

多項式の零点の位数とその応用

お茶の水女子大学 藤原正彦

$f(x_1, \dots, x_n)$ を p 進整数環 \mathbb{Z}_p に係数をもつ n 変数の多項式とする。 f の、素数 p を法とした時の、零点の位数を考えることは、数論の中にしばしば重要性をもつて登場する。

ν を p を任意の素数とし、これを fix する。 ν を、 $f \equiv 0 \pmod{p^\nu}$ なる方程式の解の位数とする。 また、 $\nu > 2\lambda$ を満たす λ の正整数を fix する。 この場合 ν の集合を定義する。

$$S_{\nu, \lambda} = \left\{ \underline{x} = (x_1, \dots, x_n) \text{ point mod } p^\nu ; \begin{array}{l} f(\underline{x}) \equiv 0 \pmod{p^\nu}, \\ \frac{\partial f}{\partial x_i}(\underline{x}) \equiv 0 \pmod{p^\lambda} \text{ for any } i \text{ and } \frac{\partial f}{\partial x_k}(\underline{x}) \not\equiv 0 \pmod{p^{\lambda+1}} \\ \text{for some } k \end{array} \right\}$$

$$S_{\nu, \lambda, k} = \left\{ \underline{x} = (x_1, \dots, x_n) \in S_{\nu, \lambda} ; \begin{array}{l} \frac{\partial f}{\partial x_i}(\underline{x}) \equiv 0 \pmod{p^{\lambda+1}} \text{ for} \\ \text{any } i < k, \frac{\partial f}{\partial x_k}(\underline{x}) \not\equiv 0 \pmod{p^{\lambda+1}} \end{array} \right\}$$

明らか

$$S_{\nu, \lambda} = \bigcup_{k=1}^n S_{\nu, \lambda, k} \quad (\text{disjoint})$$

同様に次の集合を定義しよう。

$$\overline{S_{\nu, \lambda}} = \{ \underline{x} \in S_{\nu, \lambda} \text{ point mod } p^{\nu-\lambda} \}$$

$$\overline{S_{\nu, \lambda, k}} = \{ \underline{x} \in S_{\nu, \lambda, k} \text{ point mod } p^{\nu-\lambda} \}$$

明らか

$$\overline{S_{\nu, \lambda}} = \bigcup_{k=1}^n \overline{S_{\nu, \lambda, k}} \quad (\text{disjoint})$$

$\alpha \in \mathbb{Z}$, mod p^ν の数 α に $\bar{\alpha} \in \mathbb{Z}$ mod $p^{\nu-\lambda}$ の数 $\bar{\alpha}$ を,

$$\bar{\alpha} \equiv \alpha \pmod{p^{\nu-\lambda}} \quad \text{と定義しよう。}$$

Lemma 1 Red 写像 $(x_1, \dots, x_n) \mapsto (\bar{x}_1, \dots, \bar{x}_n)$

により定義すると, $\text{Red} : S_{\nu, \lambda, k} \xrightarrow{\text{onto}} \overline{S_{\nu, \lambda, k}}$ である。

$$\text{すなわち, } |\text{Red}^{-1}(\underline{a})| = p^{\lambda n} \quad \text{for } \underline{a} \in \overline{S_{\nu, \lambda, k}}$$

Lemma 2

$$|S_{\nu+1, \lambda}| = p^{n-1} |S_{\nu, \lambda}|$$

Lemma 3 $f(x_1, \dots, x_n)$ を \mathbb{Z}_p 上 non-singular

とする。すると、或る正数 δ, μ が存在して、任意の $\nu \geq \mu$ と $f(\underline{x}) \equiv 0 \pmod{p^\nu}$ (1) $\frac{\partial f}{\partial x_k}(\underline{x}) \not\equiv 0 \pmod{p^{\delta+1}}$ があることが成り立つ。

Theorem 1 $f(x_1, \dots, x_n)$ を \mathbb{Z}_p 上 non-singular と

する。すると、或る正数 ν_0 が存在して $\Delta_{\nu+1} = p^{n-1} \Delta_\nu$ for $\nu \geq \nu_0$ 。

(注意) この結果は、 $f(x_1, \dots, x_n) = x_1^R + \dots + x_n^B - N$
 なる形の時には知られている。例えば E. Landau "Vorlesungen über Zahlentheorie" を見よ。

