べき根拡大体のノルム形式における Brocard-Ramanujan 問題の解の構成

東京理科大学理学部　武田　渉

Wataru Takeda
Faculty of Science, Tokyo University of Science

1　Brocard-Ramnujan 問題

Brocard-Ramnujan 問題とは Brocard と Ramnujan によって独立に提起された以下の予想である.

Conjecture ([1, 2, 3])**.** 方程式 $x^2 - 1 = \ell!$ の解は $(x, \ell) = (5, 4), (11, 5), (71, 7)$ である.

この問題は現在も未解決であるが, $\ell < 10^{15}$ までには予想されている 3 つしかないことが知られていたり, より一般に整数係数多項式 $P(\boldsymbol{x})$ と階乗 $\ell!$ からなる方程式

$$P(\boldsymbol{x}) = \ell!. \tag{1.1}$$

の解を求めることや解の個数を考える様々な研究がある.

例えば, (1.1) の左辺の多項式を代数体のノルムに変えた場合が論文 [4] において考えられている. 先行研究の結果を述べる前に, 代数体のノルムを定義する. まず, 代数体 K に対して, $\mathcal{O}_K$ を整数環とし, K から $\mathbb{C}$ への $\mathbb{Q}$ 上準同型写像全体の集合を $G(K)$ とする. 例えば, 平方数でない整数 a に対して, $K = \mathbb{Q}(\sqrt{a})$ のときは $G(K) = \{\mathrm{id}, \sigma\}$ $(\sigma : \sqrt{a} \mapsto -\sqrt{a})$ である. このとき, 代数体 K のノルム N_K は以下で定義される.

$$N_K(x) = \prod_{\sigma \in G(K)} \sigma(x).$$

ノルムの例も 2 つ挙げる. 以下, a は 3 乗の因子を持たない整数とする.

- $N_{\mathbb{Q}(\sqrt{2})}(x+\sqrt{2}y) = (x+\sqrt{2}y)(x-\sqrt{2}y) = x^2 - 2y^2$;
- $N_{\mathbb{Q}(\sqrt[3]{a})}(x + y\sqrt[3]{a} + z\sqrt[3]{a^2}) = x^3 + ay^3 + a^2z^3 - 3axyz$.

代数体のノルムに関する Brocard-Ramanujan 問題として, 以下の結果が知られている.

Theorem 1.2 ([4, Theorem 5.2])**.** 任意の代数体 $K \neq \mathbb{Q}$ に対して, $N_K(x) = \ell!$ の解 $(x, \ell) \in \mathcal{O}_K \times \mathbb{Z}$ は単元倍の違いを除いて有限個である.

$K = \mathbb{Q}$ の場合は $N_K(x) = x$ であるため, (1.1) の解は無限個であるため, 上の Theorem 1.2 はすべての代数体のノルムに対して, 解の有限性に関する解決を与えている. しかし, この定理は解の有限性を証明している一方, 実際の解の個数については何もわからない. 以下では具体的に解を構成することにより, 解の個数について考える. まず, 考える解の集合を以下のように定める.

$$S(K) = \{\ell \geq 2 \mid \exists \boldsymbol{x} \in \mathcal{O}_K \text{ s.t. } N_K(\boldsymbol{x}) = \ell!\}.$$

ここで, $\ell \geq 2$ としている理由は任意の代数体 K に関して, $N_K(1) = 1$ であるため, それを自明な解として除いているからである. 具体的な $S(K)$ の例をいくつか挙げる. まず, $K = \mathbb{Q}(\sqrt{-1})$ のとき, Erdős-Obláth によって, $S(\mathbb{Q}(\sqrt{-1})) = \{2, 6\}$ であることが観察されている. 他にも, 以下の具体例も計算できる.

Example (類数 1 の虚 2 次体)**.**

d	$S(\mathbf{Q}(\sqrt{-d}))$	d	$S(\mathbf{Q}(\sqrt{-d}))$
1	$\{2, 6\}$	7	$\{10, 11\}$
2	$\{3, 4\}$	11	$\{6\}$
3	$\{10\}$	19	$\{6, 7, 10, 11\}$

また, $d = 43, 67, 163$ に対しては $S(\mathbf{Q}(\sqrt{-d})) = \emptyset$ である.

Example (類数 3 の虚 2 次体)**.**

d	$S(\mathbf{Q}(\sqrt{-d}))$	d	$S(\mathbf{Q}(\sqrt{-d}))$
23	$\{3, 4\}$	139	$\{7, 10, 11\}$
31	$\{6, 7, 8, 9, 10\}$	283	$\{11\}$
59	$\{6, 7, 10\}$	307	$\{11\}$
83	$\{10, 11, 12\}$		

また, $d = 107, 211, 331, 379, 499, 547, 643, 883, 907$ に対しては $S(\mathbf{Q}(\sqrt{-d})) = \emptyset$ である.

