P-10

Thue-Mahler 方程式の整数解の個数とその応用

The number of solutions to the Thue-Mahler equation and its applications

○中村建太 [1]
Kenta Nakamura

Abstract: We show that an upper bound for the number of solutions to the S-unit equation gives a bound for the number of solutions to the Thue–Mahler equation, as well as a bound for the number of S-Diophantine quadruples.

1. S-単数方程式の解の有限性

定義 1. K を代数体とし，$\mathcal{O}_K$ を K の整数環とする．また，S を $\mathcal{O}_K$ の素イデアルの有限個の集合とする．このとき，素イデアル分解をしたときに現れる素イデアルが全て S に含まれるような K の元を **S-単数**という．

定理 2. ([2]) K を代数体とし，$m=[K:\mathbb{Q}]$ とする．λ,μ を 0 でない K の元とし，S を $\mathcal{O}_K$ の r 個の素イデアルの集合とする．このとき，方程式

$$\lambda x+\mu y=1,\ \ x,y \text{ は } S\text{-単数} \tag{1}$$

は高々$3\times 7^{3m+2r}$ 個の解を持つ．

定理 2 を使うことで，**Thue-Mahler 方程式**

$$F(x,y)\mathcal{O}_K=\mathfrak{p}_1^{k_1}\cdots\mathfrak{p}_r^{k_r},\ \ x,y\in\mathcal{O}_K,\ k_1,\cdots,k_r\in\mathbb{Z}$$

の解の個数の上界を示すことができる．より正確には，$\{\mathfrak{p}_1,\cdots,\mathfrak{p}_r\}$ を（空でもよい）相異なる素イデアルの集合としたとき，次数 $n\geq 3$ の斉次多項式 $F(X,Y)\in\mathcal{O}_K[X,Y]$ に対して、高々 $7^{n^3(3m+2r)}$ 個の解を持つ．([2])

注意. 無限素点と呼ばれるものの個数を用いると，(1) 式や Thue-Mahler 方程式の解の個数の上界を低くすることができる．

2. S-ディオファントスの組

定理 2 は S-ディオファントスの組の有限性にも応用することができる．本来**ディオファントスの m 組**とは，相異なる正整数の組 $(a_1,\cdots,a_m)$ が，$1\leq i<j\leq m$ となる任意の i,j に対して a_ia_j+1 が平方数となることである．最近の研究で，ディオファントスの 5 組が存在しないことが証明された．([3])

このディオファントスの組の定義の平方数の部分を S-単数に変えたものが **S-ディオファントスの組**である．

定義 3. S を素数の有限集合として固定する．このとき相異なる m 個の正整数の組 $(a_1,\cdots,a_m)$ が **S-ディオファントスの m 組**であるとは，$1\leq i<j\leq m$ となる任意の i,j に対して a_ia_j+1 の全ての素因数が S に含まれることである．

特別な S に対しては以下が知られている．

定理 4. ([6]) $S=\{2,q\}$ で $q\equiv 3\pmod 4$ なら S-ディオファントスの 4 組は存在しない．

3. S-ディオファントスの 4 組の有限性

集合 S を任意にした場合の S-ディオファントスの 4 組については以下の定理がある．

定理 5. ([4]) S を r 個の素数の集合とする．S-ディオファントスの 4 組は，高々$e^{27398+5136r}$ 個である．

Proof. S-ディオファントスの 4 組の個数を求める問題を，S-単数方程式の解の個数を求める問題に帰結させる．

(a,b,c,d) を S-ディオファントスの 4 組とし $a<b<c<d$ とする．また $s_1,\cdots,s_6$ を以下のようにおく．

$$ab+1=s_1,\quad ac+1=s_2,\quad ad+1=s_3,$$
$$bc+1=s_4,\quad bd+1=s_5,\quad cd+1=s_6.$$

すると，

$$\begin{aligned} abcd &= (s_1-1)(s_6-1)=s_1s_6-s_1-s_6+1\\ &= (s_2-1)(s_5-1)=s_2s_5-s_2-s_5+1\\ &= (s_3-1)(s_4-1)=s_3s_4-s_3-s_4+1 \end{aligned}$$

となる．以上より，

$$\begin{cases} s_1s_6-s_1-s_6-s_2s_5+s_2+s_5=0 & (2)\\ s_1s_6-s_1-s_6-s_3s_4+s_3+s_4=0 & (3) \end{cases}$$

