RIMS Kôkyûroku Bessatsu
B53 (2015), 305–324

Maeda's conjecture and related topics

By

Yoshitaka Maeda*

Contents

Abstract

Since we published the so-called Maeda conjecture in [HM97], many verifications and related results have been obtained by many researchers. In this note, we report on the recent progress and mention the conjecture of Tsaknias and Dieulefait which is a generalization to higher levels.

§ 1. Maeda's conjecture and verifications

We denote by $S_k(SL_2(\mathbb{Z}))$ the space of cusp forms on the full modular group $SL_2(\mathbb{Z})$ of weight k. We simply write $\mathcal{S}_k$ for $S_k(SL_2(\mathbb{Z}))$. Let $f(z) \in \mathcal{S}_k$ be a normalized Hecke eigenform of weight k:

$$f(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i n z}, \quad (a_1 = 1),$$

and we denote by

$$\mathbb{Q}(f) := \mathbb{Q}(a_1, a_2, a_3, \cdots)$$

Received March 31, 2014. Revised December 25, 2014.
2010 Mathematics Subject Classification(s): 11F11, 11F67.
Key Words: *modular forms, special values.*
*e-mail: `maeda@math.sci.hokudai.ac.jp`

the field generated by the Fourier coefficients $\{a_n\}_{n=1}^{\infty}$ and by $G(f)$ the Galois group of the Galois closure of $\mathbb{Q}(f)$ over $\mathbb{Q}$. We call $\mathbb{Q}(f)$ *Hecke's field* of $f(z)$. It is well known that $\mathbb{Q}(f)$ is a number field of finite degree and for any $\sigma \in G(f)$

$$f^{\sigma}(z) := \sum_{n=1}^{\infty} a_n^{\sigma} e^{2\pi i n z}$$

is also a normalized Hecke eigenform in $\mathcal{S}_k$ which is called a *conjugate* of $f(z)$. It is also well known that $\mathcal{S}_k$ has a basis consisting of normalized Hecke eigenforms. In the following, we take any one of them and denote by $f_k(z)$. $\mathcal{S}_k$ is called *non-splitting* if the conjugetes $\{f_k^{\sigma}(z)\}_{\sigma\in G(f_k)}$ of $f_k(z)$ span $\mathcal{S}_k$. This is independent of the choice of $f_k(z)$. When the following properties (H_a) and (H_b) hold for $\mathcal{S}_k$, we say $H(k)$ *holds*:

(H_a) $\mathcal{S}_k$ is non-splitting;

(H_b) $G(f_k)$ is isomorphic to the symmetric group of degree $\dim_{\mathbb{C}}\mathcal{S}_k$.

The following conjecture is called Maeda's conjecture:

Conjecture 1.1 ([HM97], Conjecture 1.2). *$H(k)$ holds for any k.*

Let $T(n)$ be the n-th Hecke operator on $\mathcal{S}_k$ and $\varphi_n(x)(\in \mathbb{Q}[x])$ the characteristic polynomial of $T(n)$. When the following properties (Φ_a) and (Φ_b) hold for $\mathcal{S}_k$, we say $\Phi(n)$ *holds* for $\mathcal{S}_k$:

(Φ_a) $\varphi_n(x)$ is irreducible over $\mathbb{Q}$;

(Φ_b) The Galois group of the minimal splitting field of $\varphi_n(x)$ is isomorphic to the symmetric group of degree $\dim_{\mathbb{C}}\mathcal{S}_k$.

From now on, we assume $\dim_{\mathbb{C}}\mathcal{S}_k \geq 2$ and $n \geq 2$ whenever $\Phi(n)$ is in question. The following lemmas are useful for the verification of $H(k)$ and $\Phi(n)$:

Lemma 1.2. *If $\Phi(n)$ holds for $\mathcal{S}_k$ for some $n \geq 2$, then $H(k)$ holds.*

Lemma 1.3 ([HM97], Proposition 5.1). *Let $\varphi(x) \in \mathbb{Z}[x]$ be a monic polynomial. If there exist three primes p_1, p_2 and p_3 satisfying the following conditions, then $\varphi(x)$ is irreducible over $\mathbb{Q}$ and the Galois group of the minimal splitting field of $\varphi(x)$ is isomorphic to the symmetric group of degree* $\deg(\varphi(x))$*:*

(i) $\varphi(x) \mod p_1$ *is irreducible over* $\mathbb{F}_{p_1}$*;*

(ii) $\varphi(x) \equiv \varphi_1(x)\varphi_2(x)\cdots\varphi_s(x) \mod p_2$ $(s \geq 2)$ *with polynomials* $\varphi_i(x) \in \mathbb{Z}[x]$ *such that* $\varphi_i(x) \mod p_2$ *are distinct irreducible polynomials in* $\mathbb{F}_{p_2}[x]$, $\deg(\varphi_1(x)) = 2$ *and* $\deg(\varphi_i(x))$ *are odd for* $i \geq 2$*;*

(*iii*) $\varphi(x) \equiv \psi_1(x)\psi_2(x) \mod p_3$ *with polynomials* $\psi_i(x) \in \mathbb{Z}[x]$ *such that* $\psi_i(x) \mod p_3$ *are distinct irreducible polynomials in* $\mathbb{F}_{p_3}[x]$ *and* $\deg(\psi_1(x)) = 1$.

Here $\mathbb{F}_p$ stands for the finite field of p elements.

Remark 1 ([CF99], Lemma 4). The condition (iii) can be replaced with the following condition:

(*iii*)' $\varphi(x) \equiv \psi_1(x)\psi_2(x)\cdots\psi_t(x) \mod p_3$ $(t \geq 2)$ *with polynomials* $\psi_i(x) \in \mathbb{Z}[x]$ *such that* $\psi_i(x) \mod p_3$ *are distinct irreducible polynomials in* $\mathbb{F}_{p_3}[x]$, $\deg(\psi_1(x))$ *is prime and* $\deg(\psi_1(x)) > \frac{\deg(\varphi(x))}{2}$.

Theorem 1.4. *$H(k)$ holds for* $k \leq 14000$.

