数理解析研究所講究録
第517巻 1984年 1-11

On a series derived from diophantine equations

お茶の水女子大理 藤原正彦 (Masahiko Fujiwara)

pを素数、$\mathbb{Z}_p$をp進整数環とし、$\mathbb{Z}_p[X_1,\cdots,X_n]$を$\mathbb{Z}_p$を係数とする$n$変数多項式環とする。さて、

$f_1,\cdots,f_m\in\mathbb{Z}_p[X_1,\cdots,X_n]$ とし、

$$\begin{aligned}
s_\nu &= \text{the number of solutions of } f_1=0,\cdots,f_m=0 \mod p^\nu \\
&= \left|\{\underline{x} \bmod p^\nu \,;\, f_1(\underline{x})\equiv 0,\cdots,f_m(\underline{x})\equiv 0 \pmod{p^\nu}\}\right|
\end{aligned}$$

とおく。この時、次の級数

$$P(z)=\sum_{\nu=0}^{\infty} s_\nu z^\nu$$

を$f_1,\cdots,f_m$に付随したPoincaré seriesという。この級数がrationalであろう、との予想がBorevich-Schafarevichの"Number Theory"(A.P. 1966 Chap I §5 のproblem 9)にある。1975年にJ. Igusaは、この予想を、$m=1$の時に肯定的に解決した。本稿では、これを一般のmに対して証明することを眼目とする。証明はまず、$f_1,\cdots,f_m$がcomplete intersectionをなす場合を全く elementaryに処理した後、一般

のmについて、特異点の還元を用いて行なう。complete intersectionの場合は、かなり強引にHensel's lemma型にひきずり込むような証明で、初等的であるが複雑で泥くさいものと言えよう。一般のmについては、Igusaの方法に従がい進むもので、本質的には真似事と言えるかも知れない。

<まずcomplete intersectionの場合。>

$f_1, \cdots, f_m$ がcomplete intersectionをなすとする。

$$\text{(i.e.)}\quad \left.\begin{array}{l} f_1(\underline{x}) = \cdots = f_m(\underline{x}) = 0 \\ \underline{x} \in \mathbb{Z}_p^n \end{array}\right\} \Longrightarrow \operatorname{rank}\left(\frac{\partial f_i}{\partial x_j}\right) = m$$

この仮定をしばらく保持する。次のlemmaは単に、$\mathbb{Z}_p$のcompactnessを映したものに過ぎない。

(lemma 1) $\exists \delta > 0$, $\exists \mu > 0$ such that $\forall \nu > \mu$

$$\text{“}\begin{array}{l} f_1(\underline{x}) \equiv \cdots \equiv f_m(\underline{x}) \equiv 0 \pmod{p^\nu} \\ \underline{x} \in \mathbb{Z}_p^n \end{array} \Longrightarrow p^\delta \nmid {}^\exists m\times m \text{ 小行列式 of } \left(\frac{\partial f_i}{\partial x_j}\right)\text{”}$$

以後、上のlemmaのδと$\mu > 0$をfixすることにする。

$$\Lambda \underset{\mathrm{def}}{=} \{\lambda = (\lambda_1, \cdots, \lambda_m) ;\ 0 \le \lambda_1 \le \cdots \le \lambda_m,\ \lambda_1 + \cdots + \lambda_m < \delta\}$$

とする。Λは当然、有限集合である。ここで、$\nu > \mu, 2\delta$なるνをfixする。このνに対し、

$$S_{\nu,\lambda} \overset{\text{def}}{=} \{ \underline{\underline{\gamma}} = (\gamma_1,\cdots,\gamma_n) \bmod p^\nu \,;\, f_i(\underline{\underline{\gamma}}) \equiv 0 \ (p^\nu) \text{ かつ } \underset{i=1,\cdots,m}{} $$
$$\text{elementary divisors in } \mathbb{Z}_p \text{ of } \left(\frac{\partial f_i}{\partial x_j}(\underline{\underline{\gamma}})\right) = (p^{\lambda_1},\cdots,p^{\lambda_m}) \}$$

$$S_\nu = \{ \underline{\underline{\gamma}} = (\gamma_1,\cdots,\gamma_n) \bmod p^\nu \,;\, f_i(\underline{\underline{\gamma}}) \equiv 0 \ (p^\nu) \ \ i=1,\cdots,m \}$$

