

Title	On a series derived from diophantine equations(Distribution of values of arithmetic functions)
Author(s)	藤原, 正彦
Citation	数理解析研究所講究録 (1984), 517: 1-11
Issue Date	1984-04
URL	http://hdl.handle.net/2433/98405
Right	
Type	Departmental Bulletin Paper
Textversion	publisher

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、 $\mathbb{Z}_p[X_1, \dots, X_n]$ を \mathbb{Z}_p を係数とする n 変数多項式環とする。すなわち、

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

$\Delta_\nu =$ the number of solutions of $f_1 = 0, \dots, f_m = 0 \pmod{p^\nu}$
 $= \left| \left\{ \underline{x} \pmod{p^\nu}; f_1(\underline{x}) \equiv 0, \dots, f_m(\underline{x}) \equiv 0 \pmod{p^\nu} \right\} \right|$

とおく。この時、次の級数

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

を f_1, \dots, f_m に付随した Poincaré series としう。この

級数が rational であるう、との予想が Borevich-Schafarevich の "Number Theory" (A.P. 1966 chap I §5 a 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 に対し証明

することを目とする。証明はまず、 f_1, \dots, 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 型にひまが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 の方法に従うが、 m 個の f_i の場合、本質的には真似事と言えりかも知れなう。

< まず complete intersection の場合。 >

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

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

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 $\forall \nu > \mu$

$$\left\{ \begin{array}{l} f_1(\underline{x}) \equiv \dots \equiv f_m(\underline{x}) \equiv 0 \pmod{p^\nu} \\ \underline{x} \in \mathbb{Z}_p^n \end{array} \right\} \Rightarrow p^\delta \mid \det \left(\frac{\partial f_i}{\partial x_j} \right)$$

以後、上の lemma の δ と $\mu > 0$ を fix することにする。

$$\Lambda \stackrel{\text{def}}{=} \{ (\lambda = (\lambda_1, \dots, \lambda_m)); 0 \leq \lambda_1 \leq \dots \leq \lambda_m, \lambda_1 + \dots + \lambda_m < \delta \}$$

とする。 Λ は当然有限集合である。こゝで、 $\nu > \mu, 2\delta$ なる ν を

fix する。この ν に対し、

$$S_{\nu, \lambda} \stackrel{\text{def}}{=} \left\{ \underline{x} = (x_1, \dots, x_n) \pmod{p^\nu}; f_i(\underline{x}) \equiv 0 \pmod{p^\nu} \text{ for } i=1, \dots, m \right. \\ \left. \text{elementary divisors in } \mathbb{Z}_p \text{ of } \left(\frac{\partial f_i}{\partial x_j}(\underline{x}) \right) = (p^{\lambda_1}, \dots, p^{\lambda_m}) \right\}$$

$$S_\nu = \left\{ \underline{x} = (x_1, \dots, x_n) \pmod{p^\nu}; f_i(\underline{x}) \equiv 0 \pmod{p^\nu} \text{ for } i=1, \dots, m \right\}$$

と示す。明らかに

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

と示す。 $S_{\nu, \lambda}$ の定義より、 $S_{\nu, \lambda} \ni \underline{x}$ に対し、

$GL(m, \mathbb{Z}_p) \ni \exists A$, $GL(m, \mathbb{Z}_p) \ni \exists B$ が存在し、

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

と示す。こゝで、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、

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

と定義する。 $\Lambda \ni \lambda$ を fix すれば、 $\underset{\lambda}{\sim}$ は同値関係に
なる。

さて、 $S_{\nu, \lambda}$ に含まれる各元 \underline{x} には上のように (A_x, B_x) 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 $(A_1, B_1), \dots, (A_t, B_t)$ と置くことにする。

よって、この choice は ν に independent であることが示す。

に命ず。こゝで $S_{\nu, \lambda}$ の部分集合を、 $k=1, \dots, t$ に対し

$$S_{\nu, \lambda, k} \stackrel{\text{def}}{=} \left\{ \underline{\sigma} \in S_{\nu, \lambda}; A_k \left(\frac{\partial f_i}{\partial x_j}(\underline{\sigma}) \right) B_k \equiv \begin{pmatrix} p\lambda_1 & & 0 \\ & \ddots & \\ 0 & & p\lambda_m \end{pmatrix} \pmod{p} \right\}$$

と定義す。この時、明らかに、

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

と存す。さて、 $k=1, 2, \dots, t$ につき、最初の $\underline{f} = (f_1, \dots, f_m)$ の代りに $A_k \underline{f}(B_k \underline{y})$ なる $\underline{y} = (y_1, \dots, y_n)$ につき \mathbb{Z} の多項式ベクトルを考へ、之を $\underline{h}_k(\underline{y})$ とおく。可なり、 $\underline{h}_k(\underline{y}) = A_k \underline{f}(B_k \underline{y})$