These are verified by that $\Phi(2)$ holds for $\mathcal{S}_k$. The progress of verifications until 2012 is as follows ([GM12] Table 1):

k	Source
$k \leq 62,\ k \neq 60$	Lee-Hung (1995) [LH95]
$12\ell\ (\ell : prime,\ 2 \leq \ell \leq 19)$	Buzzard (1996) [B96]
$k \leq 468$	Maeda (1997) [HM97]
$k \leq 500,\ k \equiv 0 \mod 4$	Conrey-Farmer (1999) [CF99]
$k \leq 2000$	Farmer-James (2001) [FJ01]
$k \leq 3000$	Buzzard-Stein, Kleinerman (2004) [K04]
$k \leq 6000$	Chu-Wee Lim (2005) [L05]
$k \leq 14000$	Ghitza-McAndrew (2012) [GM12]

The table given below is the list of $\varphi_2(x)$ for $\dim_{\mathbb{C}}\mathcal{S}_k = 2, 3, 4$:

k	$\varphi_2(x)$
24	$x^2 - 1080\,x - 20468736$
28	$x^2 + 8280\,x - 195250176$
30	$x^2 - 8640\,x - 454569984$
32	$x^2 - 39960\,x - 2235350016$
34	$x^2 + 121680\,x - 8513040384$
36	$x^3 - 139656\,x^2 - 59208339456\,x - 1467625047588864$
38	$x^2 + 194400\,x - 137403408384$
40	$x^3 - 548856\,x^2 - 810051757056\,x + 213542160549543936$
42	$x^3 + 344688\,x^2 - 6374982426624\,x - 520435526440845312$
44	$x^3 + 2209944\,x^2 - 15663522502656\,x - 19976984434430705664$
46	$x^3 - 3814272\,x^2 - 44544640241664\,x + 135250282417024401408$

k	$\varphi_2(x)$
48	$x^4 - 5785560\,x^3 - 467142374034432\,x^2 + 1426830562183253852160\,x + 3297913828840214320807673856$
50	$x^3 + 24225168\,x^2 - 566746931810304\,x - 13634883228742736412672$
52	$x^4 - 32756040\,x^3 - 7956172284567552\,x^2 + 269568678949709508771840\,x + 4615876968087578049834569957376$
54	$x^4 + 68476320\,x^3 - 19584715019010048\,x^2 - 1083312724663489297121280\,x + 39446133467662904714689328971776$
56	$x^4 - 208622520\,x^3 - 69659795501724672\,x^2 + 11031882363768735132549120\,x - 255678332805518077225389998997504$
58	$x^4 + 217744560\,x^3 - 411086477602603008\,x^2 - 42515907658957794091991040\,x + 18678231666950985607375948785647616$
62	$x^4 - 1146312000\,x^3 - 6156169255669690368\,x^2 + 2540887466526178560442368000\,x + 3583176547297492565952659077522784256$

In particular, we get the list of Hecke's fields $\mathbb{Q}(f_k)$ whose degree is 2:

k	$\mathbb{Q}(f_k)$
24	$\mathbb{Q}(\sqrt{144169})$
28	$\mathbb{Q}(\sqrt{131 \cdot 139})$
30	$\mathbb{Q}(\sqrt{51349})$
32	$\mathbb{Q}(\sqrt{67 \cdot 273067})$
34	$\mathbb{Q}(\sqrt{479 \cdot 4919})$
38	$\mathbb{Q}(\sqrt{181 \cdot 349 \cdot 1009})$

Since $\mathcal{S}_k$ is non-splitting if and only if $[\mathbb{Q}(f_k) : \mathbb{Q}] = \dim_{\mathbb{C}} \mathcal{S}_k$ and

$$\dim_{\mathbb{C}} \mathcal{S}_k = \left[\frac{k}{12}\right] - 1 \ \ or \ \ \left[\frac{k}{12}\right]$$

according as $k \equiv 2 \mod 12$ or not, Conjecture 1.1 implies that for any integer $d \geq 2$, there exist special 6 number fields of dimension d up to conjugate which coincide with Hecke's fileds $\mathbb{Q}(f_k)$ for some $f_k(z)$. The following question naturally arises:

Question 1. *What conditions characterize Hecke's fileds $\mathbb{Q}(f_k)$? In particular, what conditions characterize the following 6 quadratic fields?*

$$\mathbb{Q}(\sqrt{144169}),\ \mathbb{Q}(\sqrt{131 \cdot 139}),\ \mathbb{Q}(\sqrt{51349}),\ \mathbb{Q}(\sqrt{67 \cdot 273067}),$$
$$\mathbb{Q}(\sqrt{479 \cdot 4919}),\ \mathbb{Q}(\sqrt{181 \cdot 349 \cdot 1009}).$$

Now we consider ramification of primes in Hecke's fields and give a conjecture. Let $\boldsymbol{h}_k$ be the subalgebra of $\mathrm{End}_{\mathbb{C}}(\mathcal{S}_k)$ generated by all Hecke operators $T(n)$ over $\mathbb{Z}$ and $\mathcal{S}_k(\mathbb{Z}) := \{g(z) \in \mathcal{S}_k \mid \text{all Fourier coefficients of } g(z) \text{ are rational integers}\}$.

Proposition 1.5 (Hida). *There exists a basis $\{g_\ell(z)\}_{\ell=1}^d$ $(d = \dim_{\mathbb{C}}\mathcal{S}_k)$ of $\mathcal{S}_k$ such that*

$$g_\ell(z) = e^{2\pi i \ell z} + \sum_{n=d+1}^{\infty} a_{\ell,n} e^{2\pi i n z} \ \textit{with}\ a_{\ell,n} \in \mathbb{Z}, \tag{1.1}$$

and we have

$$\mathcal{S}_k(\mathbb{Z}) = \bigoplus_{\ell=1}^{d} \mathbb{Z}\, g_\ell(z), \quad \boldsymbol{h}_k = \bigoplus_{\ell=1}^{d} \mathbb{Z}\, T(\ell), \tag{1.2}$$

$$\mathrm{Hom}_{\mathbb{Z}}(\mathcal{S}_k(\mathbb{Z}), \mathbb{Z}) \cong \boldsymbol{h}_k, \quad \mathrm{Hom}_{\mathbb{Z}}(\boldsymbol{h}_k, \mathbb{Z}) \cong \mathcal{S}_k(\mathbb{Z}). \tag{1.3}$$

Proof. We denote by $g(z) = \sum_{n=1}^{\infty} a(n,g) q^n$ $(q = e^{2\pi i z})$ the Fourier expansion of $g(z) \in \mathcal{S}_k$ and define a pairing

$$\langle\ ,\ \rangle : \mathcal{S}_k \times \boldsymbol{h}_k \longrightarrow \mathbb{C}$$

by

$$\langle g, h \rangle := a(1, g|h), \quad (g(z) \in \mathcal{S}_k,\ h \in \boldsymbol{h}_k).$$