という S-単数連立方程式が得られた．この連立方程式を解いて一つの解 $(s_1,\cdots,s_6)$ が求まったとすると，

$$a=\sqrt{\tfrac{(s_1-1)(s_2-1)}{s_4-1}},\quad b=\sqrt{\tfrac{(s_1-1)(s_4-1)}{s_2-1}},$$
$$c=\sqrt{\tfrac{(s_2-1)(s_4-1)}{s_1-1}},\quad d=\sqrt{\tfrac{(s_5-1)(s_6-1)}{s_4-1}},$$

という解 (a,b,c,d) が高々一つ求まる．

従って，連立方程式 (2), (3) の解の個数を求めれば良い．ここで $\Gamma\subset\mathbb{Q}^*$ を S により生成される乗法群とし，(2) 式の部分和が 0 になるかならないかで場合分けする．

(i) (2) 式の部分和が 0 にならないとき．

$s_1s_6=y_1,\ s_1=y_2,\ s_6=y_3,\ s_2s_5=y_4,\ s_2=y_5,\ s_5=y_6$ とおくことで得られる S-単数方程式

$$y_1-y_2-y_3-y_4+y_5+y_6=0$$

1: 日大理工・院 (前)・数学

の $\mathbb{P}^5(\Gamma)$ における解の個数は [1] の定理 6.2 の証明の議論より高々$e^{25329+4616.3r}$ 個である．また一つの射影解に対して一つの解 (s_1, s_2, s_5, s_6) が対応していることに注意しておく．実際，(s_1, s_2, s_5, s_6) と (s_1', s_2', s_5', s_6') が一つの射影解から得られたとすると，$\rho \in \mathbb{Q}^*$ が存在し $s_1 = \rho s_1'$, $s_6 = \rho s_6'$, $s_1 s_6 = \rho s_1' s_6'$ と書けるため，$\rho = 1$ が分かる．

(ii) (2) 式の部分和が 0 になるとき．

まず何項の部分和で 0 になるかを考える．$s_i \neq 0$ なので一項が 0 になるということはない．二項の和が 0 になることは以下の場合分けにより，ないことが分かる．

- $s_i = s_j (i \neq j)$ の場合は，$a < b < c < d$ に矛盾する．
- $s_i = s_1 s_6$ の場合は，$s_1 = ab + 1 \geq 2 \cdot 1 + 1 > 2$ なので $s_i = s_1 s_6 > 2 s_6 > s_6 \geq s_i$ となり矛盾．
- $s_i = s_2 s_5$ の場合は，$s_i = s_2 s_5 > abcd > cd + 1 = s_6 \geq s_i$ となり矛盾．
- $s_1 s_6 = s_2 s_5$ の場合は，$(ab+1)(cd+1) = (ac+1)(bd+1) \Leftrightarrow ab + cd = ac + bd \Leftrightarrow (a-d)(b-c) = 0$ で $a = d$ または $b = c$ となり矛盾．

一項，二項の和が 0 にならないということから，四項，五項の和が 0 になることもない．よって三項の部分和が 0 になる場合のみを考えればよい．その三項間に $s_1 s_6$ と $s_2 s_5$ が一緒に存在しているかどうかを考える．一緒に存在していないと仮定すると，$s_1 s_6 = \pm s_i \pm s_j$ が成り立つ．しかし $s_1 s_6 > 2 s_6 > s_i + s_j$ となり，$s_1 s_6 \neq \pm s_i \pm s_j$ で矛盾する．

以上の結果から

$$s_1 s_6 - s_5 s_2 = s_1,\ s_6 = s_5 + s_2 \tag{4}$$

という三項間の関係が分かる．注意として，(4) 式以外のパターンは $s_1 < s_2 < s_5 < s_6$ に矛盾する．例えば，$s_1 = s_2 + s_5$ というようなパターンは s_i たちの大小関係から，$s_1 < s_2 + s_5$ であるから成立しない．次に $s_1 s_6 = y_1$, $s_2 s_5 = y_2$, $s_1 = y_3$ として得られる S-単数方程式 $y_1 - y_2 = y_3$ は，定理 2 より高々$3 \times 7^{3+2r} = e^{(\log 3 + 3 \log 7) + 2r \log 7}$ 個の解 $[y_1 : y_2 : y_3] \in \mathbb{P}^2(\Gamma)$ を持つ．ここで一個の射影解 $[y_1 : y_2 : y_3]$ に対して一つの s_6 が得られる．実際 $(s_1, s_2, s_5, s_6), (s_1', s_2', s_5', s_6')$ が一個の射影解から得られたとすると，$\rho \in \mathbb{Q}^*$ が存在し $s_1 = \rho s_1'$, $s_1 s_6 = \rho s_1' s_6'$ とできることから，$s_6 = s_6'$ となる．つまり s_6 には高々$e^{(\log 3 + 3 \log 7) + 2r \log 7}$ 個の可能性があり，(4) 式より，その各々に対して方程式 $s_6 = s_2 + s_5$ がある．この方程式の解 (s_2, s_5) は再度定理 2 より高々$e^{(\log 3 + 3 \log 7) + 2r \log 7}$ 個の解があり，結局 (ii) の場合，高々$e^{2(\log 3 + 3 \log 7) + 4r \log 7}$ 個の解が得られる．