とおくと、明らかに

$$S_\nu = \bigcup_{\lambda\in\Lambda} S_{\nu,\lambda} \quad (\text{disjoint})$$

となる。$S_{\nu,\lambda}$ の定義より、$S_{\nu,\lambda} \ni \underline{\underline{\gamma}}$ に対して、$GL(m,\mathbb{Z}_p) \ni {}^\exists A$, $GL(n,\mathbb{Z}_p) \ni {}^\exists B$ が存在し、

$$A\left(\frac{\partial f_i}{\partial x_j}(\underline{\underline{\gamma}})\right)B = \begin{pmatrix} p^{\lambda_1} & & 0 & \\ & \ddots & & \bigcirc \\ 0 & & p^{\lambda_m} & \end{pmatrix}$$

となる。ここで、やや唐突であるが $GL(m,\mathbb{Z}_p)\times GL(n,\mathbb{Z}_p)$ に含まれる (A,B), (C,D) に対し、

$$(A,B) \underset{\lambda}{\sim} (C,D) \underset{\text{def}}{\Longleftrightarrow} A^{-1}\begin{pmatrix} p^{\lambda_1} & & 0 \\ & \ddots & \\ 0 & & p^{\lambda_m} \end{pmatrix}B^{-1} \equiv C^{-1}\begin{pmatrix} p^{\lambda_1} & & 0 \\ & \ddots & \\ 0 & & p^{\lambda_m} \end{pmatrix}D^{-1} \pmod{p^\delta}$$

と定義する。$\Lambda \ni \lambda$ を fix すれば、$\underset{\lambda}{\sim}$ は同値内律になる。

さて、$S_{\nu,\lambda}$ に含まれる各元 γ には上のように (A_γ, B_γ) が付随しているが、これらを $\underset{\lambda}{\sim}$ によって分類した時の同値類を $(A_1,B_1),\cdots,(A_t,B_t)$ と書くことにする。なお、この choice は ν に independent であることがすぐ

に分る。ここで $S_{\nu,\lambda}$ の部分集合を、$k=1,\cdots,t$ に対し

$$S_{\nu,\lambda,k} \underset{\mathrm{def}}{=\!=} \left\{ \gamma \in S_{\nu,\lambda} \,;\, A_k \left(\frac{\partial f_i}{\partial x_j}(\underline{\gamma})\right) B_k \underset{\mathrm{mod}\, p^\delta}{\equiv} \begin{pmatrix} p^{\lambda_1} & & 0 \\ & \ddots & \\ 0 & & p^{\lambda_m} \; 0 \end{pmatrix} \right\}$$

と定義する。この時、明らかに、

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

となる。さて、$k=1,2,\cdots,t$ について、初めの $\underline{f}=(f_1,\cdots,f_m)$ の代りに $A_k \underline{f}(B_k \underline{y})$ なる $\underline{y}=(y_1,\cdots,y_n)$ についての多項式ベクトルを考え、それを、$\underline{h}_k(\underline{y})$ とおく。すなわち、$\underline{h}_k(\underline{y}) = A_k \underline{f}(B_k \underline{y})$

$\underline{\gamma}' = B_k^{-1}\underline{\gamma}$ とおくと、これは $\underline{h}_k(\underline{y}) \equiv 0 \ (p^\nu)$ なる連立方程式の根になっているが、$\underline{h}_k$ を $\underline{\gamma}'$ で Taylor 展開すると、$\underline{f}$ の $\underline{\gamma}$ における Jacobian 行列を $M_{\underline{f}}(\underline{\gamma})$ と書く時、

$$(*) \quad \underline{h}_k(\underline{y}) = \underline{h}_k(\underline{\gamma}') + A_k M_{\underline{f}}(\underline{\gamma}) B_k (\underline{y}-\underline{\gamma}') + \sum_{j,k} a_{j,k} \frac{\partial^2 \underline{h}_k}{\partial y_j \partial y_k}(\underline{\gamma}')(y_j-\gamma_j')(y_k-\gamma_k') + \cdots$$

となる。ここで右辺第二項の $A_k M_{\underline{f}}(\underline{\gamma}) B_k \equiv \begin{pmatrix} p^{\lambda_1} & & 0 \\ & \ddots & \\ 0 & & p^{\lambda_m} \end{pmatrix}_{\mathrm{mod}\, p^\delta}$ が重要である。

ここで $S'_{\nu,\lambda,k} = \{ B_k^{-1}\underline{\gamma} \,;\, \underline{\gamma} \in S_{\nu,\lambda,k} \}$ と書く。

