Ramanujan J (2019) 48:13–20
https://doi.org/10.1007/s11139-018-9999-5

On modular solutions of certain modular differential equation and supersingular polynomials

Tomoaki Nakaya[1]

Received: 16 May 2017 / Accepted: 19 January 2018 / Published online: 16 April 2018

Abstract We extend the results of Kaneko–Zagier and Baba–Granath on relations of supersingular polynomials and solutions of certain second-order modular differential equations.

Keywords Modular form · Supersingular polynomials · Hypergeometric series

Mathematics Subject Classification 11F11 · 11F25

1 Introduction

An elliptic curve E over a field K of characteristic $p > 0$ is called *supersingular* if it has no p-torsion over $\overline{K}$. This condition depends only on the j-invariant of E, and it is known that there are only finitely many supersingular j-invariants, all being contained in $\mathbb{F}_{p^2}$. We define the supersingular polynomial $ss_p(X)$ as the monic polynomial whose roots are exactly all the supersingular j-invariants:

$$ss_p(X) = \prod_{\substack{E/\overline{\mathbb{F}}_p \\ E:\text{supersingular}}} \big(X - j(E)\big).$$

Because the set of supersingular j-invariants in characteristic p is stable under the conjugation over $\mathbb{F}_p$, we have $ss_p(X) \in \mathbb{F}_p[X]$.

✉ Tomoaki Nakaya
t-nakaya@math.kyushu-u.ac.jp

1 Graduate School of Mathematics, Kyushu University, 744, Motooka, Nishi-ku, Fukuoka 819-0395, Japan

Various lifts of $ss_p(X)$ to characteristic 0 are reviewed and studied in Kaneko and Zagier [1]. In particular, they constructed a lift by using a certain differential operator on the space of modular forms. Baba and Granath [2] extended this construction by introducing new differential operators.

In this paper, we unify and generalize these results, by considering a differential operator arising from a product of Eisenstein series E_4, E_6, and the discriminant function Δ. With this operator we construct a second-order differential operator which gives rise to an endomorphism of M_k. We write an eigenform of this operator explicitly in terms of hypergeometric series. For $k = p - 1$, we show that the associated polynomial $\widetilde{F}$ of this eigenform F satisfies

$$ss_p(X) = X^{\delta}(X - 1728)^{\varepsilon}\widetilde{F}(X) \mod p,$$

with suitable $\delta, \varepsilon \in \{0, 1\}$.

2 Modular forms and supersingular polynomials

For positive even integer k, we denote by M_k the space of holomorphic modular forms of weight k on $\Gamma = \mathrm{PSL}_2(\mathbb{Z})$. Let $E_k(\tau)$ be the Eisenstein series of weight k on Γ defined by

$$E_k(\tau) = 1 - \frac{2k}{B_k}\sum_{n=1}^{\infty}\left(\sum_{d|n} d^{k-1}\right)q^n \qquad (q = e^{2\pi i\tau}),$$

where τ is a variable in the Poincaré upper half-plane $\mathfrak{H}$ and B_k the kth Bernoulli number. For even $k \geq 4$, we have $E_k(\tau) \in M_k$. We also define the discriminant function $\Delta(\tau) \in M_{12}$ and the elliptic modular function $j(\tau)$, respectively, by

$$\begin{aligned}\Delta(\tau) &= \frac{E_4(\tau)^3 - E_6(\tau)^2}{1728} \\ &= q\prod_{n=1}^{\infty}(1 - q^n)^{24} = q - 24q^2 + 252q^3 - 1472q^4 + \cdots\end{aligned}$$

and

$$j(\tau) = \frac{E_4(\tau)^3}{\Delta(\tau)} = \frac{1}{q} + 744 + 196884q + 21493760q^2 + \cdots.$$

The Gauss hypergeometric series is defined by

$${}_2F_1(\alpha, \beta; \gamma; x) = \sum_{n=0}^{\infty}\frac{(\alpha)_n(\beta)_n}{(\gamma)_n}\frac{x^n}{n!} \quad (|x| < 1),$$

where $(\alpha)_0 = 1$ and $(\alpha)_n = \alpha(\alpha+1)\cdots(\alpha+n-1)$ $(n \geq 1)$. We note that the series ${}_2F_1(\alpha, \beta; \gamma; x)$ becomes a polynomial when α or β is a negative integer and γ is not a negative integer.

