ある微分方程式のモジュラー形式解と
楕円曲線の超特異多項式

中屋 智瑛 (九州大学)

概 要

Kaneko, Zagier [5] による楕円曲線の超特異多項式 $ss_p(X)$ の研究から, Serre 微分を用いて構成した $M_{p-1}(SL_2(\mathbb{Z}))$ の自己準同型の固有関数から $ss_p(X)$ が得られることが分かっている．また Baba, Granath [9] は Serre 微分の類似物を用いて同様の結果を得た．本稿ではこれらの結果を特殊化に含むよう Serre 微分にパラメータを入れて拡張し, 構成した $M_{p-1}(SL_2(\mathbb{Z}))$ の自己準同型の固有関数から $ss_p(X)$ が得られることを示す.

1 導入

標数 p (素数) の体 K 上定義された楕円曲線 E に対し, 群 $E(\overline{K})$ が位数 p の元をもたないとき E は supersingular であるという．この条件は E の j 不変量のみに依存し, 各 p に対して標数 p の supersingular な楕円曲線は閉体上の同型を除いて有限個しかない．それら有限個の楕円曲線の j 不変量 ($\mathbb{F}_{p^2}$ に入ることが知られている) を根に持つモニック多項式

$$ss_p(X) = \prod_{\substack{E/\overline{\mathbb{F}}_p \\ E:\text{supersingular}}} (X - j(E)) \qquad \in \mathbb{F}_p[X]$$

は supersingular polynomial と呼ばれる．古典的には有限体上の楕円曲線を Legendre 標準形 $y^2 = x(x-1)(x-\lambda)$ で書いたとき, p を奇素数として

$$E/\overline{\mathbb{F}}_p : \text{supersingular} \iff \sum_{i=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{i}^2 \lambda^i = {}_2F_1\left(-\frac{p-1}{2}, -\frac{p-1}{2}; 1; \lambda\right) \equiv 0 \pmod p$$

が成り立つことが知られている．ここで ${}_2F_1(\alpha,\beta;\gamma;x)$ は Gauss の超幾何級数である:

$${}_2F_1(\alpha,\beta;\gamma;x) := \sum_{n=0}^{\infty} \frac{(\alpha)_n(\beta)_n}{(\gamma)_n} \frac{x^n}{n!}.$$

ただし $(\alpha)_0 := 1, (\alpha)_n := \alpha(\alpha+1)\cdots(\alpha+n-1)$ と定める．α または β が負の整数の場合は多項式を与えることに注意する．さて, 任意の偶数 $k \geq 4$ は

$$k = 12m + 4\delta + 6\varepsilon,\ m \in \mathbb{Z}_{\geq 0},\ \delta \in \{0,1,2\},\ \varepsilon \in \{0,1\}$$

と一意的に書けるが, 特に素数 $p \geq 5$ に対して $p-1 = 12m+4\delta+6\varepsilon$ と書くとき supersingular polynomial は超幾何級数を用いて次のように表せる.

定理 1.1 (Deuring [1]). 素数 $p \geq 5$ に対して $p-1 = 12m + 4\delta + 6\varepsilon$ と書くとき

$$ss_p(X) \equiv X^{m+\delta}(X-1728)^{\varepsilon}{}_2F_1\left(-m, \frac{5}{12} - \frac{2\delta - 3\varepsilon}{6}; 1; \frac{1728}{X}\right) \pmod{p}.$$

ただし Deuring は超幾何級数を用いた形では述べておらず, 若干の変形 ([5, Proposition 5]) が必要になるが本質的には上の通りである. 定理の超幾何部分は $1728/X$ に関する m 次多項式になり, 先頭の $X^{m+\delta}$ と打ち消しあうので右辺は X に関する多項式となる. その次数は $p-1 = 12m + 4\delta + 6\varepsilon$ に対して

$$\deg ss_p(X) = m + \delta + \varepsilon$$

である. その他 Deuring [1] により $ss_p(X)$ を $\mathbb{F}_p$ 上既約分解したときの既約因子の次数は高々二次であることや, D_p の類数 $h(D_p)$ と $\deg ss_p(X)$, すなわち $E/\overline{\mathbb{F}}_p$ の同型類の個数が等しいことが知られている. ここで D_p は $\mathbb{Q}$ 上の定値四元数環で p と ∞ でのみ分岐するものである. 一方 Eichler [2] は解析的な手法で, 井草 [3] は代数的な手法で $h(D_p)$ を計算し

$$h(D_p) = \frac{p-1}{12} + \frac{1}{3}\left\{1 - \left(\frac{-3}{p}\right)\right\} + \frac{1}{4}\left\{1 - \left(\frac{-4}{p}\right)\right\}$$

