P-4

不定方程式 $ax^2+bxy+cy^2=k$ の整数解

On integer solutions to the equaion $ax^2+bxy+cy^2=k$

○小林 淳人
Atsuto Kobayashi[1]

Abstract

We find all the integer solutions to the equaion $ax^2+bxy+cy^2=k$.

1　定理の紹介

ディオファントス方程式の整数解は古くから研究されていて，例えばピタゴラス数はパラメータ表示によって無限個の解があることが知られている．本研究では

$$ax^2+bxy+cy^2=k \tag{1}$$

という不定方程式の，整数解の求め方を紹介する．$D=b^2-4ac$ が平方数なら比較的簡単に求められるので，$D<0$ の場合と $D>0$ の平方数ではない場合の整数解について証明する．

Theorem 1　a, b, c, $k\in\mathbb{Z}$, $\gcd(a,b,c)=1$, $k\neq 0$, $D=b^2-4ac<0$ とする．このとき，式 (1) は $ak<0$ なら解はない．$ak>0$ なら $X=2ax+by$ とおいて，$|X|\leq 2\sqrt{ak}$, $|y|\leq 2\sqrt{\frac{ak}{|D|}}$ を満たす $X^2+|D|y^2=4ak$ の整数解のうち，$(\frac{X-by}{2a},y)\in\mathbb{Z}^2$ であるものが解．

$D>0$ の場合はより難しく，連分数の理論を導入する．

Definition　θ を無理数，[ ] をガウス記号とする．$k_0=[\theta]$，$\theta_0=\theta-k_0$ とおき，$n\in\mathbb{N}$ に対して $k_n=[\frac{1}{\theta_{n-1}}]$，$\theta_n=\frac{1}{\theta_{n-1}}-k_n$ とおく．このとき，

$$\theta=k_0+\cfrac{1}{k_1+\cfrac{1}{k_2+\cfrac{1}{\ddots}}}$$

となり，$\theta=[k_0,k_1,k_2,\ldots]$ と書く．また，$[k_0,\ldots,k_{n-1}]$ を既約分数表示したものを $\frac{p_n}{q_n}$ と書き，**近似分数** という．

$D>0$ の場合の証明では方程式

$$x^2-Dy^2=\pm 4 \tag{2}$$

の解の存在性が必要なので，次の定理を利用する．

Theorem 2　$D>1$ を平方でない整数で $D\equiv 0,1 \pmod 4$ とする．

$$\theta=\begin{cases}[\sqrt{d}]+\sqrt{d} & D=4d\\ [\frac{\sqrt{D}-1}{2}]+\frac{\sqrt{D}-1}{2} & D\equiv 1 \pmod 4\end{cases}$$

とおく．このとき θ を連分数展開すると，正の整数 $k_0,\cdots,k_{n-1}$ により $\theta=[k_0,\ldots,k_{n-1},\theta]$ と表せる．この n を最小となるように選び，$\frac{p_n}{q_n}$ を近似分数，$\varepsilon=q_n\theta+q_{n-1}$，$\varepsilon^l=\frac{x_l+y_l\sqrt{D}}{2}$ $(l\in\mathbb{Z})$ とすると，$(\pm x_l,\pm y_l)$ が式 (2) の全ての整数解（複号任意）．

Theorem 3　a, b, c, $k\in\mathbb{Z}$, $\gcd(a,b,c)=1$, $k\neq 0$ で $D=b^2-4ac>0$ は平方数でないとする．$(x_1,y_1)\in\mathbb{Z}^2$ を Theorem 2 で得られる式 (2) の解のうちの最小解，$\varepsilon=\frac{x_1+y_1\sqrt{D}}{2}$，

$$\lambda=\frac{\alpha+\beta\sqrt{D}}{2}=\begin{cases}\varepsilon & (x_1^2-Dy_1^2=4)\\ \varepsilon^2 & (x_1^2-Dy_1^2=-4)\end{cases}$$

とおき，$X=2ax+by$ とする．このとき，式 (1) の解は次のように決定できる．

〈1〉　$ak<0$ なら $2\sqrt{ak}\leq X<\alpha\sqrt{ak}$ の範囲で $X^2-Dy^2=4ak$ の整数解を見つけ，$x=\frac{X-by}{2a}\in\mathbb{Z}$ であるものを (X_i,y_i) $(i=1,\cdots,N)$ とする．$j\in\mathbb{Z}$ に対して $(X_i,y_i\sqrt{D})\lambda^j=X_{ij}+y_{ij}\sqrt{D}$ とするとき，$\{(\pm\frac{X_{ij}-by_{ij}}{2a},\pm y_{ij})|i=1,\cdots,N,j\in\mathbb{Z}\}$ が解（複号任意）．