For even $k \geq 4$, we can write k uniquely in the form

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

Under this notation, any modular form $f(\tau) \in M_k$ can be written uniquely as

$$f(\tau) = E_4(\tau)^{\delta} E_6(\tau)^{\varepsilon} \Delta(\tau)^m \widetilde{f}\big(j(\tau)\big), \tag{2}$$

where $\widetilde{f}$ is a polynomial of degree less than or equal to m. We call $\widetilde{f}$ the associated polynomial of f.

The following representation of $ss_p(X)$ is essentially due to Deuring [3].

Lemma 1 *Let $p \geq 5$ be a prime number and write $p-1$ in the form $12m+4\delta+6\varepsilon$ $(m \in \mathbb{Z}_{\geq 0},\ \delta \in \{0, 1, 2\},\ \varepsilon \in \{0, 1\})$. Then*

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

Proof We define the monic polynomial $U_n^{\varepsilon}(X)$ of degree $n \geq 0$ by

$$X^n\,{}_2F_1\left(\tfrac{1}{12}, \tfrac{5}{12}; 1; \tfrac{1728}{X}\right) = U_n^0(X) + O\left(\tfrac{1}{X}\right),$$
$$X^{n-1}(X - 1728)\,{}_2F_1\left(\tfrac{7}{12}, \tfrac{11}{12}; 1; \tfrac{1728}{X}\right) = U_n^1(X) + O\left(\tfrac{1}{X}\right).$$

By [1, Proposition 5], we have $ss_p(X) = U^{\varepsilon}_{m+\delta+\varepsilon}(X) \mod p$. The first two parameters of the hypergeometric series in (3) reduce modulo p to

$$\left(-m, \frac{5}{12} - \frac{2\delta - 3\varepsilon}{6}\right) \equiv \begin{cases} (\frac{1}{12}, \frac{5}{12}) \pmod p & \text{if } p \equiv 1 \pmod{12}, \\ (\frac{5}{12}, \frac{1}{12}) \pmod p & \text{if } p \equiv 5 \pmod{12}, \\ (\frac{7}{12}, \frac{11}{12}) \pmod p & \text{if } p \equiv 7 \pmod{12}, \\ (\frac{11}{12}, \frac{7}{12}) \pmod p & \text{if } p \equiv 11 \pmod{12}. \end{cases}$$

Since ${}_2F_1(a, b; c; x) = {}_2F_1(b, a; c; x)$, we see that $U^{\varepsilon}_{m+\delta+\varepsilon}(X)$ is congruent to the left-hand side of (3) modulo p. □

3 Construction of the endomorphism

In this section, we construct an endomorphism $\phi_{g,k}$ of M_k. Let r, s, t be integers, not all zero, and k be an even integer greater than or equal to 4. Then, for the meromorphic modular form $g(\tau) = E_4(\tau)^r E_6(\tau)^s \Delta(\tau)^t \not\equiv 0$ of weight $u := 4r + 6s + 12t$ and

$f \in M_k$, we define the differential operator ∂_g by

$$\partial_g(f)(\tau) = \partial_{g,k}(f)(\tau) = f'(\tau) - \frac{k}{u}\frac{g'(\tau)}{g(\tau)} f(\tau) \quad \left({}' = \frac{1}{2\pi i}\frac{d}{d\tau} = q\frac{d}{dq} \right),$$

and for $m \in \mathbb{Z}_{\geq 0}$, $\delta \in \{0, 1, 2\}$, and $\varepsilon \in \{0, 1\}$ with $k = 12m + 4\delta + 6\varepsilon$, define the operator $\phi_{g,k}$ by

$$\begin{aligned}\phi_{g,k}(f) = \frac{1}{E_4}\Bigg\{ &(\partial_{g,k+2} \circ \partial_{g,k})(f) - \frac{t^2 k(k+2)}{u^2} E_4 f \\ &- \frac{432}{u^2}(sk - u\varepsilon)(sk - u\varepsilon + 4(r + 2s + 3t))\frac{E_4 \Delta}{E_6^2} f \\ &+ \frac{192}{u^2}(rk - u\delta)\big(rk - u\delta + 6(r + s + 2t)\big)\frac{\Delta}{E_4^2} f \Bigg\}. \end{aligned} \tag{4}$$

Note that the function $g(\tau)$ is not always a holomorphic modular form. Except for the case of $(r, s, t) = (0, 0, 1)$, the image of $f \in M_k$ under $\partial_{g,k}$ is not holomorphic in general.

Theorem 1 *The differential operator $\phi_{g,k}$ is an endomorphism of M_k.*

To prove the theorem, we need two lemmas.