を示した. ここで $(\frac{\cdot}{p})$ は Legendre 記号である. 右辺が実際 $m + \delta + \varepsilon$ に等しいことは簡単に分かる. さて, 特に興味深い $ss_p(X)$ の性質としてモンスター群 $\mathbb{M}$ との関係があげられる.

表 1: $ss_p(X)$ の既約分解

p	$ss_p(X)$
2	X
3	X
5	X
7	$X+1$
11	$X(X+10)$
13	$X+8$
17	$X(X+9)$
19	$(X+1)(X+12)$
23	$X(X+20)(X+4)$
29	$X(X+4)(X+27)$
31	$(X+8)(X+27)(X+29)$
37	$(X+29)(X^2+31X+31)$
41	$X(X+9)(X+13)(X+38)$
43	$(X+35)(X+2)(X^2+19X+16)$
47	$X(X+11)(X+3)(X+37)(X+38)$
53	$X(X+3)(X+7)(X^2+50X+39)$
59	$X(X+42)(X+11)(X+12)(X+31)(X+44)$
61	$(X+11)(X+20)(X+52)(X^2+38X+24)$
67	$(X+14)(X+1)(X^2+8X+45)(X^2+44X+24)$
71	$X(X+47)(X+5)(X+23)(X+30)(X+31)(X+54)$

26 個ある散在型有限単純群の中で位数最大のものはモンスター群 $\mathbb{M}$ と呼ばれ, その位数は

$$\begin{aligned}\#\mathbb{M} &= 808017424794512875886459904961710757005754368000000000 \\ &= 2^{46}\cdot 3^{20}\cdot 5^{9}\cdot 7^{6}\cdot 11^{2}\cdot 13^{3}\cdot 17\cdot 19\cdot 23\cdot 29\cdot 31\cdot 41\cdot 47\cdot 59\cdot 71\end{aligned}$$

である. これらの素因数 p に対して supersingular な楕円曲線の j 不変量は $\mathbb{F}_p$ 上定義されることが知られている. すなわち

$$p \mid \#\mathbb{M} \iff ss_p(X) \text{ の } \mathbb{F}_p \text{ 上の既約因子は全て一次}$$

が成り立つ (表 1 を参照). また一次因子の個数に関して次の結果が知られている.

定理 1.2 (Deuring [1])**.** p を 5 以上の素数, $ss_p(X)$ の $\mathbb{F}_p$ 上の既約分解における一次因子の個数を $N_1(p)$, 虚二次体 $\mathbb{Q}(\sqrt{-p})$ の類数を $h(-p)$ とおくと

$$N_1(p) = \begin{cases} h(-p)/2 & p \equiv 1 \pmod 4 \text{ のとき}, \\ 2h(-p) & p \equiv 3 \pmod 8 \text{ のとき}, \\ h(-p) & p \equiv 7 \pmod 8 \text{ のとき}. \end{cases}$$

例えば $p = 23 \equiv 7 \pmod 8$ に対して, 表 1 より $N_1(23) = 3 = h(-23)$ が分かる.

定義 1.3 (Modular forms)**.** 上半平面 $\mathfrak{H}$ 上の正則関数 f が $SL_2(\mathbb{Z})$ に関する重さ k のモジュラー形式 (modular form) であるとは, 次の条件を満たすときにいう:

(i) 変換法則

$$f\left(\frac{a\tau+b}{c\tau+d}\right) = (c\tau+d)^k f(\tau), \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}),\ \tau \in \mathfrak{H}.$$

(ii) Fourier 展開に負冪の項がない. すなわち $\mathfrak{H}$ だけでなく無限遠点 $i\infty$ でも f は正則である:

$$f(\tau) = \sum_{n=0}^{\infty} a_n q^n \quad (q = e^{2\pi i\tau}).$$

以下この Fourier 展開を q 展開と呼ぶ. 特に条件 (ii) において $a_0 = 0$ となるとき, f はカスプ形式 (cusp form) であるという.

