限定されたディオファンタス不定方程式の解を効率的に算出するアルゴリズム†

八木沢 正博††

よく知られているように，Matijasevič はディオファンタスの不定方程式の一般的解法が不可能であることを証明している．しかし，ある特定の形式を持つ不定方程式に限っては，その整数解を求めることが可能である．Baker は，「$f(x,y)$ を有理整係数の既約な s 次同次式 ($s\geqq 3$) とすれば $f(x,y)=m$ ($m\neq 0$) を満たす整数解 (x,y) は，有限の範囲に存在する」ことを示している．しかし，その解を具体的に求める効率的なアルゴリズムを提示していない．このような，解の存在する限界が実効的に求められる数値で規定されたディオファンタスの不定方程式の整数解を求める効率的なアルゴリズムを提案する．R を十分大きな素数としたとき GF(R) 上で，与えられた不定方程式をモジュラ変換し，変換後の係数が超増加数列をなすように Lenstra-Lenstra-Lovasz のアルゴリズム (LLL アルゴリズム) を適用する．超増加数列が得られれば，その性質を利用することにより，その整数解を効率良く求めることが可能となる．しかし，整数解の範囲は，数値的にかなり大きな値となるため，この解法の適用例では，扱う数値の小さいもののみを示した．

1. はじめに

ディオファンタスの不定方程式の一般的解法が不可能であることは Matijasevič により証明されている[1]．しかし，ある特定の形式を持つ不定方程式に限ってはその整数解を求めることが可能である．

Baker は，「$f(x,y)$ を有理整係数の既約な s 次同次式 ($s\geqq 3$) とすれば

$$f(x,y)=m \quad (m\neq 0)$$

を満たす整数解 (x,y) は，有限の範囲に存在する」ことを示した[2),3)]．

しかし，その解を具体的に求める効率的なアルゴリズムを提示していない．

このような解の限界が実効的に求められる数値で規定されたディオファンタスの不定方程式の整数解を求める効率的なアルゴリズムを考察し，R を十分大きな素数としたとき，GF(R) 上での一次変換を考え，超増加数列の性質を利用することにより，その整数解を効率良く求めることが可能となる．具体的にその手順を3章以降に示す．

2. ディオファンタスの不定方程式

ディオファンタスの不定方程式と呼ばれる不定方程式，つまり $x_1,\cdots,x_h$ を未知数，$a_1,\cdots,a_n$ を (互いに異なる) 有理整係数，m を有理整数とした不定方程式

$$m=\sum_{i=1}^{n} a_i f_i(x_1,\cdots,x_h) \quad (n\geqq 2) \tag{2.1}$$

を考える．

ここで，

$$f_i(x_1,\cdots,x_h)=x_1^{v_{i1}}\cdots x_h^{v_{ih}} \tag{2.2}$$

v_{ij} は0または正整数

$a_1,\cdots,a_n$，m の中で絶対値が等しいものがあった場合は，次のように考える．

行列 $T(h\times h)$ を用いて，

$$(u_1,\cdots,u_h)^t=T(x_1,\cdots,x_h)^t \tag{2.3}$$

$$T=(t_{ij}) \tag{2.4}$$

$$\det T=1 \tag{2.5}$$

$(u_1,\cdots,u_h)$ に変換し，m を含めた係数の中で絶対値に等しいものがないようにする．

3. 限定されたディオファンタスの不定方程式の例

本論文の対象となる限定された不定方程式の例を挙げる．「限定された」という意味は，整数解の絶対値の範囲が，実効的に求められる数値で規定される，ということである．

次の定理1，定理2に述べられている不定方程式が典型的な例である．

(定理 1) Baker[4)]

$f(x,y)$ を有理整係数の既約な s 次同次式 ($s\geqq 3$) とすれば

$$f(x,y)=m \quad (m\neq 0) \tag{3.1}$$

を満たす整数解 (x,y) は，

$$\max(|x|,|y|)<C\exp(\log|m|)^k \tag{3.2}$$

を満たす．ここで，k は，$k>s+1$ を満たす任意の整数，C は，s と k と f の係数から実際に計算できる

† An Efficient Algorithm for Restrained Diophantine Equations by MASAHIRO YAGISAWA (Showa Engineering Corporation).