Now let

$$G_4(z) := 240 E_4(z) = 1 + 240 \sum_{n=1}^{\infty} \left(\sum_{0<t|n} t^3 \right) q^n,$$

$$G_6(z) := -504 E_6(z) = 1 - 504 \sum_{n=1}^{\infty} \left(\sum_{0<t|n} t^5 \right) q^n,$$

$$\Delta(z) := f_{12}(z) = q + \sum_{n=2}^{\infty} a(n, \Delta) q^n,$$

then we get a basis $\{g'_\ell(z)\}_{\ell=1}^d$ of $\mathcal{S}_k$ consisting of the form $g'_\ell(z) = G_4^{a_\ell}(z) G_6^{b_\ell}(z) \Delta^\ell(z)$, $(4a_\ell + 6b_\ell + 12\ell = k,\ a_\ell, b_\ell \geq 0)$. From the Fourier expansions of $G_4(z), G_6(z)$ and $\Delta(z)$, we see

$$g'_\ell(z) = q^\ell + \sum_{n=\ell+1}^{\infty} a(n, g'_\ell) q^n \in \mathbb{Z}[[q]], \quad (\ell = 1, 2, \ldots, d),$$

thus, by making suitable linear combinations of $\{g'_\ell(z)\}_{\ell=1}^d$ over $\mathbb{Z}$, we obtain a new basis $\{g_\ell(z)\}_{\ell=1}^d$ of $\mathcal{S}_k$ satisfying (1.1). Then we see for any $g(z) \in \mathcal{S}_k$

$$g(z) = \sum_{\ell=1}^{d} a(\ell, g) g_\ell(z).$$

In particular, we get $\mathcal{S}_k(\mathbb{Z}) = \bigoplus_{\ell=1}^{d} \mathbb{Z}\, g_\ell(z)$. Since

$$\langle g, T(n)\rangle = a(1, g|T(n)) = a(n, g), \tag{1.4}$$

we have

$$\langle g_\ell, T(m)\rangle = \delta_{\ell m} \quad \textit{for} \;\; 1 \le \ell, m \le d, \tag{1.5}$$

$$g(z) = \sum_{\ell=1}^{d} \langle g, T(\ell)\rangle g_\ell(z). \tag{1.6}$$

Now $\{T(\ell)\}_{\ell=1}^{d}$ are linearly independent over $\mathbb{C}$. In fact, if $\sum_{\ell=1}^{d} \lambda_\ell T(\ell) = 0$, then $0 = \langle g_m, 0\rangle = \langle g_m, \sum_{\ell=1}^{d} \lambda_\ell T(\ell)\rangle = \lambda_m$ by (1.5). On the other hand, we have for any $h \in \boldsymbol{h}_k$

$$h = \sum_{\ell=1}^{d} \langle g_\ell, h\rangle T(\ell). \tag{1.7}$$

In fact, since h is an endmorphism of $\mathcal{S}_k$ and $\{g_m(z)\}_{m=1}^{d}$ is a basis of $\mathcal{S}_k$, h is uniquely determined by $\{g_m(z)|h\}_{m=1}^{d}$, thus by $\{\langle g_m|h, T(\ell)\rangle\}_{1\le m,\ell\le d}$ by (1.6). So it is sufficient to show that $\langle g_m|h, T(\ell)\rangle = \langle g_m|\tilde{h}, T(\ell)\rangle$ $(1 \le m, \ell \le d)$ for $\tilde{h} = \sum_{n=1}^{d} \langle g_n, h\rangle T(n)$. By the bilinearity of the pairing $\langle\ ,\ \rangle$, we see

$$\begin{aligned}
\langle g_m|\tilde{h}, T(\ell)\rangle &= \sum_{n=1}^{d} \langle g_n, h\rangle \langle g_m|T(n), T(\ell)\rangle = \sum_{n=1}^{d} \langle g_n, h\rangle \langle g_m|T(\ell), T(n)\rangle \\
&= \langle \sum_{n=1}^{d} \langle g_m|T(\ell), T(n)\rangle g_n, h\rangle = \langle g_m|T(\ell), h\rangle \quad (\textit{by } (1.6)) \\
&= \langle g_m|h, T(\ell)\rangle.
\end{aligned}$$

Note that since $\boldsymbol{h}_k$ is commutative, we see

$$\langle g|h_1, h_2\rangle = a(1, g|h_1h_2) = a(1, g|h_2h_1) = \langle g|h_2, h_1\rangle \quad (h_1, h_2 \in \boldsymbol{h}_k).$$

In particular, we have for any $n \in \mathbb{N}$

$$T(n) = \sum_{\ell=1}^{d} \langle g_\ell, T(n)\rangle T(\ell). \tag{1.8}$$

Since we have $\langle g_\ell, T(n)\rangle = a(n, g_\ell) \in \mathbb{Z}$, we have $T(n) \in \sum_{\ell=1}^{d} \mathbb{Z}T(\ell)$. Moreover, since $T(m)T(n) = \sum_{d|(m,n)} d^{k-1} T(mn/d^2)$, we have $\boldsymbol{h}_k = \sum_{n=1}^{\infty} \mathbb{Z}T(n) = \sum_{\ell=1}^{d} \mathbb{Z}T(\ell) = \bigoplus_{\ell=1}^{d} \mathbb{Z}T(\ell)$. Now we can consider $\boldsymbol{h}_k$ as a submodule of $\mathrm{Hom}_{\mathbb{Z}}(\mathcal{S}_k(\mathbb{Z}), \mathbb{Z})$ via the pairing $\langle\, ,\, \rangle$. For $\psi \in \mathrm{Hom}_{\mathbb{Z}}(\mathcal{S}_k(\mathbb{Z}), \mathbb{Z})$, we see $\langle g_m, \sum_{\ell=1}^{d} \psi(g_\ell)T(\ell)\rangle = \psi(g_m)$ $(1 \le m, \ell \le d)$.

Since ψ is uniquely determined by $\{\psi(g_m)\}_{m=1}^d$, we get $\psi = \sum_{\ell=1}^d \psi(g_\ell)T(\ell)$. This implies $\mathrm{Hom}_{\mathbb{Z}}(\mathcal{S}_k(\mathbb{Z}), \mathbb{Z}) \cong \boldsymbol{h}_k$. By a similar argument, we have $\mathrm{Hom}_{\mathbb{Z}}(\boldsymbol{h}_k, \mathbb{Z}) \cong \mathcal{S}_k(\mathbb{Z})$. □

Now assume (H_a) for $\mathcal{S}_k$. Let $f_k(z) = \sum_{n=1}^\infty a_n e^{2\pi i n z}$ be the Fourier expansion of $f_k(z)$ and D_k the discriminant of the order $\mathbb{Z}[f_k] := \mathbb{Z}[a_1, a_2, \cdots]$ of $\mathbb{Q}(f_k)$. Then we see $\boldsymbol{h}_k \cong \mathbb{Z}[f_k]$ by $T(n) \mapsto a_n$ and $\mathrm{Tr}(T(n)) = \mathrm{Tr}_{\mathbb{Q}(f_k)/\mathbb{Q}}(a_n)$ where Tr (resp. $\mathrm{Tr}_{\mathbb{Q}(f_k)/\mathbb{Q}}$) stands for the trace of a Hecke operator as a matrix (resp. the trace of an algebraic number), thus we get

Corollary 1.6. *Under the assumption (H_a) for $\mathcal{S}_k$, we have*

$$\mathbb{Z}[f_k] = \bigoplus_{\ell=1}^{d} \mathbb{Z}\, a_\ell \quad (d = \dim_{\mathbb{C}} \mathcal{S}_k), \tag{1.9}$$

$$D_k = \det(\mathrm{Tr}_{\mathbb{Q}(f_k)/\mathbb{Q}}(a_i a_j))_{1\le i,j\le d} = \det(\mathrm{Tr}(T(i)T(j)))_{1\le i,j\le d}. \tag{1.10}$$

In particular, we can compute D_k using trace formulas of $T(n)$.