$SL_2(\mathbb{Z})$ に関する重さ k のモジュラー形式全体のなす $\mathbb{C}$ ベクトル空間を $M_k\big(SL_2(\mathbb{Z})\big)$ と表す. 以下では $SL_2(\mathbb{Z})$ のみを扱うので, 群についての表示を省略して単に M_k とも書く.

定義 1.4 (Eisenstein 級数)**.** 偶数 $k \geq 4$ に対して重さ k の (正規化された) Eisenstein 級数 $E_k(\tau)$ を次で定める:

$$E_k(\tau) := \frac{1}{2}\sum_{\substack{c,d\in\mathbb{Z} \\ (c,d)=1}} \frac{1}{(c\tau+d)^k} = 1 - \frac{2k}{B_k}\sum_{n=1}^{\infty}\Bigg(\sum_{d\mid n} d^{k-1}\Bigg)q^n.$$

ここで (c,d) は最大公約数を表し, B_k は k 番目の Bernoulli 数である.

偶数 $k \geq 4$ に対し $E_k(\tau) \in M_k$ である．一方で重さ 2 の Eisenstein 級数 $E_2(\tau) := 1 - 24\sum_{n=1}^{\infty}(\sum_{d|n} d)q^n$ は $\mathfrak{H}$ 上正則だがモジュラー形式ではなく, 準モジュラー形式 (quasimodular form) と呼ばれる．$E_2(\tau)$ は次の変換法則を満たす:

$$E_2\left(\frac{a\tau+b}{c\tau+d}\right) = (c\tau+d)^2E_2(\tau) + \frac{6}{\pi i}c(c\tau+d), \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}).$$

Eisenstein 級数を用いて Ramanujan の Δ 関数および楕円モジュラー関数 j を各々

$$\Delta(\tau) := \frac{E_4(\tau)^3 - E_6(\tau)^2}{1728} = q\prod_{n=1}^{\infty}(1-q^n)^{24} = q - 24q^2 + 252q^3 - 1472q^4 + \cdots,$$
$$j(\tau) := \frac{E_4(\tau)^3}{\Delta(\tau)} = \frac{1}{q} + 744 + 196884q + 21493760q^2 + \cdots$$

と定める．$\Delta(\tau)$ は $SL_2(\mathbb{Z})$ に関する重さ 12 のカスプ形式である．また $j(\tau)$ は $SL_2(\mathbb{Z})$ 不変な $\mathfrak{H}$ 上の正則関数であり, 無限遠点 $i\infty$ に一位の極をもつ．$j(\tau)$ の Fourier 係数がモンスター群の既約表現の次数の一次結合で書けるという事実 (“Monstrous moonshine”) はあまりに有名である．

命題 1.5. $M_k\bigl(SL_2(\mathbb{Z})\bigr)$ に関して次が成り立つ:

$$\bigoplus_{k\geq 0} M_k\bigl(SL_2(\mathbb{Z})\bigr) \cong \mathbb{C}[E_4, E_6].$$

すなわち $SL_2(\mathbb{Z})$ に関するモジュラー形式は E_4, E_6 の多項式で表せる．任意の偶数 $k \geq 4$ は $k = 12m + 4\delta + 6\varepsilon,\ m \in \mathbb{Z}_{\geq 0},\ \delta \in \{0,1,2\},\ \varepsilon \in \{0,1\}$ と一意的に書けることから M_k の基底として

$$\{E_4^{3m+\delta}E_6^{\varepsilon}, E_4^{3m+\delta-3}E_6^{\varepsilon}\Delta, \ldots, E_4^{\delta+3}E_6^{\varepsilon}\Delta^{m-1}, E_4^{\delta}E_6^{\varepsilon}\Delta^m\} \tag{1}$$

をとれる．ゆえに $\dim_{\mathbb{C}} M_k = m + 1$ である．

任意の $f \in M_k$ に対し, $f/(E_4^{\delta}E_6^{\varepsilon}\Delta^m)$ は重さ 0 かつ $\mathfrak{H}$ 上正則より, 高々m 次の $j(\tau)$ の多項式となる．その多項式を $\widetilde{f}$ と書くことにする:

$$f(\tau) = E_4(\tau)^{\delta}E_6(\tau)^{\varepsilon}\Delta(\tau)^m\widetilde{f}(j(\tau)).$$

