数理解析研究所講究録
第1665巻 2009年 152-159

解の少ない単数方程式について
Unit equations having few solutions

平田典子 (Noriko Hirata-Kohno)
日本大学理工学部数学科 (Department of Mathematics,
College of Science and Technology, Nihon University)

2007年10月

1 単数方程式の解の個数

単数方程式とは，未知数の範囲を有限次代数体の単数に限る方程式，あるいはその一般化の総称である．単数は乗法群を成すので，整数乗の変数は一次の変数に還元できる，即ち本質的に一次方程式のみ考えれば良い．C. L. Siegel によって導入されたこの方程式は，種数1以上の代数曲線の整数点が有限個である事実などを従える，数論に於ける非自明な有限性定理の代表的なものといえよう．

K を $[K:\mathbb{Q}]=d<\infty$ 次の代数体とする．S を K の素点の有限集合で，全ての無限素点と，有限個（無しでも良い）の有限素点を含むものとする．$s=\#S<\infty$ とおく．
S-整数 $\mathfrak{O}_S:=\{x\in K : v(x)\geq 0\, for\, \forall v\notin S\}$
S-単数 $U_S:=\{x\in K : v(x)=0\, for\, \forall v\notin S\}$ と記する．

Definition 1 $\alpha_1,\alpha_2\in K^*:=K-\{0\}$ に対し，x,y を未知数とする次の方程式を (S-) 単数方程式という．

$$\alpha_1 x+\alpha_2 y=1 \quad in \quad x,y\in U_S. \tag{1}$$

基本的な事実は次で保証されている．

Theorem 1 (Siegel-Mahler-Lang [22]) 単数方程式 $\alpha_1 x+\alpha_2 y=1$ in $x,y\in U_S$ の解は有限個に限る．

2変数の単数方程式の解の有限性は，Thue-Siegel-Roth-Mahler の定理と呼ばれる，代数的数を有理数で近似するディオファントス近似によって証明される．この定理は J. Liouville が始め，A. Thue が本質的な改良を施し，C. L. Siegel, F. Dyson らがさらに改良し，K. F. Roth が最良近似に到達，K. Malher が S-単数が扱えるよう p 進付値版を確立させたディオファントス近似不等式を総称する．

また，$n(\geq 3)$ 変数の単数方程式の解の有限性は，W. M. Schmidt の部分空間定理という，20世紀で最も重要な整数論の定理の一つから従う．

まず Roth の定理を述べよう．

Theorem 2 (Roth の定理 [19]) α を次数 $d(\geq 2)$ の代数的数とする．
任意の $\varepsilon > 0$ に対して，次の不等式を満たす有理数 $\frac{p}{q}$ $(q > 0)$ は有限個に限る :

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{2+\varepsilon}}.$$

この $2+\varepsilon$ は最良である，つまり，これ以上小さい指数では反例が生ずる．そして，この証明は簡単ではない．さらに，指数 $2+\varepsilon$ をもう少し精密なオーダーで表示しようとすると，例えば次のような問題を考えることになるが，この程度でも既に未解決問題である．

Conjecture 1 (Open) α を次数 $d(\geq 3)$ の代数的数とする．このとき α にのみ依存する定数 $\kappa_0(\alpha) > 0$ が存在して，次が成立する．$\kappa > \kappa_0(\alpha)$ を満たす任意の κ に対して，

$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2(\log q)^\kappa}$ をみたす有理数 $\frac{p}{q}$ $(q > 0)$ は有限個に限る．

以下，代数的数の「高さ」という重要な概念を定義する．

Definition 2 射影空間の代数的な点（有理点）$X \in \mathbb{P}^N(\overline{\mathbb{Q}})$ に対して $X = (x_0, \ldots, x_N) \in \mathbb{P}^N(K)$ となる有限次代数体 K を取る．

$$h(X) := \frac{1}{[K:\mathbb{Q}]} \sum_v n_v \log(\max\{|x_0|_v, \ldots, |x_N|_v\})$$