Since D_k is the discriminant of $\mathbb{Q}(f_k)$ times a square number, we can get some information of ramification primes in $\mathbb{Q}(f_k)$ from D_k. We computed D_k for $k \le 134$ and the data seem to suggest the following on ramification on primes:

Conjecture 1.7. *If an odd prime p ramifies in $\mathbb{Q}(f_k)$, then it does also in $\mathbb{Q}(f_{k+p-1})$ and $\mathbb{Q}(f_{k+p+1})$.*

The table given below is the list of D_k for $k \le 50$:

k	$[\mathbb{Q}(f_k):\mathbb{Q}]$	D_k
24	2	$2^6 \cdot 3^2 \cdot 144169$
28	2	$2^6 \cdot 3^6 \cdot 131 \cdot 139$
30	2	$2^{12} \cdot 3^2 \cdot 51349$
32	2	$2^6 \cdot 3^2 \cdot 67 \cdot 273067$
34	2	$2^8 \cdot 3^4 \cdot 479 \cdot 4919$
36	3	$2^{24} \cdot 3^6 \cdot 5^2 \cdot 7^2 \cdot 23 \cdot 1259 \cdot 269461929553$
38	2	$2^{10} \cdot 3^2 \cdot 181 \cdot 349 \cdot 1009$
40	3	$2^{20} \cdot 3^{10} \cdot 5^2 \cdot 13^2 \cdot 73 \cdot 59077 \cdot 92419245301$
42	3	$2^{22} \cdot 3^6 \cdot 5^2 \cdot 7^2 \cdot 1465869841 \cdot 578879197969$
44	3	$2^{22} \cdot 3^8 \cdot 5^2 \cdot 7^2 \cdot 37 \cdot 92013596772457847677$
46	3	$2^{31} \cdot 3^{12} \cdot 5^2 \cdot 227 \cdot 454287770269681529$
48	3	$2^{40} \cdot 3^{14} \cdot 5^6 \cdot 7^4 \cdot 31$ $\cdot 1021075361634414119924552487342394 1499439$
50	3	$2^{22} \cdot 3^{10} \cdot 5^4 \cdot 7^4 \cdot 122846286941317742619401$

In 2012, Professor Shun'ichi Yokoyama ([Y12]) kindly calculated D_k until $k \leq 500$ and checked the conjecture. The author very much appreciates his cooperation. We observe from the data that the conjecture holds for many pairs (p, k) such that p ramifies in $\mathbb{Q}(f_k)$. For some cases, the multiplicities of p in D_{k+p-1} (resp. D_{k+p+1}) are unfortunately even (but positive), thus in those cases, it is at present unknown whether p ramifies or not in $\mathbb{Q}(f_{k+p-1})$ (resp. $\mathbb{Q}(f_{k+p+1})$).

Example 1.8. The prime 131 ramifies in $\mathbb{Q}(f_{28})$ as seen in the above table. Let $p = 131, k_0 = 28$, and $k_1 = k_0 + p \pm 1,\ k_2 = k_1 + p \pm 1$ and $k_3 = k_2 + p \pm 1$. The table given below is the list of the factors of D_k whose prime factors are less than 10^3.

k		the factor of D_k whose prime factors are less than 10^3
k_0	28	$2^6 \cdot 3^6 \cdot 131 \cdot 139$
k_1	158	$2^{547} \cdot 3^{200} \cdot 5^{62} \cdot 7^{32} \cdot 11^{10} \cdot 13^{10} \cdot 17^4 \cdot 19^3 \cdot 23^4 \cdot 31^4 \cdot 37 \cdot 89 \cdot 131$
	160	$2^{600} \cdot 3^{244} \cdot 5^{70} \cdot 7^{36} \cdot 11^{12} \cdot 13^{10} \cdot 17^2 \cdot 23^6 \cdot 53^8 \cdot 71 \cdot 131 \cdot 139$
k_2	288	$2^{2159} \cdot 3^{800} \cdot 5^{258} \cdot 7^{130} \cdot 11^{46} \cdot 13^{36} \cdot 17^{34} \cdot 19^{18} \cdot 23 \cdot 29^{14} \cdot 31 \cdot 37$ $\cdot 41^{20} \cdot 89 \cdot 103 \cdot 131 \cdot 191^6 \cdot 229^2 \cdot 617$
	290	$2^{2019} \cdot 3^{752} \cdot 5^{245} \cdot 7^{128} \cdot 11^{42} \cdot 13^{34} \cdot 17^{38} \cdot 19^{15} \cdot 23^3 \cdot 29^{18} \cdot 31 \cdot 37$ $\cdot 41^{12} \cdot 83 \cdot 89 \cdot 131 \cdot 179 \cdot 271$
	292	$2^{2195} \cdot 3^{844} \cdot 5^{258} \cdot 7^{134} \cdot 11^{44} \cdot 13^{34} \cdot 17^{36} \cdot 19^{14} \cdot 23^7 \cdot 29^{18} \cdot 31 \cdot 37^7$ $\cdot 41^6 \cdot 73^{12} \cdot 83 \cdot 89 \cdot 97^{16} \cdot 131$
k_3	418	$2^{4481} \cdot 3^{1708} \cdot 5^{551} \cdot 7^{270} \cdot 11^{96} \cdot 13^{76} \cdot 17^{38} \cdot 19^{34} \cdot 23^{26} \cdot 29^4 \cdot 31 \cdot 37$ $\cdot 41^6 \cdot 47^6 \cdot 59^8 \cdot 67 \cdot 83^{12} \cdot 131^2 \cdot 139^{24} \cdot 167^5 \cdot 173$
	420	$2^{4748} \cdot 3^{1744} \cdot 5^{571} \cdot 7^{282} \cdot 11^{102} \cdot 13^{74} \cdot 17^{42} \cdot 19^{36} \cdot 23^{24} \cdot 31 \cdot 37 \cdot 47^{14}$ $\cdot 53^8 \cdot 89 \cdot 113 \cdot 131 \cdot 139 \cdot 167^5 \cdot 173$
	422	$2^{4547} \cdot 3^{1676} \cdot 5^{553} \cdot 7^{274} \cdot 11^{94} \cdot 13^{74} \cdot 17^{42} \cdot 19^{34} \cdot 23^{20} \cdot 31 \cdot 37 \cdot 47^{22}$ $\cdot 53^{16} \cdot 59 \cdot 89 \cdot 113 \cdot 131 \cdot 139 \cdot 173 \cdot 257 \cdot 347 \cdot 401 \cdot 571$
	424	$2^{4685} \cdot 3^{1802} \cdot 5^{569} \cdot 7^{286} \cdot 11^{100} \cdot 13^{76} \cdot 17^{46} \cdot 19^{37} \cdot 23^{21} \cdot 29^4 \cdot 31^5 \cdot 37$ $\cdot 43^6 \cdot 47^{30} \cdot 53^{26} \cdot 59^2 \cdot 61^{10} \cdot 71^{10} \cdot 89 \cdot 113 \cdot 131 \cdot 157 \cdot 523 \cdot 661$

Thus 131 ramifies in $\mathbb{Q}(f_{158})$, $\mathbb{Q}(f_{160})$, $\mathbb{Q}(f_{288})$, $\mathbb{Q}(f_{290})$, $\mathbb{Q}(f_{292})$, $\mathbb{Q}(f_{420})$, $\mathbb{Q}(f_{422})$ and $\mathbb{Q}(f_{424})$. But the ramification in $\mathbb{Q}(f_{418})$ is unknown.

