数理解析研究所講究録
第 837 巻 1993 年 178-184

On the Waring Type Problem for Integral Symmetric Matrices

江上繁樹（富山大学）
〒930 富山市五福 3190
EGAMI Shigeki
(Toyama University)
Gofuku 3190, Toyama city, 930

Introduction. 加法的整数論の古典的問題 —— Waring 問題，Goldbach 問題，分割数の問題 —— を他の代数系へ拡張することは、問題自身に関する興味以外にも、様々な代数的，解析的問題を提起するという点からも興味深い。代数体への拡張は、Rademacher, Siegel 等によって始められ、それ以後の研究によって、現在ではかなり満足すべき形になっている（[4]，[5] 参照）。しかし、非可換な代数系への拡張は、三井による対称行列の分割数、Waring 問題の研究がほとんど唯一のものと思われる。その主要な結果は講義録 [2] にまとめられているが、その序文にも書かれている通り、「多くの問題をかかえた未完成」な分野であり、これからの研究課題を多くふくんでいる。

この小論では、その中の一つの問題 —— Waring 型問題の

Singular series — について，若干の結果を報告したい。

筆者がこのような問題に関心を持つようになったのは[2]のもとになった講義（1983年度，学習院大学）を聴講したことによります。当時，未公刊であった研究内容を話して下さった三井先生に深く感謝致します。

記号： $\mathcal{S} = \mathcal{S}^{(n)} = \{ X \in M_n(\mathbb{R}) \mid {}^tX = X \} \cong \mathbb{R}^\nu \quad \nu = \frac{n(n+1)}{2}$

$\mathcal{P} = \mathcal{P}^{(n)} = \{ X \in \mathcal{S} \mid X$ は正定値 $\}$

$\mathcal{S}$ の部分集合 A に対し，$A_{\mathbb{Z}} = A \cap M_n(\mathbb{Z})$ と表わす．

$r, s \in \mathbb{N}$，$M \in \mathcal{P}_{\mathbb{Z}}$ に対して

$$I_{r,s}(M) = \#\{ (X_1, \cdots, X_s) \in \mathcal{P}_{\mathbb{Z}}^{s} \mid X_1^r + \cdots + X_s^r = M \}$$

とおく．

対称行列に関する Waring 型問題とは

「任意の r に対し，十分大きい s をとれば，$\mathrm{Tr}\,M$ が十分大きい M に対して つねに $I_{r,s}(M) > 0$ となるか？

また，$\mathrm{Tr}\,M \to \infty$ となるとき，その漸近表示を求めよ」

を意味するものとする。

§1. Mitsui's results

講義[2]に述べられている結果を簡単に復習する

Theorem A. $s > 2^{\nu} \cdot r$ のとき、次の漸近表示が成りたつ

$$I_{r,s}(M) = C_0(M) \cdot S(M) \cdot N^{\nu(s-r)} + o\left(N^{\nu(s-r)}\right),$$

ただし、$N = (\mathrm{Tr}\, M)^{\frac{1}{r}}$, また、$C_0(M)$, $S(M)$ は以下で定義される：

$$C_0(M) = \int_{\mathcal{S}} \left(\int_{D} e^{2\pi i \mathrm{Tr}(S^r X)} dS \right)^{s} e^{-2\pi i \mathrm{Tr}(MX)} dX,$$

ただし、$D = \{ S \in \mathcal{P} \mid \mathrm{Tr}\, S \leqq 1 \}$.

$$S(M) = \prod_{p} S_p(M), \quad S_p(M) = 1 + \sum_{k=1}^{\infty} W_{p^k}(M),$$

ただし、$q \in \mathbb{N}$ に対し

$$W_q(M) = \frac{1}{q^{s\nu}} \sum_{A \bmod q}{}' \left(\sum_{D \bmod q} e^{2\pi i \frac{1}{q} \mathrm{Tr}(D^r A)} \right)^{s} e^{-2\pi i \frac{1}{q} \mathrm{Tr}(MA)},$$

ここで、$\sum_{D \bmod q}$ は $D \in \mathcal{S}_{\mathbb{Z}}$ の各成分が mod q の完全代表系を動くような和をあらわし、$\sum'_{A \bmod q}$ はそのようなものの部分和で「Aの成分の最大公約数が q と互いに素」という条件をつけた和を表わす。

以上の $C_0(M)$, $S(M)$ の収束はいずれも自明でないが、$s>2^\nu r$ という条件下では証明されている。後で必要なので、$S(M)$ の収束に必要であった補題も述べておく。

Lemma B. ある正定数が存在して、任意の素数 p, $M\in S_{\mathbb{Z}}$ に対して、

$$|W_{p^t}(M)| \leqq c\cdot p^{t(\nu-\frac{s}{r})}$$

Theorem A を見ると、この式が漸近式として意味をもつためには、$C_0(M)$, $S(M)$ が M に無関係な正定数で下から押えられなければならない（簡単に non-vanishing ということにする）が、これはまだ証明されていない。この論文では、$S(M)$ の non vanishing のための十分条件について論じるが、$S(M)$ は消えることもあるという例を一つ述べておこう。この場合、Waring 型問題そのものが、否定的になる（筆者による）：

$n=2$, $r=6$ のとき $\begin{bmatrix} a & b \\ b & c \end{bmatrix}^6 \equiv \begin{bmatrix} * & 0 \\ 0 & * \end{bmatrix} \pmod 2$