上記の例を見ると, $6, 10$ が多く表れているように見える. これは,

$$6! = 2^4 \cdot 3^2 \cdot 5,\ 10! = 2^8 \cdot 3^4 \cdot 5^2 \cdot 7$$

であることに注意すると $5, 7$ が完全分解する場合は解になりやすいからである. (類数が 1 の場合は必ず解になる.)

2 いくつかの観察

ここでは $S(K) \neq \emptyset$ なる K が無限個あることを示す.

Theorem 2.1 ([5, Theorem 2.1])**.** n を 2 以上の整数とする. このとき, $S(K) \neq \emptyset$ となる n 次体 K は無限個存在する.

Proof. 正の整数 $\ell \geq 2$ に対して, ℓ の n 次因子と非 n 次因子の分解を $\ell! = m^n k$ とする. ここで, k は因子に n 乗べきを持たない整数である. ここで Bertrand-Chebyshev の原理によって, 任意の $x \geq 2$ に対して, 素数 $p \in (x, 2x)$ が存在するため, $\ell!$ はべき乗数でなく, $k > 1$ となる. ここで $K = \mathbf{Q}(\sqrt[n]{-k})$ とする. このとき, K は n 次体である. また, $m\sqrt[n]{-k}$ は $x^n + m^n k$ の根であることから, $m\sqrt[n]{-k} \in \mathcal{O}_K$ である. さらに,

$$N_K(-m\sqrt[n]{-k}) = \prod_{i=0}^{n-1} \left(-m\sqrt[n]{-k}\zeta_n^i\right) = (-\ell!) \cdot (-1) = \ell!.$$

よって, $N_K(-m\sqrt[n]{-k}) = \ell!$ となるため, $S(K) \neq \emptyset$ である. 再度, Bertrand-Chebyshev の原理によって, 階乗 $\ell!$ の非 n 乗因子 k として, 無限個のものが現れる. 特に新しい素因子が現れることが無限回起こることが分かる. よって, 以上により $S(K) \neq \emptyset$ となる n 次体 K は無限個存在することが示された. □

Theorem 2.2 ([5, Theorem 3.1])**.** $K = \mathbb{Q}(\sqrt[n]{2})$ とする.

1. 6 と互いに素な整数 n に対して, $\{\ell \mid 2 \leq \ell \leq 10\} \subset S(K)$;
2. 30 と互いに素な整数 n に対して, $\{\ell \mid 2 \leq \ell \leq 22\} \subset S(K)$.

この結果から, $\#S(K) \geq 21$ となる代数体 K が無限個あることがわかる.

Proof. 2 つ目の方を示す. ノルムの乗法性から, $p \leq 19$ なる素数 p に対して, $N_K(x) = p$ となるような代数的整数 $x \in \mathcal{O}_K$ が存在することを示す. まず, $N_K(\sqrt[n]{2}) = 2$ である. 続いて, $(n, k) = 1$ となる整数に対して, $N_K(x + \sqrt[n]{2^k}) = x^k + 2^k$ であることか

ら, $N_K(1+\sqrt[n]{2})=3, N_K(1+\sqrt[n]{4})=5, N_K(-1+\sqrt[n]{8})=7, N_K(1+\sqrt[n]{16})=17$ の 4 つが従う.

また, $N_K(1+\sqrt[n]{32})=33$ と $N_K(1+\sqrt[n]{2})=3$ から, $N_K(1-\sqrt[n]{2}+\sqrt[n]{4}-\sqrt[n]{8}+\sqrt[n]{16})=11$ である. このとき, $(n,5)=1$ を使っていることに注意する. これによって, 1 つ目の場合は 11 の構成ができるとは限らないため, 10 までとなる.

同様に $N_K(1-\sqrt[n]{4}+\sqrt[n]{16})=13$ が $N_K(1+\sqrt[n]{4}^3)=65$ と $N_K(1+\sqrt[n]{4})=5$ からわかる. よって, ノルムの乗法性から, $2\leq\ell\leq 18$ なる任意の整数 ℓ に対して, $N_K(x)=\ell!$ となるような代数的整数 $x\in\mathcal{O}_K$ が存在する.

