Dynamical Zsigmondy theorem

t888

2026 年 11 月 7 日

概要

本稿は, 2026 年 11 月 7, 8 日にて行なわれた理工展 2026 の Wathematica ポスター展示『数論力学系への招待 (Zsigmondy の定理とその力学系 version)』をまとめたものである.

定理 1 (Zsigmondy)**.** 互いに素な正の整数 $a > b$ と正の整数 n をとる. このとき, $a^n - b^n$ の素因数 p が存在して, 整数 $1 \leq k \leq n-1$ に対して p は $a^k - b^k$ を割らない. ただし, 次の 3 つの場合は除く.

1. $n = 1, a - b = 1$ のとき.
2. $n = 2, a + b = 2^m$ $(m \geq 1)$ のとき.
3. $n = 6, a = 2, b = 1$ のとき.

証明. [3], [4] 参照. □

注意 2. 定理 1 を満たさない 3 つの例外について述べる.
1. $n = 1, a - b = 1$ のとき, $a^n - b^n = 1$ となるので不適である.
2. $n = 2, a + b = 2^m$ のとき, $a^2 - b^2 = (a + b)(a - b)$ を考えると分かる.
3. $n = 6, a = 2, b = 1$ のとき, 下の例 3 参照.

例 3. 具体例として $2^n - 1$ を考えよう (すなわち $a = 2, b = 1$ のときを考えよう). 各段階 (正の整数 n が大きくなるごと) に新しい素数が現れるかどうかに着目しよう.

n	$2^n - 1$	素因数分解
1	1	−
2	3	3
3	7	7
4	15	3×5
5	31	31
6	63	$3^2 \times 7$
7	127	127
8	255	$3 \times 5 \times 17$
9	511	7×73
10	1023	$3 \times 11 \times 31$

例えば $2^4 - 1 = 15 = 3 \times 5$ において, 3 は既に $2^2 - 1 = 3$ にて登場しているが, 5 は初登場である. この表

では $n=6$ を除く各 $n\geq 2$ において, 新しい素因数が現れていることが分かる (上の注意 2 の 3 参照).

このように **(いくつか例外はあるが) a^n-b^n にはそれまでには見たことのない素数が現れる**, というのが Zsigmondy の定理の主張である.

Zsigmondy の定理には楕円曲線への一般化がある. 楕円曲線 $E/\mathbb{Q}$ と無限位数の点 $P\in E(\mathbb{Q})$ に対して, $x([n]P)=A_n/B_n^2$ を既約分数表示とする. このとき Silverman は [2] において, 十分大きいすべての n に対して, B_n が primitive divisor を持つことを示した (primitive divisor の定義は後に行なう). この数列 $(B_n)_{n\geq 1}$ は elliptic divisibility sequence (EDS) と呼ばれる.

さらに Ingram–Silverman [1] は, 有理写像の反復軌道に対して同様の結果を証明した. その結果は数体上の有理写像にも適用され, 基準点が前周期点である場合を含む. 以下では, この結果の特殊な場合を考察する. そのために記号の準備をする.

定義 4. 整数の列 $(a_n)_n$ に対して, $p\mid a_n$ かつ $p\nmid a_m$ かつ $a_m\neq 0$ $(0<\forall m<n)$ となるような素数 p を **primitive divisor** という. また, 数列 $(a_n)_n$ の **Zsigmondy 集合** $\mathcal{Z}((a_n)_n)$ を次で定める.

$$\mathcal{Z}((a_n)_n) \coloneqq \{n\in\mathbb{Z}_{>0} \mid a_n \text{ は primitive divisor を持たない }\}.$$

例 5. Zsigmondy の定理 (定理 1) より, $a>b$ が互いに素な正の整数ならば $\mathcal{Z}((a^n-b^n)_n)$ は有限集合である. 特に, $\mathcal{Z}((a^n-b^n)_n)\subseteq\{1,2,6\}$ が成り立つ.

以上の準備のもと, Zsigmondy の定理の力学系版を考察する.

定理 6. $\phi\in\mathbb{Q}(z)$ を次数 d の有理関数とし, $\phi(0)=0$ とする. 0 における ϕ の零点の位数 e が $2\leq e<d$ を満たすとする. 軌道 $\{\alpha,\phi(\alpha),\phi^2(\alpha),\cdots\}$ が無限集合となるような $\alpha\in\mathbb{Q}$ に対し, $\phi^n(\alpha)=\frac{A_n}{B_n}$ を既約分数表示とする. このとき, Zsigmondy 集合 $\mathcal{Z}((A_n)_n)$ は有限集合である. すなわち, 十分大きいすべての n に対し, A_n は primitive divisor を持つ.

