論文　**Original Paper**

整数環のイデアルを用いた不定方程式の解法について

関　口　勝　右*，石　川　賢　太*

On the solutions of the Diophantine equation by using the ideal of the ring of integers

Katsusuke Sekiguchi*，Kenta Ishikawa*

Abstract: In the Senior high school textbooks, the solution of the 2-variable Diophantine equation is given by using the Euclidean algorithm. The purpose of this paper is to solve it by using the ideal of the commutative ring. By this method, we can also solve the n-variable Diophantine equation.

Key words: Diophantine equation, Euclidean algorithm, ideal , commutative ring.

1. はじめに

指導要領の改訂により高等学校で学ぶ数学に整数に関する項目が入った。所謂初等整数論の基礎的な部分である。その中で大きな位置を占めるのがユークリッドの互除法と2変数不定方程式の解法に関する項目である。初等整数論を学ぶことによって数的感覚を豊かなものとし，またそこから代数的構造の理解への第一歩を踏み出すことができる。大学の数学教育に携わる者としては歓迎すべき変更であると考えている。ただ，この中では整係数不定方程式の整数解はユークリッドの互除法を用いて求められている。高校の範囲では仕方がないことだが，この方法では解き方がテクニカルなため，何故そのように解くのかが分かりにくい。また，3変数以上の場合にはそのまま適用することができない。そこで本論文では代数学の環論に於いて重要な概念であるイデアルの考え方を用いて整数解を求める方法について考察する。この方式による解法は高校数学と大学で学ぶ抽象的な数学との橋渡しとなりうるものと考えられる。

本論文で使用する記号は以下の通りである。

$\mathbb{N}$：自然数全体の集合

$\mathbb{Z}$：整数全体の集合

aとbを自然数とするとき

(a, b)：aとbの最大公約数

$a \mid b$：aはbを割り切る。

2. 高校数学における不定方程式の概略

ここでは高校数学における不定方程式の解法について述べる。そのためには，ユークリッドの互除法について述べる必要がある。証明等は省略し，内容の概略のみを述べる。

ユークリッドの互除法

最初に次の定理を述べる。証明は省略する。

定理2.1　$a, b, q \in \mathbb{N}$とし$a<b, 0 \leq b-qa$とすると$(a, b)=(a, b-qa)$である。

整数の除法　$a, b \in \mathbb{N}$とするとき

$$b=q_1a+r_1 \quad (q_1, r_1 \in \mathbb{N},\ 0 \leqq r_1 \leqq a-1) \tag{1}$$

となるq_1, r_1が一意的に存在する。

次にaとr_1に関して除法を行う。更にその除法を次のように繰り返す。

$$(*)\begin{cases} b = q_1a + r_1 \quad (q_1, r_1 \in \mathbb{N},\ 0 \lneqq r_1 < a) \\ a = q_2r_1 + r_2 \quad (q_2, r_2 \in \mathbb{N},\ 0 \lneqq r_2 < r_1) \\ r_1 = q_3r_2 + r_3 \quad (q_3, r_3 \in \mathbb{N},\ 0 \lneqq r_3 < r_2) \\ \quad \cdots \\ r_{n-3} = q_{n-1}r_{n-2} + r_{n-1} \quad (q_{n-1}, r_{n-1} \in \mathbb{N},\ 0 \lneqq r_{n-1} < r_{n-2}) \\ r_{n-2} = q_nr_{n-1} + r_n \quad (q_n, r_n \in \mathbb{N},\ 0 \lneqq r_n < r_{n-1}) \\ r_{n-1} = q_{n+1}r_n \end{cases}$$

：r_n が最後の余りである。

このとき（∗）に定理2.1を繰り返し適用すると最大公約数(a, b)が次のようにして求まる。

$$(a, b)=(a, b-q_1a)=(a, r_1)=(a-q_2r_1, r_1)=(r_2, r_1)$$
$$= \cdots =(r_{n-1}, r_n)=r_n$$

