Effective method
and applications in Diophantine problems

日本大学理工学部 * 平田典子
Noriko Hirata-Kohno
Dept. of Math., College of Science and Tech., Nihon University

1 Introduction

この数年，数論の諸定理に対する証明が **effective** であるか否か，そして結果を **explicit** に示せるかが，応用上の理由により話題になっている．ディオファントス近似で effective 或いは explicit という成果を得るには，何よりも Alan Baker の対数一次形式（いわゆる Baker 理論）そして Padé 近似（Hermite-Padé 近似），加えて超越近似が有効である．近似そのものの証明も面白い．

本稿は H. G. Senge-E. G. Straus 及び C. L. Stewart の結果に関し，京都大学の尾高悠志氏から受けた質問がきっかけになって計算したもの，そしてディオファントス問題における **effectivity** 即ち effective な成果を与える証明方法について簡単に概説したものである．Shanta Laishram 氏，川島 誠氏との共同研究を含む．

1973 年，Senge と Straus は Pisot 数の考究から発展したディオファントス問題の一つとして，次の問を考えた [18]．Stony Brook で開催された Summer School (1969) で提出された問題が発端になっている．

* 東京都千代田区神田駿河台 1-8-14 (hiratakohno.noriko at nihon-u.ac.jp)

Question 1.1. 正整数を 2 つの異なる正整数 a, b で展開したときに，a 進展開における各桁に現れる数と，b 進展開における各桁に現れる数との総和が有界になるような正整数は，無限個存在し得るか？

この Question 1.1に対し，[18] では「K. Mahler や S. Lang の，1 つの代数的数を（固定された代数体に属する）代数的数で近似するディオファントス近似で答えを出す」と述べられているが，Senge と Straus の用いたこの近似は effective ではない．その後に Stewart [20] が対数一次形式を適用して Senge-Straus の結果を effective にしたが，各情報への explicit な依存度を見るため，少々計算したものの報告である．なお，現存する方法のうち，effective かつ最も精密な評価を与える Padé 近似（Hermite-Padé 近似）[15] により，effective な無理数度 [14]，超幾何級数の値及び多重対数の一次独立性についての判定基準 [8] [9] [10] [11] も得られる．

2 Effectivity

Effectivity とは，有限回の操作で有限時間内に実行可能なアルゴリズムにより最終的な目標物が決定できる状況を示す言葉である．計算量が膨大であっても有限時間に終わるならば effective であると言って良い．

ディオファントス問題における典型例，例えば方程式の全ての整数解が有限個である場合等においても，その整数解を全て決定することが有限時間内に終了するならば，解もしくは解を求めるための証明は **effective** であると称する．対象物である解を全て列記できる場合，**explicit** という単語を用いる．

対象物が有限個に限ることが証明できる場合であっても，対象物を全て求め得る計算方法が実際に存在しなければ，effective とは言えずに，**ineffective** となる．現時点でどのようなディオファントス近似が ineffective であるかを羅列する．

Axel Thue や C. L. Siegel らが示した，2 次以上の代数的数に対する有理数による近似の指数の改良によって K. F. Roth はフィールズ賞を受賞したが，この近似の証明は effective ではない．即ち以下の定理において，有限個であることが示せている有理数 $\dfrac{p}{q} \in \mathbb{Q}$ を決定する方法は知られていない．

Theorem 2.1 (Roth, 1955). α を次数 $d \geq 2$ の実代数的数とする．任意の $\varepsilon > 0$ に対し，不等式

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

を満たす $\frac{p}{q} \in \mathbb{Q}$ は有限個に限る．

Roth の定理は次の形で W. M. Schmidt により一般化され，Schmidt の部分空間定理 [17] と名付けられた．部分空間定理は Roth の近似のいわば同時近似版である．部分空間定理の活用により，ディオファントス問題に関する多くの新発見が最近も得られているが [6][21]，Schmidt の部分空間定理は effective ではなく，effective になる技術革新は今のところ無い．