〈2〉 $ak>0$ なら $0\leq X<\beta\sqrt{-akD}$ の範囲で $X^2-Dy^2=4ak$ の整数解を見つけ，$x=\frac{X-by}{2a}\in\mathbb{Z}$ であるものを (X_i,y_i) $(i=1,\cdots,N)$ とする．$j\in\mathbb{Z}$ に対して $(X_i,y_i\sqrt{D})\lambda^j=X_{ij}+y_{ij}\sqrt{D}$ とするとき，$\{(\pm\frac{X_{ij}-by_{ij}}{2a},\pm y_{ij})|i=1,\cdots,N,j\in\mathbb{Z}\}$ が解（複号任意）．

2　定理の証明

Proof (of Theorem 1)　$a=0$ とすると $D=b^2$ となるが，$D<0$ より D は平方数ではないので $a\neq 0$．式 (1) の両辺を $4a$ 倍して変形すると次の式が得られる．

$$\begin{aligned}4a^2x^2+4abxy+4acy^2&=(2ax+by)^2-(b^2-4ac)y^2\\&=X^2-Dy^2=4ak\end{aligned} \tag{3}$$

ここで $D<0$ なので $X^2+|D|y^2=4ak$．よって，$ak<0$ のときは解をもたない．$ak>0$ のときは $0\leq X^2$, $|D|y^2\leq 4ak$ より $|X|\leq 2\sqrt{ak}$, $|y|\leq 2\sqrt{\frac{ak}{|D|}}$ となるので X, y の可能性は有限個である．これらを満たす (X,y) の中で $x=\frac{X-by}{2a}\in\mathbb{Z}$ となるような (x,y) が解．　□

Theorem 3 の証明ではいくつか補題を利用する．

[1]日大理工・院 (前)・数学

Lemma 1　K を体，L を K の有限次ガロア拡大体，$x,\ y\ \in\ L$，$\mathrm{Gal}(L/K)\ =\ \{\sigma_1,\cdots,\sigma_n\}$，$N_{L/K}(x)=\prod_{i=1}^{n}\sigma_i(x)$ とする．このとき $N_{L/K}(xy)=N_{L/K}(x)N_{L/K}(y)$.

Proof　σ_i の準同型性より示せる．

$$\begin{aligned}N_{L/K}(xy)&=\prod_{i=1}^{n}\sigma_i(xy)=\prod_{i=1}^{n}\sigma_i(x)\sigma_i(y)\\&=N_{L/K}(x)N_{L/K}(y)\end{aligned}$$ □

Lemma 2　$a,\ b,\ c\in\mathbb{Z}$, $\gcd(a,b,c)=1$ で $D=b^2-4ac>0$ は平方数ではないとする．このとき $x,y\in\mathbb{Z}$ が式 (2) の解なら $\frac{x-by}{2}\in\mathbb{Z}$.

Proof　b が奇数なら $D\equiv 1\pmod 4$ であり，$\pm4=x^2-Dy^2\equiv x^2-y^2\equiv 0\pmod 4$．よって $x\equiv y\pmod 2$．b が奇数であることを踏まえると $\frac{x-by}{2}\in\mathbb{Z}$.
b が偶数なら $D\equiv 0\pmod 4$ であり，$\pm4=x^2-Dy^2\equiv x^2\equiv 0\pmod 4$．よって $x\equiv 0\pmod 2$．b が偶数であることを踏まえると $\frac{x-by}{2}\in\mathbb{Z}$. □

Lemma 3　Theorem 3 の仮定に加えて $A=X+y\sqrt{D}$ とする．このとき (x,y) が式 (1) の整数解なら，$A\lambda=2ax'+by'+y'\sqrt{D}$ によって得られる (x',y') も式 (1) の整数解.

Proof　$K=\mathbb{Q}(\sqrt{D})$, $\sigma\in\mathrm{Gal}(K/\mathbb{Q})$ を自明でない元とする．(x,y) が式 (1) の整数解なら，$A\sigma(A)=X^2-Dy^2=4ak$ を満たす.

$$\begin{aligned}N_{K/\mathbb{Q}}(\lambda)&=\left(\frac{\alpha+\beta\sqrt{D}}{2}\right)\left(\frac{\alpha-\beta\sqrt{D}}{2}\right)\\&=\frac{\alpha^2-D\beta^2}{4}\end{aligned}$$

は $N_{K/\mathbb{Q}}(\varepsilon)$ か $N_{K/\mathbb{Q}}(\varepsilon)^2$ となり 1 なので，$A\lambda\sigma(A)\sigma(\lambda)=A\sigma(A)=4ak$．したがって $(x',y')\in\mathbb{Z}^2$ を確認すれば良い.

$$\begin{aligned}A\lambda&=(2ax+by+y\sqrt{D})\left(\frac{\alpha+\beta\sqrt{D}}{2}\right)\\&=\left(a\alpha x+\frac{b\alpha+D\beta}{2}y\right)+\left(a\beta x+\frac{\alpha+b\beta}{2}y\right)\sqrt{D}\end{aligned}$$