†† 昭和エンジニアリング(株)

定数である．

(定理 2) Baker[4]

$$y^t=a_0x^t+a_1x^{t-1}+\cdots+a_t \tag{3.3}$$

を満たす整数解 (x, y) は，

$$\max(|x|, |y|)<\exp(\exp((5t)^{10}(s^{10}H)^{ts})) \tag{3.4}$$

を満たす．ここで，$t, s\geqq 3$，$a_0\neq 0$，$a_0, a_1, \cdots a_t$ は，有理整数で，

$$H=\max\{|a_j| \quad |j=1, 2, \cdots, s\} \tag{3.5}$$

また，方程式の右辺は少なくとも2つの単根をもつものとする．

4. 限定されたディオファンタスの不定方程式の解法

定理1，2に記述されているような整数解の絶対値の範囲が，実効的に求められる数値で規定されるディオファンタスの不定方程式の解法について述べる．

まず，これらのディオファンタスの不定方程式の解の絶対値は，いずれもある範囲内 $(-r/2, r/2)$ にある．ここで，r は適当な正整数である．

さて，定理1，2のディオファンタスの不定方程式を含めて，

$f(x, y)$ を有理整係数の不定方程式として，

$$f(x, y)=m \quad (m\neq 0) \tag{4.1}$$

を満たす整数解 (x, y) は，いずれもある範囲内 $(-r/2, r/2)$ にある．

さて，

$$|a_1f_1(x, y)|+\cdots+|a_nf_n(x, y)|<R \tag{4.2}$$

を満たす素数 R を選ぶ．

$f(x, y)$ を，次のように表現する．

x, y を未知数，$a_1, \cdots, a_n$ を互いに異なる有理整係数とした不定方程式

$$f(x, y)=\sum_{i=1}^{n} a_if_i(x, y) \tag{4.3}$$

を考える．

ここで，

$$f_i(x, y)=x^{p_i}y^{q_i} \tag{4.4}$$

p_i, q_i は0または正整数であり，p_i, q_i ともに0の時は定数項を表す．

R の大きさの目安として，

$$o(R/2)=\sum_{i=1}^{n} |a_if_i(r/2, r/2)| \tag{4.5}$$

とする．

modd R 演算を次のように定義する．

任意整数 M に対して

$$M \text{ modd } R=\begin{cases} M \bmod R & (0\leqq M \bmod R<R/2) \\ M \bmod R-R & (R/2\leqq M \bmod R<R) \end{cases} \tag{4.6}$$

とする．つまり，絶対値が最小の剰余を与える演算である．

R は十分大きいので，

$$f(x, y)=f(x, y) \text{ modd } R \tag{4.7}$$

が成立する．

R と互いに素な，ある整数 β を選び，

$$f(x, y)\beta \text{ modd } R \tag{4.8}$$

を考える．つまり，

$$\sum_{i=1}^{n} a_if_i(x, y)*\beta \text{ modd } R$$

$$=\sum_{i=1}^{n} b_if_i(x, y) \text{ modd } R \tag{4.9}$$

ここで，

b_i $(i=1, \cdots, n)$ を，次のように生成する．

$$Q_i=2*|f_i(r/2, r/2)| \quad (i=1, \cdots, n) \tag{4.10}$$

とすると，

$$b_1=o(1), \quad r_1=0 \tag{4.11}$$

$$b_2>2*|Q_1b_1| \tag{4.12}$$

かつ

$$o(b_2)=2*|Q_1b_1|=r_2 \tag{4.13}$$

$$\vdots$$

$$b_n>2(|Q_{n-1}b_{n-1}|+\cdots+|Q_1b_1|) \tag{4.14}$$

かつ

$$o(b_n)=2(|Q_{n-1}b_{n-1}|+\cdots+|Q_1b_1|) \tag{4.15}$$

$$=r_n$$

$$R>2(|Q_nb_n|+\cdots+|Q_1b_1|) \tag{4.16}$$

$$a_i\equiv b_i\beta \text{ modd } R \tag{4.17}$$

とすれば，超増加数列 $\{b_i\}$ の性質を利用することにより，f_i を求めることができる．

$$\left.\begin{array}{l} a_1\equiv b_1\beta \text{ modd } R \\ a_2\equiv b_2\beta \text{ modd } R \\ \cdots \\ a_n\equiv b_n\beta \text{ modd } R \end{array}\right\} \tag{4.18}$$