Theorem 2.2 (部分空間定理). $n \in \mathbb{Z}_{\geq 2}$ とする．変数 $X_1, \cdots X_n$ に対し n 個の一次独立な代数的数係数の一次形式 $L_1, \cdots, L_n$ を考える．このとき，任意の $\varepsilon > 0$ に対し，有限である ℓ 個の真の線形部分空間 $T_1, \cdots, T_\ell \subset \mathbb{Q}^n$ で，以下を満たすものが存在する：整数ベクトル $\mathbf{0} \neq \mathbf{x} = (x_1, \cdots, x_n) \in \mathbb{Z}^n$ で

$$|L_1(\mathbf{x}) \cdots L_n(\mathbf{x})| \leq \max_{1 \leq i \leq n} (|x_i|)^{-\varepsilon} \tag{1}$$

を満たすものは，必ず $T_1, \ldots, T_\ell$ の和集合に属する．

さらなる一般化もあるが, 残念ながら全て ineffective である．ℓ の上界は explicit に得られている．部分空間定理の応用には Siegel (1921) らによる単数方程式の解の有限性を経由する場合も多い．一般的な単数方程式の解の有限性定理としては J.-H. Evertse-H. P. Schlickewei-Schmidt [12] があるが，2 変数の単数方程式に限り Baker 理論 [4] が適用可能で，effective な結果が得られる（Roth の定理からも解の有限性は出るが ineffective）．即ち K が有限次代数体，$0 \neq \alpha, \beta \in K$ のとき，単数方程式 $\alpha x + \beta y = 1$ の解 $x, y \in U_K$ は有限個であり，2 変数の場合に限って，以下の手順で解 x, y は effective に求まる（ディオファントス方程式の effective な結果は，2 変数の単数方程式の解の effectivity に帰着される場合が多い）．

Theorem 2.3 (A. Baker [4]). 0 でない $\alpha_1, \cdots, \alpha_\ell \in K$ を固定し，これらの高さの最大値を A とおく．全てが 0 ではない整数 $b_1, \cdots, b_\ell \in \mathbb{Z}$ に対し，$\alpha_1^{b_1} \cdots \alpha_\ell^{b_\ell} \neq 1$ を仮定．$B = \max_{1 \leq j \leq \ell} |b_j| + 3$ とおく．このとき $\ell, A, [K : \mathbb{Q}]$ による *effective* な定数 $C > 0$ が存在して，以下が成立：

$$|\alpha_1^{b_1} \cdots \alpha_\ell^{b_\ell} - 1| > B^{-C}.$$

簡単のため係数 1 の単数方程式 $x + y = 1 \quad (x, y \in U_K)$ に Theorem 2.3を適用して，2 変数の単数方程式の解を effective に求めよう．$x \neq 0, y \neq 0$ 即ち $x = 1 - y \neq 0$, $1 - y \neq 1$ とする．$C_1, C_2, \ldots$ は effective な正定数とする．

Dirichlet の単数定理から $x = \zeta \varepsilon_1^{a_1} \cdots \varepsilon_r^{a_r}$, $y = \zeta' \varepsilon_1^{b_1} \cdots \varepsilon_r^{b_r}$ と表せる．但し ζ, ζ' は K に属する 1 のべき根，$\varepsilon_1, \cdots, \varepsilon_r$ は単数群 U_K の基底とする．$x = 1 - y$ より，$\log |x| = \log |\zeta \varepsilon_1^{b_1} \cdots \varepsilon_r^{b_r} - 1|$. この $0 \neq x = 1 - \zeta \varepsilon_1^{b_1} \cdots \varepsilon_r^{b_r}$ に対して Theorem 2.3を適用すると

$$\log |x| = \log |\zeta \varepsilon_1^{b_1} \cdots \varepsilon_r^{b_r} - 1| > -C_1 \log B.$$

一方，高さの性質や Dirichlet の単数定理より $\log |x| \leq -C_2 B$ が成立（実数 B は未知であることに注意）．以上の不等式をつなげると $-C_1 \log B < -C_2 B$.

$$\therefore B < \frac{C_1}{C_2} \log B.$$

$\log B$ は B より小さいので，これより B は有界．B の定義より，$y = \zeta \varepsilon_1^{b_1} \cdots \varepsilon_r^{b_r}$ における指数部分の整数 $b_1, \cdots, b_r$ が定まる．ζ, ζ' や $\varepsilon_1, \cdots, \varepsilon_r$ は K に依存した情報で effective に求め得るので，y，従って x も effective に定まる．残念ながらこの証明は 3 変数以上の単数方程式では走らない．

