

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 $\mathbb{Q}$ 上正規拡大で, $G(\Omega/\mathbb{Q}) \cong D_3$ 。

(**) E は $\mathbb{Q}$ 上定義されていて, Ω は $\mathbb{Q}$ 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 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 $\mathbb{Q}$ 上, 正規拡大で, ガロワ群 $G(K/\mathbb{Q})$ 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ずために

- 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,

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

- (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。

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

(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, E_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。 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。 $G = \text{Gal}(K/\mathbb{Q})$ とおく。

$L(s, \psi_G) = \sum_{n=1}^{\infty} a(n) n^{-s}$ を ψ_G の Artin L-関数, N を ψ_G のコンダクターとする。複素上半平面 $\mathfrak{H}$ 上の関数,

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

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

を考えると, $\theta(\tau, K) \in S_1(N, (\cdot^1/*))$,

$$\theta'(\tau, K) \in S_1(4N, (\cdot^1/*))$$

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 $a(p)$, $C(p)$ は次の様にとえられる。

$$(1.1) \quad a(p) = \begin{cases} \text{trace } \psi_{\mathbb{F}}(\sigma_p) & \text{if } p \nmid N, \\ 0 & \text{if } p \mid f, \end{cases}$$

$$a(2) = 0, \pm 1.$$

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

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 $\gamma = 0 \iff f \equiv 0 \pmod{4}$ 。

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

$$\theta(\tau, K) \equiv \theta(\tau, E) \pmod{4}$$

さらに f が偶数ならば、

$$\theta(\tau, K) \equiv \theta(\tau, E) \pmod{4}.$$

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。

$$S(P) = \# \{ \alpha \in \mathbb{F}_P \mid \alpha^4 \equiv m \pmod{P} \}$$

このとき $\alpha(P)$, $C(P)$ が $S(P)$ で次の様に表わされる。

Lemma 1 $P \nmid N$ ならば

$$\alpha(P) = S(P) - 1 - \left(\frac{m}{P}\right).$$

(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,

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

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

$$C(P) \equiv -S(P) - \left(\frac{-1}{P}\right) - \left(\frac{-m}{P}\right) + \gamma(P) \pmod{8}$$

ここで

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

(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

$$T(P) = 3 + \left(\frac{-1}{P}\right) + S(P)$$

を得る。次に, 合同式

$$N_P \equiv T(P) + \mu(P) \pmod{8}$$

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

を示す。 $P \equiv 3 \pmod{4}$ のときは明らか。 $P \equiv 1 \pmod{4}$ 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

$$\#(M^+) \equiv T(P) \pmod{8}, \quad \#(M^-) \equiv 1 \pmod{4}$$

これより $N_P \equiv T(P) \pmod{8}$ 。 (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

$$(1.3) \quad a(P) \equiv c(P) + \gamma(P) \pmod{8}$$

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なえられる。

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

§ 2. Hilbert modular form の合同

(II) の場合を考える。すなわち $K = F(\sqrt{f}, \sqrt[4]{E_n})$, E を方程式 $y^2 = x^3 + 4E_n x$ 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。

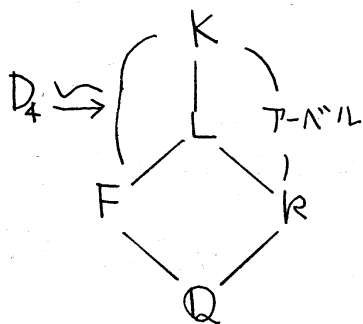
$G = \text{Gal}(K/F)$, $G_0 = \text{Gal}(K/\mathbb{Q})$ とおく。 $\psi_G^{G_0}$ で, ψ_G の G_0 への誘導表現とする。 $\psi_G^{G_0}$ を既約表現に分解すると

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

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 $L = \mathbb{Q}(\sqrt{f}, \sqrt{n})$, $k = \mathbb{Q}(\sqrt{n})$ とおけば



