数理解析研究所講究録
第 689 巻 1989 年 57-63

Theta 級数の mod p について

広大 理 小池正夫 (Masao Koike)
名大 理 谷川好男 (Yoshio Tanigawa)

我々は [K-T] において、primitive form の p 番目の Fourier 係数 (p はレベル) のある性質について数値実験をおこなったが、その結果が、最近 Ponomarev による mod p した theta 級数の basis problem の数値と一致していることがわかった。この小論ではこれらの間の関係についてのべてみたい。まず [K-T] の復習から始める。

p を $p \equiv 1 \bmod 4$ である素数、$\chi(n) = (\frac{n}{p})$ を平方剰余記号とする。$M_2(p,\chi)$ および $S_2(p,\chi)$ で $\Gamma_0(p)$ に関する weight 2 、character χ の integral modular forms および cusp forms の空間をあらわす。$f(z) = \sum_{n=1}^{\infty} a(n)q^n \in S_2(p,\chi)$, $q = e^{2\pi iz}$ を primitive form 即ち $a(1) = 1$ かつすべての Hecke operators の固有関数とすると、その Fourier 係数について

(1) $a(n)^\rho = \chi(n)a(n)$ for $(n,p) = 1$

(2) $a(p)a(p)^\rho = p$

がわかっている。ここで w^ρ は複素数 w の複素共役である。特に (2) より、p の上にある $\bar{\mathbb{Q}}$ の素因子 $\mathfrak{P}$ を一つ固定しておけば

$$a(p) \equiv 0 \bmod \mathfrak{P} \quad \text{または} \quad a(p)^\rho \equiv 0 \bmod \mathfrak{P}$$

であるが、我々が [K-T] で考えたのはこれらが同時に成り立つ f(z)

はいつ存在するかということである。即ち

(#) $a(p) \equiv a(p)^{\rho} \equiv 0 \mod \mathfrak{p}$

とおいたとき、次の実験結果を得た。

$p < 650$ の範囲で (#) を満たす primitive form が存在するのは $p = 229,\ 257$ の二つの場合に限る。

このとき $f(z)$ の一般の Fourier 係数はある種の合同式を満たすことが予想される。実際 $p = 229,\ 257$ の場合には、$\mathbb{Q}(\sqrt{p})$ 上の A_4 拡大を構成することによりその合同式を証明した。

ここで講演以降に Ponomarev により [K-T] Theorem 0.1 の誤りを指摘されたので述べておきたい。Theorem 0.1 では (#) を満たす primitive form が存在する p は $p < 760$ の範囲で $p = 229,\ 257$ のみであると述べたが、これは我々が $a(n)^2$ が $\mathbb{F}_p$-rational であると思い込んでいたための誤りであって、実際には $p = 653$ も [K-T] Cor 1.2 の条件を満たしている。計算機を動かしてみた結果、$p = 653$ にも (#) を満たす primitive form の存在することが確かめられた。この form の一般の Fourer 係数は我々の予想した合同式 Conj. 0.1 (0.1) (0.2) を満たさない。$p = 229,\ 257$ には $\mathbb{Q}$ 上 p のみ分岐する S_4 拡大が対応していたが ([K-T] §4)、$p = 653$ には p のみ分岐の A_5 拡大が対応することを Serre に教わった。こういう p として他には 1381, 2861, 5413 がある。(Mestre の計算)

我々は [K-T] での計算に小池 [Ko] による modular form mod p の理論を使った。即ち M_k , S_k を $\Gamma_0(1)$ に関する weight k の integral modular forms および cusp forms の空間とすると、$S_2(p, \chi)$ は

$$S_2(p,\chi) = \mathbb{C}\cdot V_1 \oplus \mathbb{C}\cdot V_2$$

と分解される。ここで V_i は適当に大きい代数体の整数環上の加群であり、また W を Atkin-Lehner involution とすると、

$$\tilde{V}_1 \cong \tilde{S}_{(p+3)/2}\ ,\quad \widetilde{V_2|W} \cong \tilde{S}_{(p+3)/2}$$

が成り立つ。同様に

$$M_2(p,\chi) = \mathbb{C}\cdot V'_1 \oplus \mathbb{C}\cdot V'_2$$

$$V'_i \supset V_i\ ,\quad \tilde{V}'_1 \cong \tilde{M}_{(P+3)/2}$$

と分解しておく。以下の記述では $\tilde{V}_1$ ($\tilde{V}'_1$) と $\tilde{S}_{(p+3)/2}$ ($\tilde{M}_{(p+3)/2}$) を同一視してかく。

