数理解析研究所講究録
546巻 1985年 159-170

重さ1の保型形式，4次剰余と楕円曲線

阪府大総合　石井伸郎（Noburo Ishii）

D_3 を位数6の2面体群として，次の様な体Ωと楕円曲線Eのpair (Ω, E)を考える。

(*) ΩはQ上正規拡大で，$G(\Omega/Q) \cong D_3$。

(**) EはQ上定義されていて，ΩはQ上Eの2等分点で生成される。

このとき，Ωから構成される重さ1のcusp formのFourier係数と，谷山－Weil予想を仮定することにより，Eから構成できる重さ2のcusp formのFourier係数の間に〝2は法〟とする合同式が成立することを，Ωを最小分解体にもつ有理整係数の3次既約方程式の〝高次相互法則〟から，小池氏[3]は示した。ここでは、位数8の2面体群D_4に対して同様な問題を考える。すなわち

1) KはQ上，正規拡大で．ガロワ群$G(K/Q)$がD_4と同型なる体，

2) Eは$\mathbb{Q}$上定義された楕円曲線で，Kは$\mathbb{Q}上E$の，
ある2巾－等分点で生成される。

この2条件をみたすpair(K,E)から，cusp formの間の〝2巾を法〟とする合同式を得ることを考える。谷山－Weil予想を仮定せずにすますために

3) Eは虚数乗法をもつ。

という条件を付け加えることにする。さらに基礎体を$\mathbb{Q}$から実2次体Fにしたときに，F上条件1)～3)と同様の条件をみたす体と楕円曲線のpair(K,E)から，F上のHilbert modular formの間の合同式が得られるかを考える。ここでは次の様な，典型的なD_4－拡大と虚数乗法$\mathbb{Z}[\sqrt{-1}]$をもつ，楕円曲線のpair(K,E)をそれぞれ$\mathbb{Q}$上，実2次体上に考える。

(I) mを非平方な正整数として，

$K=\mathbb{Q}(\sqrt{-1},\sqrt[4]{m})$，$E:\ y^2=x^3+4mx$。

(II) $F=\mathbb{Q}(\sqrt{n})$（n: square freeな正整数）を総正な基本単数をもつ実2次体で，ε_nをFの$a+b\sqrt{n}$（$a,b\in\mathbb{Z}$, $a>0$）なる形の最小の単数とする。

$K=F(\sqrt{-1},\sqrt[4]{\varepsilon_n})$，$E:\ y^2=x^3+4\varepsilon_n x$。

(I), (II)の場合共に，Kは基礎体上，Eの$(1+\sqrt{-1})^3$－等分点で生成されていて，pair(K,E)から重さ1，重さ2のcusp form（(II)に於ては，Hilbert cusp form）の間の

〃4を法〃とする合同式が，m，ε_nの〃4次剰余性〃から得られる。

以下、記号の説明をする。群D_4は，唯一の既約2次元複素表現をもつ。これをψで示す。群GがD_4と同型なるとき，ψとその同型との合成で得られるGの表現をψ_Gで表す。k，Nを自然数とする。χを$(\mathbb{Z}/N)^\times$の指標とするとき，

$S_k(N,\chi)$で重さkの指標χに属する，モジュラー群$\Gamma_0(N)$に関するcusp formのなす空間を表す。

§1. cusp formの合同

ここでは(I)の場合を扱う。$G=\mathrm{Gal}(K/\mathbb{Q})$とおく。$L(s,\psi_G)=\sum_{n=1}^{\infty}a(n)n^{-s}$を$\psi_G$のArtin L-関数，$N$を$\psi_G$のコンダクターとする。複素上半平面$\mathfrak{H}$上の関数，

$$\theta(\tau,K)=\sum_{n=1}^{\infty}a(n)q^n,\quad \theta'(\tau,K)=\sum_{n:\mathrm{odd}}a(n)q^n$$

$$(q=\exp(2\pi\sqrt{-1}\tau))$$

を考えると，$\theta(\tau,K)\in S_1(N,(\frac{-1}{*}))$，

$$\theta'(\tau,K)\in S_1(4N,(\tfrac{-1}{*}))$$

となる（Serre [4]，志村 [5]）。

Eの L-関数を $L(s,E)=\sum_{n=1}^{\infty}c(n)n^{-s}$，Eのコンダクターを$C_E$とおけば，$\mathfrak{H}$上の関数 $\theta(\tau,E)=\sum_{n=1}^{\infty}c(n)q^n$は$S_2(C_E,1)$に属す（志村 [5]）。体$K$は$\mathbb{Q}(\sqrt{-1})$上