上の Theorem はいくつかの応用をもつ。まずホアケル級数への応用を考える。次の中級数、

$$P(z) = \sum_{\nu=1}^{\infty} A_{\nu} z^{\nu}$$

を多項式 f の Poincaré series という。基本予想は、
 "P(z) が有理函数" であるが、これは、最近、J. Igusa
 "Complex Power and Asymptotic Expansion II" Crelle 278/279
 (1976) により肯定的に解決された。そこで、彼自身の
 Asymptotic Expansion の理論、及び左中の特異点還元
 の定理を用いている。f が non-singular の時は、簡単に解
 決される。

Theorem 2 f が non-singular なら、その Poincaré
 series は rational である。

(*) Th. 1 から trivial

同様の定理が form に対しても成立する。

Theorem 3 F が、 $(0, \dots, 0)$ を除いて non-singular
 な form とすると、その Poincaré series は rational である。

② Th. 2 では、分母 = $1 - p^{n-1}z$ とする。

Th. 3 では、分母 = $(1 - p^{n(d-1)}z^d)(1 - p^{n-1}z)$ とする。

ただし $d = \text{degree of } F$

②、次に singular series の応用を考へる。

今より通り、 $f(x_1, \dots, x_n) \in \mathbb{Z}[x_1, \dots, x_n]$ とする。

$e(t) = \exp(2\pi i t)$ $t: \text{real}$ と略記する。より前

記を如く、 $f \equiv 0 \pmod{p^v}$ の解の個数とする。すると、

$$\begin{aligned} A_v &= p^{-v} \sum_{t=1}^{p^v} \sum_{x_1=1}^{p^v} \cdots \sum_{x_n=1}^{p^v} e\left(\frac{t}{p^v} f(x_1, \dots, x_n)\right) \\ &= p^{-v} \sum_{\lambda=0}^v \sum_{\substack{u=1 \\ (u,p)=1}}^{p^\lambda} \sum_{x_1=1}^{p^\lambda} \cdots \sum_{x_n=1}^{p^\lambda} e\left(\frac{u}{p^\lambda} f(x_1, \dots, x_n)\right) \end{aligned}$$

②、任意の q に対して、次を定義する。

$$S_{u,q} = \sum_{x_1=1}^q \cdots \sum_{x_n=1}^q e\left(\frac{u}{q} f(x_1, \dots, x_n)\right)$$

$$A(q) = q^{-n} \sum_{\substack{u=1 \\ (u,q)=1}}^q S_{u,q}$$

$$\begin{aligned} \text{すなわち、} \quad A_v &= p^{-v} \sum_{\lambda=0}^v \sum_{\substack{u=1 \\ (u,p)=1}}^{p^\lambda} p^{(v-\lambda)n} S_{u,p^\lambda} = p^{v(n-1)} \sum_{\lambda=0}^v A(p^\lambda) \\ &= p^{v(n-1)} \left\{ 1 + \sum_{\lambda=1}^v A(p^\lambda) \right\} \end{aligned}$$

従つて、

$$\frac{p^\nu}{p^{\nu(n-1)}} = 1 + \sum_{\lambda=1}^{\nu} A(p^\lambda)$$

±2. f の singular series G は $\sum_{q=1}^{\infty} A(q)$ と定義される。 $A(q)$ は multiplicative であることが簡単に証明できるから、 G が絶対収束であることが分れば、

$$G = \prod_{\substack{\text{all} \\ \text{primes}}} \left(\sum_{\nu=0}^{\infty} A(p^\nu) \right) = \prod_{\substack{\text{all} \\ \text{primes}}} \chi(p)$$

、ただし $\chi(p) = \sum_{\nu=0}^{\infty} A(p^\nu)$ とする。

この G の絶対収束と正値性は重要である。例えば E. Landau "Vorlesungen über Zahlentheorie" とか H. Davenport "Analytic Methods for Diophantine Equations and Diophantine Inequalities"。

±2. この G に関して我々は次の定理を証明することが出来る。

Theorem 4 f を絶対既約, 絶対非特異 とする。あると、singular series G は $n \geq 4$ の下で絶対収束する。

±2. $F(x_1, \dots, x_n) \in \mathbb{Z}[x_1, \dots, x_n]$ \pm degree d の form

とする。

Theorem 5 F を絶対既約かつ絶対非特異 (原点を除く) とする。すなわち、singular series G は $n \geq 2d+1$ の条件の下で絶対収束する。

(注意) 証明は一般に \mathbb{Z} を除いて初等的である。多項式の有限体における解の位数に用いる Deligne の結果を本質的に用いるからである。しかし、 f (或いは F) が additive な polynomial の時は、Chebychev の方法によつて、これを回避することが出来、完全に初等的となる。すなわち、上の Th. 4 と 5 は、 f (或いは F) が additive の時には、既知である。

(以上)