5 & 6 & 8 & 1 \\
6 & -11 & 7 & 9 \\
\hline
1 & 0 & 0 & \\
0 & 1 & 0 & \\
0 & 0 & 1 &
\end{array}
\Rightarrow
\begin{array}{cccc|c}
5 & 6 & 8 & 1 \\
1 & -17 & -1 & 8 \\
\hline
1 & 0 & 0 & \\
0 & 1 & 0 & \\
0 & 0 & 1 &
\end{array}
\Rightarrow
\begin{array}{cccc|c}
0 & 91 & 13 & -39 \\
1 & -17 & -1 & 8 \\
\hline
1 & 0 & 0 & \\
0 & 1 & 0 & \\
0 & 0 & 1 &
\end{array}
$$

$$
\Rightarrow
\begin{array}{cccc|c}
0 & 91 & 13 & -39 \\
1 & 0 & 0 & 8 \\
\hline
1 & 17 & 1 & \\
0 & 1 & 0 & \\
0 & 0 & 1 &
\end{array}
\Rightarrow
\begin{array}{cccc|c}
0 & 0 & 13 & -39 \\
1 & 0 & 0 & 8 \\
\hline
1 & 10 & 1 & \\
0 & 1 & 0 & \\
0 & -7 & 1 &
\end{array}
$$

$$
\Rightarrow
\begin{array}{cccc|c}
1 & 0 & 0 & 8 \\
0 & 0 & 13 & -39 \\
\hline
1 & 10 & 1 & \\
0 & 1 & 0 & \\
0 & -7 & 1 &
\end{array}
\Rightarrow
\begin{array}{cccc|c}
1 & 0 & 0 & 8 \\
0 & 13 & 0 & -39 \\
\hline
1 & 1 & 10 & \\
0 & 0 & 1 & \\
0 & 1 & -7 &
\end{array}
$$

3 おわりに

Gilbert-Pathria の記事 [13] は、30 年も前 (1990 年) のものである。類似のテーマの記事があるかどうか? ネット検索では見つからない。彼らの参考文献を見る限り、彼らは線形計画法あるいは整数計画法の研究者らしい。彼らの方法は (すべてを行列に持ち込む手法など) そこからヒントを得たのではないかと思える。また、“Further Reading” として線形計画法と整数計画法を挙げているのだが、これらの守備範囲は広大で、特に整数計画は計算機のパワーに依拠する極めて困難な分野である。連立 1 次ディオファントス方程式は計画法の一分野として考えるような問題ではなかろう。独自の世界を持つ易しい問題なのである。

[13] `https://www.math.uwaterloo.ca/~wgilbert/Research/AlgAndGeomPapers.html` によると論文ではなく、manuscript となっている。論文にする程ではないが、公表の価値はあると判断したのであろう

行列の三角行列化あるいは対角化自体はありふれた手法である[14]。それと連立1次ディオファントス方程式の解法を結びつけたのがGilbert-Pathriaだとしたら、彼らは非常に良い仕事をしたことになる。そのヒントが計画法の中にあった可能性が高いが、筆者はそれを確認する資料を持ち合わせていない。

References

[1] P.G.L.Dirichlet, J.W.R.Dedekind (酒井孝一訳):『整数論講義』(共立出版, 1970)

[2] 高木貞治:『初等整数論講義 (第2版)』(共立出版, 1971)

[3] L.M.Vinogradoff (三瓶与右衛門、山中健訳):『整数論入門』(共立全書, 1962)

[4] G.H.Hardy, E.M.Wright: “An Introduction to the Theory of Numbers” (Oxford Science Publication,1979)

[5] A.G.Kurosh (本田欣哉校閲、吉崎敬夫訳):『群論 (1)』(東京図書, 1960)

[6] van der Waerden (銀林浩訳): 『現代代数学 3』(東京図書, 1960)

[7] Willliam J. Gilbert, Anu Pathria: “Linear Diophantine Equations” (`https://www.math.uwaterloo.ca/~wgilbert/Research/GilbertPathria.pdf` 1990)

[14] Gilbert-Pathriaが、対角化ではなく、三角行列に変形したのは、明らかに整数線形計画法の影響である。この分野では、三角行列が好まれているようである。しかし、この問題に関する限り、それは負の影響でもあった