$$R>2(|Q_nb_n|+\cdots+|Q_1b_1|) \tag{4.19}$$

を満足する b_i $(i=1, \cdots, n)$，β，R が存在し，それらを求めることができるか．

まず，

$$\begin{array}{l} (R, 0, \cdots, 0, 0) \\ (0, R, \cdots, 0, 0) \\ \quad \cdots \\ \quad \cdots \\ (0, 0, \cdots, R, 0) \\ (a_1, a_2, \cdots, a_n, 1) \end{array} \tag{4.20}$$

を基底ベクトルとする $n+1$ 次元ラティスを考えたいが，求めるベクトルは

$$(r_1, r_2, \cdots, r_n, 0) \tag{4.21}$$

からの距離が最短になるので，次のような $n+3$ 次元基底ベクトルを考える．

$$\begin{aligned}
V_0 &= (r_1, r_2, \cdots, r_n, c, d, 0)\\
V_1 &= (R, 0, \cdots, 0, 0, d, 0)\\
V_2 &= (0, R, \cdots, 0, 0, d, 0)\\
&\cdots\\
&\cdots\\
V_n &= (0, 0, \cdots, R, 0, d, 0)\\
V_{n+1} &= (a_1, a_2, \cdots, a_n, 0, d, 1)\\
V_{n+2} &= (R, R, \cdots, R, 0, d, 0)
\end{aligned} \tag{4.22}$$

$$c<d \quad c, d \text{ は整数} \tag{4.23}$$

$$o(c)=o(d)=R^2 \tag{4.24}$$

この基底ベクトルに LLL アルゴリズムを適用し，最短ベクトルを見出す．ベクトル W が次の条件を満たせば最短ベクトルとなる可能性が高い．

W を次のように表す．

$$W=e_0V_0+e_1V_1+\cdots+e_{n+2}V_{n+2} \tag{4.25}$$

ここで，e_i は整数．

c, d は他の要素の値と比べて，十分大きいので，

$$e_0+e_1+\cdots+e_{n+2}=0 \tag{4.26}$$

かつ，

$$e_0=1 \text{ or } -1 \tag{4.27}$$

の時を考える．

つまり，

$$e_0=1 \text{ or } -1,\ e_1+\cdots+e_{n+2}=-1 \text{ or } 1 \tag{4.28}$$

となるから，このベクトル V_i は，

$$\begin{aligned}
V_i=(&a_1\beta^{-1}+\mathrm{Re}_1+\mathrm{Re}_{n+2}-r_1,\ a_2\beta^{-1}+\mathrm{Re}_2\\
&+\mathrm{Re}_{n+2}-r_2, \cdots, a_n\beta^{-1}+\mathrm{Re}_n+\mathrm{Re}_{n+2}\\
&-r_n,\ -c,\ 0,\ \beta^{-1})
\end{aligned} \tag{4.29}$$

または，

$$\begin{aligned}
V_i=(&a_1\beta^{-1}+\mathrm{Re}_1+\mathrm{Re}_{n+2}+r_1,\ a_2\beta^{-1}+\mathrm{Re}_2\\
&+\mathrm{Re}_{n+2}+r_2, \cdots, a_n\beta^{-1}+\mathrm{Re}_n+\mathrm{Re}_{n+2}\\
&+r_n,\ c,\ 0,\ \beta^{-1})
\end{aligned} \tag{4.30}$$

となる．ただし，

$$\beta^{-1}=e_{n+1} \tag{4.31}$$

このベクトルの前から n 個の要素から，b_i $(i=1, \cdots, n)$ を生成する．つまり，

$$\begin{aligned}
b_i&=a_i\beta^{-1}+\mathrm{Re}_i+\mathrm{Re}_{n+2}-r_i+r_i\\
&=a_i\beta^{-1}+\mathrm{Re}_i+\mathrm{Re}_{n+2}\\
&\qquad (i=1, \cdots, n)
\end{aligned} \tag{4.32}$$