とおき，X の（絶対的射影的）対数的高さという．ここで $n_v = [K_v : \mathbb{Q}_v]$ は *local degree* とする．

$\alpha \in \overline{\mathbb{Q}}$ に対して $h(\alpha) := h(1 : a)$ と定める．

この定義は，射影座標の取り方や，有限次代数体 K の選び方によらないことが分かっている．本質的な性質は，与えられた正の数 D と H に対し，$\deg \alpha \leq D$ かつ $h(\alpha) \leq H$ を満たす代数的数 $\alpha \in \overline{\mathbb{Q}}$ は有限個であり，なおかつ，α の満たし得る定義方程式の全てを具体的に書き下すことが出来るという事実である．いわば，α はこれこれの解となる代数的数である，と決定できるわけである．

「高さ」が重要なのは，距離のような性質を持つ点と，具体的に決められる有限個の代数的数のうちの一つに α は等しいという「等式」を $\deg \alpha \leq D$ かつ $h(\alpha) \leq H$ という「不等式」から得ることを可能にするような性質を持つ概念であるという点である．距離のような性質であることは，もともと付値を用いて定義されていることから自然に従うが，それでも，各付値において $N+1$ 個の座標の絶対値の最大値を取っていることが，後者の性質を与えるカギになっているのである．
高さの導入により，「不等式から等式が出る」という画期的な原理が有理点の世界には成立する．

そうすれば，等式の証明が難しい状況でも，不等式を証明すれば欲しい結論が得られるのである．不等式を示すには解析の手法が有効であるから，「高さ」のおかげで一気に道具の範囲が広がることになった．
次もあわせて定義する．

Definition 3 射影空間の代数的な点（有理点）$X=(x_0,\ldots,x_N)\in\mathbb{P}^N(K)$ に対し，X の（絶対的射影的）指数的高さとして $H(X):=\exp(h(1,x_1,\cdots,x_N))$ を定める．*Affine* 座標 $(x_1,\cdots,x_N)\in K^N$ に対しては $X=(1,x_1,\ldots,x_N)\in\mathbb{P}^N(K)$ とみなして $H(X)$ を定義する．

さて W. M. Schmidt の部分空間定理を述べる．

Theorem 3 (The Subspace Theorem, W. M. Schmidt [20] [21])
$N(\geq 2)$ 個の K 係数一次形式 $L_i(X)=a_{i1}X_1+\cdots+a_{iN}X_N$ $(i=1,\cdots,N)$ は一次独立であるとする．任意の $\delta>0$ をとる．次の不等式を考える：

$$|L_1(x)\cdots L_N(x)|\leq H(x)^{-\delta}. \tag{2}$$

このとき，不等式 (2) の整数解 $x=(x_1,\cdots,x_N)\in\mathbb{Z}^N$ は，codim≥ 1 の有限個の $\mathbb{Q}$ 係数線形部分空間 $T_1,\cdots,T_t\subset\mathbb{Q}^N$ の和集合 $T_1\cup\cdots\cup T_t$ に含まれる．

この定理で重要なのは，(2) の整数解になる点が codim≥ 1 という，ぺしゃんこの空間にしか存在しないという事実である．(2) の左辺は内積いわば距離であるから，N 次元での代数的数座標の点と距離の近い有理数座標の点はあまり無いということを示しているし，その「近さ」を「近似する有理点の高さ」でコントロールするのがディオファントス近似なのである．

部分空間定理からは $n(\geq 3)$ 変数の単数方程式の解の有限性が出るが，現在は次の形に一般化されているので，そちらを以下に述べることにする．

2 一般型単数方程式

下記の定理が Evertse-Schlickeweri-Schmidt [13] によって得られている．

まず K を標数 0 の体とする（複素数体でも良い訳であるから，「係数の代数性」は不要となる）．$(K^*)^n$ は K^* の n 個の直積とする；即ち乗法は成分ごとに $(x_1,\cdots,x_n)\times(y_1,\cdots,y_n)=(x_1y_1,\cdots,x_ny_n)$ と定められているとする．

Γ を $(K^*)^n$ の乗法部分群で，rank $r<\infty$ なるものとする．すなわち $u_1,u_2,\cdots,u_r\in\Gamma$ が存在し次を満たす：全ての $x=(x_1,\cdots,x_n)\in\Gamma\subset(K^*)^n$ に対して $x^z=u_1^{z_1}\cdots u_r^{z_r}$ をみたす整数 $z,z_1,\cdots,z_r\in\mathbb{Z}$ が存在する．