次に Ponomarev [P] の結果を紹介する。正定値、4 変数、判別式が p の 2 次形式の類の代表を

$$L_1,\ L_2,\ \ldots,\ L_H \quad (\text{ H は類数 })$$

とし、L_i によりつくられる theta 級数を $\theta_i(z) = \theta(z, L_i)$ とおく。L_i^* を L_i の dual 、$\theta_i^*(z) = \theta(z, L_i^*)$ とおく。$\theta_i,\ \theta_i^* \in M_2(p,\chi)$ であるが、更に $\tilde{\theta}_i \in \tilde{M}_{(p+3)/2}$ であることもすぐにわかる。

定理 [P]. $\tilde{M}_{(p+3)/2}$ が $\{\tilde{\theta}_i\}$ で生成されるならば、$M_2(p,\chi)$ は $\{\theta_i\ ,\ \theta_i^*\}$ で生成される。

彼は $p < 509$ の範囲で条件 " $\tilde{M}_{(p+3)/2}$ は $\{\tilde{\theta}_i\}$ で生成される " をチェックし、これが満たされない p は $p = 229,\ 257$ だけであることを確かめた。この素数は我々の実験のものと一致する。このように (#) と [P] の条件の間には何か関係があると思われるが、$p = 653$, 761 の場合も込めて数値例をあげる。

p	二次形式の類数 H	dim $\{\tilde{\theta}_i\}$	dim $\tilde{M}_{(p+3)/2}$
229	10	9	10
257	12	10	11
653	31	26	28
761	46	31	32

このように $p = 653, 761$ も (#) と [P] の条件の間の同値性を暗示している。しかし、いずれの場合にも $M_2(p,\chi)$ 自身は theta 級数で張られていることに注意しておく。

まず、Waldspurger [W] の結果を我々の場合にいいかえて引用する。

定理 [W].

$$S_2^-(p,\chi) = \{ f(z) = \sum_{n=1}^{\infty} c(n) e^{2\pi i n z} \in S_2(p,\chi) \mid c(n)=0 \text{ if } \chi(n)=1 \}$$

とおくと、$S_2^-(p,\chi)$ は θ_i^* 達で生成される。

また同様に $M_2^-(p,\chi)$ を $\chi(n) = 1$ ならば $c(n) = 0$ であるような integral modular form の空間とする。

定理 1. (#) をみたす primitive form が存在すれば $\{\tilde{\theta}_i\}$ は $\tilde{M}_{(p+3)/2}$ を張らない。

証明　定理 [W] により $M_2^-(p,\chi)$ は θ_i^* で張られるからその basis として θ_i^* $(i = 1,\dots,t)$ を選んでおく。従って θ_i $(i = 1,\dots,t)$ も $\mathbb{C}$ 上一次独立である。今 $f(z)$ を (#) をみたす primitive form とすると $f - f^{\rho} \in S_2^-(p,\chi)$ であるから、

$$f - f^{\rho} = \sum_{i=1}^{t} a_i \theta_i^*$$

とかける。両辺に Hecke 作用素 T(p) を作用させる。$\theta_i^* | T(p) = \theta_i$ に注意すれば

$$c(p)f - c(p)^{\rho} f^{\rho} = \sum_{i=1}^{t} a_i \theta_i$$

を得るが、左辺は仮定より mod $\mathfrak{P}$ で 0 である。

逆向きを示すために primtive form の Fourier 係数について次を仮定する。

仮定 primitive forms f, g が $f^{\rho} \neq g$ かつ $f \not\equiv g \bmod \mathfrak{P}$ ならば ある $\chi(n) = 1$ なる n に対して $c_f(n) \not\equiv c_g(n) \bmod \mathfrak{P}$ が成り立つ。ここで $c_f(n)$, $c_g(n)$ はそれぞれ f および g の Fourier 係数である。

定理 2. 上の仮定のもとで $\Sigma a_i\theta_i \neq 0$, $\Sigma a_i\theta_i \equiv 0 \bmod \mathfrak{P}$ かつ $\Sigma a_i\theta_i^* \not\equiv 0 \bmod \mathfrak{P}$ が成立するならば、(#) を満たす primitive form が存在する。