*国士舘大学理工学部

つまり，最後の余りr_nが最大公約数である。
この様にして最大公約数を求める方法をユークリッドの互除法という。

整係数不定方程式（2変数）の解法

$a, b, c \in \mathbb{Z}$とするとき，x, yを未知数とする不定方程式

$$ax+by=c \qquad (2)$$

を満たす整数の組(x, y)を方程式（2）の整数解と呼ぶ。このとき，次の定理は基本的である。

定理2.2　$ax+by=c$が整数解を持つための必要十分条件は$(a, b) \mid c$となることである。

証明）定義より$a=(a, b)a_1$，$b=(a, b)b_1$（$a_1, b_1 \in \mathbb{Z}$）と書ける。

$$ax+by=(a, b)(a_1x+b_1y)=c$$

よって整数解を持つためには$(a, b) \mid c$が必要である。

逆に$(a, b) \mid c$のとき整数解をもつことを示す。$ax+by=(a, b)$が整数解をもつことを示せば十分である。a, bの互除法の式（∗）より

$$(a, b)=r_n=r_{n-2}-q_nr_{n-1}$$

この式に$r_{n-1}=r_{n-3}-q_{n-1}r_n$を代入すると

$$\begin{aligned}(a, b) &= r_{n-2}-q_n(r_{n-3}-q_{n-1}r_{n-2}) \\ &= -q_nr_{n-3}+(1+q_nq_{n-1})r_{n-2}\ 。\end{aligned}$$

このとき$-q_n$，$1+q_nq_{n-1} \in \mathbb{Z}$に注意する。更に$r_{n-2}=r_{n-4}-q_{n-2}r_{n-3}$を代入する。
この操作を繰り返すと

$$(a, b)=ax_0+by_0$$

となる$x_0. y_0$　$(x_0, y_0 \in \mathbb{Z})$が見つかる。

この操作により$ax+by=(a, b)$の整数解は求まるが，後に例で示すように，この計算は一般には煩雑になることが多い。また3変数以上の不定方程式には適用できない。そこで本論文では，代数学の環論におけるイデアル（ideal）の概念を利用して整数解を求める方法について考える。

3. 環論における必要事項

本論文では環は可換環のみを扱う。また単位元1を持つことを前提とする。

定義3.1　Rを可換環とする。Rの空でない部分集合Iが次の条件を満たすとき，IをRのイデアル（ideal）という。

$$I \ni a, b,\quad R \ni r, s \ \Rightarrow\ I \ni ra+sb \qquad (3)$$

（注）条件（2）は次の2つの条件（i），（ii）をともに満たすことと同値である。

（i）$I \ni a, b \ \Rightarrow\ I \ni a+b$
（ii）$I \ni a, R \ni r \ \Rightarrow\ I \ni ra$

本論文で重要な役割を演ずるイデアルの例を挙げよう。

定義3.2　$R \ni a_1, a_2, \cdots, a_n$とするとき，
集合$I_R(a_1, a_2, \cdots, a_n)$を

$$\begin{aligned}&I_R(a_1, a_2, \cdots, a_n) \\ &=\{a_1x_1+a_2x_2+\cdots+a_nx_n \mid x_i \in R,\ 1 \leqq i \leqq n\}\end{aligned}$$

で定める。特に$R=Z$のとき，$I_Z(a_1, a_2, \cdots, a_n)$を単に$I(a_1, a_2, \cdots, a_n)$と書くことにする。
次の命題は容易なので証明は省略する。

命題3.1　$I_R(a_1, a_2, \cdots, a_n)$は$R$のイデアルである。特に$n=1$のとき$I_R(a)=\{ax \mid x \in R\}$を（$R$の）単項イデアルという。
上記の定義を用いて方程式の問題を言い換えると次のようになる。

命題3.2　$Z \ni a_1, a_2, \cdots, a_n$とするとき次は同値である
（1）不定方程式　$a_1x_1+a_2x_2+\cdots+a_nx_n=b$は整数解を持つ。
（2）$b \in I(a_1, a_2, \cdots, a_n)$

このことから，不定方程式の整数解の存在は方程式の右辺の項bが，イデアル$I(a_1, a_2, \cdots, a_n)$に含まれるか否かと言う問題になる。そこで我々はこのイデアルについて詳しく調べることにする。そのためにいくつかの定義を述べる。