代数的数 $\alpha_1,\cdots,\alpha_n\in K^*$ に対して，一般型単数方程式とは

$$\alpha_1x_1+\cdots+\alpha_nx_n=1 \quad \text{in } x:=(x_1,\cdots,x_n)\in\Gamma \qquad \text{かつ } \sum_{i\in I}\alpha_ix_i\neq 0 \tag{3}$$

ただし I は $\{1\cdots n\}$ の全ての non-empty な真の部分集合を走るとする．

上記の単数解 $x=(x_1,\cdots,x_n)$ を "non-degenerate" なる解と称する．それ以外の解，つまり，ある I に対する vanishing subsum $\sum_{i\in I}\alpha_i x_i=0$ を満たす解を "degenerate" なる解と言う．

未知数を Γ 内に求める，一般型単数方程式 $\alpha_1x_1+\cdots+\alpha_nx_n=1$ の non-degenerate 解の個数を $N(\alpha_1,\cdots,\alpha_n:\Gamma)$ とおく．

代数体 K に属する，0 でない係数 $\alpha_1,\cdots,\alpha_n$ に対し，U_S に未知数をとる単数方程式（一般型ではない）$\alpha_1x_1+\cdots+\alpha_nx_n=1$ の non-degenerate な解の個数を $N(\alpha_1,\cdots,\alpha_n:(U_S)^n)$ と表す．

Theorem 4 (Evertse-Schlickeweri-Schmidt[13])
一般型単数方程式 $\alpha_1x_1+\cdots+\alpha_nx_n=1$ *in* $x=(x_1,\cdots,x_n)\in\Gamma$ を考える．このとき $N(\alpha_1,\cdots,\alpha_n:\Gamma)\le c^{r+1}$ である．ただし $c=c(n)=\exp\left((6n)^{3n}\right)$.

この定理には G. Rémond [18] により更に一般の場合に対し，別証明（方法は [14] および P. Vojta の不等式に依る）がある．上記の定理の場合に限ったとき，解の個数の上からの評価は $2^{(n^{4n^2})\times(r+1)}$ である．これらは，いずれも $N(\alpha_1,\cdots,\alpha_n:\Gamma)$ とおいた解の個数が実際には n と r にのみ依存し，係数 $\alpha_1,\cdots,\alpha_n$ および Γ の他の情報には依存しないことを示す．そして，この n と r への依存は，いずれも必要である．

$n=2$ の場合の Beukers-Schlickewei[2] による 1996 年の評価はこれよりも良く，単数解の個数は $2^{8(r+2)}$ 個以下となる．

単数方程式の non-degenerate な解が常に有限個である一方，好きなだけ多くの解をもつ単数方程式を構成することも出来る．例えば Erdős-Stewart-Tijdeman [3] の結果とその Konyagin-Soundararajan[15] による改良として次の定理がある．この場合，解析数論つまり素数の分布の話に帰着させるため，代数的な条件下での単数方程式の扱いに，現状では限られている．

Theorem 5 (Erdős-Stewart-Tijdeman[3]) 絶対定数 $c>0$ が存在して次を満たす．$K=\mathbb{Q}$ とし，任意の自然数 s を取る．このとき $s-1$ 個の有理素数を含む，付値の集合 S が存在して次が成立する．

$$N(1,1:(U_S)^2)\ge\exp\left(c(s/\log s)^{1/2}\right).$$

Theorem 6 (Konyagin-Soundararajan[15]) 絶対定数 $0<\gamma<2-\sqrt{2}$ が存在して次を満たす．$K=\mathbb{Q}$ とし，任意の自然数 s を取る．このとき $s-1$ 個の有理素数を含む，付値の集合 S が存在して次が成立する．

$$N(1,1:(U_S)^2)\ge\exp\left(s^{\gamma}\right).$$

これから，U_S に解を持つ単数方程式の解の個数について，S によらない uniform upper bound は存在し得ないことが分かる．同様の結果は $n\ge3$ の場合に於いても一部考察されている [10].