3 Senge-Straus の問題と答え

Question 1.1には Theorem 2.2の特別な場合から次の答えが出るが，これをどのように effective にできるのかを見てみよう．具体的に以下の問を考察する．

$y \in \mathbb{Z}, y > 1, y \neq 10$ の累乗とする．$d \in \mathbb{Z}_{>0}$ に対して，y^d を 10 進展開して $y^d = x_0 + x_1 \cdot 10 + x_2 \cdot 10^2 + \cdots + x_n \cdot 10^n$ と表示し，10 進展開の digits の和を $s_{10}(y^d) = x_0 + x_1 + \cdots + x_n$ とおく．

一般には $N \in \mathbb{Z}_{\geq 2}$ を考え，整数 $a, b \in \mathbb{Z}_{\geq 2}$ を固定．$\alpha, \beta \in \mathbb{Z}$，$0 \leq \alpha < a$，$0 \leq \beta < b$，$L_{\alpha,a}(N) :=$ N の a 進展開における，α とは異なる digits の個数，$L_{\beta,b}(N) :=$ N の b 進展開における，β とは異なる digits の個数とする． また $L_{\alpha,a,\beta,b}(N) := L_{\alpha,a}(N) + L_{\beta,b}(N)$ とおく．

今の場合は $L_{0,10}(y^d)$ が y^d の 10 進展開における非零 digits の個数で，明らかに $L_{0,10}(y^d) \leq s_{10}(y^d)$ が成立する．この場合の Question 1.1の問題と答えとしては下記を考察することができる．

1. 数列 $y, y^2, y^3, \ldots, y^d, \ldots$ を考える．
2. $d \to \infty$ のとき，$s_{10}(y^d) \to \infty$ であろうか？
3. $d \to \infty$ のとき，非零の digits の個数 $L_{0,10}(y^d) \to \infty$ であろうか？
4. 一般に，$L_{0,10}(N) + L_{0,y}(N)$ が下から評価される場合，10 及び y は乗法的に独立になるであろうか？
5. Senge-Straus の答え [18]：$\dfrac{\log y}{\log 10} \notin \mathbb{Q}$ であることと，$L_{0,10}(y^d) + L_{0,y}(y^d)$ が下から評価され, その下界が無限大に発散することは同値（但し ineffective である）．

この Senge-Straus の答えの explicit 版が，以下の定理である．

Theorem 3.1 (Laishram, Kawashima and NHK). $\dfrac{\log a}{\log b} \notin \mathbb{Q}$ ならば

$$L_{\alpha,a,\beta,b}(N) + 1 > \frac{\log\log(N)}{\log\log\log(N+30) + 10^5 \cdot a^b + 10^5 \cdot b^a + 10^7 \cdot ab(a+b)}.$$

即ち，対数一次形式から explicit な計算によって explicit Stewart つまり Senge-Straus の effective (explicit) な答えが得られたことになる．

この Theorem 3.1から以下が得られる．

1. y^d を 10 進展解する：$y^d = x_0 + x_1 \cdot 10 + x_2 \cdot 10^2 + \cdots + x_n \cdot 10^n$.
2. 10 進展開の digits の和を $s_{10}(y^d) := x_0 + x_1 + \cdots + x_n$ とおく．
3. $L_{0,10}(y^d) = y^d$ の 10 進展開における非零 digits の個数であるが，明らかに $L_{0,10}(y^d) \le s_{10}(y^d)$.
4. 例えば $s_{10}(y^d) \le 35$ と仮定すると，$L_{0,10}(y^d) \le 35$ である．
5. しかし上記の定理より $36 \gg \log\log y^d$ が得られる．
6. 不等式をつなげると，$d \ll 1$.
7. d は explicit に定まる．
8. つまり，$s_{10}(y^d)$ が有界となる d はこのように定まってしまう．

4 超越近似による effective な結果

超越近似の手法を用いると，以下の effective な結果が得られる．

1. F. Amoroso-S. David, David ら [1][7] による，Lehmer 問題の評価 [16]．例えば代数体 K 上の Abelian variety A の N-torsion 点 $p \in A$ に対する評価（詳しくは [7] 参照のこと，予想の解説もある）：

   $$[\mathbb{Q}(p) : \mathbb{Q}] \ge C \cdot N^{\lambda}$$

   は explicit な定数 $C > 0$, $\lambda > 0$ を用いて記述される．
   ちなみに Abelian variety ではなく，元の Lehmer 問題の評価に対する現時点で最良の結果は [2] である．
2. Pila-Wilkie の一連の定理に関する評価の一部に対しても，effective な結果が得られる（現在，Work in progress).