のアーベル拡大で，そのコンダクターは正整数 f で生成されている。p を素数とするとき，p 番目の Fourier 係数 $a(p)$，$c(p)$ は次の様に与えられる。

$$(1.1)\qquad a(p)=\begin{cases}\operatorname{trace}\psi_G(\sigma_p) & \text{if } p\nmid N,\\ 0 & \text{if } p\mid f,\end{cases}$$

$$a(2)=0,\pm 1。$$

$$(1.2)\qquad c(p)=\begin{cases}p+1-N_p & \text{if } p\nmid C_E,\\ 0 & \text{otherwise。}\end{cases}$$

ここで σ_p は拡大 $K/\mathbb{Q}$ における p の Frobenius 置換を表し，N_p は，楕円曲線 E を p で reduction して得られる $\mathbb{F}_p(=\mathbb{Z}/p)$ 上の楕円曲線 E_p の $\mathbb{F}_p$-有理点の個数を示す。

注意－1. N，C_E と f の間の関係は次の通りである。

$$N=4f^2,\quad C_E=2^\gamma N,\quad \gamma=\max(0,3-2e),$$

e は f の 2-指数である。特に $\gamma=0 \iff f\equiv 0 \bmod 4$。

上で定義した cusp form の間に次の合同式が成立する。

定理－1. 上の記号の下で

$$\theta(\tau,K)\equiv\theta(\tau,E)\mod 4$$

さらに f が偶数ならば，

$$\theta(\tau,K)\equiv\theta(\tau,E)\mod 4。$$

以下定理の証明の概略を示す。(詳しくは[1]を参照)

$p \nmid N$ なる素数 p に対して m の p を法とする〝4次剰余性〟を表す量 $S(p)$ を次の様に定義する。

$$S(p) = \#\{\alpha \in \mathbb{F}_p \mid \alpha^4 \equiv m \mod p\}$$

このとき $a(p)$、$c(p)$ が $S(p)$ で次の様に表わされる。

Lemma 1　$p \nmid N$ ならば

$$a(p) = S(p) - 1 - \left(\frac{m}{p}\right).$$

(証) K の部分体 $\mathbb{Q}(\sqrt[4]{m})$ の各元を不変にする G の部分群を H とする。1_H で H の恒等指標，1_H^G でその G への誘導指標を示せば.

$$S(p) = 1_H^G(\sigma_p).$$

となる。1_H^G を既約指標に分解すれば.

$$1_H^G = 1 + \mathrm{trace}\,\psi_G + \chi,$$

χ は $\mathbb{Q}(\sqrt{m})$ に対する G の一次表現である。(1.1) より上の結果を得る。

Lemma 2　$p \nmid N$ ならば

$$c(p) \equiv -S(p) - \left(\frac{-1}{p}\right) - \left(\frac{-m}{p}\right) + \gamma(p) \mod 8$$

ここで

$$\gamma(p) = \begin{cases} 4 & p \equiv 5 \mod 8 \text{ のとき,} \\ 0 & \text{その他} \end{cases}$$

(証) $p \nmid N$ ならば $p \nmid C_E$ である。$T(p)$ で E_p の $\mathbb{F}_p$-有理的な $(1+\sqrt{-1})^3$-等分点の個数を示せば，$S(p)$ がその中の primitive な $(1+\sqrt{-1})^3$-等分点の個数を表わしているので

$$T(p) = 3 + \left(\frac{-m}{p}\right) + S(p)$$

を得る。次に，合同式

$$N_p \equiv T(p) + \mu(p) \mod 8$$

$$\mu(p) = \begin{cases} 4 & \text{if } p \equiv 7 \mod 8 \\ 0 & \text{otherwise.} \end{cases}$$