集合 $S'_{\nu,\lambda,k}$ は、集合 $S_{\nu,\lambda,k}$ が $\underline{f}$ より定義されたのと同じ

方法で、$\underline{\underline{h}}_k$ より定義された集合となっている（k を fix して考えると）。

$\underline{\underline{x}} = (x_1, \cdots, x_n)$ が point mod $(\nu_1, \cdots, \nu_n)$ とは、各 x_i が integer mod p^{ν_i} のこととする。この notation を用いて、reduction map $Red^{\nu}_{\nu-\lambda}$ を次のように定義する。

$$Red^{\nu}_{\nu-\lambda} : \{\text{points mod } (\nu, \cdots, \nu)\} \longrightarrow \{\text{points mod } (\nu-\lambda_1, \cdots, \nu-\lambda_m, \nu, \cdots, \nu)\}$$

$$(\gamma_1, \cdots, \gamma_n) \longmapsto (\bar{\gamma}_1, \cdots, \bar{\gamma}_m, \gamma_{m+1}, \cdots, \gamma_n)$$

ただし $\gamma_i \equiv \bar{\gamma}_i \pmod{p^{\nu-\lambda_i}}$
$(i = 1, 2, \cdots, m)$

また、$Red : \{\text{points mod } (\nu+1, \cdots, \nu+1)\} \longrightarrow \{\text{points mod } (\nu, \cdots, \nu)\}$

$$(\gamma_1, \cdots, \gamma_n) \longmapsto (\bar{\gamma}_1, \cdots, \bar{\gamma}_n)$$

ただし $\gamma_i \equiv \bar{\gamma}_i \pmod{p^{\nu}}$
$(i = 1, \cdots, n)$

とおく。この時、

$$\begin{tikzcd}
S_{\nu+1,\lambda,k} \arrow[r, "B_k^{-1}\cdot", "1:1"'] \arrow[d, "Red"'] \arrow[dr, phantom, "\circlearrowright"] & S'_{\nu+1,\lambda,k} \arrow[d, "Red"] \\
S_{\nu,\lambda,k} \arrow[r, "1:1", "B_k^{-1}\cdot"'] & S'_{\nu,\lambda,k} \arrow[d, "onto"', "Red^{\nu}_{\nu-\lambda}"] \\
 & \overline{S'_{\nu,\lambda,k}}
\end{tikzcd}$$

となることが分るが、$\overline{S'_{\nu,\lambda,k}} \underset{def}{=} Red^{\nu}_{\nu-\lambda}(S'_{\nu,\lambda,k}) \ni {}^{\forall}\underline{\underline{\bar{\gamma}}}'$ に対して、$(Red^{\nu}_{\nu-\lambda})^{-1}(\underline{\underline{\bar{\gamma}}}') \subset S'_{\nu,\lambda,k}$

となることがすぐ分るから、$\overline{S'_{\nu,\lambda,k}} = \{\underline{\underline{\mu}}_1, \cdots, \underline{\underline{\mu}}_A\}$ とおくと、

$$S'_{\nu,\lambda,k} = \bigcup_{i=1}^{s} (\mathrm{Red}^{\nu}_{\nu-\lambda})^{-1}(\underline{\underline{\mu}}_i) \quad (\text{disjoint})$$

となる。一方、$S'_{\nu+1,\lambda,k}$ の元は全て $S'_{\nu,\lambda,k}$ の延長ゆえ、$\overline{S_{\nu,\lambda,k}}$ の元の延長と考えられる。すなわち、

$$S'_{\nu+1,\lambda,k} = \mathrm{Red}^{-1}(S'_{\nu,\lambda,k}) = \bigcup_{i=1}^{s} (\mathrm{Red}^{\nu}_{\nu-\lambda} \circ \mathrm{Red})^{-1}(\underline{\underline{\mu}}_i)$$

$$(\text{disjoint})$$

(lemma 2) $\left|(\mathrm{Red}^{\nu}_{\nu-\lambda})^{-1}(\underline{\underline{\mu}}_i)\right| = p^{\lambda_1+\cdots+\lambda_m}$ for $i=1,2,\cdots,s$

これは、$\underline{\underline{h}}_k(\underline{\underline{y}})$ を $\underline{\underline{\mu}}_i$ で展開した後に、(p.4 の(*)式)

$$\underline{\underline{y}} = \underline{\underline{\mu}}_i + \begin{pmatrix} p^{\nu-\lambda_1}\xi_1 \\ \vdots \\ p^{\nu-\lambda_m}\xi_m \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$ とおくと、

$$\underline{\underline{h}}_k\left(\underline{\underline{\mu}}_i + \begin{pmatrix} p^{\nu-\lambda_1}\xi_1 \\ \vdots \\ p^{\nu-\lambda_m}\xi_m \\ 0 \\ \vdots \\ 0 \end{pmatrix}\right) \equiv \underline{\underline{h}}_k(\underline{\underline{\mu}}_i) + \begin{pmatrix} p^{\lambda_1} & & * & \\ & \ddots & & * \\ * & & p^{\lambda_m} & \end{pmatrix} \begin{pmatrix} p^{\nu-\lambda_1}\xi_1 \\ \vdots \\ p^{\nu-\lambda_m}\xi_m \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