特に $\widetilde{f}(j)$ における j^m の係数は f の q 展開の定数項に等しい．なお Eisenstein 級数から構成した多項式 $\widetilde{E}_{p-1}(X)$ と supersingular polynomial には次の関係が成り立つ．

定理 1.6 (Deligne)**.** 素数 $p \geq 5$ に対して $p - 1 = 12m + 4\delta + 6\varepsilon$ と書くとき

$$ss_p(X) \equiv X^{\delta}(X-1728)^{\varepsilon}\widetilde{E}_{p-1}(X) \pmod{p}.$$

例えば $E_{12} = E_4^3 - \frac{432000}{691}\Delta$ より $\widetilde{E}_{12}(X) = X - \frac{432000}{691} \equiv X + 8 \equiv ss_{13}(X) \pmod{13}$ である．以下では記号 “$\prime$” は通常の微分ではなく $(2\pi i)^{-1}d/d\tau = q \cdot d/dq$ $(q = e^{2\pi i\tau})$ を表すものとする．モジュラー形式を微分すると保型性が崩れてしまいモジュラー形式にならないが, 同じく保型性が崩れている E_2 と組み合わせることで保型性を保つことが出来る．

定義 1.7 (Serre 微分)**.** Serre 微分 $\partial_{\Delta} = \partial_{\Delta,k} : M_k \to M_{k+2}$ を次で定める:

$$\partial_{\Delta}(f)(\tau) := f'(\tau) - \frac{k}{12}E_2(\tau)f(\tau).$$

$\partial_\Delta(f) \in M_{k+2}$ は f の変換法則の微分と E_2 の変換法則から従う．$\Delta(\tau)$ の重さが 12 であることと, $\Delta'(\tau)/\Delta(\tau) = E_2(\tau)$ に注意する．また, ∂_Δ は $\bigoplus_{k\geq 0} M_k$ 上の重さ 2 の微分でカスプ形式の空間を保つものとして, 定数倍を除き一意に定まる．

命題 1.8 (Ramanujan)**.** Eisenstein 級数の微分に関して次が成り立つ:

$$E_2' = \frac{E_2^2 - E_4}{12},\ E_4' = \frac{E_2E_4 - E_6}{3},\ E_6' = \frac{E_2E_6 - E_4^2}{2}. \tag{2}$$

証明. $\partial_\Delta(E_4) \in M_6, \partial_\Delta(E_6) \in M_8$ であり, $\dim_{\mathbb{C}} M_6 = 1, \dim_{\mathbb{C}} M_8 = 1$ よりこれらは各々 E_6, E_4^2 の定数倍になる．あとは q 展開の定数項を比較して比例定数を求め, Serre 微分の定義に戻って展開すればよい．一方 $E_2' - \frac{1}{12}E_2^2$ が M_4 に入ることは E_2 の変換法則から直接確かめられるので, 同様の議論で示される． □

定義 1.9 (Modular Linear Differential Equation, MLDE)**.** 二階線形常微分方程式

$$f''(\tau) + A(\tau)f'(\tau) + B(\tau)f(\tau) = 0$$

が $SL_2(\mathbb{Z})$ に関する重さ k の MLDE であるとは次を満たすときにいう:

(i) $A(\tau), B(\tau)$ は $\mathrm{Im}(\tau) \to \infty$ で有界であり, 微分方程式 (1.9) は $SL_2(\mathbb{Z})$ の楕円点を確定特異点に持つ．すなわち $E_4(\tau)E_6(\tau)A(\tau)$ および $E_4(\tau)^2E_6(\tau)^2B(\tau)$ は $\mathfrak{H}$ 上正則[1]である．

(ii) $f(\tau)$ が解ならば, 任意の $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$ に対して $(c\tau + d)^{-k} f\left(\frac{a\tau+b}{c\tau+d}\right)$ もまた解である．

