数理解析研究所講究録
294巻 1977年 9-14

多項式の零点の個数とその応用

お茶の水女子大学　藤原正彦

$f(X_1, \cdots, X_n)$ 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、零点の個数を考えることは、数論の中にしばしば重要性をもって登場する。

ここで p を任意の素数とし、それを fix する。Δ_ν を、$f \equiv 0 \pmod{p^\nu}$ なる方程式の解の個数とする。また、$\nu > 2\lambda$ を満す二つの正整数を fix する。ここで次の二つの集合を定義する。

$$S_{\nu,\lambda} = \left\{ \underline{x} = (x_1, \cdots, x_n) \text{ point mod } p^\nu ;\ f(\underline{x}) \equiv 0 \ (p^\nu),\ \frac{\partial f}{\partial X_i}(\underline{x}) \equiv 0 \ (p^\lambda) \text{ for any } i \text{ and } \frac{\partial f}{\partial X_k}(\underline{x}) \not\equiv 0 \ (p^{\lambda+1}) \text{ for some } k \right\}$$

$$S_{\nu,\lambda,k} = \left\{ \underline{x} = (x_1, \cdots, x_n) \in S_{\nu,\lambda} ;\ \frac{\partial f}{\partial X_i}(\underline{x}) \equiv 0 \ (p^{\lambda+1}) \text{ for any } i < k,\ \frac{\partial f}{\partial X_k}(\underline{x}) \not\equiv 0 \ (p^{\lambda+1}) \right\}$$

明らかに

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

同様に次の集合を定義しよう。

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

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

明らかに

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

さて、$\bmod p^{\nu}$ の数 γ に対して $\bmod p^{\nu-\lambda}$ の数 $\bar{\gamma}$ を、

$\bar{\gamma} \equiv \gamma \pmod{p^{\nu-\lambda}}$ で定義しよう。

Lemma 1 Red なる写像を、$(\gamma_1, \cdots, \gamma_n) \longmapsto (\bar{\gamma}_1, \cdots, \bar{\gamma}_n)$ により定義すると、$\mathrm{Red} : S_{\nu,\lambda,k} \xrightarrow{\text{onto}} \overline{S_{\nu,\lambda,k}}$ で、

しかも、 $|\mathrm{Red}^{-1}(\underline{a})| = p^{\lambda n}$ for $\forall \underline{a} \in \overline{S_{\nu,\lambda,k}}$

Lemma 2

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

Lemma 3 $f(x_1, \cdots, x_n)$ を $\mathbb{Z}_p$ で 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 $f(\underline{\xi}) \equiv 0 \ (p^{\nu})$ (に対して)、$\frac{\partial f}{\partial x_k}(\underline{\xi}) \not\equiv 0 \ (p^{\delta+1})$ があるkで成り立つ。

Theorem 1 $f(x_1, \cdots, x_n)$ を $\mathbb{Z}_p$ で non-singular とする。すると、ある正数 ν_0 が存在して $\Delta_{\nu+1} = p^{n-1} \Delta_{\nu}$ for $\forall \nu \geq \nu_0$。

(注意) この結果は、$f(x_1,\cdots,x_n)=x_1^{k_1}+\cdots+x_n^{k_n}-N$ 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。まずポアンカレ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。そこでは、彼自身の Asymptotic Expansion の理論、及び広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。

(証) 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、$(0,\cdots,0)$ を除いて non-singular な form とすると、その Poincaré series は rational である。

(注) Th. 2 では、分母 $= 1 - p^{n-1}z$ となり、

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

ただし $d =$ degree of F

さて、次に singular series への応用を考える。

今まで通り、$f(x_1, \cdots, x_n) \in \mathbb{Z}[x_1, \cdots, x_n]$ とする。

$e(t) = \exp(2\pi i t)$ t: real と略記する。A_ν は、前記の如く、$f \equiv 0 \pmod{p^\nu}$ の解の個数とする。すると、

$$A_\nu = p^{-\nu} \sum_{t=1}^{p^\nu} \sum_{x_1=1}^{p^\nu} \cdots \sum_{x_n=1}^{p^\nu} e\left(\frac{t}{p^\nu} f(x_1, \cdots, x_n)\right)$$

$$= p^{-\nu} \sum_{\lambda=0}^{\nu} \sum_{\substack{u=1 \\ (u,p)=1}}^{p^\lambda} \sum_{x_1=1}^{p^\nu} \cdots \sum_{x_n=1}^{p^\nu} e\left(\frac{u}{p^\lambda} f(x_1, \cdots, x_n)\right)$$

さて、任意の q に対して、次を定義する。

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

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

すると、 $A_\nu = p^{-\nu} \sum_{\lambda=0}^{\nu} \sum_{\substack{u=1 \\ (u,p)=1}}^{p^\lambda} p^{(\nu-\lambda)n} S_{u,p^\lambda} = p^{\nu(n-1)} \sum_{\lambda=0}^{\nu} A(p^\lambda)$

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

従って、

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

さて、f の singular series $\mathfrak{S}$ は等に $\sum_{q=1}^{\infty} A(q)$ 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、上が絶対収束であることが分れば、

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

, ただし $\chi(p) = \sum_{\nu=0}^{\infty} A(p^\nu)$, と為る。

この $\mathfrak{S}$ 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".

さて、この $\mathfrak{S}$ に関して我々は次の定理を証明することができる。

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

さて、$F(X_1, \cdots, X_m) \in \mathbb{Z}[X_1, \cdots, X_m]$ を degree d の form

とする。

Theorem 5 F を絶対既約 かつ 絶対非特異(原点を除いて) とする。すると、singular series $\mathfrak{S}$ は $n \geq 2d+1$ の条件の下で絶対収束する。

(注意) 証明は一ケ所を除いて初等的である。多項式の有限体における解の個数に関する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 の方法によって、それを回避することが出来、完全に初等的となる。ちなみに、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)