を示す。$p \equiv 3 \mod 4$ のときは明らか。$p \equiv 1 \mod 4$ のとき，E_p の $\mathbb{F}_p$-有理点のなす群を M として，M^+ でその 2-Sylow 群，M^- でその直和補因子を表す。すなわち $M = M^+ \oplus M^-$。虚数乗法 $\sqrt{-1}$ が $\mathbb{F}_p$ 上定義されることにより，群 $\langle\sqrt{-1}\rangle$ は M^+, M^- に作用する。$\langle\sqrt{-1}\rangle$ の orbit を考えることより

$$\#(M^+) \equiv T(p) \mod 8, \quad \#(M^-) \equiv 1 \mod 4$$

これより $N_p \equiv T(p) \mod 8$。(1.2) に注意すれば，上の結果を得る。

これらの事より，$p \nmid N$ ならば

$$(1.3) \qquad a(p) \equiv c(p) + \gamma(p) \mod 8$$

を得る。f が偶数ならば $a(2) = c(2) = 0$ に注意して，Fourier 係数が乗法的なることより，定理-1が示される。

注意－2　$m=2^{\alpha}\cdot m_1$, $(m_1,2)=1$ とおくとき，f が奇数であるための条件は次の様に与えられる。

$$f:\text{奇数} \iff \alpha:\text{偶数},\ m_1\equiv(-1)^{\frac{\alpha}{2}} \bmod 8$$

§2. Hilbert modular form の合同

(II)の場合を考える。すなわち $K=F(\sqrt{-1},\sqrt[4]{\varepsilon_n})$，$E$ を方程式 $y^2=x^3+4\varepsilon_n x$ で定義された楕円曲線とする。

2.1. Hilbert modular form の構成

Kから次の様に、Hilbert modular form を構成する。

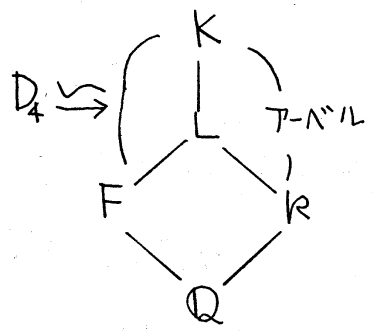
$G=Gal(K/F)$, $G_0=Gal(K/\mathbb{Q})$ とおく。$\psi_G^{G_0}$ で，ψ_G の G_0 への誘導表現とする。$\psi_G^{G_0}$ を既約表現に分解すると

$$\psi_G^{G_0}=\psi_0\oplus\psi_1$$

ここで ψ_0,ψ_1 は2次元既約表現で，F に対応する G_0 の一次表現を χ_F とすれば

$$(2.1)\quad \psi_1=\psi_0\otimes\chi_F$$

なる関係がある。今 $L=\mathbb{Q}(\sqrt{-1},\sqrt{n})$, $k=\mathbb{Q}(\sqrt{n})$ とおけば



Kは k 上アーベル拡大である。ψ_i を $Gal(K/k)$ に制限し，相異なる指標に分解できる。すなわち

$$\psi_i|Gal(K/k)\simeq\xi_i\oplus\xi_i'.$$

ξ_i^* で ξ_i によってきまる k のイデアル

指標，$\tilde{\xi}_i^*$ で ξ_i^* の primitive な指標を表せば，

$$L(s, \psi_i) = L(s, \tilde{\xi}_i^*)$$

となる。$\tilde{\xi}_i^*$ が分岐しているときには，$L(s, \xi_i^*) = L(s, \tilde{\xi}_i^*)$ となる。上の図式より次の事が分る。

(2·2) ξ_0^* と ξ_1^* が共に分岐 $\Longleftrightarrow$ K が L 上分岐。

χ で k の L に対応するイデアル指標を示せば，(2·1) より

$$\xi_1^* = \chi \cdot \xi_0^*$$

なることが分る。

今 $L(s, K) = L(s, \psi_G^{G_0})$ とおけば (2·2) の仮定の下で

$$\begin{aligned} L(s, K) &= L(s, \psi_0) L(s, \psi_1) = L(s, \xi_0^*) L(s, \xi_1^*) \\ &= L(s, \xi_0^* \circ N_{L/k}) \\ &= \prod_{\mathfrak{f}} L_{\mathfrak{f}}(s, K), \end{aligned}$$