堤 [4] によってこの条件を満たす $SL_2(\mathbb{Z})$ に関する重さ k, 二階の MLDE は具体的な表示が決定されている．係数にかかる条件をより強くして $A(\tau), B(\tau)$ が $\mathfrak{H}$ 上正則とすると, $SL_2(\mathbb{Z})$ に関する重さ k, 二階の MLDE は本質的には次節の $(\sharp)_k$ に限ることが知られている．

2　既知の結果

本節ではある M_k の自己準同型の固有関数と supersingular polynomial との関係を紹介する．Serre 微分を二回施した作用素 $\partial_\Delta^2 = \partial_{\Delta,k+2} \circ \partial_{\Delta,k} : M_k \to M_{k+4}$ を考える．$k \not\equiv 2 \pmod 3$ に対して $\dim M_k = \dim M_{k+4}$ となることから, $M_{k+4} = E_4 \cdot M_k$ である．ゆえに $\phi_k(f) := E_4^{-1}\partial_\Delta^2$ は M_k の自己準同型を与えるが, ϕ_k は q 展開の定数項を $k(k+2)/144$ 倍し, 余次元 1 のカスプ形式の空間を保つ．よって ϕ_k は $k(k+2)/144$ を固有値の一つとして持つ．そこで固有値問題

$$\partial_\Delta^2(f) = \frac{k(k+2)}{144}E_4 f \tag{3}$$

を考え, 正規化 (定数項 $= 1$) された解を $F_{\Delta,k} \in M_k$ とする．このとき次が成り立つ．

定理 2.1 (Kaneko, Zagier [5])**.** 素数 $p \geq 5$ に対して $p - 1 = 12m + 4\delta + 6\varepsilon$ と書くとき

$$ss_p(X) \equiv X^\delta(X - 1728)^\varepsilon \widetilde{F}_{\Delta,p-1}(X) \pmod p.$$

[1] 講演では単に $A(\tau), B(\tau)$ が $\mathfrak{H}$ 上正則としていましたが条件が抜けていました．

Serre 微分の定義に従って (3) を展開すると

$$f''(\tau) - \frac{k+1}{6}E_2(\tau)f'(\tau) + \frac{k(k+1)}{12}E_2'(\tau)f(\tau) = 0 \qquad (\sharp)_k$$

となるが, これは先に定義した MLDE の代表的な例である. $(\sharp)_k$ は $ss_p(X)$ との関係以外にも, 様々なモジュラー形式解や準モジュラー形式解を持つこと [6, 7] や混合モックモジュラー形式解を持つこと [8] が分かっている.

MLDE の解と $ss_p(X)$ の関係に話を戻すと, Serre 微分と類似する微分作用素

$$\partial_{E_4}(f)(\tau) := f'(\tau) - \frac{k}{4}\frac{E_4'(\tau)}{E_4(\tau)}f(\tau),\ \partial_{E_6}(f)(\tau) := f'(\tau) - \frac{k}{6}\frac{E_6'(\tau)}{E_6(\tau)}f(\tau)$$

を用いて構成した固有値問題の正規化された解に対し, 次が成り立つ.

定理 2.2 (Baba, Granath [9])**.** 素数 $p \geq 5$ に対して $p-1 = 12m + 4\delta + 6\varepsilon$ と書くとき

$$ss_p(X) \equiv X^\delta(X-1728)^\varepsilon \widetilde{F}_{E_4,p-1}(X) \equiv X^\delta(X-1728)^\varepsilon \widetilde{F}_{E_6,p-1}(X) \pmod p.$$

注意 2.3. Serre 微分の場合と異なり, $f \in M_k$ に対して一般的には $\partial_{E_4}(f) \notin M_{k+2}$, $\partial_{E_6}(f) \notin M_{k+2}$ となる.

解から構成する多項式の零点について以下が成り立つ. これらの多項式は超幾何級数表示を持ち, それが古典的直交多項式になっていることから証明される.

定理 2.4 (Kaneko, Zagier [5])**.** $\widetilde{F}_{\Delta,k}(X)$ の根は全て実単根で, 区間 $(0, 1728)$ に存在する.

定理 2.5 (Baba, Granath [9])**.** $\widetilde{F}_{E_4,k}(X), \widetilde{F}_{E_6,k}(X)$ の根は全て実単根で, 各々区間 $(1728, \infty)$ および $(-\infty, 0)$ に存在する.