証明. 仮定より, ϕ を次のように書ける.

$$\phi(z)=z^eR(z),\qquad R(z)=\frac{F(z)}{G(z)},\qquad F,G\in\mathbb{Z}[z],\quad F(0)G(0)\neq 0$$

$S\coloneqq\{p\text{: 素数} \mid p\mid F(0)G(0)\}$ とおき, $v_p(p)=1$ と正規化した p 進付値を v_p とする. また $A_{n,S}\coloneqq\prod_{p\notin S}p^{v_p(A_n)}$ とおく.

$m\in\mathbb{Z}_{\geq 1}$ に対して, $p\notin S$ が $p\mid A_m$ を満たすとする. $p\nmid B_m$ であるから $v_p(\phi^m(\alpha))=v_p(A_m)-v_p(B_m)=v_p(A_m)>0$ である.

以下では p を法とする. B_m の逆元が存在するので, $\phi^m(\alpha)\equiv 0\pmod p$ である. 従って, F は多項式ゆえ $F(\phi^m(\alpha))\equiv F(0)$ が得られる. 同様に $G(\phi^m(\alpha))\equiv G(0)$ である. $p\notin S$ より, $F(0)$ と $G(0)$ は共に p で割れないので, $v_p(F(\phi^m(\alpha)))=v_p(F(0))=0, v_p(G(\phi^m(\alpha)))=v_p(G(0))=0$ である.

ここで $\phi^{m+1}(\alpha)=\phi^m(\alpha)^e\frac{F(\phi^m(\alpha))}{G(\phi^m(\alpha))}$ ゆえ, 上の議論と合わせて $v_p(\phi^{m+1}(\alpha))=e\,v_p(\phi^m(\alpha))=e\,v_p(A_m)>0$ となる. 一方, $p\mid A_m$ であったから $v_p(\phi^{m+1}(\alpha))=v_p(A_{m+1})-v_p(B_{m+1})=ev_p(\phi^m(\alpha))>0$ となり, $p\mid A_{m+1}$ である. $\frac{A_{m+1}}{B_{m+1}}$ は既約分数表示だったので, $p\nmid B_{m+1}$ ゆえ $v_p(A_{m+1})=v_p(\phi^{m+1}(\alpha))=e\,v_p(A_m)>0$ を得る.

この議論を繰り返すことにより, 一般に $n\geq 2$ に対して $p\notin S$ が $A_1,\cdots,A_{n-1}$ のいずれかを割ることと,

$p \mid A_{n-1}$ であることは同値であることが分かる．よって $A_{n,S} \coloneqq \prod_{p\notin S} p^{v_p(A_n)} > 0$ に対して次が得られる．

$$\frac{A_{n,S}}{A_{n-1,S}^e} = \prod_{\substack{p\notin S\\ p\mid A_n,\ p\nmid A_{n-1}}} p^{v_p(A_n)}.$$

右辺に現れる素数はすべて A_n の primitive divisor である．

各 $v \in S\cup\{\infty\}$ に対し，$|\cdot|_v$ を $|p|_p = p^{-1}$ と正規化した p 進絶対値または通常の絶対値とする．$R(0)\neq 0$ と $e\geq 2$ より，十分小さい $r_v > 0$ をとれば，$|z|_v < r_v$ において $|R(z)|_v$ は正の定数で上下から抑えられ，$|\phi(z)|_v < r_v$ が成り立つ．実際，この近傍での $|R(z)|_v$ の上界を C_v とし，$C_v r_v^{e-1} < 1$ となるように r_v をとればよい．軌道がこの近傍の外にある間は $\lambda_{v,n} \leq -\log r_v$ である．ただし，$\lambda_{v,n} \coloneqq \log\max\{1, |\frac{B_n}{A_n}|_v\}$ とおく．一度この近傍に入ると以後もその中にとどまり，次が成り立つ．

$$\lambda_{v,n+1} = e\lambda_{v,n} - \log|R(\phi^n(\alpha))|_v = e\lambda_{v,n} + O(1).$$

この式を e^{n+1} で割り，$\sum_{n\geq 0} e^{-n-1}$ が収束することを用いると，$\lambda_{v,n} = O(e^n)$ を得る．

一方，次が成り立つことに注意する．

$$\lambda_{p,n} = \log\max\{1, p^{v_p(A_n)-v_p(B_n)}\} = \max\{0, v_p(A_n)-v_p(B_n)\}\log p = v_p(A_n)\log p.$$