したがって、s がどんな数でも

$X_1^6+\cdots+X_s^6 \equiv \begin{bmatrix} * & 0 \\ 0 & * \end{bmatrix}_{(\mathrm{mod}\,2)}$ となり、 $M=\begin{bmatrix} u & v \\ v & w \end{bmatrix}$

で v が奇数のとき、解は存在しない。

実は類似の現象は代数体の Waring 問題でも存在する。すなわち、すべての整数が r 乗数の和になるわけではない (Siegel)

ので、r乗数で生成される加群を対象とする（[3], [5]）。したがって、行列の場合もMに同様な制限をつければよいと思われるが、この論文ではそういう場合を単に除外することにする。

§2. Non-vanishing of $S(M)$

Lemma B および、$S(M)$の定義から、$S(M)$が消えないためには、任意の素数pに対して、Mに無関係な正定数c_pが存在して

$$(*) \qquad |S_p(M)| \geq c_p$$

が成立すればよいことがわかる。実際、次の定理が成りたつ；

Theorem $s > 2^r \nu$ のとき 次の場合、$(*)$は正しい。

(1) $p \neq 2$

(2) $p = 2$のとき、rは奇数または2の巾

以下、証明のアウトラインを述べよう。ほぼ、古典的な場合と同様であり、$S_p(M)$を合同式の解の個数の極限値として表現し、それが実際、消えないことを示すのである。

$\lambda \in \mathbb{N}$, $M \in \mathcal{S}_{\mathbb{Z}}$ および素数pに対して

$$N_{r,s}(p^\lambda, M) = \#\{(X_1, \cdots, X_s) \bmod p^\lambda \mid X_1^r + \cdots + X_s^r \equiv M \pmod{p^\lambda}\}$$

とおくと、古典的な場合と同様に

$$\frac{1}{p^{(s-1)\nu r}} N_{r,s}(p^\lambda, M) = 1 + \sum_{\mu=1}^{\lambda} w_{p^\lambda}(M) \qquad p > 2$$

$$\leqq (\quad '' \quad) \qquad p = 2$$

が成立する。

Lemma 1. $r, n \in \mathbb{N}$, 素数 p に対し、$\lambda_0 \in \mathbb{N}$ が存在し

$A \in \mathcal{S}_{\mathbb{Z}}^{(n)}$, $A \equiv I \pmod{p^{\lambda_0}}$ ならば、任意の $\lambda \in \mathbb{N}$ に対し

$X \in \mathcal{S}_{\mathbb{Z}}^{(n)}$ が存在し、$X^r \equiv A \pmod{p^\lambda}$

特に $(p, r) = 1$ のとき、$\lambda_0 = 1$ にとれる

証明は たとえば [3], p.136 とほぼ同様

Lemma 2.

(1) $s > 2^r \nu$ で r が奇数のとき 任意の $M \in \mathcal{S}_{\mathbb{Z}}$ に対し

$$X_1^r + \cdots + X_s^r = M$$

は $X_1, \cdots, X_s \in \mathcal{S}_{\mathbb{Z}}$ となる解をもつ

(2) $s \geqq 8\nu r$, $p \neq 2$ のとき ある $\mu_0 \in \mathbb{N}$ があり 任意の $\mu \geqq \mu_0$ なら 任意の $M \in \mathcal{S}_{\mathbb{Z}}$ に対し

$$X_1^r + \cdots + X_s^r \equiv M \pmod{p^\mu}$$

は解をもつ

(3) $r=2^k$, $s \geqq 8\nu r$ のとき、ある $\mu \in \mathbb{N}$ が存在して $\mu \geqq \mu_0$ ならば 任意の $M \in \mathcal{S}_{\mathbb{Z}}$ に対し

$$X_1^r+\cdots+X_s^r \equiv M \pmod{2^\mu}$$

は解をもつ。

これは、古典的 Waring 型等式，合同式に対する解を使い、$X_1,\dots,X_s$ を構成することにより、証明される。

以上、2つの Lemma から、Theorem は以下のように示される。p を固定すると、Lemma 2 により ある μ_0 に対し、（$\mu_0 \geqq \lambda_0$ にとる）

$$X_1^r+\cdots+X_s^r \equiv M \pmod{p^{\mu_0}}, \quad X_1 \equiv I \pmod{p^{\mu_0}}$$

をみたす $X_1,\dots,X_s \in \mathcal{S}_{\mathbb{Z}}$ がとれる。（後者の条件は Lemma 2 で M のかわりに $M-I$ とし、s を1つ増やせばよい） $\mu \geqq \mu_0$ となる μ に対し $Y_2,\dots,Y_s$ を $Y_j \equiv X_j \pmod{p^{\mu_0}}$ をみたす任意の $\mathcal{S}_{\mathbb{Z}}$ の元とすると、このようなものは mod p^μ で $p^{\nu(\mu-\mu_0)(s-1)}$ 個存在する。このとき、$M-Y_1^r-\cdots-Y_s^r \equiv I \pmod{p^{\mu_0}}$ となるので Lemma 1 から $Y_1^r \equiv M-Y_2^r-\cdots-Y_s^r \pmod{p^\mu}$ となる $Y_1 \in \mathcal{S}_{\mathbb{Z}}$ が存在する。

$$\therefore \liminf_{\lambda\to\infty} \frac{N_{r,s}(p^\lambda, M)}{p^{(s-1)\nu\lambda}} \geqq \frac{1}{p^{(s-1)\nu\mu_0}}$$

となり、Theorem が示された。