3 主結果

主結果は前節で述べた定理 2.1 および定理 2.2 を特殊化として含むようパラメータを入れたものである. まず $r, s, t \in \mathbb{Z}, u := 2r + 3s + 6t \neq 0$ に対して

$$g(\tau) = g_{r,s,t}(\tau) := E_4(\tau)^r E_6(\tau)^s \Delta(\tau)^t$$

とおく. このとき

$$\partial_g(f)(\tau) = \partial_{g,k}(f)(\tau) := f'(\tau) - \frac{k}{2u}\frac{g'(\tau)}{g(\tau)}f(\tau)$$

と定める. この作用素は対数微分の性質より

$$\partial_g(f) = \frac{2r}{u}\partial_{E_4}(f) + \frac{3s}{u}\partial_{E_6}(f) + \frac{6t}{u}\partial_\Delta(f)$$

と書き直せるから, 互いに素な (r, s, t) の組を考えれば十分である. また ∂_g は Leibnitz 則を満たす:

$$\partial_{g,k+l}(FG) = \partial_{g,k}(F)G + F\partial_{g,l}(G).$$

定理 3.1. 偶数 $k \geq 4$ を $k = 12m + 4\delta + 6\varepsilon$ と一意的に書く．さらに $1 \leq n \leq m$ なる整数 n に対して $t(k+1) \neq nu$ であるとする．

(1) 次の二階微分作用素 $\phi_{g,k}$ は M_k の自己準同型を与える:

$$\begin{aligned}\phi_{g,k}(f) = \frac{1}{E_4}\Bigg\{(\partial_{g,k+2} \circ \partial_{g,k})(f) - \frac{t^2 k(k+2)}{4u^2} E_4 f \\ - \frac{1}{16u^2}(sk - 2u\varepsilon)(sk - 2u\varepsilon + 4(r + 2s + 3t)) \frac{E_4(E_4^3 - E_6^2)}{E_6^2} f \\ + \frac{1}{36u^2}(rk - 2u\delta)\big(rk - 2u\delta + 6(r + s + 2t)\big) \frac{E_4^3 - E_6^2}{E_4^2} f \Bigg\}.\end{aligned}$$

また $\phi_{g,k}$ は固有値 0 をもつ．

(2) 次のモジュラー形式 $F_{g,k} = 1 + O(q) \in M_k$ は固有値 0 に対応する $\phi_{g,k}$ の固有関数である:

$$F_{g,k}(\tau) = E_4(\tau)^{3m+\delta} E_6(\tau)^{\varepsilon}\ {}_2F_1\left(-m,\, \mu\,; 1 - \frac{t(k+1)}{u}; \frac{1728}{j(\tau)}\right),$$
$$\mu = \frac{5}{12} + \frac{(2r - 3s - 6t)(k+1)}{12u} - \frac{2\delta - 3\varepsilon}{6}.$$

(3) 素数 $p \geq 5$ に対し $k = p - 1$ とし, $u \not\equiv 0 \pmod{p}$ とする．このとき

$$ss_p(X) \equiv X^{\delta}(X - 1728)^{\varepsilon} \widetilde{F}_{g,p-1}(X) \pmod{p}.$$

$(r, s, t) = (0, 0, 1) \Leftrightarrow g = \Delta$ が定理 2.1 に, $(r, s, t) = (1, 0, 0), (0, 1, 0) \Leftrightarrow g = E_4, E_6$ が定理 2.2 に対応する．以下, 証明の概略を述べる．

(1) まず M_k の基底 (1) の $\phi_{g,k}$ による行先は微分公式 (2) により計算できる．結果だけ書くと, $\delta \leq a \leq 3m + \delta, 0 \leq c \leq m, 4a + 12c = k - 6\varepsilon$ に対して

$$\phi_{g,k}(E_4^a E_6^{\varepsilon} \Delta^c) = c\left\{c - \frac{t(k+1)}{u}\right\} E_4^a E_6^{\varepsilon} \Delta^c - (\lambda(a) - \lambda(\delta)) E_4^{a-3} E_6^{\varepsilon} \Delta^{c+1},$$
$$\lambda(x) = \frac{48}{u^2}(rk - 2ux)(rk - 2ux + 6(r + s + 2t))$$