$\underline{\sigma}' = B_k^{-1} \underline{\sigma}$ とおくと、之は $\underline{h}_k(\underline{y}) \equiv 0 \pmod{p}$ なる連立方程式の根に存するが、 \underline{h}_k を $\underline{\sigma}'$ で Taylor 展開すると、 \underline{f} の $\underline{\sigma}$ における Jacobian 行列を $M_{\underline{f}}(\underline{\sigma})$ と書く時、

$$(*) \quad \underline{h}_k(\underline{y}) = \underline{h}_k(\underline{\sigma}') + A_k M_{\underline{f}}(\underline{\sigma}) B_k (\underline{y} - \underline{\sigma}') +$$

$$\sum_{i, k} a_{i, k} \frac{\partial^2 \underline{h}_k}{\partial y_j \partial y_k}(\underline{\sigma}') (y_j - \sigma'_j)(y_k - \sigma'_k) + \dots$$

と存す。こゝで右辺第一項の $A_k M_{\underline{f}}(\underline{\sigma}) B_k \equiv \begin{pmatrix} p\lambda_1 & & 0 \\ & \ddots & \\ 0 & & p\lambda_m \end{pmatrix} \pmod{p}$ が重要である。

こゝで $S'_{\nu, \lambda, k} = \{ B_k^{-1} \underline{\sigma}; \underline{\sigma} \in S_{\nu, \lambda, k} \}$ と書く。

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

方法で、 \mathcal{P}_k より定義された集合となる、という (k を fix し
て考える)。

$\underline{x} = (x_1, \dots, x_n)$ が point mod (ν_1, \dots, ν_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 $\text{Red}_{\nu-\lambda}^\nu$ を次のように定義する。

$$\begin{aligned} \text{Red}_{\nu-\lambda}^\nu : \{ \text{points mod } (\nu, \dots, \nu) \} &\longrightarrow \{ \text{points mod } (\nu-\lambda_1, \dots, \nu-\lambda_m, \\ &\quad \nu, \dots, \nu) \} \\ \downarrow & \\ (\delta_1, \dots, \delta_n) &\longmapsto (\bar{\delta}_1, \dots, \bar{\delta}_m, \delta_{m+1}, \dots, \delta_n) \\ \text{ただし } \delta_i &\equiv \bar{\delta}_i \pmod{p^{\nu-\lambda_i}} \\ &(i=1, 2, \dots, m) \end{aligned}$$

$$\begin{aligned} \text{また、Red} : \{ \text{points mod } (\nu+1, \dots, \nu+1) \} &\longrightarrow \{ \text{points mod } (\nu, \dots, \nu) \} \\ \downarrow & \\ (\delta_1, \dots, \delta_n) &\longmapsto (\bar{\delta}_1, \dots, \bar{\delta}_n) \\ \text{ただし } \delta_i &\equiv \bar{\delta}_i \pmod{p^\nu} \\ &(i=1, \dots, n) \end{aligned}$$

と置く。この時、

$$\begin{array}{ccc} S_{\nu+1, \lambda, k} & \xrightarrow[\text{I=I}]{B_k^{-1}} & S'_{\nu+1, \lambda, k} \\ \text{Red} \downarrow & \curvearrowright & \downarrow \text{Red} \\ S_{\nu, \lambda, k} & \xrightarrow[\text{B}_k^{-1}]{\text{I=I}} & S'_{\nu, \lambda, k} \\ & & \text{onto } \downarrow \text{Red}_{\nu-\lambda}^\nu \\ & & \overline{S'_{\nu, \lambda, k}} \end{array}$$

と置くことが分かるが、 $\overline{S'_{\nu, \lambda, k}} \stackrel{\text{def}}{=} \text{Red}_{\nu-\lambda}^\nu(S'_{\nu, \lambda, k}) \ni \bar{\delta}' = \delta'$
と、 $(\text{Red}_{\nu-\lambda}^\nu)^{-1}(\bar{\delta}') \subset S'_{\nu, \lambda, k}$

と置くことが分かるが、 $\overline{S'_{\nu, \lambda, k}} = \{ \mu_1, \dots, \mu_d \}$ とおくと、

$S'_{r, \lambda, k} = \bigcup_{i=1}^{\Lambda} (\text{Red}_{\nu-\lambda}^{\nu})^{-1}(\underline{\mu}_i)$ (disjoint)
 とする。一方、 $S'_{r+1, \lambda, k}$ の元は全て $S'_{r, \lambda, k}$ の延長ゆえ、
 $\overline{S'_{r, \lambda, k}}$ の元は延長と考へらる。ゆえに、

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

(disjoint)

(lemma 2) $|(\text{Red}_{\nu-\lambda}^{\nu})^{-1}(\underline{\mu}_i)| = p^{\lambda_1 + \dots + \lambda_m}$ for $i=1, 2, \dots, \Lambda$
 といふは、 $\underline{h}_k(\underline{y})$ を $\underline{\mu}_i$ の展開した後、(p.4の(*)式)