We here note a short history we obtained Conjectures 1.1 and 1.7. In about 1979, Professor Koji Doi hoped $\mathcal{S}_k$ is splitting for some k, so the author computed $\varphi_2(x)$ for $\mathcal{S}_k$ with $\dim_{\mathbb{C}} \mathcal{S}_k \leq 12$. But they were all irreducible against Doi's hope, and then Doi and the author have come to expect (H_a) holds for all $\mathcal{S}_k$. Under this assumption, Doi, Hida and Maeda [DHM84] obtaind an interesting result which suggests the existance of relations between infinitely many Hecke fields and the fields of division points of elliptic curves defined over $\mathbb{Q}$ (see also the comment after Theorem 3.1). Then in 1996, Professor Haruzo Hida told the author about the results by Lee and Hung [LH95] and Buzzard [B96], so the author again computed more cases for $k \leq 460$ and observed (H_b) held. So Hida recommended the author to publish these results as a conjecture. When Hida gave a lecture at the symposium at Johns Hopkins University in 1997 and mentioned Conjecture 1.1, someone, perhaps Professor Buzzard, asked Hida whether the $\varphi_n(x)$ are irreducible not only for $n = 2$ but also for all $n \geq 3$. Hida repeated the question to the author. Since the author had no examples of $\varphi_n(x)$ for $n \geq 3$, he answered he did not know about that, then the questioner said "This (Conjecture 2.1 below) is my conjecture!". As for Conjecture 1.7, the author obtained it in 1997 and talked about it at Mathematical seminar of Muroran Institute of Technology in Japan on Feb. 23, 2000.

§ 2. A stronger conjecture and related results

The following conjecture also seems to be called Maeda's conjecture. But it is probably done by Buzzard, not by Maeda as mentioned above.

Conjecture 2.1 (Buzzard). *In any $\mathcal{S}_k$, $\Phi(n)$ holds for any n.*

There are many results on the following question:

Question 2. *If $\Phi(\ell)$ holds for some $\ell \geq 2$, then so does $\Phi(n)$ for any $n \neq \ell$?*

In the following, we enumerate the results:

Theorem 2.2 ([CFW00], Theorem 1). *If $\Phi(\ell)$ holds for some $\ell \geq 2$, then so does $\Phi(p)$ for any prime p such that*

$$p \not\equiv \pm 1 \mod 5 \text{ or } p \not\equiv \pm 1 \mod 7.$$

This is generalized as follows:

Theorem 2.3 ([A08], Corollary 1.6, Corollary 1.7). *If $\Phi(\ell)$ holds for some ℓ, then so does $\Phi(n)$ for n such that*

$$n(n^2-1)\sigma_1(n) \not\equiv 0 \mod 5$$

or

$$\begin{cases} n^2\sigma_1(n) - n\sigma_3(n) \not\equiv 0 \mod 7, & \text{if } k \equiv 0,\ 2 \mod 6, \\ n\sigma_1(n) - n^3\sigma_3(n) \not\equiv 0 \mod 7, & \text{if } k \equiv 4 \mod 6. \end{cases}$$

Here $\sigma_\ell(n) = \sum_{0<d|n} d^\ell$.

Theorem 2.4 ([BM03], Theorem 1.2). *If $\Phi(p)$ holds for some prime p, then so does $\Phi(n)$ for $n \leq \dim_{\mathbb{C}} \mathcal{S}_k$.*

Theorem 2.5 ([A08], Theorem 1.5). *If $\Phi(\ell)$ holds for some ℓ, then so does $\Phi(n)$ for $n \leq 10000$ and $\Phi(p)$ for a prime $p < 4000000$.*

Theorem 2.6 ([GM12], Theorem 1.5). *In $\mathcal{S}_k$ for $k \leq 14000$, $\Phi(n)$ holds for $n \leq 10000$ and so does $\Phi(p)$ for a prime $p < 4000000$ or*

$$p \not\equiv \pm 1 \mod 5 \text{ or } p \not\equiv \pm 1 \mod 7.$$

There are some results on the density of primes p for which $\Phi(p)$ hold.

Theorem 2.7 ([CFW00], the comment after Theorem 1). *If $\Phi(n)$ holds for some $n \geq 2$, then the density of primes p for which $\Phi(p)$ hold is no less than $\frac{5}{6}$.*

Theorem 2.8 ([JO98], Theorem 1). *If there are distinct primes q and ℓ such that $\varphi_q(x) \mod \ell$ is irreducible, then*

$$\#\{p < X \ (p : \textit{prime}) \mid \varphi_p(x) \textit{ is irreducible}\} \gg \frac{X}{\log X}.$$

Theorem 2.9 ([BM03], Theorem 1.1). *If $\varphi_q(x)$ is irreducible for some prime q, then there exists $\delta > 0$ such that*

$$\#\{p \leq X \ (p : \textit{prime}) \mid \varphi_p(x) \textit{ is reducible}\} \ll \frac{X}{(\log X)^{1+\delta}}.$$

§ 3. Some consequences from Maeda's conjecture

In this section, we enumerate applications of Conjecture 1.1 or (H_a).

Let $M_k(N)$ (resp. $S_k(N)$) be the space of modular forms (resp. cusp forms) on the modular group $\Gamma_0(N)$ of weight k. Here

$$\Gamma_0(N) := \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}) \;\middle|\; c \equiv 0 \mod N \right\}.$$

For $f(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i n z} \in S_k(N)$ and $g(z) = \sum_{n=0}^{\infty} b_n e^{2\pi i n z} \in M_\ell(N)$, we put

$$L(s, f) := \sum_{n=1}^{\infty} \frac{a_n}{n^s},$$
$$D(s, f, g) := \sum_{n=1}^{\infty} \frac{a_n b_n}{n^s},$$

and we define the normalized Petersson inner product by

$$\langle f,g\rangle := (\frac{\pi}{3}[SL_2(\mathbb{Z}):\Gamma_0(N)])^{-1}\int_{\mathfrak{H}/\Gamma_0(N)} \overline{f(z)}g(z)y^{k-2}dxdy, \quad (z=x+yi),$$
$$\mathfrak{H} := \{z\in\mathbb{C} \mid \mathrm{Im}(z)>0\}.$$

Note that $\langle f,g\rangle$ is independent of the choice of a level N of $f(z)$ and $g(z)$ such that $f(z)\in S_k(N)$ and $g(z)\in M_\ell(N)$.