よって $y'=a\beta x+\frac{\alpha+b\beta}{2}y$, $x'=\frac{\alpha-b\beta}{2}x-c\beta y$．$\lambda$ の仮定から $\alpha^2-D\beta^2=4$ なので，Lemma 2 より $\frac{\alpha\pm b\beta}{2}\in\mathbb{Z}$ であり，$x',\ y'\in\mathbb{Z}$. □

Proof (of Theorem 3)　Theorem 1 と同様に変形し，$X^2-Dy^2=4ak$ $(a\neq 0)$．また，A, K, σ を Lemma 3 と同様に定める．$A\sigma(A)=4ak$ であり，$D=b^2-4ac$ より $D\equiv 0,1\pmod 4$．したがって Theorem 2 より，$\varepsilon=\frac{x_1+y_1\sqrt{D}}{2}>1$ で $\varepsilon^n=\frac{x_n+y_n\sqrt{D}}{2}(n\in\mathbb{Z})$ とすると，$(\pm x_n,\pm y_n)$ が式 (2) の全ての解となる．
$x_n^2-Dy_n^2=-4$ を満たす (x_n,y_n) に対して，

$$\begin{aligned}-1=\frac{x_n^2-Dy_n^2}{4}&=\frac{(x_n+y_n\sqrt{D})(x_n-y_n\sqrt{D})}{4}\\&=N_{K/\mathbb{Q}}\left(\frac{x_n+y_n\sqrt{D}}{2}\right)\end{aligned}$$

であるから，Lemma 1 より次の式が成り立つ.

$$\begin{aligned}N_{K/\mathbb{Q}}\left(\frac{x_{2n}+y_{2n}\sqrt{D}}{2}\right)&=N_{K/\mathbb{Q}}\left(\left(\frac{x_n+y_n\sqrt{D}}{2}\right)^2\right)\\&=N_{K/\mathbb{Q}}\left(\frac{x_n+y_n\sqrt{D}}{2}\right)^2=1\end{aligned}$$

よって $x_1^2-Dy_1^2=-4$ なら，$(\pm x_{2n},\pm y_{2n})$ が $x^2-Dy^2=4$ の全ての解である.
〈1〉　$ak>0$ のとき
$\varepsilon,\ \varepsilon^2>1$ より $\lambda>1$ なので，A が解に対応するとき $2\sqrt{ak}\le A\lambda^n<2\sqrt{ak}\lambda$ を満たすような唯一の $n\in\mathbb{Z}$ が存在し，Lemma 3 よりこの $A\lambda^n$ も解に対応する．よって $A\lambda^n=A'$ とおくと，$2\sqrt{ak}\le A'<2\sqrt{ak}\lambda$ の解それぞれに $\pm\lambda^n$ をかけて得られる (X,y) が式 (3) の全ての解である．また，$A'=X'+y'\sqrt{D}$ $(X',\ y'\in\mathbb{Z})$ とすると，$X'=\frac{A'+\sigma(A')}{2}$ である．$f(t)=t+\frac{4ak}{t}$ について，$f'(t)=1-\frac{4ak}{t^2}$ より $t\ge 2\sqrt{ak}$ で $f(t)$ は単調増加するので，$2\sqrt{ak}\le X'<\alpha\sqrt{ak}$ である．ここで $X'\in\mathbb{Z}$ より，X' の候補は有限個なので，式 (3) を満たす (X',y') は有限個になる．したがって，これらの条件を満たす有限個の A' のうち，$x'=\frac{X'-by'}{2a}\in\mathbb{Z}$ であるような A' に $\pm\lambda^n$ をかけたものが式 (1) の全ての解である.
〈2〉　$ak<0$ のとき
〈1〉と同様の議論によって $2\sqrt{-ak}\le A'<2\sqrt{-ak}\lambda$ を満たすような解それぞれに $\pm\lambda^n$ をかけて得られる (X,y) が式 (3) の全ての解である．$f(s)=s+\frac{4ak}{s}$ について，$f'(s)=1-\frac{4ak}{s^2}$ より $s\ge 2\sqrt{-ak}$ で $f(s)$ は単調増加するので，$0\le X'<\beta\sqrt{-akD}$ である．よってこの場合も X' の候補が有限なので，式 (3) を満たす (X',y') は有限個になる．この中で $x'\in\mathbb{Z}$ である A' に $\pm\lambda^n$ をかけたものが式 (1) の全ての解である． □

References

[1] 雪江明彦,『整数論 1　初等整数論から p 進数へ』，日本評論社 (2013)

[2] 雪江明彦,『整数論 2　代数的整数論の基礎』，日本評論社 (2013)