Centre de Recherches Mathématiques
CRM Proceedings and Lecture Notes
Volume **30**, 2001

Hypergeometric Modular Forms and Supersingular Elliptic Curves

Masanobu Kaneko and Naoya Todaka

ABSTRACT. We give a new series of "hypergeometric" modular forms which bear a close relation to supersingular elliptic curves.

1. Introduction

At least for the moment, supersingular elliptic curves have little to do with the monstrous moonshine. However, the two are not completely irrelevant, as the famous observation of A. Ogg stated below suggests.

It is known since Deuring [**D**] that the j-invariant of any supersingular elliptic curve in characteristic p, for any prime number p, lies in the field $\mathbb{F}_{p^2}$ of p^2 elements. As it turns out, there are finitely many "special" primes p such that *all* j-invariants of supersingular elliptic curves in characteristic p lie in the prime field $\mathbb{F}_p$ of p elements. An equivalent form of Ogg's observation [**O**] is then stated as:

> Such special primes are exactly those prime numbers that divide the order of the Monster simple group.

On the other hand, connections between supersingular elliptic curves and modular forms have been established in various ways and frameworks, examples of which can be found in [**DR, KZ, S**].

In this paper, we shall give a new series of modular forms whose zeros are closely connected to supersingular j-invariants, as a solution of certain differential equations of hypergeometric type of third order. This is viewed as a continuation of our previous work [**KZ**] where modular forms satisfying second order differential equations were discussed.

2000 *Mathematics Subject Classification.* Primary: 11F11; Secondary: 11G20.

The authors would like to thank Professor Tomoyoshi Ibukiyama for his valuable comments and discussions. We had treated only some special cases before he suggested to looking at the more general setting. Thanks are also due to Professor Don Zagier, whose comments clarified the statement of our main theorem. We would also like to thank the referee for useful comments.

This is the final form of the paper.

2. Preliminaries

Let $\Gamma = \mathrm{PSL}_2(\mathbb{Z})$ be the modular group. For an even integer $k \geq 0$, denote by M_k the space of holomorphic modular forms of weight k on Γ. M_k is a finite-dimensional $\mathbb{C}$-vector space and its dimension is $[k/12]+1$ if $k \not\equiv 2 \pmod{12}$ and $[k/12]$ if $k \equiv 2 \pmod{12}$, as is well-known. The graded ring $\bigoplus_{k\geq 0} M_k$ of all modular forms on Γ is isomorphic to the polynomial algebra $\mathbb{C}[E_4, E_6]$ where

$$E_4 = E_4(\tau) = 1 + 240\sum_{n=1}^{\infty}\Big(\sum_{d|n} d^3\Big)q^n, \quad (q = e^{2\pi i\tau}, \tau \in \mathfrak{H}\colon \text{ the upper half-plane})$$

and

$$E_6 = E_6(\tau) = 1 - 504\sum_{n=1}^{\infty}\Big(\sum_{d|n} d^5\Big)q^n$$

are the Eisenstein series of weights 4 and 6 respectively. The discriminant function $\Delta = \Delta(\tau) \in M_{12}$ and the elliptic modular invariant $j(\tau)$ are defined respectively by

$$\Delta(\tau) = \frac{1}{1728}(E_4(\tau)^3 - E_6(\tau)^2) = q - 24q^2 + 252q^3 - 1472q^4 + \cdots$$

and

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

We associate to each modular form $f(\tau) \in M_k$ a polynomial $\Omega_f(X) \in \mathbb{C}[X]$ whose roots are exactly the values of $j(\tau)$ at the ($\mathbb{C}$-equivalence classes of) zeros of $f(\tau)$ in $\mathfrak{H}$. For this, write k (uniquely) in the form