であり，式(4.19)を満足するか，否かを調べる．満足しない場合は，R を換えて，(4.22)式から，上記の手順を繰り返す．

また，次のような基底ベクトルを用いても

$$(r_1, r_2, \cdots, r_n, 0)$$

に近いベクトルを求めることができる．

$$\begin{aligned}
V_0&=(a_1*k_1, a_2*k_2, \cdots, a_n*k_n, 1)\\
V_1&=(R*k_1,\ 0\ , \cdots,\ 0\ , 0)\\
V_2&=(\ 0\ ,\ R*k_2, \cdots,\ 0\ , 0)\\
&\cdots\\
&\cdots\\
V_n&=(\ 0\ ,\ 0\ , \cdots,\ R*k_n, 0)
\end{aligned}$$

ここで，

$$k_1=o(R/r_1), \cdots, k_n=o(R/r_n)$$

である．

原不定方程式を GF(R) 上で考え，得られた β^{-1} をかけ，modd R 変換することにより原不定方程式を変換させる．

与えられた m から f_i $(i=1, \cdots, n)$ を求めるには，

$$\begin{aligned}
m'=m\beta^{-1} \text{ modd } R &\equiv \sum_{i=1}^{n} a_if_i\beta^{-1} \text{ modd } R\\
&\equiv \sum_{i=1}^{n} b_if_i \text{ modd } R
\end{aligned} \tag{4.33}$$

$$-R/2<\sum_{i=1}^{n} b_if_i<R/2 \tag{4.34}$$

だから，

$$m'=\sum_{i=1}^{n} b_if_i \tag{4.35}$$

したがって，

$$[m'/b_n]=f_n \tag{4.36}$$

$$[(m'-b_nf_n)/b_{n-1}]=f_{n-1} \tag{4.37}$$

ここで，$[M]$ は M に最も近い整数を表す．

例えば，$[1.3]=1$, $[-2.4]=-2$ となる．

以下同様にして，f_i $(i=n, \cdots, 2)$ を求めることができる．

$$f_i=[(m'-b_nf_n\cdots-b_{i+1}f_{i+1})/b_i] \tag{4.38}$$

最後に，

$$f_1=(m'-b_nf_n\cdots-b_2f_2)/b_1 \tag{4.39}$$

f_1 が整数にならない時は，整数解が存在しない．

5. 未知数 $(x_1, \cdots, x_h)$ の解法

中間解 $F=(f_1, f_2, \cdots, f_n)$ が得られたので，次に未知数 $(x_1, \cdots, x_h)$ を求めることを考える．

未知数 $x_1, \cdots, x_h$ は，自然数であることを前提としている点に注意してほしい．これ以降は $h=2$ の場合について，議論する．

連立方程式

$$\begin{cases} f_1 = x^{p1} y^{q1} & (5.1\,a) \\ f_2 = x^{p2} y^{q2} & (5.1\,b) \\ \cdots \\ \cdots \\ f_n = x^{pn} y^{qn} & (5.1\,c) \end{cases}$$

で，$f_1, f_2, \cdots, f_n$ が与えられたとき，整数解 (x, y) を求める．

両辺の絶対値をとり，常用対数をとる．

$$g_i = \log|f_i| \quad (i=1, \cdots, n) \tag{5.2}$$

$$u = \log|x| \tag{5.3}$$

$$v = \log|y| \tag{5.4}$$

とすると，

$$\begin{cases} g_1 = p_1 u + q_1 v & (5.5\,a) \\ g_2 = p_2 u + q_2 v & (5.5\,b) \\ \cdots \\ \cdots \\ g_n = p_n u + q_n v & (5.5\,c) \end{cases}$$

が得られる．

これは，u，v を未知数とする一般的な線型一次連立方程式であり，浮動小数点演算で u，v の近似値を求め．整数解 x，y を得ることができるであろう．

6. 計 算 量

与えられた不定方程式から，整数解を得るまでに必要な計算量を求める．不定方程式として，x，y を変数とする s 次の同次式を考える．変数 x，y の範囲は与えられているものとする．