超越近似については，いわゆる Baker 理論に加え様々な背景を述べてある本としては [5] が良いが，対数一次形式の定理の証明そのものは [4] を参照されたし．

謝辞　本研究は JSPS 科学研究費補助金 Grant No. 21K03171 の助成を受けています．国際共同利用・共同研究拠点としての京都大学数理解析研究所の支援も受けております．この場をお借りして厚くお礼申し上げます．

References

[1] F. Amoroso and S. David, *Le problème de Lehmer en dimension supérieure*, J. Reine Angew. Math., **513**, (1999), 145–179.

[2] F. Amoroso and S. David, *Covolumes, unités, régulateur: conjectures de D. Bertrand et F. Rodriguez-Villegas*, Annales mathématiques du Québec, **45**, (2021), 1–18.

[3] A. Baker, *Linear forms in the logarithms of algebraic numbers. I, II, III, IV*, Mathematika, **13**, (1966), 204–216, 102–107, 220–228, 204–216.

[4] A. Baker, *Transcendental Number Theory*, Cambridge Univ. Press, 1975.

[5] A. Baker and Gisbert Wüstholz, *Logarithmic Forms and Diophantine Geometry*, New Mathematical Monographs **9**, Cambridge Univ. Press, 2007.

[6] P. Corvaja and U. Zannier, *Applications of Diophantine Approximation to Integral Points and Transcendence*, Cambridge Tracts in Math., **212**, Cambridge Univ. Press, 2018.

[7] S. David, Bulletin de la Société Math. de France, **121**, no. 4, (1993), 509–544.

[8] S. David, N. Hirata-Kohno and M. Kawashima, *Can polylogarithms at algebraic points be linearly independent?*, Mosc. J. Comb. Number Theory, **9**, no, 4, (2020), 389–406.

[9] S. David, N. Hirata-Kohno and M. Kawashima, *Linear Forms in Polylogarithms*, Ann. Scuola Nor. Sup. Pisa, Classe di Scienze, series 5, **23** (3), (2022), 1447–1490.

[10] S. David, N. Hirata-Kohno and M. Kawashima, *Linear independence criteria for generalized polylogarithms with distinct shifts*, Acta Arith., **206**, (2022), 127–169.

[11] S. David, N. Hirata-Kohno and M. Kawashima, *Linear independence of values of hypergeometric functions and arithmetic Gevrey series*, preprint, arXiv:2203.00207 .

[12] J.-H. Evertse, H. P. Schlickewei and W. M. Schmidt, *Linear equations in variables which lie in a multiplicative group*, Annals of Math., **155**, no. 3 (2002), 807–836.

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

[14] M. Kawashima and A. Poëls, *Padé approximations for shifted functions and parametric geometry of numbers*, J. Number Theory, **243**, (2023), 646–687.

[15] K. Mahler, *Perfect systems*, Compos. Math., **19**, (1968), 95–166.

[16] D. Masser, *Auxiliary Polynomials in Number Theory*, Cambridge Tracts in Math., **207**, Cambridge Univ. Press, 2016.

[17] W. M. Schmidt, *Diophantine Approximation*, Lecture Notes in Math., **785**, Springer, 1980.

[18] H. G. Senge and E. G. Straus, *PV-numbers and sets of multiplicity*, Periodica Math. Hungarica, **3**, (1973), no. 1-2, 93–100.

[19] C. L. Siegel, *Transcendental Numbers*, Annals of Mathematics Studies, **16**, Princeton University Press, Princeton, 1949.

[20] C. L. Stewart, *On the representation of an integers in two different bases*, J. Reine Angew. Math., **319**, (1980), 63–72.

[21] U. Zannier, *Diophantine equations with linear recurrences, An overview of some recent progress*, J. Théor. Nombres Bordeaux. **17**, (2005), no. 1, 423–435.