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

(with this notation, $m = \dim M_k$). Then $f(\tau)$ is written uniquely as

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

for some polynomial $\tilde{f}$ of degree $\leq m$ in $j(\tau)$ (because $f(\tau)/(E_4(\tau)^{\delta}E_6(\tau)^{\varepsilon}\Delta(\tau)^m)$ is of weight 0 and holomorphic in $\mathfrak{H}$), the coefficient of j^m in $\tilde{f}$ being equal to the constant term of the Fourier expansion of $f(\tau)$. The required polynomial is then given by

$$\Omega_f(X) := X^{\delta}(X-1728)^{\varepsilon}\tilde{f}(X).$$

Recall that the graded ring $\bigoplus_{k\geq 0} M_k$ has a unique (up to constant multiple) derivation of degree 2 which sends cusp forms to cusp forms. Specifically, the system of differential operators $\{\partial_k\}_{k\geq 0}$ defined by

$$\partial_k(f)(\tau) := \frac{1}{2\pi i}\frac{df}{d\tau}(\tau) - \frac{k}{12}E_2(\tau)f(\tau),$$

for $f(\tau) \in M_k$ has the required property (c.f. Serre [**S**]). Here, $E_2(\tau) = qd/dq\log\Delta(\tau) = 1 - 24\sum_{n=1}^{\infty}(\sum_{d|n} d)q^n$ is the "quasi-modular" Eisenstein series of weight 2. We denote this derivation on $\bigoplus_{k\geq 0} M_k$ by ∂. Note that, since $\partial\Delta = 0$, the action of ∂ commutes with multiplication by Δ; $\partial_{k+2}(\Delta f) = \Delta\partial_k f$ for $f \in M_k$.

For a prime p, let $ss_p(X)$ be the polynomial having all supersingular j-invariants as its roots:

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

the product running over the isomorphism classes of supersingular elliptic curves over $\overline{\mathbb{F}}_p$.

Hypergeometric series ${}_3F_2(\alpha_1, \alpha_2, \alpha_3; \beta_1, \beta_2; x)$ and ${}_2F_1(\alpha_1, \alpha_2; \beta_1; x)$ are defined by

$$ {}_3F_2(\alpha_1, \alpha_2, \alpha_3; \beta_1, \beta_2; x) = \sum_{n=0}^{\infty} \frac{(\alpha_1)_n(\alpha_2)_n(\alpha_3)_n}{(\beta_1)_n(\beta_2)_n} \frac{x^n}{n!} $$

and

$$ {}_2F_1(\alpha_1, \alpha_2; \beta_1; x) = \sum_{n=0}^{\infty} \frac{(\alpha_1)_n(\alpha_2)_n}{(\beta_1)_n} \frac{x^n}{n!}, $$

respectively, where $(\alpha)_0 = 1$ and $(\alpha)_n = \alpha(\alpha+1)\cdots(\alpha+n-1)$, $(n \geq 1)$.

3. Main Result

From ∂ we can form two differential operators $\partial^3 (= \partial_{k+4} \circ \partial_{k+2} \circ \partial_k)$ and $E_4\partial (= E_4(\tau) \cdot \partial_k)$ which send forms in M_k to M_{k+6}. If $k + 6 \equiv 2 \pmod 4$, then (the ε for $k + 6$ in the previous section should be 1 and so) every element of M_{k+6} is divisible by $E_6(\tau)$ (in this case $\dim_\Gamma M_k = \dim_\Gamma M_{k+6}$). Thus we are led to consider the third order equation

$$ (3.1) \qquad (\partial^3 + cE_4\partial)F(\tau) = (\text{constant}) \cdot E_6(\tau)F(\tau) $$

with a parameter c (which may depend on k). In other words, we have an endomorphism $\phi_{k,c}$ of M_k defined by $\phi_{k,c}(f) = E_6(\tau)^{-1}(\partial_{k+4} \circ \partial_{k+2} \circ \partial_k + cE_4(\tau)\partial_k)(f)$ if $k \equiv 0 \pmod 4$, and we want to look for an eigenform of $\phi_{k,c}$ in M_k. Since the constant term of $\phi_{k,c}(f)$ is $\kappa_{k,c} := -k(k+2)(k+4)/12^3 - kc/12$ times the constant term of f, this map $\phi_{k,c}$ preserves the codimension 1 subspace of cusp forms and induces on the quotient space the map multiplication by $\kappa_{k,c}$. It follows that $\kappa_{k,c}$ is an eigenvalue of $\phi_{k,c}$. The following theorem gives us a corresponding eigenform in an explicit way under a certain (mild) restriction on c.