$$(\mathrm{mod}\ p^{\nu+1})$$

ただし $* \equiv 0 \ (\mathrm{mod}\ p^{\delta})$

となるから、左辺 $\equiv 0\ (p^{\nu})$ であるために $\xi_1, \cdots, \xi_m$ は任意の値をとってよいことから分る。

(lemma 3) $\left|(\mathrm{Red}^{\nu}_{\nu-\lambda} \circ \mathrm{Red})^{-1}(\underline{\underline{\mu}}_i)\right| = p^{\lambda_1+\cdots+\lambda_m} p^{n-m}$

これは、lemma 2 の証明における $\underline{\underline{y}}$ を、

$$\underline{\underline{y}} = \underline{\underline{\mu}}_i + \begin{pmatrix} p^{\nu-\lambda_1}\xi_1 \\ \vdots \\ p^{\nu-\lambda_m}\xi_m \\ p^{\nu}\xi_{m+1} \\ \vdots \\ p^{\nu}\xi_n \end{pmatrix}$$ とおきかえれば、$\xi_1, \cdots, \xi_m$ は mod p

で unique , $\xi_{m+1}, \cdots, \xi_n$ は任意であることより分る。

lemma 2 と lema 3 より明らかに、$|S'_{\nu+1,\lambda,k}| = p^{n-m}|S'_{\nu,\lambda,k}|$

従って、$|S'_{\nu+1,\lambda,k}|$ と $|S_{\nu+1,\lambda,k}|$ が等しいことを考えれば $|S_{\nu+1,\lambda,k}| = p^{n-m}|S_{\nu,\lambda,k}|$ となる。

従って

$$\begin{cases} S_{\nu+1,\lambda} = \bigcup_{k=1}^{t} S_{\nu+1,\lambda,k} & (\text{disjoint}) \\ S_{\nu,\lambda} = \bigcup_{k=1}^{t} S_{\nu,\lambda,k} & (\text{disjoint}) \end{cases}$$

を考えると、$|S_{\nu+1,\lambda}| = p^{n-m}|S_{\nu,\lambda}|$

同様に、

$$\begin{cases} S_{\nu+1} = \bigcup_{\lambda\in\Lambda} S_{\nu+1,\lambda} & (\text{disjoint}) \\ S_{\nu} = \bigcup_{\lambda\in\Lambda} S_{\nu,\lambda} & (\text{disjoint}) \end{cases}$$

を考えると、次の定理が得られたことになる。

(Theorem) $\quad s_{\nu+1} = p^{n-m} s_\nu$

すなわち、$f_1, \cdots, f_m$ が complete intersection の時、大きな ν に対しては常に、$s_{\nu+1} = p^{n-m} s_\nu$ の成立することが分った。従って特に、

(Theorem) $f_1, \cdots, f_m$ が complete intersection の時、Poincaré series $P(z)$ は rational である。

＜一般の場合＞

k = local field $\supset R$ = integer ring = maximal compact subring

$R \supset P$ = unique maximal ideal $= \pi R$ とする。

また、$|\{R/\pi R\}| = q$, $|\pi|_k = \frac{1}{q}$ なる k の valuation を fix する。また、$X = k^n \supset X^0 = R^n$ とおく。

locally compact abelian group X 上の Haar measure $|dx|$ を、compact subset X^0 上で 1 となるように normalize しておく。

i.e. $\displaystyle\int_{X^0} |dx| = 1$

$f_1, \cdots, f_m \in R[X_1, \cdots, X_n]$ とし、s を複素変数とする。

また、$q^{-s} = z$ とおく時、次の積分を定義する。

$$Q(z) \underset{\mathrm{def}}{=} \int_{X^0} (\max_i |f_i(x)|_k)^s |dx|$$

ここで、

$$E_e \underset{\mathrm{def}}{=} \{x \in X^0 ; \max_i |f_i(x)|_k = q^{-e}\} = \{x \in X^0 ; \min_i \{\mathrm{ord} f_i(x)\} = e\}$$