証明 $\phi = \Sigma a_i\theta_i$, $\phi^* = \Sigma a_i\theta_i^*$ とおく。$f_j(z) = \sum_{n=1}^{\infty} c_j(n) e^{2\pi i n z}$ を $S_2(p, \chi)$ の primitive forms でどの i, j ($i \neq j$) に対しても $f_i \neq f_j^{\rho}$ なるもの全体とする。$S_2^-(p, \chi)$ は明らかに $f_j - f_j^{\rho}$ 達で生成される。いま $\tilde{S}_2^-(p, \chi)$ の basis を $f_j - f_j^{\rho}$ ($j=1, \ldots, t$) として

$$\phi^* \equiv \sum_j x_j (f_j - f_j^{\rho}) \bmod \mathfrak{P} \quad , \quad x_j \not\equiv 0 \bmod \mathfrak{P}$$

と書いたとき、仮定によって、上の和に現れる各 j について

$f_j - f_j^{\rho} \equiv$ (ϕ^* に適当な $T(n), T(n'), \ldots,$ $\chi(n) = \chi(n') = \ldots = 1$, を何回も施したものの一次結合)

という形で解き直すことができる。そこで改めて T(p) を施すと、T(p)

と T(n) の可換性より

$$c_j(p)f_j - c_j(p)^{\rho} f_j^{\rho} \equiv (\ \phi \text{ に適当な } T(n), T(n'), \ldots,\ \chi(n)=\chi(n')=\ldots=1,\ \text{を何回も施したものの一次結合})$$

$$\equiv 0 \mod \mathfrak{P}$$

ところが $c_j(p)$, $c_j(p)^{\rho}$ のうち一方はすでに $\mathfrak{P}$ で割れているから f_j に対して (#) が成り立つ。

Remark

1. [W] で示されている basis problem に関する結果に、我々の場合に当てはめれば、次のことがある。

$M_2(p,\chi)$ は theta 級数で張られる $\Leftrightarrow$ T(p) は $\pm\sqrt{p}$ を eigenvalue にもたない

T(p) が $\pm\sqrt{p}$ を eigenvalue にもてば当然 (#) が満たされることになるから、定理 1, 2 は Waldspurger の結果の mod p 版とみることができる。この mod p 版では確かに張られない場合があるわけだが、global には今のところわかっていない。p 番目の Fourier 係数が $\pm\sqrt{p}$ であるような primitive form が存在するのかどうか非常に興味ぶかい。

2. その後 $\{\tilde{\theta}_i\}$ が $\tilde{M}_{(p+3)/2}$ を張らない p を大きいところで捜してみた。そのリストは $769 \le p \le 2601$ の範囲で

1129, 1229, 1489, 2089, 2213

1061, 1381, 1553, 1733, 2029, 2053, 2293, 2609

である。ここで、上段は corank = 1、下段は corank = 2 である。やはり上段のものは S_4 拡大に、下段のものは A_5 拡大に対応していると思われる。$\mathbb{Q}(\sqrt{p})$ の類数が 3 のものでは p = 2677, 2917, 3221, 3229 が corank = 1、p = 2777 が corank = 2 である。p = 2777 の場合も T(2), T(3), ... ,T(19) をみる限り A_5 拡大に対応すると思

われる。また $p = 2861$ では corank $= 2$ となっている。

3. [Ki] に示されているように、正定値、4変数、判別式$=p$ の二次形式の類のうち 1 を表すものの個数は $t_p = \dim M_{(p+3)/2}$ にひとしい。それらに対応する theta 級数を θ_i $(i = 1, \ldots, t_p)$ とすると、当初 $\{\theta_i, \theta_i^*\}$ が $M_2(p, \chi)$ の basis をなすと予想されたが $p = 389$ で θ_i $(i = 1, \ldots, t_p)$ の $\mathbb{Z}$ 上の一次関係式が見つかった。どの p に対して θ_i $(i = 1, \ldots, t_p)$ 達が一次独立でないかということに関して橋本喜一郎氏が $p \leq 5023$ まで計算されている。

文献

[Ki] Y. Kitaoka, Quaternary even positive deinite quadratic forms of prime discriminant, Nagoya Math. J. 52 (1973), 147-161.

[Ko] M. Koike, A note on modular forms mod p, Nagoya Math. J. 89 (1983), 89-107.

[K-T] M. Koike and Y. Tanigawa, A_4-extensions over real quadratic fields and Hecke operators, Advanced Studies in Pure Math. 13 (1988), 171-192.

[P] P. Ponomarev, Theta series mod p and the basis problem for Nebentypus, preprint.

[W] J.-L. Waldspurger, Engendrement par des series theta de certains espaces de formes modulaires, Inv. Math. 50 (1979), 135-168.