Lemma 2 *The operator ∂_g is written as*

$$\partial_g(f) = \frac{4r}{u}\partial_{E_4}(f) + \frac{6s}{u}\partial_{E_6}(f) + \frac{12t}{u}\partial_{\Delta}(f) = \partial_{\Delta}(f) + \frac{k}{6u}\left(2r\frac{E_6}{E_4} + 3s\frac{E_4^2}{E_6}\right) f. \tag{5}$$

Proof This is easily computed by using the well-known relation (due to Ramanujan)

$$E_2' = \frac{E_2^2 - E_4}{12}, \quad E_4' = \frac{E_2 E_4 - E_6}{3}, \quad E_6' = \frac{E_2 E_6 - E_4^2}{2}. \tag{6}$$

□

Lemma 3 *Put $v = (sk - u\varepsilon)/2$ and $w = (rk - ua)/3$. Then*

$$\begin{aligned} u\,\partial_{g,k}(E_4^a E_6^\varepsilon \Delta^c) &= vE_4^{a+2}E_6^{\varepsilon-1}\Delta^c + wE_4^{a-1}E_6^{\varepsilon+1}\Delta^c, \\ u^2\,(\partial_{g,k+2} \circ \partial_{g,k})(E_4^a E_6^\varepsilon \Delta^c) &= 1728v(v + 2(r + 2s + 3t))E_4^{a+1}E_6^{\varepsilon-2}\Delta^{c+1} \\ &\quad + (v + w)(v + w - 2t)E_4^{a+1}E_6^\varepsilon \Delta^c \\ &\quad - 1728w(w + 2(r + s + 2t))E_4^{a-2}E_6^\varepsilon \Delta^{c+1}. \end{aligned} \tag{7}$$

Proof One can easily see that the operator ∂_Δ satisfies the Leibniz rule:

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

for $F \in M_k$ and $G \in M_l$. Hence we can prove the lemma by direct calculation using (5) and the following relations:

$$\partial_\Delta(E_4) = -\frac{1}{3}E_6, \quad \partial_\Delta(E_6) = -\frac{1}{2}E_4^2, \quad \partial_\Delta(\Delta) = 0, \quad E_4^3 - E_6^2 = 1728\Delta.$$

□

Proof of Theorem 1 For even $k \geq 4$, write k in the form $k = 12m + 4\delta + 6\varepsilon$ as before and assume the numbers a, c satisfy $a \equiv \delta \mod 3$ $(0 \leq a \leq 3m + \delta)$, $0 \leq c \leq m$, and $k = 4a + 6\varepsilon + 12c$, so that the forms $E_4^a E_6^\varepsilon \Delta^c$ constitute basis elements of M_k. We now compute $\phi_{g,k}(E_4^a E_6^\varepsilon \Delta^c)$.

Since $(v + w)(v + w - 2t) = t^2k(k + 2) - 2t(k + 1)uc + u^2c^2$, we can obtain from (7) the following equation:

$$\begin{aligned} &u^2\,(\partial_{g,k+2} \circ \partial_{g,k})(E_4^a E_6^\varepsilon \Delta^c) - t^2k(k + 2)E_4 \cdot E_4^a E_6^\varepsilon \Delta^c \\ &\quad = 1728v(v + 2(r + 2s + 3t))E_4^{a+1} E_6^{\varepsilon-2} \Delta^{c+1} \\ &\qquad + u^2c\{c - 2t(k + 1)/u\}E_4^{a+1} E_6^\varepsilon \Delta^c - 1728w(w + 2(r + s + 2t))E_4^{a-2} E_6^\varepsilon \Delta^{c+1}. \end{aligned}$$

Furthermore, by using $1728v(v + 2(r + 2s + 3t)) = 432(sk - u\varepsilon)(sk - u\varepsilon + 4(r + 2s + 3t))$, we have

$$\begin{aligned} &u^2\,(\partial_{g,k+2} \circ \partial_{g,k})(E_4^a E_6^\varepsilon \Delta^c) - t^2k(k + 2)E_4 \cdot E_4^a E_6^\varepsilon \Delta^c \\ &\quad - 432(sk - u\varepsilon)(sk - u\varepsilon + 4(r + 2s + 3t))\frac{E_4\Delta}{E_6^2}\, E_4^a E_6^\varepsilon \Delta^c \\ &= u^2c\left\{c - \frac{2t(k + 1)}{u}\right\} E_4^{a+1} E_6^\varepsilon \Delta^c \\ &\quad - 1728w(w + 2(r + s + 2t))E_4^{a-2} E_6^\varepsilon \Delta^{c+1}. \end{aligned}$$