このとき，$n = s+1$ である．

Q_i $(i=1, \cdots, n)$ を得るのに $M_1 = n*s$ 個の乗算が必要．

次に，モジュラ変換後の係数の大きさを示す r_i $(i=2, \cdots, n)$ を求めるには，

$M_2 = 2n$ 個の乗算と $A_1 = n-1$ 個の加算

が必要．

$n+3$ 次元のラティス上で LLL アルゴリズムを用いて，b_i $(i=1, \cdots, n)$ を得るには，

$$M_3 = o((n+3)^6 (\log B)^3)$$

の演算が必要となる．

ここで，B は基底ベクトルの座標の上界であり，

$$B = o(R^2)$$

である．

b_i $(i=1, \cdots, n)$ が得られた後，超増加数列の性質を利用して，f_i $(i=1, \cdots, n)$ を求めるには，

$M_4 = n$ 個の除算と $A_4 = n-1$ 個の減算

が必要．

f_i $(i=1, \cdots, n)$ が得られた後，その絶対値の常用対数 g_i を得るのに，

$M_5 = n$ 個の対数演算

が必要．

g_i $(i=1, \cdots, n)$ から，$\log|x|, \log|y|$ を得るのに，

$M_6 =$ 4 個の乗算，2 個の除算，2 個の減算

および $2(n-2)$ 個の乗算，$n-2$ 個の加算

が必要．

$\log|x|, \log|y|$ が得られたら，x，y を得るのに

$M_7 = 2$ 個の指数演算

が必要．

$|x|, |y|$ が得られたら，(x, y) を得るのに最悪で，

$M_8 = n*s$ 個の乗算と $A_8 = 4(n-1)$ 個の加算

が必要となる．

以上，まとめると整数解を得るのに必要な計算量は LLL アルゴリズムの走行時間が支配的となり，その時間は，

$$T = o((n+3)^6 (\log R^2)^3) \tag{6.1}$$

で与えられる．

また，このとき必要な記憶容量 S は，R の語長を 1 語長として，

$$S = o(n) \text{ の語長} \tag{6.2}$$

である．

n と R の大きさを，

$$n = o(10), \quad R = o(10^{20}) \tag{6.3}$$

とすると，

$$T = o(13^6 (40 \log_e 10)^3) = o(10^{13}) \tag{6.4}$$

となる．

7. 数 値 例

理解を助けるため簡単な数値例を示す．

$$21432360 f_1 + 88782005 f_2 + 17448649 f_3 = 32617377910 = m \tag{7.1\,a}$$

$$\begin{cases} f_1 = x^4 & (7.1\,b) \\ f_2 = x^2 * y^2 & (7.1\,c) \\ f_3 = y^4 & (7.1\,d) \end{cases}$$

を満足する (x, y) を求める．

まず，f_1, f_2, f_3 の範囲を調べる．この例では，(7.1 a) 式の左辺の各項が正だから，

$$0 \leqq f_1 \leqq \mathrm{INT}(m/21432360) = 1521 \tag{7.2\,a}$$

$$0 \leqq f_2 \leqq \mathrm{INT}(m/88782005) = 367 \tag{7.2\,b}$$

$$0 \leqq f_3 \leqq \mathrm{INT}(m/17448649) = 1869 \tag{7.2\,c}$$

となる．INT( ) は ( ) 内の数値の整数部分を表す．

さて，

$$\begin{cases} m<R & (7.3)\\ 21432360\equiv b_1\beta \bmod R & (7.4)\\ 88782005\equiv b_2\beta \bmod R & (7.5)\\ 17448649\equiv b_3\beta \bmod R & (7.6)\\ 1521*|b_1|+367*|b_2|+1869*|b_3|<R/2 & (7.7)\end{cases}$$

を同時に満足する b_1, b_2, b_3, β, R を求めることを考える．(7.4)～(7.6)式を書き替えて，

$$\begin{cases} m<R & (7.3)\\ b_1\equiv 21432360*\beta^{-1} \bmod R & (7.8)\\ b_2\equiv 88782005*\beta^{-1} \bmod R & (7.9)\\ b_3\equiv 17448649*\beta^{-1} \bmod R & (7.10)\\ 1521*|b_1|+367*|b_2|+1869*|b_3|<R/2 & (7.7)\end{cases}$$