最後に $N_K(x)=19$ となる代数的整数 $x\in\mathcal{O}_K$ を一般に見つけることが難しいため, $N_K(1-\sqrt[n]{8}+\sqrt[n]{64})=57=3\cdot 19$ を使う. これは $N_K(1+\sqrt[n]{8}^3)=513$ かつ $N_K(1+\sqrt[n]{8})=9$ であることから両辺の比をとって示される. また, これまでの計算で $N_K(x_{18})=18!$ となる $x_{18}\in\mathcal{O}_K$ の存在を示したため,

$$N_K\left(\frac{x_{18}(1-\sqrt[n]{8}+\sqrt[n]{64})}{(1+\sqrt[n]{2})}\right)=19!$$

がわかる. 以上の計算により, $2\leq\ell\leq 22$ なる任意の整数 ℓ に対して, $N_K(x)=\ell!$ となるような代数的整数 $x\in\mathcal{O}_K$ が存在する. □

Theorem 2.2 は, 一般に $N_K(x)=23$ となる代数的整数 $x\in\mathcal{O}_K$ の構成が難しいため, 上限が 22 となっている. しかし, 30 と互に素な最小の整数 $n\geq 2$ である $n=7$ の場合, つまり, $K=\mathbf{Q}(\sqrt[7]{2})$ の場合は $N_K(1+\sqrt[7]{4}+\sqrt[7]{32})=23$ であることから, 22 を越えて以下の結果を得る.

Theorem 2.3. $K=\mathbf{Q}(\sqrt[7]{2})$ とする. このとき,

$$\{\ell \mid 2\leq\ell\leq 28\}=S(K).$$

また, 次の素数 29 は $K=\mathbf{Q}(\sqrt[7]{2})$ 上において惰性するため, $\ell=29$ は解にならないことがわかり, それ以降も惰性する素数が “頻繁に” 出てくるため解とならない.

3 べき根拡大の解の構成

先の章 (Theorem 2.2, Theorem 2.3) で見たようにべき根拡大は解の構成がしやすい. 以下では素イデアル分解の Dedekind の定理をべき根拡大体の整数環の部分環 (整環, オーダー) に対して用いて, 解の構成をする.

Theorem 3.1 (Dedekind の定理)**.** 代数体 $K = \mathbf{Q}(\alpha)$ $(\alpha \in \mathcal{O}_K)$ に対して, $f(x) \in \mathbf{Z}[x]$ を α の最小多項式とする. このとき, $p \nmid [\mathcal{O}_K : \mathbf{Z}[\alpha]]$ なる素数に対して, $f \mod p$ の既約分解が

$$f(x) = \prod_{i=1}^{r} f_i(x)^{e_i} \mod p,$$

であったとする. ここで f_i は $\mathbf{F}_p[x]$ 内の相異なる既約多項式である. このとき, イデアル $p\mathcal{O}_K$ の素イデアル分解は

$$p\mathcal{O}_K = \prod_{i=1}^{r} \mathfrak{p}_i^{e_i} \tag{3.2}$$

となる. 特に $\mathcal{O}_K = \mathbf{Z}[\alpha]$ のとき, 上の素イデアル分解 (3.2) は任意の p に対して成立する.

n 次体 $K = \mathbf{Q}(\sqrt[n]{a})$ に対して, $D(a,n) = [\mathcal{O}_K : \mathbf{Z}[\sqrt[n]{a}]]$ とする. このとき, $\gcd(p-1,n) = 1$ を満たす任意の素数 p に対して,

$$b^n - a \equiv 0 \mod p$$

となる整数 $b \in \mathbf{Z}$ が存在する. これは $\#(\mathbf{Z}/p\mathbf{Z})^\times = p-1$ であることからわかる. よって, $x^n - b \mod p$ は 1 次因子を持つため, 定理 3.1 より, $p \nmid D(a,n)$ かつ $\gcd(p-1,n) = 1$ なる任意の素数 p に対して, $\mathfrak{p}$ という p の上にある素イデアルが存在し, $\mathfrak{N}\mathfrak{p} = p$ となる. ここで $\mathbf{Z}[\sqrt[n]{a}]$ の判別式の絶対値が $a^{n-1}n^n$ であるため, $p|D(a,n)$ ならば $p|an$ となる. したがって, 以下の定理を得る.

Theorem 3.3. 整数 a, n に対して, $K = \mathbf{Q}(\sqrt[n]{a})$ とする. このとき, K の類数が 1 の場合,

$$\{\ell \mid 2 \le \ell \le P-1\} \subset S(K),$$

である. ここで, $P = P(n,a)$ は 以下の $S_1(n,a) \cup S_2(n,a) \cup S_3(n,a)$ の最小値である. ここで,

$$\begin{aligned} S_1(n,a) &= \{p : \text{素数} \mid \gcd(p-1,n) > 1\}; \\ S_2(n,a) &= \{p : \text{素数} \mid p^2|a\}; \\ S_3(n,a) &= \{p : \text{素数} \mid p|n, a^{p-1} \equiv 1 \mod p^2\}. \end{aligned}$$

Proof. 上で述べたように, an と互いに素である任意の素数 $p \le P-1$ に対して, $\mathfrak{N}\mathfrak{p} = p$ となる $\mathfrak{p}$ が存在する. 類数に関する仮定から, $\mathfrak{p}$ は単項イデアルとなるため, $\mathfrak{p} = x\mathcal{O}_K$ かつ $N_K(x) = p$ を満たす $x \in \mathcal{O}_K$ が存在する.