定義3.3　可換環Rの任意のイデアルが単項イデアルであるときRを単項イデアル環という。

定義3.4　Rを可換環とする。Rの元a, bが$a \neq 0, b \neq 0$かつ$ab=0$とあるときa, bを零因子という。

定義3.5
（1）零因子を持たない可換環を整域（domain）という。
（2）可換環Rが単項イデアル環であり，かつ整域のとき，Rを単項イデアル整域（principal ideal domain，略してPID）という。

次の定理は不定方程式の整数解の存在について考えるときに重要である。証明はよく知られているが，後の証明との対比のため簡単な証明を記す。

定理3.1　有理整数環ZはPIDである。

証明）Zが整域であることは明らかである。
IをZの$\{0\}$でないイデアルとする。Iに含まれる0でない元で絶対値が最小なものをaとする。$a>0$としてよい。イデアルの定義より$I\supset I(a)=\{ax\mid x\in\mathbb{Z}\}$である。
$I\ni b$を任意にとる。bをaで割ると

$$b=qa+r(q, r\in\mathbb{Z}, 0\leqq r\leqq a-1)$$

となる。Iはイデアルなので$I\ni b-qa=r$となる。仮に$r\neq0$とするとaの最小性に反する。故に$r\neq0$，つまり$b=qa$と書ける。これは$I(a)\ni b$を意味する。

この定理が成立するために必要なことは除法（1）が成り立つことである。従って，除法が成立する整域では同様な結果が期待される。次のような場合で同様の定理が成り立つ。

1. 体k上の多項式環$k[x]$。
2. ガウス整数環$Z[i]$，ただし$i=\sqrt{-1}$とする。

更に，一般化されたユークリッド整域という概念がある。

定義3.6（ユークリッド整域）　整域Rが次の条件を満たすときユークリッド整域と言う。
写像　$g:R\setminus\{0\}\to\mathbb{N}$があり，$a, b\in R$で$b\neq0$ならば$q, r\in R$があり，$a=qb+r$で$r=0$又は$g(r)<g(b)$となる。
このとき，一般に次の定理が成り立つ。

定理3.2　整域Rがユークリッド整域ならばRはPIDである。

4. イデアルを用いた不定方程式の解法アルゴリズム

不定方程式$ax+by=(a, b)$の整数解を求めるために次の定理を証明する。この定理は
定理2.2をイデアルの言葉で書き直したものである。

定理4.1　$a, b\in\mathbb{Z}$とする。このとき，次が成り立つ。

$$I(a, b)=I((a, b))$$

証明）　Step1．任意の$q\in\mathbb{Z}$に対して$I(a, b)=I(a, b-qa)$が成り立つ。
$\because I(a, b)\ni ax_1+by_1=ax_1+(b-qa)y_1+qay_1$
$=a(x_1+qy_1)+(b-qa)y_1\in I(a, b-qa)$
より$I(a, b)\subset I(a, b-qa)\cdots①$
逆に$I(a, b-qa)\ni ax_2+(b-qa)y_2$
$=a(x_2-qy_2)+by_2\in I(a, b)$
より$I(a, b-qa)\subset I(a, b)\cdots②$
①②より証明終。
Step2．Step1を（∗）の第1式に適用すると

$$I(a, b)=I(a, b-q_1a)=I(a, r_1)$$

更に第2式に適用すると

$$I(a, r_1)=I(a-q_2r_1, r_1)=I(r_2, r_1)$$

以下同様の操作を繰り返すと

$$I(a, b)=I(a, r_1)=I(r_2, r_1)=\cdots=I(r_{n-1}, r_n)$$

となる。$r_n\mid r_{n-1}$より$I(r_{n-1}, r_n)=I(r_n)=I((a, b))$。
$\therefore I(a, b)=I((a, b))$。

$a_1, a_2, \cdots, a_n, b\in\mathbb{Z}$のとき，不定方程式$a_1x_1+a_2x_2+\cdots+a_nx_n=b$が整数解を持つとは$I(a_1, a_2, \cdots, a_n)\ni b$となることであることに注意する。
不定方程式$ax+by=(a, b)$をイデアルの概念を利用して求めるアルゴリズム。

$$I(a, b)\ni a=a\cdot1+b\cdot0 \quad \text{(i)}$$
$$b=a\cdot0+b\cdot1 \quad \text{(ii)}$$
(i)，(ii)より$I(a, b)\ni r_1=b-q_1a$ (iii)
(i)，(iii)より$I(a, b)\ni r_2=a-q_2r_1$ (iv)
(iii)，(iv)より$I(a, b)\ni r_3=r_1-q_3r_2$ (v)