が得られる．

これらを満足する b_1, b_2, b_3, β, R として，例えば，

$$R=90000000019 \quad (7.11)$$

$$\beta^{-1}=9077556090 \quad (7.12)$$

を選び，

$$b_1=\quad 5 \quad (7.13)$$

$$b_2=\quad 21017 \quad (7.14)$$

$$b_3=-41215709 \quad (7.15)$$

を得る．

このとき，確かに

$$1521*|b_1|+367*|b_2|+1869*|b_3|<R/2 \quad (7.16)$$

が成立している．

したがって，(7.1 a)式の両辺を β^{-1} modd R でモジュラ変換すると，

$$5*f_1+21017*f_2-41215709*f_3 = -25755088895 \quad (7.17)$$

さて，f_3 から順次求める．

$$[-25755088895/-41215709]=[625.88\cdots]=625$$

したがって，

$$f_3=625 \quad (7.18)$$

$$[(-25755088895+41215709*f_3)/(21017)] = [4729230/21017]=[225.019\cdots]=225$$

となる．したがって，

$$f_2=225 \quad (7.19)$$

$$(4729230-225*21017)/5=81$$

$$f_1=81 \quad (7.20)$$

が得られる．

次に，f_1, f_2, f_3 の値から，x_1, x_2, x_3 を求める．

連立方程式

$$\begin{cases} f_1=x^4 & (7.21\,a)\\ f_2=x^2*y^2 & (7.21\,b)\\ f_3=y^4 & (7.21\,c)\end{cases}$$

の両辺の絶対値をとり，その対数をとると，

$$\begin{cases} g_1=\log 81 =4*u & (7.22\,a)\\ g_2=\log 225=2*u+2*v & (7.22\,b)\\ g_3=\log 625=4*v & (7.22\,c)\end{cases}$$

が得られる．ただし，

$$u=\log|x| \quad (7.23\,a)$$

$$v=\log|y| \quad (7.23\,b)$$

である．(7.22 a，c)式より，

$$1.908\cdots=4*u \quad (7.24\,a)$$

$$2.795\cdots=4*v \quad (7.24\,b)$$

$$u\fallingdotseq 0.477\cdots \quad (7.25)$$

$$v\fallingdotseq 0.698\cdots \quad (7.26)$$

が得られる．

$$|x|\fallingdotseq 10^{0.477}\fallingdotseq 3 \quad (7.27)$$

$$|y|\fallingdotseq 10^{0.698}\fallingdotseq 5 \quad (7.28)$$

x, y は整数だから，

$$|x|=3 \quad (7.29)$$

$$|y|=5 \quad (7.30)$$

が得られる．このとき，

$$x^2*y^2=225=f_2 \quad (7.31)$$

が成立している．求める解として，

$$(x,y)=(3,5),(-3,5),(3,-5),(-3,-5) \quad (7.32)$$

を得る．

8. おわりに

整数解の限界が実効的に求められる数値で規定されたディオファンタスの不定方程式の効率的な解法を具体的に示した．この解法では，取り扱う数値がかなり大きくなり，実際に適用するには，大きな数値を扱うことができる計算機が必要となる．

本解法の特徴は，GF(R) 上で LLL アルゴリズムを用いることにより，解法が容易になる形に方程式を変換させることである．この発想は，単にディオファンタスの不定方程式の解法ばかりでなく，整数解の限界が実効的に求められる数値で規定された問題を扱う分野への応用が考えられる．例えば，

1) 整数係数の n 次方程式の整数解の解法
2) 整数係数の連立方程式の整数解の解法
3) 素因数分解

などへの応用である．

参考文献

1) Матиясеич, Ю.В.: Диофантовость перечислимых множеств, *Dokl. Akad. Nauk SSSR*, 191 (1970).
2) Baker, A.: *Transcendental Number Theory*,

Cambridge (1975).
3) Baker, A. and Masser, D. W. (eds.): *Transcendence Theory, Advances and Applications*, Academic Press (1977).
4) 広瀬 健：帰納的関数，pp. 162-163，共立出版，東京 (1989).
5) 鹿野 健：解析数論，教育出版，東京 (1978).

(平成2年10月26日受付)
(平成3年7月8日採録)

八木沢正博（正会員）

昭和25年生．昭和49年東京大学工学部計数工学科卒業．昭和51年同大学院修士課程修了．同年昭和電工(株)入社．川崎工場勤務．昭和61年昭和エンジニアリング(株)に出向，現在に至る．化学プラントの計装エンジニアとして，プラントの設計，保全に従事．現在，素因数分解アルゴリズムに興味を持つ．