次に, $p \leq P-1$ かつ $p|a$ を満たす素数 p を固定する. p が a を一度しか割り切らないため, 多項式 $x^n - a$ は p で Eisenstein 多項式であり, p は $K = \mathbf{Q}(\sqrt[n]{a})$ で完全分岐することがわかる. したがって, $N_K(x) = p$ を満たす p の上にある素イデアル $\mathfrak{p} = x\mathcal{O}_K$ が存在する.

最後に, $\gcd(p, a) = 1$ かつ $a^{p-1} \not\equiv 1 \mod p^2$ を満たす n を割り切る素数 $p \leq P-1$ に対して考える. このような素数 p を 1 つ固定し, $p^r|n$ かつ $p^{r+1} \nmid n$ を仮定する. 慣性次数には乗法性があるため, p が $K = \mathbf{Q}(\sqrt[p^r]{a})$ で完全分岐することを示すことで $K = \mathbf{Q}(\sqrt[n]{a})$ において完全分岐することが示される. ここで, $a^{p^r} \equiv a^p \mod p^2$ かつ $a^p \not\equiv a \mod p^2$ であるため, 多項式 $(x+a)^{p^r} - a = x^n + \cdots + a^{p^r} - a$ は p で Eisenstein 多項式である. 以上より, $N_K(x) = p$ を満たす p の上にある素イデアル $\mathfrak{p} = x\mathcal{O}_K$ が存在する.

従って, ノルム N_K の乗法性から, 任意の $\ell \leq P-1$ に対して, $N_K(x) = \ell!$ を満たす $x \in \mathcal{O}_K$ が存在する. □

Theorem 3.3 の例として以下の二つを挙げる.

Example. 代数体 $K = \mathbf{Q}(\sqrt[p]{2})$ に対して, 以下が成立する.

1. $p = 17$ のとき, $S(K) = \{\ell \mid 2 \leq \ell \leq 102\}$.
2. $p = 19$ のとき, $S(K) = \{\ell \mid 2 \leq \ell \leq 190\}$.

4 解の上限について

本研究では解の構成に焦点を置いていたため, 解の上限を求めることやすべての解を求めることはあまりしていないが一般に以下の事実が知られている.

Theorem 4.1 ([5, Theorem A.5])**.** 代数体 K に対して, $K/\mathbf{Q}$ の Galois 閉包を K^{gal} とする. その拡大次数を $n = [K^{\mathrm{gal}} : \mathbf{Q}]$ とし, K^{gal} の判別式の絶対値を D とする. このとき, 計算可能なある正の定数 $c > 0$ が存在して, 方程式 $N_K(x) = \ell!$ の解が

$$\ell > (Dn^n)^{c \log\log(Dn^n)}$$

内に存在しない.

この結果により, 解の有限性とともに解を調べるべき限界も分かる. ただ, この定理は任意の代数体に対して, 方程式 $N_K(x) = \ell!$ の解について考えるものであるため, 実際に解を求める際は具体的に素数の分岐を観察する方が有効である. 特にアーベル拡

大の場合は Dirichlet の算術級数定理, より正確には等差数列中の素数定理を用いることで考えられるため, Theorem 4.1 で与えられている解の上限は大きく下がる.

謝辞

2023 年度 RIMS 共同研究 (公開型)「解析的整数論とその周辺」における講演の機会を与えてくださった安福 悠先生, 中筋 麻貴先生にこの場をお借りして感謝いたします. 本研究は JSPS 科研費 JP22K13900 の助成を受けたものです.

参考文献

[1] H. Brocard. Question 166, *Nouv. Corres. Math.* **2**, 287. 1876.

[2] H. Brocard, Question 1532, *Nouv. Ann. Math.* (3)**4**, 391. 1885.

[3] S. Ramanujan. Question 469. *Journal of the Indian Mathematical Society.* **5**, 59. 1913.

[4] W. Takeda. On the finiteness of solutions for polynomial-factorial Diophantine equations. *Forum Math.*, **33**(2), 361–374 (2021)

[5] W. Takeda. Existence of the solutions to the Brocard-Ramanujan problem for norm forms, *Proc. Amer. Math. Soc. Ser. B* **10**, 413–421 (2023)