(i), (ii) より (2) 式の解の個数は高々$e^{25329+4616.3r} + e^{2(\log 3 + 3 \log 7) + 4r \log 7}$ である．最後に (3) 式について考える．今までの議論から，(s_1, s_6) には $e^{25329+4616.3r} + e^{2(\log 3 + 3 \log 7) + 4r \log 7}$ 個の可能性がある．つまり (3) 式は $a \in \mathbb{Q}$ を定数として，

$$s_3 s_4 - s_3 - s_4 = a \tag{5}$$

の形の方程式が $e^{25329+4616.3r} + e^{2(\log 3 + 3 \log 7) + 4r \log 7}$ 個ある，と考えることができる．ここで (5) 式には部分和が 0 になる解は存在しない．実際，$s_3 s_4 = s_3$ または s_4 なら $s_3 = 1$ もしくは $s_4 = 1$ となり矛盾．$s_3 + s_4 = 0$ なら s_3, s_4 のどちらかが 0 以下となり矛盾．よって (5) 式は [1] の定理 6.2 の議論から高々$e^{2069+518.8r}$ 個の解を持つ．以上をまとめると，$(e^{25329+4616.3r} + e^{2(\log 3 + 3 \log 7) + 4r \log 7}) \times e^{2069+518.8r} \leq e^{27398+5136r}$ が成り立つ．　□

注意. 定理 5 の証明内で (4) 式は $2 \notin S$ のとき解を持たない．実際，$2 \notin S$ なら s_6 は奇数で $s_2 + s_5$ は偶数となるためである．さらに $r = 2$ のときも (4) 式は解を持たない．なぜならば，上記の結果から $S = \{2, p\}$ としてよく，すると $s_6 = s_2 + s_5$ は，$2^{\alpha_6} p^{\beta_6} = 2^{\alpha_2} p^{\beta_2} + 2^{\alpha_5} p^{\beta_5}$ と書ける．ここで両辺を $2, p$ で割り切れるだけ割ったとき，$2, p$ で割り切れる項の数はそれぞれ一項である．そうでなければ素因数分解の一意性に矛盾する．よって $x, y \in \mathbb{N}$ を用いて $2^x - p^y = \pm 1$ と変形できる．(もう一つの可能性 $2^x p^y \pm 1 = \pm 1$ は明らかに成立しない.) この方程式に解があるのは [5] より $p = 3$ のみであるが，定理 4 より $\{2, 3\}$-ディオファントスの 4 組は存在しない．従って $2 \notin S$ または $r = 2$ のとき (ii) は起きないので，定理 5 の上界をさらに低くすることができる．

4. 参考文献

[1] Francesco Amoroso and Evelina Viada, *Small points on subvarieties of a torus*, Duke Math. J. **150** (2009), no. 3, 407–442. MR 2582101

[2] J.-H. Evertse, *On equations in S-units and the Thue-Mahler equation*, Invent. Math. **75** (1984), no. 3, 561–584. MR 735341

[3] Bo He, Alain Togbé, and Volker Ziegler, *There is no Diophantine quintuple*, Trans. Amer. Math. Soc. **371** (2019), no. 9, 6665–6709. MR 3937341

[4] Florian Luca and Volker Ziegler, *A note on the number of S-Diophantine quadruples*, Commun. Math. **22** (2014), no. 1, 49–55. MR 3233726

[5] Preda Mihăilescu, *Primary cyclotomic units and a proof of Catalan's conjecture*, J. Reine Angew. Math. **572** (2004), 167–195. MR 2076124

[6] László Szalay and Volker Ziegler, *S-Diophantine quadruples with $S = \{2, q\}$*, Int. J. Number Theory **11** (2015), no. 3, 849–868. MR 3327847