3 解の少ない単数方程式

次に，少ない個数しか解を持たない単数方程式を考える．実は大抵の単数方程式は，殆どが非常に少数の解しか持たないと考えられている．

まず次の同値類を定義する.

Definition 4 (Γ-equivalence class)
Γ を 有限ランク $r < \infty$ の $(K^*)^n$ の部分群とする.
$\alpha := (\alpha_1, \alpha_2, \cdots, \alpha_n) \in (K^*)^n$ と $\beta := (\beta_1, \beta_2, \cdots, \beta_n) \in (K^*)^n$ が Γ-*equivalent* とは, ある $\sigma \in \Gamma$ が存在して $\beta = \sigma \cdot \alpha$ (乗法は *coordinatewise*) を満たすときに言うとする.
α と β が Γ-*equivalent* のとき $\alpha \sim \beta$ と記する.

$\alpha \sim \beta$ ならば, 単数方程式 $\alpha_1 x_1 + \cdots + \alpha_n x_n = 1$ および $\beta_1 x_1 + \cdots + \beta_n x_n = 1$ は, 明らかに同じ個数の解をもつ.

代数体 K に対して知られている結果としては, まず 1988 年の Evertse-Győry-Stewart-Tijdeman, 次いで Bérczes[1] らにより一般化された次の主張がある :

Theorem 7 (Evertse-Győry-Stewart-Tijdeman[10]) 無限素点を全て含む, 代数体 K の素点の有限集合 S を固定したとき, 有限集合 $A \subset (K^*)^2$ が存在して, A のどの元にも $(U_S)^2$-*equivalent* ではない任意の係数 $(\alpha_1, \alpha_2) \in (K^*)^2$ に対する単数方程式 $\alpha_1 x_1 + \alpha_2 x_2 = 1$ の解の個数は 2 個以下である.

この結果は ineffective 即ち例外集合 A の元は決定できない. また, この 2 個という数が best possible であることは非常に簡単に分かる.

さて, ここで我々の定理を述べる. 一般型の単数方程式に対する主張である.

Theorem $n = 2$ とする. Γ を $(K^*)^2$ の有限ランク r の部分群とする. 未知数を $x = (x_1, x_2) \in \Gamma$ にとる一般型の単数方程式 $\alpha_1 x_1 + \alpha_2 x_2 = 1$ を考える. このとき有限集合 $B \subset (K^*)^2$ で次の性質を持つものが存在する.
どの $(\beta_1, \beta_2) \in B$ に対しても決して Γ-*equivalent* にならないような, 任意の $(\alpha_1, \alpha_2) \in (K^*)^2$ に対して

$$N(\alpha_1, \alpha_2 : \Gamma) \leq 2$$

かつ $\#B \leq \exp(50^2(r+2))$ である.

証明には超幾何級数法を用いて, 精密な近似を与えることによって得られる. ただし, この超幾何級数法による証明は $n = 2$ のときにしか適用できない.

この定理の意味は, 有限集合 B に属さない元に代表される Γ-equivalent classes 内の係数を持つ単数方程式の解は, 必ず 2 個以下に押さえられると言うことである. この 2 個という数は, $\alpha_1 = \alpha_2$ の場合でも (x, y) と (y, x) を同一視しない数え方である.

$n = 2$ の場合であるから, $n \geq 3$ の場合とは異なり, A. Baker の linear forms in logarithms を用いて集合 B の元を具体的に effective に記述可能であり, 現在計算中である. ただし linear forms

in logarithms を用いるためには，現時点では代数的条件が必要である；即ち一般型の単数方程式ではなく，代数体 K 係数の単数方程式で U_S に解を持つ場合に，考察可能である．この場合，S の中の素点の大きさに評価は依存する．

effective に記述することが代数的条件抜きに出来るかどうか，これはいわゆる specialization argument の類似をしうるかどうか，という問題になる．実は非常に面白い問題であり，考察進展中である．