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

$$\psi|_{\text{Gal}(K/k)} \hookrightarrow \varepsilon_i \oplus \varepsilon_i'$$

ε_i^* で ε_i によってきまる k のイデアル

指標, ξ_i^* で ξ_i^* の primitive な指標を表せば,

$$L(\mathcal{A}, \psi_i) = L(\mathcal{A}, \xi_i^*)$$

となる。 ξ_i^* が分岐しているときには, $L(\mathcal{A}, \xi_i^*) = L(\mathcal{A}, \xi_i^*)$

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 $\iff K$ が L 上分岐。

χ で k の L に対応するイデアル指標を表せば, (2.1) より

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

なることが分る。

今 $L(\mathcal{A}, K) = L(\mathcal{A}, \psi_{\mathbb{Q}}^{\mathbb{Q}_0})$ とおけば (2.2) の仮定の下で

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

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

$$(2.3) \quad L_{\mathfrak{f}}(\mathcal{A}, K) = \prod_{\substack{\mathfrak{p} | \mathfrak{f} \\ \mathfrak{p}: \text{prime in } L}} \left(1 - \xi_0(N_{L/K}(\mathfrak{p})) N_{L/\mathbb{Q}}(\mathfrak{p})^{-s} \right)^{-1}$$

である。このことにより

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

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, $\mathfrak{a}_1, \dots, \mathfrak{a}_h$ で F の狭義の各類を代表する整イデアルの一组を表わすものとする。 $\chi \times \chi$ 上の関数

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

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

ここで ξ は $\mathbb{Q}$ 上の共役を示し, $\xi \gg 0$ は ξ が純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

$L(s, E) = \sum_m C(m) N_{F/Q}(m)^{-s}$ の形に表し,
 $\mathfrak{o} \times \mathfrak{o}$ 上の関数 $f_\lambda(z, z')$ を

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

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

$g_\lambda(z, z')$, $f_\lambda(z, z')$ $\lambda = 1, \dots, h$ 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,

$$g_\lambda(z, z') \equiv f_\lambda(z, z') \pmod{4}$$

が $\lambda = 1, \dots, h$ 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 $\mathfrak{f}$ に対して, $\mathbb{F}_{\mathfrak{f}}$ で $\mathfrak{f}$ の剰余体, $\sigma_{\mathfrak{f}}$ で拡大 K/F での $\mathfrak{f}$ の Frobenius 置換を表す。

ε_n の “4 次剰余性” を示す量

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

と $\text{trace } \psi_{\mathbb{F}}(\sigma_{\mathfrak{f}})$, $C(\mathfrak{f})$ との関係は §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

$$\text{trace } \psi_{\mathbb{F}}(\sigma_{\mathfrak{f}}) \equiv C(\mathfrak{f}) + \gamma(\mathfrak{f}) \pmod{8}$$

ここで

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

今 $L_{\mathfrak{f}}(\chi, E)$ で $L(\chi, E)$ の積表示における “ $\mathfrak{f}$ -part”, $L_p(\chi, \psi_i)$ で $L(\chi, \psi_i)$ 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, $\mathfrak{f}$ で p をわる F の素イデアルとすると, $L_{\mathfrak{f}}(\chi, E)$, $L_p(\chi, \psi_i)$ を変数 $x = p^{-s}$ の整係数をもつ中級数とみなしたとき, 次の合同式が成立する。

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

となるので (2.3) の $L_g(\lambda, K)$ は

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

となるので, Lemma 4 より $g_n(z, \bar{z})$, $f_n(z, \bar{z})$ の Fourier 係数の間の合同式を (2.2) の仮定の下で得ることが出来る。すなわち, すべての F の整イデアル m に対して,

$$a(m) \equiv c(m) \pmod{4}$$

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定める。

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

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

となる。例えば 次の様な n に対して $F = \mathbb{Q}(\sqrt{n})$ 上の $(\mathbb{I})$ で定義された K は (2.2) をみたす。

(i) n は素数で $n \equiv 3 \pmod{4}$ 。

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

(ii-b) $p_1 = 2$, $p_2 \equiv 3 \pmod{8}$ 。

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.