In the following, let $f_k(z)\in\mathcal{S}_k$ be a normalized Hecke eigenform and $\varphi_n(x)$ the characteristic polynomial of the Hecke operator $T(n)$ on $\mathcal{S}_k$ as in §1.

1. **[Hecke's fields and the fields of division points of elliptic curves]**
For $h(z)\in S_k(N)$, we put

$$\Phi(X;h) := \prod_{\gamma\in\Gamma_0(N)\backslash SL_2(\mathbb{Z})} (X - h|_k\gamma),$$
$$\mathrm{Tr}(h) := \sum_{\gamma\in\Gamma_0(N)\backslash SL_2(\mathbb{Z})} h|_k\gamma, \tag{3.1}$$

where

$$(h|_k\gamma)(z) := h(\frac{az+b}{cz+d})(cz+d)^{-k} \quad (\gamma = \begin{bmatrix} a\ b \\ c\ d\end{bmatrix}\in SL_2(\mathbb{Z})).$$

Let $s_m(h)$ be the m-th elementary symmetric polynomial of $\{h|_k\gamma\}_{\gamma\in\Gamma_0(N)\backslash SL_2(\mathbb{Z})}$, then we have $s_m(h)\in\mathcal{S}_{km}$,

$$\Phi(X;h) = X^d + \sum_{m=1}^{d}(-1)^m s_m(h)X^{d-m}, \quad (d=[SL_2(\mathbb{Z}):\Gamma_0(N)]),$$

and $\mathrm{Tr}(h)\in\mathcal{S}_k$. The equation $\Phi(X;h)=0$ is called *the transformation equation.* It is well known that $f(z)\in\mathcal{S}_k$ is written as

$$f(z) = \sum_{k=4m+6n,\ m,n\in\mathbb{Z}} c_{m,n}E_4(z)^m E_6(z)^n, \quad (c_{m,n}\in\mathbb{C}).$$

Here

$$E_\ell(z) := \frac{\zeta(1-\ell)}{2} + \sum_{n=1}^{\infty}\sigma_{\ell-1}(n)e^{2\pi inz}, \tag{3.2}$$

where $\zeta(s)$ is the Riemann zeta function. Then for an elliptic curve $\mathcal{E}$ over $\mathbb{Q}$ defined by

$$\mathcal{E}: y^2 = 4x^3 - \tilde{g}_2 x - \tilde{g}_3, \quad (\tilde{g}_2,\tilde{g}_3\in\mathbb{Q}),$$

we define the specialization of $f(z)$ and $\Phi(X;h)$ at $\mathcal{E}$ by

$$f(\mathcal{E}) := \sum_{k=4m+6n,\ m,n\in\mathbb{Z}} c_{m,n}\tilde{g}_2^m\tilde{g}_3^n,$$

$$\Phi(X;h,\mathcal{E}) := X^d + \sum_{m=1}^{d}(-1)^m s_m(h)(\mathcal{E})X^{d-m}.$$

Note that under the uniformization

$$\mathcal{E} \cong \mathbb{C}/(\mathbb{Z}\omega_1+\mathbb{Z}\omega_2), \quad (\mathcal{E}\ni(\wp(z),\wp'(z))\leftrightarrow z\in\mathbb{C}/(\mathbb{Z}\omega_1+\mathbb{Z}\omega_2)),$$

$$\wp(z) := \frac{1}{z^2} + \sum_{0\neq\omega\in\mathbb{Z}\omega_1+\mathbb{Z}\omega_2}\left(\frac{1}{(z-\omega)^2}-\frac{1}{\omega^2}\right), \quad (\mathrm{Im}(\omega_1/\omega_2)>0),$$

we have

$$f(\mathcal{E}) = (2\pi/\omega_2)^k f(\omega_1/\omega_2),$$

$$\Phi(X;h,\mathcal{E}) = X^d + \sum_{m=1}^{d}(-1)^m(2\pi/\omega_2)^{km}s_m(h)(\omega_1/\omega_2)X^{d-m}.$$

Theorem 3.1 ([DHM84], Theorem, Corollary)**.** *Let $g(z)\in S_\ell(N)$ and $\lambda\geq 4$ an even integer. We put $k:=\ell+\lambda$.*

(a) *For any integer $\mu\geq 1$, we have*

$$\mathrm{Tr}((gE^*_{\lambda,N})^\mu)(z) = 3\cdot 4^{-(k\mu-1)}\Gamma(k\mu-1) \times \sum_{f\in\mathcal{P}(k\mu)}\frac{D(k\mu-1,f,g^\mu(E^*_{\lambda,N})^{\mu-1})}{\pi^{k\mu}\langle f,f\rangle}f(z).$$

Here $\mathcal{P}(m)$ is the set of normalized Hecke eigenforms in $\mathcal{S}_m$ and

$$E^*_{\lambda,N}(z) := \sum_{\gamma\in\Gamma_\infty\backslash\Gamma_0(N)}(cz+d)^{-\lambda}\in M_\lambda(N),$$

$$\Gamma_\infty = \left\{\begin{bmatrix} * & * \\ 0 & * \end{bmatrix}\in SL_2(\mathbb{Z})\right\}.$$

(b) *Assume that (H_a) holds for any $\mathcal{S}_k$. If all Fourier coefficients of $g(z)$ are rational and $\Phi(X;gE^*_{\lambda,N},\mathcal{E})$ $(\in\mathbb{Q}[X])$ is irreducible over $\mathbb{Q}$, then we have for $f_{k\mu}\in\mathcal{P}(k\mu)$:*

(i) *[Sh76, Theorem 3]* $\dfrac{D(k\mu-1,f_{k\mu},g^\mu(E^*_{\lambda,N})^{\mu-1})}{\pi^{k\mu}\langle f_{k\mu},f_{k\mu}\rangle}\in\mathbb{Q}(f_{k\mu})$;

(ii) $f_{k\mu}(\mathcal{E})\in\mathbb{Q}(f_{k\mu})$;

(iii) $(gE^*_{\lambda,N})(\mathcal{E})$ *is a root of* $\Phi(X; gE^*_{\lambda,N}, \mathcal{E}) = 0$ *and an algebraic number. Moreover*

$$\begin{aligned}\mathrm{Tr}_{K_N/\mathbb{Q}}\left(\{(gE^*_{\lambda,N})(\mathcal{E})\}^{\mu}\right) = \ & 3\cdot 4^{-(k\mu-1)}\Gamma(k\mu-1)\\ & \times \mathrm{Tr}_{\mathbb{Q}(f_{k\mu})/\mathbb{Q}}\left(\frac{D(k\mu-1, f_{k\mu}, g^{\mu}(E^*_{\lambda,N})^{\mu-1})}{\pi^{k\mu}\langle f_{k\mu}, f_{k\mu}\rangle}\cdot f_{k\mu}(\mathcal{E})\right),\end{aligned}$$

where $K_N = \mathbb{Q}((gE^*_{\lambda,N})(\mathcal{E}))$.