ここで積は F の 2 と素な素イデアル $\mathfrak{f}$ 全体を渡り，$L_{\mathfrak{f}}(s, K)$ は，

$$(2\cdot3)\quad L_{\mathfrak{f}}(s, K) = \prod_{\substack{\mathfrak{P} \mid \mathfrak{f} \\ \mathfrak{P}: \text{prime in } L}} \left(1 - \xi_0(N_{L/k}(\mathfrak{P}))\, N_{L/\mathbb{Q}}(\mathfrak{P})^{-s}\right)^{-1}$$

である。このことにより

$$L(s, K) = \sum_{m} a(m)\, N_{F/\mathbb{Q}}(m)^{-s}$$

和は F の整イデアルの全てを渡ると表わせる。今 h を F の狭義の類数として，$\mathfrak{A}_1, \cdots \mathfrak{A}_h$ で F の狭義の各類を代表する整イデアルの一組を表わすものとする。$\mathfrak{f} \times \mathfrak{f}$ 上の関数

$g_\lambda(z,z')$, $\lambda=1,\cdots,h$ を次の様に定義する。

$$g_\lambda(z,z')=\sum_{\substack{\xi\in\mathfrak{o}_\lambda\\ \xi\gg 0}} a(\xi\mathfrak{o}_\lambda^{-1})\, e^{2\pi\sqrt{-1}(\xi z+\xi' z')}$$

ここで ξ' は ξ の $\mathbb{Q}$ 上の共役を示し，$\xi\gg 0$ は ξ が総正であることを意味する。$g_\lambda(z,z')$ は重さ1の $GL_2(F)^+$ の合同部分群に関する Hilbert cusp form である（志村 [6]）。次に E の F 上の L-関数を

$$L(s,E)=\sum_{m} C(m) N_{F/\mathbb{Q}}(m)^{-s}$$ の形に表し，

$\mathfrak{h}\times\mathfrak{h}$ 上の関数 $f_\lambda(z,z')$ を

$$f_\lambda(z,z')=\sum_{\substack{\xi\in\mathfrak{o}_\lambda\\ \xi\gg 0}} C(\xi\mathfrak{o}_\lambda^{-1})\, e^{2\pi\sqrt{-1}(\xi z+\xi' z')}$$

と定義すれば，E は虚数乗法をもち，$L(s,E)$ が L の量指標の L-関数と一致することより，$f_\lambda(z,z')$ は重さ2の $GL_2(F)^+$ のある合同部分群に関する Hilbert cusp form である。

2・2 合同式

$g_\lambda(z,z')$, $f_\lambda(z,z')$ $\lambda=1,\cdots,h$ の間に次の合同式が成立する。$a(m)$, $C(m)$ はすべて整数である。

定理－2. K が L 上分岐しているならば，

$$g_\lambda(z,z')\equiv f_\lambda(z,z') \mod 4$$

が $\lambda=1,\cdots,h$ に対して成立する。

この定理は次のLemmasから証明される。詳しくは[2]を参照して下さい。体Fの2と素な素イデアル$\mathfrak{p}$に対して，$\mathbb{F}_{\mathfrak{p}}$で$\mathfrak{p}$の剰余体，$\sigma_{\mathfrak{p}}$で拡大K/Fでの$\mathfrak{p}$のFrobenius置換を表す。$\varepsilon_n$の〝4次剰余性〟を示す量

$$S(\mathfrak{p}) = \#\{\alpha \in \mathbb{F}_{\mathfrak{p}} \mid \alpha^4 \equiv \varepsilon_n \bmod \mathfrak{p}\}$$

と$\operatorname{trace}\psi_G(\sigma_{\mathfrak{p}})$, $C(\mathfrak{p})$との関係を§1と同じ議論でもとめることによって次の結果を得る。