4 指数方程式への拡張

K は標数 0 の体，Γ を $(K^*)^n$ の，rank $r < \infty$ の乗法部分群とする．$n \geq 2$ に対して $f_1, \cdots, f_R \in K[x_1, \cdots, x_n] - \{0\}$ とする．未知数 $x = (x_1, \cdots, x_n) \in \Gamma$ に対して，連立方程式

$$f_i(x_1, \cdots, x_n) = 0 \quad (i = 1, \cdots, R)$$

を考える．

Definition 5 変数 λ に対し，$x = (x_1, \cdots, x_n)$ が次の条件を満たすときに *degenerate* 解と称する．$gcd(c_1, \cdots, c_n) = 1$ なる整数の組 $c_1, \cdots, c_n \in \mathbb{Z}$ が存在して，λ に関して恒等的に

$$f_i(\lambda^{c_1} x_1, \cdots, \lambda^{c_n} x_n) = 0 \quad (i = 1, \cdots, R) \tag{4}$$

すなわち，λ に関して $f_i(\lambda^{c_1} x_1, \cdots, \lambda^{c_n} x_n)$ を展開したときに，λ の累乗で左辺を整理するときに現れる係数 ($x_1, \cdots, x_n$ の多項式となる) が恒等的に消える，ということを意味するとする．*degenerate* 解ではない解を *non-degenerate* 解と言う．

[8][16] の議論より，つぎの一般化が従う．

Theorem 8 連立方程式 *(4)* の *non-degenerate* 解 x は有限個である．

$X = \{(x_1, \cdots, x_n) \in (K^*)^n : f_i(x_1, \cdots, x_n) = 0 \quad (i = 1, \cdots, R)\}$ とおく．S. Lang により予想されていた問題における M. Laurent[16] の torus の場合の解決，その発展である Evertse らの議論 [8][25] により，解 $x \in \Gamma$ は次の形の，有限個の coset の和集合 $x_1 H_1 \cup \cdots \cup x_t H_t$ に含まれる．ここで $xH = \{x \times y : y \in H\}$，$x \in \Gamma$ であり，また H は $(K^*)^n$ の既約な代数部分群（乗法群）で $xH \subset X$ となるものとする．X は有限集合というわけではない，あくまで我々の設定は $(x_1, \cdots, x_n) \in \Gamma$ の場合に限るのであり，$X \cap \Gamma$ を考えていることになる．Lang の有限性予想の $\mathbb{G}_m^n$ の場合である．

有限個の coset の個数の評価のうち，[25] にあるものは，$A = \dfrac{(n+d)!}{n!d!}$ とおくと

$$t \leq c(n,d)^{r+1}, \quad c(n,d) \leq \exp\left((6dA)^{5dA}\right)$$

である．

さて $x \in \Gamma$，$xH \subset X$，$\dim H > 0$ の場合，H_0 を次元 1 の H の既約な代数部分群としたとき，$gcd(c_1, \cdots, c_n) = 1$ なる整数の組 $c_1, \cdots, c_n \in \mathbb{Z}$ が存在して，$H_0 = \{(\lambda^{c_1}, \cdots, \lambda^{c_n}) : \lambda \in K^*\}$ と

書ける．従って $xH_0 = \{(x_1\lambda^{c_1}, \cdots, x_n\lambda^{c_n}) : \lambda \in K^*\} \subset xH \subset X$ となってしまい，λ に関して恒等的に 0 になる，つまり $f_i(\lambda^{c_1}x_1, \cdots, \lambda^{c_n}x_n) = 0 \quad (i = 1, \cdots, R)$ の場合に至り，degenerate 解となる．また逆に x が degenerate 解のときは，ある次元 1 の H_0 が存在して $xH_0 \subset X$ となる．

従って，$x \in \Gamma$，$xH \subset X$，$\dim H > 0$ の場合とは，degenerate 解の場合に一致する．つまり non-degenerate 解は $\dim H = 0$ の場合，すなわち $H = (1, \cdots, 1)$ の場合に限られる．これより xH の coset の個数の有限性が，そのまま x の個数の有限性を従える．以上で指数方程式の場合の解の個数の有限性が証明される．あとは，個数の評価を適用させる議論を行えば良い．

これに我々の超幾何級数法を適用すると，以下の結果が得られる．

各多項式 f_i の total 次数の最大値を d とおく．これは X の次数に相当する数である．

Theorem $n = 2$ とする．Γ を $(K^*)^2$ の有限ランク r の部分群とする．未知数を $x = (x_1, x_2) \in \Gamma$ にとる連立方程式 *(4)* の *non-degenerate* 解 x は有限個で $\exp(5d^{2d^3}(r+2))$ 個以下である．

単数方程式の評価を経由せずに，ダイレクトに近似から評価を再計算すると．さらに良い評価が得られるはずである．

参考文献

[1] A. Bérczes, On the number of solutions of norm form equations, Period. Math. Hungar. 43, 2001, 165–176.