とおくと、明らかに、

$$X^0 = \sum_{e \geq 0} E_e \cup E_\infty \quad (\text{disjoint})$$ となる。

ただし $E_\infty = X^0 \cap (\bigcap_i f_i^{-1}(0))$

さて、$E_e \ni x$ に対して、$(\max_i |f_i(x)|_k)^s = q^{-es} = z^e$ となり、

また、$|dx|$ の定める measure を m と記す時、

$$\int_{E_e}|dx| = m(E_e) = m(X^0 \cap \underset{=}{f}^{-1}(P^e)) - m(X^0 \cap \underset{=}{f}^{-1}(P^{e+1}))$$
$$= s_e q^{-ne} - s_{e+1} q^{-n(e+1)}$$

であることが容易に分る。従って、

$$Q(z) = \sum_{e\geq 0} z^e \int_{E_e}|dx| = \sum_{e\geq 0} z^e s_e q^{-ne} - \sum_{e\geq 0} z^e s_{e+1} q^{-n(e+1)}$$
$$= \sum_{e\geq 0} s_e (q^{-n}z)^e - \sum_{e\geq 0} \frac{1}{z} s_{e+1} (q^{-n}z)^{e+1}$$
$$= P(q^{-n}z) - (P(q^{-n}z)-1)z^{-1}$$

すなわち、

rationality of $Q(z) \Longleftrightarrow$ rationality of $P(z)$

$Q(z)$ の rationality を調べるために、resolution を用いる。affine space X に含まれる m 個の divisors（ただし、それぞれ $f_1=0, \cdots, f_m=0$ で定められるもの）を $D_1, \cdots, D_m$ とした時、$X, D_1, \cdots, D_m$ の resolution over K を、(Y, h) とする。すなわち、Y は irreducible non-singular algebraic variety $/K$ で、h は Y から X への everywhere regular な birational map $/K$ であり、また、h^{-1} は各 D_i の simple point で regular（従って birregular）、$Y \ni {}^\forall b$ について $h^*(D_i)$ 達の irreducible components（b を通るような）は b において mutually transversal とする。この時、$Y_K \ni {}^\forall b$ に

ついて、K上定義されたY上の local coordinates $y_1, \cdots, y_n$ が存在して、

$$\begin{cases} y_1(b) = \cdots = y_n(b) = 0 \\ f_i \circ h = \varepsilon_i \prod_k y_k^{N_{ik}} \quad (i=1,\cdots,m) \\ h^*(dx) = \eta \prod_k y_k^{\nu_k - 1} dy \end{cases}$$

ただし ε_i, η は b の周りの invertible K-analytic function.

と書ける。

さて、$Q(z)$ の rationality に戻ると、$Q(z)$ の定義式の右辺を考えた時、X^0 を compact open subset で cover することにより、

$$\int_U (\max_i |f_i(x)|_K)^{\lambda} |dx| \qquad U \text{は compact open}$$

が rational を言えばよいことが分る。これは更に、上より

$$\int_V (\max_i |\varepsilon_i \prod_k y_k^{N_{ik}}|_K)^{\lambda} |\eta \prod_k y_k^{\nu_k - 1} dy| \qquad V \text{は compact open}$$

が rational を言うことに帰着スル。ここに V は $b' + (p^e)^{(n)}$ の形ととれる。この積分は、$b' \notin (p^e)^{(n)}$ の時はごく簡単に z に関して rational であることが証明される。

$b' \in (p^e)^{(n)}$ の時は $V = (p^e)^{(n)}$ となるが、$\int_V$ を

$\sum_{k_1,\cdots,k_n \geq e} \int_{\pi^{k_1}U \times \cdots \times \pi^{k_n}U}$ と変形すると、(ここで U は K の単数群) 積分の中味が計算でき、結局は、

積分内のmaxを達成するlごとに、すなわち別の表現をすれば、ある整係数一次連立不等式を満たす$(k_1,\cdots,k_n)$ごとに(このような連立不等式により全$(k_1,\cdots,k_n)$は丁度m個のsubsetに分割される)上記の積分を行なうことになる。この積分をした結果、上の級数がm個のsubsetごとにrational(zに関して)になることが分るのである。この部分は初等的であるがここでは割愛することにする。

≪added in proof≫ 京大数理研にてこの講演をした後、帰京してから、立教大の佐藤文広氏よりの手紙で、上記結果がすでに D. Meurer "On the rationality of certain generating functions", Math. Annalen 256, 303-310 (1981) に証明されていることを知った。一般の場合にやはりIgusaの方法を用いており本質的にはほとんど同じであることが判明した。ただし、本稿で述べたcomplete intersectionの場合の初等的証明については触れられておらず、またこの証明がHenselのlemmaの最終的形を与えているという点で面白く思えたので、上に詳述した。また、この初等的方法によると、rational以上のこと、つまり多項式+等比級数となることまで分り、興味あるように思える。