以下，同様の操作を行うと

$$I(a, b)\ni r_n=(a, b)$$

が言えるが，この操作を$az_1+bz_2(z_1, z_2\in\mathbb{Z})$の形で以下の様に追っていく。

(i)（ii）を（iii）に代入して

$$\begin{aligned}r_1&=b-q_1a=(a\cdot0+b\cdot1)-q_1(a\cdot1+b\cdot0)\\&=a(-q_1)+b\cdot1\\r_2&=a-q_2r_1=(a\cdot1+b\cdot0)-q_2(a(-q_1)+b\cdot1)\\&=a(1+q_1q_2)+b(-q_2)\\r_3&=r_1-q_3r_2=(a(-q_1)+b\cdot1)-q_3(a(1+q_1q_2)+b(-q_2))\\&=a(-q_1-q_3-q_1q_2q_3)+b(1+q_2q_3)\end{aligned}$$

以下，この操作を繰り返すことにより$ax_0+by_0=(a, b)$となる整数x_0, y_0が求まる。この様に整数解は求まるが計算が煩雑になることが多い。

以下では例により不定方程式の解法が簡略化できることを示す。計算の方針は次の通りである。

計算の方針

方程式$a_1x_1+a_2x_2+\cdots+a_nx_n=b$を解くために$I(a_1, a_2, \cdots, a_n)\ni b$を具体的に示す。その際，$I(a_1, a_2, \cdots, a_n)\ni a_1, a_2, \cdots a_n$から出発してイデアルの性質（3）を使用して$I(a_1, a_2, \cdots, a_n)\ni b$を示し，その過程を式で追っていく。（3）の使用方法は自由で，ユークリッドの互除法に沿う必要はない。

例1　$150x+252y=12$

（解法1）（ユークリッドの互除法に沿った解法）

$$\begin{cases} 252=1\times150+102 \\ 150=1\times102+48 \\ 102=2\times48+6 \\ 48=8\times6 \end{cases}$$

$I(150, 252)\ni150=150\cdot1+252\cdot0\cdots①$

$252=150\cdot0+252\cdot1\cdots②$

②－①を計算すると

$I(150, 252)\ni102=252-150$

$=(150\cdot0+252\cdot1)-(150\cdot1+2520)$

$=150\cdot(-1)+252\cdot1\cdots③$

①－③より

$I(150, 252)\ni48=150-102$

$=150\cdot2+252\cdot(-1)\cdots④$

③－④×2より

$I(150, 252)\ni6=102-48\cdot2$

$=150\cdot(-5)+252\cdot3\cdots⑤$

⑤×2より

$I(150, 252)\ni12=150\cdot(-10)+252\cdot6\cdots⑥$

以上により$x=-10, y=6$の解が求まる。

（解法2）（簡略化）

$I(150, 252)\ni150=150\cdot1+252\cdot0\cdots①$

$252=150\cdot0+252\cdot1\cdots②$

①×2－②

$I(150, 252)\ni48=150\cdot2-252$

$=150\cdot2+252\cdot(-1)\cdots③$

②－③×5

$I(150, 252)\ni12=252-48\cdot5$

$=150\cdot(-10)+252\cdot6\cdots④$

以上により$x=-10, y=6$の解が求まる。

例2　$129x+57y=3$

（解法1）ユークリッドの互除法に沿って解くと次の様になる。

$$\begin{cases} 129=2\times57+15 \\ 57=3\times15+12 \\ 15=1\times12+3 \\ 12=4\times3 \end{cases}$$