We define $\lambda(x) = \frac{192}{u^2}(rk - ux)(rk - ux + 6(r + s + 2t))$, then $1728w(w + 2(r + s + 2t)) = u^2\lambda(a)$. Adding $u^2\lambda(\delta)E_4^{a-2} E_6^\varepsilon \Delta^{c+1}$ to both sides of the above equation and dividing them by u^2E_4, we get

$$\begin{aligned} \phi_{g,k}(E_4^a E_6^\varepsilon \Delta^c) = \frac{1}{E_4}\Bigg\{&(\partial_{g,k+2} \circ \partial_{g,k})(E_4^a E_6^\varepsilon \Delta^c) - \frac{t^2k(k + 2)}{u^2}E_4 \cdot E_4^a E_6^\varepsilon \Delta^c \\ &- \frac{432}{u^2}(sk - u\varepsilon)(sk - u\varepsilon + 4(r + 2s + 3t))\frac{E_4\Delta}{E_6^2}\, E_4^a E_6^\varepsilon \Delta^c \\ &+ \frac{48}{u^2}(rk - u\delta)(rk - u\delta + 6(r + s + 2t))\frac{\Delta}{E_4^2}\, E_4^a E_6^\varepsilon \Delta^c \Bigg\} \end{aligned}$$

$$= c\left\{c - \frac{2t(k+1)}{u}\right\} E_4^a E_6^\varepsilon \Delta^c - (\lambda(a) - \lambda(\delta)) E_4^{a-3} E_6^\varepsilon \Delta^{c+1}. \quad (8)$$

The right-hand side is an element of M_k if $a \geq 3$. If $a < 3$, we have $a = \delta$ (because $a \equiv \delta \pmod 3$) and the coefficient $\lambda(a) - \lambda(\delta)$ of $E_4^{a-3} E_6^\varepsilon \Delta^{c+1}$ vanishes, hence the right-hand side is in M_k. Thus $\phi_{g,k}$ is an endomorphism of M_k. □

4 Modular solutions of $\phi_{g,k}(f) = 0$ and supersingular polynomials

Throughout this section, we assume $2t(k+1) \neq cu$ $(1 \leq c \leq m)$ for given r, s, t, and $k = 12m + 4\delta + 6\varepsilon$. By Eq. (8), we see that the matrix representation of $\phi_{g,k}$ in the ordered base $\{E_4^{3m+\delta} E_6^\varepsilon, \ldots, E_4^\delta E_6^\varepsilon \Delta^m\}$ is a triangular matrix and obtain the eigenvalues $c(c - \frac{2t(k+1)}{u})$, $0 \leq c \leq m$ of $\phi_{g,k}$ as diagonal elements. Hence, under the assumption, all eigenvalues of endomorphism $\phi_{g,k}$ are different.

Theorem 2 (i) *The following modular form $F_{g,k}(\tau) = 1 + O(q)$ is the unique eigenvector of $\phi_{g,k}$ with eigenvalue 0:*

$$F_{g,k}(\tau) = E_4(\tau)^{3m+\delta} E_6(\tau)^\varepsilon \times {}_2F_1\left(-m, \frac{5}{12} + \frac{(2r - 3s - 6t)(k+1)}{6u} - \frac{2\delta - 3\varepsilon}{6}; 1 - \frac{2t(k+1)}{u}; \frac{1728}{j(\tau)}\right). \quad (9)$$

(ii) *Let $k = p - 1$ where $p \geq 5$ is prime and assume that $u \not\equiv 0 \pmod p$. Then the associated polynomial $\widetilde{F}_{g,p-1}(X)$ of $F_{g,p-1}(\tau)$ has p-integral coefficients and*

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

Proof (i) By using (5) and (6) to expand the differential equation $\phi_{g,k}(f) = 0$, we obtain

$$f''(\tau) + A(\tau) f'(\tau) + B(\tau) f(\tau) = 0,$$
$$A(\tau) = -\frac{k+1}{6} E_2 + \frac{k+1}{3u}\left(3s\frac{E_4^2}{E_6} + 2r\frac{E_6}{E_4}\right),$$
$$B(\tau) = \frac{k(k+1)}{12} E_2' - \frac{k(k+1)}{36u} \cdot \frac{9sE_4' E_4^2 + 4rE_6' E_6}{E_4 E_6} + \frac{E_4^3 - E_6^2}{E_4^2 E_6^2}\left\{\frac{s\varepsilon(k+1)}{2u} E_4^3 - \frac{2r\delta(k+1) - u\delta(\delta - 1)}{9u} E_6^2\right\}. \quad (10)$$