[2] F. Beukers & H. P. Schlickewei, The equation $x + y = 1$ in finitely generated groups, Acta Arith. 78, 1996, 189-199.

[3] P. Erdős, C.L. Stewart & R. Tijdeman, Some Diophantine equations with many solutions, Compositio Math. 66, 1988, 37–56.

[4] J. -H. Evertse, On equations in S-units and the Thue-Mahler equation, Invent. Math. 75, 1984, 561–584.

[5] J. -H. Evertse, Decomposable form equations with a small linear scattering, J. reine angew. Math. 432, 1992, 177-217.

[6] J. -H. Evertse, Symmetric improvements of Liouville's inequality. J. reine angew. Math. 527, 2000, 69–95.

[7] J. -H. Evertse, Points on subvarieties of tori, in A Panorama of Number Theory (ed. G. Wüstholz), Cambridge Univ. Press, 2002, 214–230.

[8] J. -H. Evertse, Linear equations with unknowns from a multiplicative group whose solutions lie in a small number of subspaces, Indag. Math. 15, 2004, 347-355.

[9] J. -H. Evertse & R. G. Ferretti, Diophantine inequalities on projective varieties, Intern. Math. Res. Not. , 2002, 1295–1330.

[10] J. -H. Evertse, K. Győry, C. L. Stewart & R. Tijdeman, On S-unit equations in two unknowns, Invent. Math. 92, 1988, 461-477.

[11] J. -H. Evertse & H. P. Schlickewei, The Absolute Subspace Theorem and linear equations with unknowns from a multiplicative group, in Number Theory in Progress, I, (eds. K. Győry, H. Iwaniec, J. Urbanowicz), Walter de Gruyter, 1999, 121–142.

[12] J. -H. Evertse & H. P. Schlickewei, A quantitative version of the Absolute Subspace Theorem, J. reine angew. Math. 548, 2002, 21–127.

[13] J. -H. Evertse, H. P. Schlickewei & W.M. Schmidt, Linear equations in variables which lie in a multiplicative group, Ann. Math. 155, 2002, 1–30.

[14] G. Faltings & G. Wüstholz, Diophantine approximations on projective spaces, Invent. Math., 116, 1994, 109–138.

[15] S. Konyagin & K. Soundararajan Two S-unit equations with many solutions, Journal of Number Theory, 124 (1), 2007, 193-199.

[16] M. Laurent, Équations diophantiennes exponentielles, Invent. Math. 78, 1984, 299-327.

[17] A. N. Parshin & I. R. Schfarevich (eds.), N. I. Fel'dman & Yu. V. Nesterenko (authors), Number Theory IV, Encyclopaedia of Mathematical Sciences Vol 44, 1998.

[18] G. Rémond, Sur les sous-variétés des tores, Compos. Math. 134, 2002, 337-366.

[19] K. F. Roth, Rational approximations to algebraic numbers, Mathematika 2, 1955, 1–20, Corrigendum, ibid., 168.

[20] W. M. Schmidt, Norm form equations, Ann. of Math., 96, 1972, 526–551.

[21] W. M. Schmidt, Diophantine approximation, Lecture Notes in Math., 785, Springer, 1980.

[22] W. M. Schmidt, Diophantine approximation and Diophantine Equations, Lecture Notes in Math., 1467, Springer, 1991.

[23] A. Thue, Über Annäherungswerte algebraischer Zahlen, J. reine angew. Math. 135, 1909, 184–305.

[24] M. Waldschmidt, Nombres transcendents et groupes algébriques, Astérisque 69/70, 1979.

[25] G. Wüstholz, A Panorama of Number Theory, Cambridge Univ. Press, 2002.