Lemma 3　上の記号の下で

$$\operatorname{trace}\psi_G(\sigma_{\mathfrak{p}}) \equiv C(\mathfrak{p}) + \gamma(\mathfrak{p}) \bmod 8$$

ここで

$$\gamma(\mathfrak{p}) = \begin{cases} 4 & p \equiv 5 \bmod 8,\ \left(\frac{n}{p}\right) \neq -1 \text{ のとき} \\ 0 & \text{その他} \end{cases}$$

今$L_{\mathfrak{p}}(s, E)$で$L(s, E)$の積表示における〝$\mathfrak{p}$-part〟，$L_p(s, \psi_i)$で$L(s, \psi_i)$のEuler積表示の〝p-part〟を示せば、Lemma 3から次の合同式を得る。

Lemma 4　pを奇素数，$\mathfrak{p}$でpをわるFの素イデアルとすると，$L_{\mathfrak{p}}(s, E)$, $L_p(s, \psi_i)$を変数$x = p^{-s}$の整係数をもつ巾級数とみなしたとき、次の合同式が成立する。

$$L_{\mathfrak{p}}(s, E) \equiv \begin{cases} L_p(s, \psi_0) = L_p(s, \psi_1) \bmod 4 & \text{if } \left(\frac{F}{p}\right) = 1, \\ L_p(s, \psi_0) L_p(s, \psi_1) \bmod 4 & \text{otherwise.} \end{cases}$$

ところで(2·3)の $L_g(s,K)$ は

$$L_g(s,K)=\begin{cases} L_p(s,\psi_0) & \text{if } \left(\frac{F}{p}\right)=1, \\ L_p(s,\psi_0)L_p(s,\psi_1) & \text{otherwise.} \end{cases}$$

となるので，Lemma 4より $g_n(z,z')$，$f_n(z,z')$ のFourier係数の間の合同式を(2·2)の仮定の下で得ることができる。すなわち，すべてのFの整イデアル $\mathfrak{m}$ に対して，

$$a(\mathfrak{m}) \equiv c(\mathfrak{m}) \mod 4$$

が成立する。これは定理-2の結果を示す。

注意-3　KがL上不分岐なるための条件をきめる。

$\varepsilon_n = A+B\sqrt{n}$ $(A,B\in\mathbb{Z},\ A>0)$ とおくとき，

$$K\text{は}L\text{上不分岐} \iff \begin{cases} A\equiv 1 \mod 8,\ B\equiv 0 \mod 8 & \text{if } n\equiv 1 \mod 4, \\ A\equiv 1 \mod 8,\ B\equiv 0 \mod 4 & \text{if } n\equiv 3 \mod 4, \\ B\equiv 0 \mod 4 & \text{if } n\equiv 2 \mod 4. \end{cases}$$

となる。例えば次の様な n に対して，$F=\mathbb{Q}(\sqrt{n})$ 上の(II)で定義されたKは(2·2)をみたす。

(i) n は素数で $n\equiv 3 \mod 4$。

(ii) n は相異なる素数 p_1, p_2 の積で p_1, p_2 は次をみたす。

(ii-a) $p_1\equiv \pm 5 \mod 8$，$p_2\equiv 3 \mod 4$，$\left(\frac{p_1}{p_2}\right)=-1$。

(ii-b) $p_1=2$，$p_2\equiv 3 \mod 8$.

参考文献

[1] N. Ishii, Cusp forms of weight one, quartic reciprocity and elliptic curves, to appear in Nagoya Math. J., 98 (1985).

[2] ———, Quadratic units and congruences between Hilbert modular forms, preprint.

[3] M. Koike, Higher reciprocity law, modular forms of weight one and elliptic curves, to appear in Nagoya Math. J.

[4] J. P. Serre, Modular forms of weight one and Galois representations, Proc. Symposium on algebraic number fields, Academic Press, London 1977, 193 - 268.

[5] G. Shimura, On elliptic curves with complex multiplication as factors of the jacobians of modular function fields, Nagoya Math. J., 43 (1971), 199-208.

[6] ———, The special values of the zeta functions associated with Hilbert modular forms, Duke Math. J., 45 (1978), 637 - 679.