Since we see

$$\begin{aligned}K_N =&\mathbb{Q}(j(\omega_1/\omega_2),\ j(N\omega_1/\omega_2))\\ &\subset \mathbb{Q}\left(\wp(\frac{a\omega_1+b\omega_2}{N}), \wp'(\frac{a\omega_1+b\omega_2}{N}) \ \middle|\ a, b \in \mathbb{Z}\right),\end{aligned}$$

K_N is a subfield of the field of N-division points of $\mathcal{E}$. Here $j(z)$ stands for the invariant function of elliptic curves. Thus Theorem 3.1(b) suggests that there are some relations between the field of N-division points of $\mathcal{E}$ and infinitely many Hecke fields $\{\mathbb{Q}(f_{k\mu}) \mid \mu = 1, 2, 3, \ldots\}$:

Question 3. *What relations are there between the field of N-division points of $\mathcal{E}$ and infinitely many Hecke fields $\{\mathbb{Q}(f_k) \mid k \in \mathbb{N}\}$?*

Example 3.2. Let $g(z) \in S_4(5)$ be a normalized Hecke eigenform. Since $\dim S_4(5) = 1$, $g(z)$ is uniquely determind and the Fourier coefficients are rational. Put simply $\Phi(X) := \Phi(X; gE^*_{4,5}, \mathcal{E})$. Then we have:

(a) $\mathcal{E} : y^2 = 4x^3 - 4x + 1$

$$\begin{aligned}\Phi(X) = X^6 &- 44400X^4 - 1971360X^3 + 488897280X^2\\ &+ 47063460096X + 1162360730560.\end{aligned}$$

(b) $\mathcal{E} : y^2 = 4x^3 - \frac{40}{3}x + \frac{251}{27}$

$$\begin{aligned}\Phi(X) = X^6 &- 148000X^4 - 1971360X^3 + 5432192000X^2\\ &+ 1029841968640X + 14284097373120.\end{aligned}$$

In §5, we will give the proof of Theorem 3.1(a). Theorem 3.1(b) is obtained by specializing the equation in Theorem 3.1(a) at elliptic curves under (H_a) .

2. **[Non-vanishing of L-functions]**
It is well known that the functional equation holds:

$$(2\pi)^{-s}\Gamma(s)L(s,f_k) = (-1)^{k/2}(2\pi)^{-k+s}\Gamma(k-s)L(k-s,f_k).$$

In paticular, if $k \equiv 2 \mod 4$, then

$$L(k/2, f_k) = 0.$$

For $k \equiv 0 \mod 4$, the following theorem holds under (H_a):

Theorem 3.3 ([CF99],Theorem 1)**.** *Suppose $k \equiv 0 \mod 4$. If (H_a) holds for $\mathcal{S}_k$, then*

$$L(k/2, f_k) \neq 0.$$

In §5, we will give the proof of Theorem 3.3.

3. **[Inverse Galois problem]**
For a positive integer n, let $\mathcal{P}_S(n)$ (resp. $\mathcal{P}_G(n)$) be the set of primes p such that there is a number field K with Galois group $\mathrm{Gal}(K/\mathbb{Q})$ isomorphic to $PSL_2(\mathbb{F}_{p^n})$ (resp. $PGL_2(\mathbb{F}_{p^n})$) in which only p ramifies.

Theorem 3.4 ([W12], Theorem 1.1)**.** *If Conjecture 1.1 holds, then the following hold:*

(1) *For any even integer $n \geq 2$, the density of $\mathcal{P}_S(n)$ is 1.*
(2) *For any odd integer $n \geq 1$, the density of $\mathcal{P}_G(n)$ is 1.*

4. **[Divisibility of $f_k(z)$ by another eigenform]**

Theorem 3.5 ([BJX11], Theorems 1.3, 1.4, Lemmas 2.5, 3.1, Proposition 6.1)**.** *Assume that $\varphi_n(x)$ in $\mathcal{S}_k$ is irreducible for some n.*

(a) *$f_k(z) = f_\ell(z)g(z)$ with some normalized Hecke eigenform $f_\ell(z) \in \mathcal{S}_\ell$ $(\ell < k)$ and a modular form $g(z)$ if and only if $\dim_{\mathbb{C}}\mathcal{S}_\ell = 1$ and $k - \ell \geq 12$ satisfies that*

$$k-\ell \mod 12 = \begin{cases} 0,\ 2,\ 4,\ 6,\ 8,\ 10, & (\ell = 12), \\ 0,\ 4,\ 6,\ 10, & (\ell = 16), \\ 0,\ 4,\ 8, & (\ell = 18), \\ 0,\ 6, & (\ell = 20), \\ 0,\ 4, & (\ell = 22), \\ 0, & (\ell = 26). \end{cases}$$

(*b*) *$f_k(z) = E_\ell(z)g(z)$ with the Eisenstein series $E_\ell(z)$ of weight ℓ ($\ell < k$) defined by (3.2) and a modular form $g(z)$ if and only if* $\dim_{\mathbb{C}} M_\ell(1) = 1$ *and $k-\ell$ satisfies that*

$$k-\ell \mod 12 = \begin{cases} 0,\ 4,\ 6,\ 10, & (\ell=4), \\ 0,\ 4,\ 8, & (\ell=6), \\ 0,\ 6, & (\ell=8), \\ 0,\ 4, & (\ell=10), \\ 0, & (\ell=14). \end{cases}$$

§ 4. A generalization to higher levels

P. Tsaknias investigated the decompositions of the spaces of cusp forms of higher levels and made a conjecture which is a generalization of (H_a). In this section, we will explain his research.

Let $S_k^0(N)$ be the subspace of newforms of $S_k(N)$ and $S_k^0(N;\overline{\mathbb{Q}})$ the subspace over the algebraic closure $\overline{\mathbb{Q}}$ consisting of elements whose Fourier coefficients are algebraic. Then the absolute Galois group $G := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on $S_k^0(N;\overline{\mathbb{Q}})$ by

$$\left(\sum_{n=1}^{\infty} a_n e^{2\pi i n z}\right)^{\sigma} = \sum_{n=1}^{\infty} a_n^{\sigma} e^{2\pi i n z} \quad (\sigma \in G).$$

We call a normalized Hecke eigenform $h(z) \in S_k^0(N)$ a *primitive form* of level N. A primitive form $h(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i n z} \in S_k^0(N)$ is contained in $S_k^0(N;\overline{\mathbb{Q}})$ and $h^\sigma(z)$ is also a primitive form of level N. We call $h^\sigma(z)$ a *conjugate* of $h(z)$ and the field $\mathbb{Q}(h) := \mathbb{Q}(a_1, a_2, \cdots)$ *Hecke's field* of $h(z)$. Since $S_k^0(N)$ has a basis consisting of primitive forms, $S_k^0(N;\overline{\mathbb{Q}})$ is decomposed as a direct sum of $\overline{\mathbb{Q}}$-subspaces spanned by G-orbits $\{h^\sigma(z)\}_{\sigma\in G}$ for primitive forms $h(z)$ of level N.