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

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

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

ただし $* \equiv 0 \pmod{p^{\nu}}$

となるから、左辺 $\equiv 0 \pmod{p^{\nu}}$ であるために ξ_1, \dots, ξ_m は任意
 の値をとってよいことが分る。

$$(lemma 3) \quad |(\text{Red}_{\nu-\lambda}^{\nu} \circ \text{Red})^{-1}(\underline{\mu}_i)| = p^{\lambda_1 + \dots + \lambda_m} p^{n-m}$$

といふは、lemma 2 の証明における \underline{y} を、

$$\underline{y} = \underline{\mu}_i + \begin{pmatrix} p^{\nu-\lambda_1} \xi_1 \\ \vdots \\ p^{\nu-\lambda_m} \xi_m \\ p^{\nu} \xi_{m+1} \\ \vdots \\ p^{\nu} \xi_n \end{pmatrix} \text{ とおきか之れは、} \xi_1, \dots, \xi_m \text{ は mod } p$$

unique, ξ_{m+1}, \dots, ξ_n は任意であることより命ずる。

lemma 2 と lemma 3 より明らかなに、 $|S_{\nu+1, \lambda, k}| = p^{n-m} |S'_{\nu, \lambda, k}|$
 従って、 $|S_{\nu+1, \lambda, k}|$ と $|S'_{\nu, \lambda, k}|$ が等しいことを示せば
 $|S_{\nu+1, \lambda, k}| = p^{n-m} |S_{\nu, \lambda, k}|$ となる。

従って

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

と考へると、 $|S_{\nu+1, \lambda}| = p^{n-m} |S_{\nu, \lambda}|$

同様に、

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

と考へると、次の定理が得られたことに存する。

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

可存ゆえ、 f_1, \dots, f_m が complete intersection の時、大抵
 の ν に対し $\Delta_{\nu+1} = p^{n-m} \Delta_{\nu}$ の成立することが
 命じた。従って特に、

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

< 一般の場合 >

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

$R \supset P = \text{unique maximal ideal} = \pi R$ 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 とするよう normalize しておく。

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

$f_1, \dots, f_m \in R[X_1, \dots, X_n]$ とし、 Δ を 複素変数 とする。

また、 $q^{-\Delta} = z$ とおくと、次の積分を定義する。

$$Q(z) \stackrel{\text{def}}{=} \int_{X^0} (\max_i |f_i(x)|_k)^{\Delta} |dx|$$

$z = z^e$ 、

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

とおくと、明らかに、

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

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

すなわち、 $E_e \ni x$ に対し、 $(\max_i |f_i(x)|_k)^{\Delta} = q^{-e\Delta} = z^e$ とする。

また、 $|dx|$ の定まる measure を m と記す時、

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

よある: e が容易に ∞ へ \rightarrow する。従って、

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

よある \Leftarrow .

rationality of $Q(z) \iff$ 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、 e 個 $f_1=0, \dots, f_m=0$ が定めてくれた) を D_1, \dots, D_m

とした時、 X, D_1, \dots, D_m の resolution over K を、

(Y, h) とする。よある \Leftarrow . Y は irreducible non-singular algebraic variety / K 上、 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 上 regular (従って birational)、 $Y \ni \forall b$ に対して $h^{-1}(D_i)$ の irreducible components (b を通るもの) は b において mutually transversal とする。この時、 $Y_K \ni \forall b$ には

つまり、 K 上定義された Y 上の local coordinates y_1, \dots, y_n が存在して、

$$\begin{cases} y_1(b) = \dots = y_n(b) = 0 \\ f_i \circ h = \varepsilon_i \prod_{\mathbb{R}} y_{\mathbb{R}}^{N_{i\mathbb{R}}} \quad (i=1, \dots, m) \\ h^*(dx) = \eta \prod_{\mathbb{R}} y_{\mathbb{R}}^{2k-1} dy \end{cases}$$

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 U で cover できることにより、

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

が rational を意味するといふことが分る。これは更に、上より

$$\int_V (\max_i |\varepsilon_i \prod_{\mathbb{R}} y_{\mathbb{R}}^{N_{i\mathbb{R}}}|_K) \left| \prod_{\mathbb{R}} y_{\mathbb{R}}^{2k-1} dy \right| \quad V \text{ は compact open}$$

が rational を言うことに帰着する。これは V は $b' + (pe)^{(n)}$ の形をとれる。この積分は、 $b' \notin (pe)^{(n)}$ の時はごく簡単に U に内包した rational U があることが証明できる。

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

$$\sum_{k_1, \dots, k_n \geq 0} \int_{\pi^{k_1} U \times \dots \times \pi^{k_n} U} \quad \text{と表すことができ、} (\dots \cup U \text{ は } K \text{ の}$$

単数群) 積分の意味が計算でき、結局は、

積分内の max を達成する点ごとに、それぞれ別の表現をすれば、ある整数係数一次連立不等式を満たす (k_1, \dots, k_n) ごとに (このような連立不等式により全 (k_1, \dots, 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する。この積分をした結果、上の級数が m 個の subset ごとに rational (2 に内して) に存在す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。

<< added in proof >> 京大数理研に 2 回の講演をした後、帰京し 2 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が面白く思えたので、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 + 等比級数と存在することが分り、興味あるように思える。