THEOREM 3.1. *Assume* $k \equiv 0 \mod 4$ *and let* $m = [k/12]$. *Suppose that*

$$ c = -\frac{1}{576}(9\lambda^2 + 3k^2 + 12k - 4), $$

for some complex number λ *which satisfies the condition*

$$ (3.2) \qquad \lambda \neq \pm(8i - k - 2) \text{ for any integer } i, \quad 1 \leq i \leq m, $$

so that $\kappa_{k,c} = -k(k+6-3\lambda)(k+6+3\lambda)/6912$. *Then:*

(i) *The following modular form* $F_{k,c}(\tau)$ *is an eigenvector of* $\phi_{k,c}$ *with eigenvalue* $\kappa_{k,c}$:

$$ F_{k,c}(\tau) = \sum_{\ell=0}^{m} \frac{(-k/4)_{3\ell}}{p_\ell} E_4(\tau)^{k/4-3\ell} \Delta(\tau)^\ell $$

where

$$ p_\ell = 2^{-12\ell}\ell! \prod_{i=1}^{\ell} (8i - k - 2 + \lambda)(8i - k - 2 - \lambda) \quad (\neq 0 \text{ by } (3.2)), $$

with the empty product being 1.

$F_{k,c}(\tau)$ *can also be written using hypergeometric series as*

$$ F_{k,c}(\tau) = E_4(\tau)^{k/4} {}_3F_2\left(-\frac{k}{12}, -\frac{k-4}{12}, -\frac{k-8}{12}; \frac{\lambda - k + 6}{8}, \frac{-\lambda - k + 6}{8}; \frac{1728}{j(\tau)}\right). $$

(ii) *Let* $k = p-1$ *where* p *is a prime congruent to* 1 (mod 4). *Take* $\lambda \in \mathbb{Q}\cap\mathbb{Z}_p$ *which satisfies* (3.2) *and* $\lambda \equiv \pm 1 \mod p$. *Then the associated polynomial* $\Omega_{F_{p-1,c}}(X)$ *for* $F_{p-1,c}(\tau)$ *has* p*-integral rational coefficients and*

$$\Omega_{F_{p-1,c}}(X) \equiv ss_p(X) \mod p.$$

PROOF.

(i) We have found the formula for $F_{k,c}(\tau)$ by inspection with the aid of computer. Once a candidate of the exact form of the solution was found, it is a routine task to verify that the form is indeed the solution of the differential equation. We may instead proceed as follows. Since $4|k$, any form in M_k can be written as $\sum_{\ell=0}^{m} a_\ell E_4^{k/4-3\ell}\Delta^\ell$ with some a_ℓ. The image of $E_4^j\Delta^\ell$ ($j = k/4-3\ell$) under $\phi_{k,c}$ equals $A_jE_4^{j-3}\Delta^{\ell+1}+B_jE_4^j\Delta^\ell$ with $A_j = 64j(j-1)(j-2)$ and $B_j = -j(j+1)(2j+1)/54 - jc/3$. (Use $\partial(\Delta) = 0$, $\partial(E_4) = -E_6/3$, $\partial(E_6) = -E_4^2/2$.) From this we can find the values a_ℓ systematically to solve $\phi_{k,c}(\sum_{\ell=0}^{m} a_\ell E_4^{k/4-3\ell}\Delta^\ell) = \kappa_{k,c}(\sum_{\ell=0}^{m} a_\ell E_4^{k/4-3\ell}\Delta^\ell)$.

We note that

$$\left(-\frac{k}{4}\right)_{3\ell} = 3^{3\ell}\left(-\frac{k}{12}\right)_\ell\left(-\frac{k-4}{12}\right)_\ell\left(-\frac{k-8}{12}\right)_\ell$$

and

$$p_\ell = 2^{-6\ell}\ell!\left(\frac{\lambda-k+6}{8}\right)_\ell\left(\frac{-\lambda-k+6}{8}\right)_\ell,$$

hence our hypergeometric formula follows.