最後の等号は，$\gcd(A_n, B_n) = 1$ より，$v_p(A_n) > 0$ ならば $v_p(B_n) = 0$ となり，$v_p(A_n) = 0$ ならば最大値が 0 となることから従う．また $h(\phi^n(\alpha)) = \log\max\{|A_n|, |B_n|\}$ より，次が成り立つことにも注意する．

$$\lambda_{\infty,n} = \log\frac{\max\{|A_n|, |B_n|\}}{|A_n|} = h(\phi^n(\alpha)) - \log|A_n|.$$

このとき，次が得られる．

$$\begin{aligned} h(\phi^n(\alpha)) &= \log|A_n| + \lambda_{\infty,n} \\ &= \log A_{n,S} + \sum_{p\in S} v_p(A_n)\log p + \lambda_{\infty,n} \quad (\because |A_n| = A_{n,S}\prod_{p\in S} p^{v_p(A_n)}) \\ &= \log A_{n,S} + \sum_{v\in S\cup\{\infty\}} \lambda_{v,n} \\ &= \log A_{n,S} + O(e^n). \quad (\because v\in S\cup\{\infty\} \text{ に対して} \lambda_{v,n} = O(e^n) \text{ かつ } S \text{ は有限集合}) \end{aligned}$$

S は有限集合なので，この和も $O(e^n)$ である．

一方，$H(\alpha) \coloneqq \widehat{h}_\phi(\alpha) > 0$ とおく．α の軌道 $\{\alpha, \phi(\alpha), \phi^2(\alpha), \cdots\}$ が無限集合であるから，$H(\alpha) > 0$ である．標準高さの性質から次が成り立つ．

$$h(\phi^n(\alpha)) = \widehat{h}_\phi(\phi^n(\alpha)) + O(1) = d^n H(\alpha) + O(1).$$

以上より，$\log A_{n,S} = d^n H(\alpha) + O(e^n)$ である．この式を n と $n-1$ に適用すると，次が得られる．

$$\log\frac{A_{n,S}}{A_{n-1,S}^e} = \log A_{n,S} - e\log A_{n-1,S} = (d-e)d^{n-1}H + O(e^n).$$

両辺を d^{n-1} で割って，極限 $n\to\infty$ をとると，$e < d$ に注意すれば十分大きいすべての n に対して $\frac{A_{n,S}}{A_{n-1,S}^e} > 1$ となる．

積表示 $\frac{A_{n,S}}{A_{n-1,S}^e} = \prod_{\substack{p\mid A_n,\ p\nmid A_{n-1}\\ p\notin S}} p^{v_p(A_n)}$ があったことを思い出そう．積表示を各 $j \geq 2$ に適用すると，商 $\frac{A_{j,S}}{A_{j-1,S}^e}$ は正の整数である．従って次が得られる．

$$A_{j-1,S} \mid A_{j-1,S}^e \mid A_{j,S}.$$

これを繰り返すと，$1 \leq m < n$ に対して，$A_{m,S} \mid A_{n-1,S}$ を得る．よって素数 p に対して「$p \mid A_j \Rightarrow p \mid A_{j+1}$」が成り立つので，$j = n-1$ とした場合の対偶を考えると次が得られる．

$$p \nmid A_{n-1} \implies \big(\forall\, m \in \{1,\dots,n-1\},\ p \nmid A_m\big).$$

これは p が A_n の primitive divisor であることを意味する． □

注意 7. 本稿では [1] の定理の特殊な場合として，$\mathbb{Q}$ 上の有理写像 ϕ が 0 を不動点とし，その零点の位数 e が $2 \leq e < \deg\phi$ を満たす場合を証明した．一方 [1] では，一般の代数体 K 上の有理写像 ϕ とその周期点 $\gamma \in K$ を考え，ϕ が γ において“polynomial type”でない場合に，無限軌道を持つ点 $\alpha \in K$ に対する $\phi^n(\alpha) - \gamma$ の分子に新たな素因子 (素イデアル) が現れないような n は有限個であることを証明している．特に，0 が不動点の場合には $e = 1$ も含まれる．この一般的な結果の証明には，Roth の定理に基づく Diophantus 近似の深い結果が用いられている．

参考文献

[1] Patrick Ingram, Joseph H. Silverman, *Primitive divisors in arithmetic dynamics*, Math. Proc. Cambridge Philos. Soc. 146 (2009), 289-302.

[2] Joseph H. Silverman, *Wieferich's criterion and the abc-conjecture*, Journal of Number Theory 30, No 2, 226-237 (1988).

[3] Karl Zsigmondy, *Zur Theorie der Potenzreste*, Monatsh. Math. Phys. Volume 3, 265-284 (1892).

[4] じゅんにー, 『ジグモンディーの定理』, Mathlog, 2026 年 11/7 閲覧.