This is a special case of modular differential equations with regular singularities at elliptic points for $SL_2(\mathbb{Z})$ treated in [4]. More explicitly, the differential equation (10) is expressed as follows using the symbol in [4, Theorem B]:

$$\mathcal{D}_k\left(\frac{s(k+1)}{u}, \frac{2r(k+1)}{3u}, \frac{s\varepsilon(k+1)}{2u}, \frac{2r\delta(k+1)-u\delta(\delta-1)}{9u}\right).$$

Applying [4, Theorem C] to this parameters, we get the hypergeometric representation of $F_{g,k}(\tau)$. We note that the exponent of $E_6(\tau)$ is a solution of the following quadratic equation:

$$x^2-\left(\frac{2s(k+1)}{u}+1\right)x+\frac{2s\varepsilon(k+1)}{u}=0.$$

Since $\varepsilon\in\{0,1\}$, we have $\varepsilon(\varepsilon-1)=0$ and thus the left-hand side of the above equation factors into $(x-\varepsilon)(x-2s(k+1)/u+\varepsilon-1)$. As pointed out in [4, Remark 4], we can choose ε as exponent of $E_6(\tau)$. (ii) For $k=p-1$, by (2) and the hypergeometric formula (9), the associated polynomial $\widetilde{F}_{g,p-1}(X)$ of $F_{g,p-1}(\tau)$ is as follows:

$$\begin{aligned}\widetilde{F}_{g,p-1}(X)&=X^m{}_2F_1\left(-m, \frac{5}{12}+\frac{(2r-3s-6t)p}{6u}-\frac{2\delta-3\varepsilon}{6}; 1-\frac{2tp}{u}; \frac{1728}{X}\right)\\&\equiv X^m{}_2F_1\left(-m, \frac{5}{12}-\frac{2\delta-3\varepsilon}{6}; 1; \frac{1728}{X}\right) \mod p.\end{aligned}$$

Hence $X^\delta(X-1728)^\varepsilon\widetilde{F}_{g,p-1}(X)$ is congruent to $ss_p(X)$ modulo p by Lemma 1. □

Remark 1 The case of $(r,s,t)=(0,0,1)$ was studied in the paper [1] by Kaneko and Zagier. The corresponding operator

$$\partial_{\Delta,k}(f)(\tau)=f'(\tau)-\frac{k}{12}E_2(\tau)f(\tau)\ : M_k\to M_{k+2}$$

is called the Ramanujan–Serre derivative. We note that the logarithmic derivative of $\Delta(\tau)$ is equal to $E_2(\tau)$. If $k\not\equiv 2 \pmod 3$, the function $F_{\Delta,k}(\tau)$ coincides with $F_k(\tau)$ in [1, Sect. 8] up to a constant multiple. Moreover, Baba and Granath studied the cases of $(r,s,t)=(1,0,0)$ and $(0,1,0)$ in [2]. The corresponding operators are given, respectively, by

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

Hence, the differential equations $\phi_{E_4,k}(f)=0$ and $\phi_{E_6,k}(f)=0$ coincide with [2, Eq. (5)] and [2, Eq. (8)], respectively. Consequently, the symbols $F_{E_4,k}(\tau)$ and $F_{E_6,k}(\tau)$ we use are same as theirs, but the definition of our operator $\phi_{g,k}$ and their operator ϕ are slightly different.

Acknowledgements The author would like to thank Professor Masanobu Kaneko for helpful advice. He also thanks the anonymous referee for valuable suggestions.

References

1. Kaneko, M., Zagier, D.: Supersingular j-invariants, hypergeometric series, and Atkin's orthogonal polynomials. In: Computational Perspectives on Number Theory (Chicago, IL, 1995). AMS/IP Stud. Adv. Math., 7, pp. 97–126. American Mathematical Society, Providence, RI (1998)
2. Baba, S., Granath, H.: Orthogonal systems of modular forms and supersingular polynomials. Int. J. Number Theory **7**, 249–259 (2011)
3. Deuring, M.: Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. Abh. Math. Sem. Univ. Hamburg **14**, 197–272 (1941)
4. Tsutsumi, H.: Modular differential equations of second order with regular singularities at elliptic points for $SL_2(\mathbb{Z})$. Proc. Am. Math. Soc. **134**, 931–941 (2006)