(ii) When $\lambda \equiv \pm 1 \mod p$, we have

$$\frac{\pm\lambda-k+6}{8} \equiv 1, \frac{3}{4} \mod p.$$

Since both $(1)_\ell$ and $(3/4)_\ell$ never vanish modulo p for ℓ in the range $0 \le \ell \le m = [k/12]$, we have

$$\begin{aligned}\Omega_{F_{p-1,c}}(X) &= X^{m+\delta}{}_3F_2\left(-\frac{k}{12}, -\frac{k-4}{12}, -\frac{k-8}{12}; \frac{\lambda-k+6}{8}, \frac{-\lambda-k+6}{8}; \frac{1728}{X}\right)\\ &\equiv X^{m+\delta}{}_3F_2\left(\frac{1}{12}, \frac{5}{12}, \frac{3}{4}; \frac{3}{4}, 1; \frac{1728}{X}\right) \mod p\\ &\equiv X^{m+\delta}{}_2F_1\left(\frac{1}{12}, \frac{5}{12}; 1; \frac{1728}{X}\right) \mod p.\end{aligned}$$

It is a classical fact, reviewed in [**KZ**], that the last term is congruent to $ss_p(X)$ modulo p when $p \equiv 1 \mod 4$.

□

REMARK 3.2.

(i) The other eigenvectors of $\phi_{k,c}$ are the functions $\Delta^iF_{k-12i,c}$ with eigenvalues $\kappa_{k-12i,c}$ ($1 \le i \le m$), provided the corresponding condition (3.2) for each $k-12i$ with the same c is satisfied. This is because the relation $\partial_k \circ \Delta^i = \Delta^i \circ \partial_{k-12i}$ holds by the commutativity of ∂ and multiplication by Δ as mentioned earlier. The condition (3.2) is equivalent to saying that $\kappa_{k,c}$ is different from any $\kappa_{k-12i,c}$ for $1 \le i \le m$.

(ii) In [**KZ**], we investigated an eigenform of the endomorphism

$$f \mapsto E_4(\tau)^{-1}\partial_{k+2}(\partial_k(f)),$$

of M_k when $k+4 \not\equiv 0 \pmod 3$. The associated polynomial of a unique (up to constant multiple) noncusp eigenform is

$$X^{m+\delta}(X-1728)^{\varepsilon}{}_2F_1\left(-m, -m+\frac{1-2\delta}{3}; 1-\frac{k+1}{6}; \frac{1728}{X}\right),$$

where $k = 12m + 4\delta + 6\varepsilon$, and this reduces modulo p to $ss_p(X)$ when $k = p-1$.

If furthermore $k \equiv 0 \pmod 4$, this eigenform can also be obtained from our ${}_3F_2$ form by putting $\lambda = (k-2)/3$ (for this the condition (3.2) is satisfied).

References

[DR] P. Deligne and M. Rapoport *Les schémas de modules de courbes elliptiques*, Proc. Internat. Summer School (Antwerp, 1972), Lecture Notes in Math., vol. 349, Springer, Berlin, 1973, pp. 143–316.

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

[KZ] M. Kaneko and D. Zagier *Supersingular j-invariants, hypergeometric series, and Atkin's orthogonal polynomials*, Computational Perspectives on Number Theory (Chicago, 1995) (Buell and Teitelbaum, eds.) AMS/IP Stud. Adv. Math., vol. 7, Amer. Math. Soc., Providence, RI, 1998, pp. 97–126.

[O] A. Ogg *Automorphismes de courbes modulaires*, Théorie des nombres, Séminaire Delange-Pisot-Poitou (1974/75), Fasc. 1, Exp. no. 7, Secrétariat Mathématique, Paris, 1975. pp. 1–8.

[S] J-P. Serre *Congruences et formes modulaires* (*d'après H. P. F. Swinnerton–Dyer*), Séminaire Bourbaki (1971/72), Exp. No. 416, Lecture Notes in Math., vol. 317, Springer, Berlin, 1973, pp. 319–338.

GRADUATE SCHOOL OF MATHEMATICS, KYUSHU UNIVERSITY 33, FUKUOKA 812-8581, JAPAN.
E-mail address, Masanobu Kaneko: `mkaneko@math.kyushu-u.ac.jp`
E-mail address, Naoya Todaka: `ntodaka@math.kyushu-u.ac.jp`