となる．いま $\delta \in \{0, 1, 2\}$ なので $a = \delta$ のとき二項目の E_4^{a-3} が負冪になり M_k の元を与えない恐れがあるが, そのとき $\lambda(a) - \lambda(\delta)$ が消えるので $\phi_{g,k}$ は M_k の自己準同型を与える．一項目の係数は仮定から $c = 0$ のときのみ消えるから $\phi_{g,k}$ は 0 を固有値に持つ．

(2) モジュラー形式解を

$$F_{g,k} = \sum_{c=0}^{m} \nu_c E_4^{3(m-c)+\delta} E_6^{\varepsilon} \Delta^c, \quad \nu_0 = 1$$

とおいて $\phi_{g,k}$ に代入すると消えることから, 基底の一次独立性より係数 ν に関する漸化式を得る．これを解くことで $F_{g,k}$ が超幾何級数を用いて表せる．あるいは同じことだが $\phi_{g,k}(f) = 0$ を直接解いてもよい．$\phi_{g,k}(f) = 0$ を ∂_g の定義にしたがって展開し整理すると

$$\begin{aligned}f'' - \frac{k+1}{u}\frac{g'}{g} f' + \frac{k(k+1)}{2u}\left(\frac{g'}{g}\right)' f + \frac{s(k+1)(k+2\varepsilon)}{8u} \frac{E_4(E_4^3 - E_6^2)}{E_6^2} f \\ - \left\{\frac{r(k+1)(k+2\delta)}{18u} - \frac{\delta(\delta-1)}{9}\right\} \frac{E_4^3 - E_6^2}{E_4^2} f = 0\end{aligned}$$

となり, $h = f/E_4^{3m+\delta}E_6^{\varepsilon}$ とおいて変数変換 $z = 1728/j(\tau)$ を施すことで超幾何微分方程式が現れる.

(3) $F_{g,k}$ の具体形において $k = p-1$ とおくと, 仮定から $u \not\equiv 0 \pmod{p}$ なので

$$\frac{5}{12} + \frac{(2r-3s-6t)(k+1)}{12u} - \frac{2\delta - 3\varepsilon}{6} \equiv \frac{5}{12} - \frac{2\delta - 3\varepsilon}{6}, \ 1 - \frac{t(k+1)}{u} \equiv 1 \pmod{p}$$

となり, 定理 1.1 から $ss_p(X)$ との関係を得る.

謝辞

本稿は 2016 年 8 月に開催された第 10 回福岡数論研究集会における筆者の講演に基づくものです. 今回講演および報告集執筆の機会を与えてくださった世話人の金子先生, 権先生, 岸先生に心より感謝申し上げます.

参考文献

[1] M. Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*, Abh. Math. Sem. Univ. Hamburg **14** (1941), 197–272.

[2] M. Eichler, *Über die Idealklassenzahl total definiter Quaternionenalgebren*, Math. Z. **43** (1938), 102–109.

[3] J. Igusa, *Class number of a definite quaternion with prime discriminant*, Proc. Nat. Acad. Sci. U.S.A. **44** (1958), 312–314.

[4] H. Tsutsumi, *Modular differential equations of second order with regular singularities at elliptic points for $SL_2(\mathbb{Z})$*, Proc. Amer. Math. Soc. **134** (2006), 931–941.

[5] M. Kaneko and D. Zagier, *Supersingular j-invariants, hypergeometric series, and Atkin's orthogonal polynomials*, In: Computational perspectives on number theory (Chicago, IL, 1995), 97–126, AMS/IP Stud. Adv. Math., 7, Amer. Math. Soc., Providence, RI, 1998.

[6] M. Kaneko and M. Koike, *On modular forms arising from a differential equation of hypergeometric type*, Ramanujan J. **7** (2003), 145–164.

[7] M. Kaneko, *On modular forms of weight $(6n+1)/5$ satisfying a certain differential equation*, In: Number theory, 97–102, Dev. Math., 15, Springer, New York, 2006.

[8] P. Guerzhoy, *A mixed mock modular solution of the Kaneko-Zagier equation*, Ramanujan J. **36** (2015), 149–164.

[9] S. Baba and H. Granath, *Orthogonal systems of modular forms and supersingular polynomials*, Int. J. Number Theory **7** (2011), 249–259.