$I(129, 57)\ni129=129\cdot1+57\cdot0\cdots①$

$I(129, 57)\ni57=129\cdot0+57\cdot1\cdots②$

①－②×2を行うと

$I(129, 57)\ni15=129\cdot1+57\cdot(-2)\cdots③$

②－③×3を行うと

$I(129, 57)\ni12=129\cdot(-3)+57\cdot7\cdots④$

③－④を行うと

$I(129, 57)\ni3=129\cdot4+57\cdot(-9)$

∴ $x=4, y=-9$が解である。

この方法ではユークリッドの互除法の順に従う必要はないので，次の様に簡略化できる。

（解法2）

$I(129, 57)\ni129=129\cdot1+57\cdot0\cdots①$

$I(129, 57)\ni57=129\cdot0+57\cdot1\cdots②$

$I(129, 57)\ni15=129\cdot1+57\cdot(-2)\cdots③$

③×4－②　$3=129\cdot4+57\cdot(-9)$

∴ $x=4, y=-9$が解である。

この方法は3変数以上の場合にも同様に適用できる。また，計算の順序は自由なため，簡潔な解法を各自で工夫できる利点がある。

以下に例を挙げる。

例3　$60x+315y+154z=1$

（解法1）

$I=I(60, 315, 154)$とおくと

$I\ni315=60\cdot0+315\cdot1+154\cdot0\cdots①$

$300=60\cdot5+315\cdot0+154\cdot0\cdots②$

$15=60\cdot(-5)+315\cdot1+154\cdot0\cdots③$

$154=60\cdot0+315\cdot0+154\cdot1\cdots④$

④－③×10　$4=60\cdot50+315\cdot(-10)+154\cdot1\cdots⑤$

⑤×4－③　$1=60\cdot205+315\cdot(-41)+154\cdot4$

∴ $x=205, y=-41, z=4$が解である。

（解法2）

$I=I(60, 315, 154)$とおくと

$I\ni60=60\cdot1+315\cdot0+154\cdot0\cdots①$

①×3　$180=60\cdot3+315\cdot0+154\cdot0\cdots②$

$154=60\cdot0+315\cdot0+154\cdot1\cdots③$

②－③　$26=60\cdot3+315\cdot0+154\cdot(-1)\cdots④$

④×6　$156=60\cdot18+315\cdot0+154\cdot(-6)\cdots⑤$

⑤－③　$2=60\cdot18+315\cdot0+154\cdot(-7)\cdots⑥$

$315=60\cdot0+315\cdot1+154\cdot0\cdots⑦$

⑦－⑤×2－⑥　$1=60\cdot(-54)+315\cdot1+154\cdot19$

∴ $x=-54, y=1, z=19$が解である。

例4　$150x+252y+280z+1155w=1$

$I=I(150, 252, 280, 1155)$とおくと

$$I \ni 150=150\cdot 1+252\cdot 0+280\cdot 0+1155\cdot 0\cdots ①$$
$$1155=150\cdot 0+252\cdot 0+280\cdot 0+1155\cdot 1\cdots ②$$
②－①×8　$-45=150\cdot(-8)+252\cdot 0+280\cdot 0+1155\cdot 1\cdots ③$
$$280=150\cdot 0+252\cdot 0+280\cdot 1+1155\cdot 0\cdots ④$$
④＋③×6　$10=150\cdot(-48)+252\cdot 0+280\cdot 1+1155\cdot 6\cdots ⑤$
$$252=150\cdot 0+252\cdot 1+280\cdot 0+1155\cdot 0\cdots ⑥$$
⑥－⑤×25　$2=150\cdot 1200+252\cdot 1+280\cdot(-25)+1155+(-150)\cdots ⑦$
⑦×23＋③　$1=150\cdot 27592+252\cdot 23+280\cdot(-575)+1155\cdot(-3449)\cdots ⑧$

$\therefore$ $x=27592, y=23, z=-575, w=-3449$が解である。

5. おわりに

本論文で述べた計算アルゴリズムは一般のn−変数不定方程式にも適用できる。計算の順序は自由なため，簡潔な解法を各自で工夫できる利点がある。計算の難易度は変数を増やしてもほとんど変わらないため計算時間は大幅に短縮できることが多い。また，例でも示したように解き方により何種類もの異なる解が求められる。

参考文献

1）片山孝次：代数学入門　新曜社
2）雪江明彦：整数論1初等整数論からp進数へ　日本評論社