Moreover for an imaginary quadratic field K with discriminant $-D$ ($D > 0$) and a primitive Hecke character λ mod $\mathfrak{m}$ such that

$$\begin{aligned} \lambda((\alpha)) &= \alpha^u && (\alpha \equiv 1 \bmod^\times \mathfrak{m},\ \alpha \in K,\ u \in \mathbb{N}\,(u>0)), \\ \lambda((a)) &= \left(\tfrac{-D}{a}\right) a^u && (a \in \mathbb{Z},\ (a, DN(\mathfrak{m})) = 1), \end{aligned}$$

we put

$$f_\lambda(z) = \sum_{\mathfrak{a}} \lambda(\mathfrak{a}) e^{2\pi i N(\mathfrak{a}) z}.$$

Here $\mathfrak{m}$ is a non-zero integral ideal of K, $\bmod^\times$ stands for the multiplicative congruence, $\mathfrak{a}$ runs over all non-zero integral ideals in K, and $N(\mathfrak{a})$ is the norm of $\mathfrak{a}$. Then it is known that $f_\lambda(z)$ belongs to $S^0_{u+1}(DN(\mathfrak{m});\overline{\mathbb{Q}})$ and is a primitive form (cf. [Sh71], Lemma 3 or [Mi89], Theorem 4.8.2). We call such a primitive form $f_\lambda(z)$ a *CM form with complex multiplication field* K *of type* $(\mathfrak{m}, u)$. Since $f^\sigma_\lambda(z) = f_{\lambda^\sigma}(z)$ $(\sigma \in G)$ where

$$\lambda^\sigma(\mathfrak{a}) = \lambda(\mathfrak{a}^{\sigma^{-1}})^\sigma,$$

the conjugate $f^\sigma_\lambda(z)$ is also a CM form in $S^0_{u+1}(DN(\mathfrak{m});\overline{\mathbb{Q}})$ with complex multiplication field K of type $(\mathfrak{m}^\sigma, u)$. Therefore both the subset consisting of CM forms and the subset consisting of non-CM forms in $S^0_k(N)$ are closed under the action of G, and thus we can consider the G-orbits of CM forms and non-CM forms. We denote by $CM(N,k)$ (resp. $NCM(N,k)$) the number of distinct G-orbits of CM forms (resp. non-CM forms) of level N and weight k.

Now by William Stein's indication that $\{CM(N,k)\}_{k=2}^\infty$ are periodic with respect to k (see [T12], §4), P. Tsaknias focused his research on non-CM forms and computed many $NCM(N,k)$ and he and L. Dieulefait made the following conjecture which is regarded as a generalization of (H_a).

Conjecture 4.1 (Tsaknias [T12], §2, Tsaknias-Dieulefait [DT12]).

(1) *For large k, $NCM(N,k)$ is a constant $\nu(N)$.*

(2) *$\nu(N)$ is multiplicative, namely*

$$\textit{if } (N,M) = 1 \textit{ then } \nu(NM) = \nu(N)\nu(M).$$

(3) *$\nu(p) = 2$ for any prime p.*

(4) *Let $n \geq 2$ be an integer.*

  (a) *For an odd prime p:*

$$\nu(p^n) = \begin{cases} \sigma_0(p-1) + \sigma_0(p+1) - 1, & n = 2, \\ \sigma_0(p-1) + \sigma_0(p+1), & n \geq 4 : \textit{even}, \\ 4, & p > 3 \textit{ and } n : \textit{odd}, \textit{ or } n = 3, \\ 8, & p = 3 \textit{ and } n \geq 5 : \textit{odd}. \end{cases}$$

  (b) *For $p = 2$:*

$$\nu(2^n) = \begin{cases} 2, & n = 3, \\ 6, & n = 4, \\ 4, & n = 5, \\ 16, & n = 6, \\ 8, & n \geq 7 : \textit{odd}, \\ 12, & n \geq 8 : \textit{even}. \end{cases}$$

Tsaknias and L. Dieulefait have examined the Galois groups of the Galois closures of Hecke's fields too. In higher levels, the Galois groups seem to be better understood if they are considered over cyclotomic subfields included in the Hecke fields; then they seem to be isomorphic to symmetric groups of degrees of the Hecke fields over the cyclotomic subfields. Moreover, they seem to try the cases of the spaces of cusp forms with non-trivial character and Hilbert modular cases. We hope many researchers will face these problems and throw light on the mysteries about Hecke's fields.

§ 5. The proofs of Theorems 3.1(a) and 3.3

Since Theorems 3.1(a) and 3.3 are most interesting to the author and both can shown by using $D(s,f,g)$, we give here the proofs. About the properties of $D(s,f,g)$, see [Sh76].

The proof of Theorem 3.1(a). First we will show

Theorem 5.1 ([DHM84], §4). *For $h \in S_\ell(N)$, and an even integer $\lambda \geq 4$, we have*

$$\mathrm{Tr}(hE^*_{\lambda,N})(z) = 3\cdot 4^{-(k-1)}\Gamma(k-1)\sum_{f\in\mathcal{P}(k)}\frac{D(k-1,f,h)}{\pi^k\langle f,f\rangle}f(z).$$

Here $k := \ell+\lambda$.

Proof. Since $h(z)E^*_{\lambda,N}(z)\in S_k(N)$, $\mathrm{Tr}(hE^*_{\lambda,N})\in\mathcal{S}_k(=S_k(1))$ and

$$\mathfrak{H}/\Gamma_0(N) = \bigcup_{\gamma\in\Gamma_0(N)\backslash SL_2(\mathbb{Z})}\gamma^{-1}(\mathfrak{H}/SL_2(\mathbb{Z}))$$

as fundamental domains, we have for $f(z)\in\mathcal{P}(k)$

$$\begin{aligned}\frac{\pi}{3}\langle f,\mathrm{Tr}(hE^*_{\lambda,N})\rangle &= \int_{\mathfrak{H}/SL_2(\mathbb{Z})}\overline{f(z)}\sum_{\gamma\in\Gamma_0(N)\backslash SL_2(\mathbb{Z})}(hE^*_{\lambda,N})|_k\gamma(z)y^{k-2}dxdy\\ &= \int_{\mathfrak{H}/\Gamma_0(N)}\overline{f(z)}h(z)E^*_{\lambda,N}(z)y^{k-2}dxdy \qquad (5.1)\\ &= (4\pi)^{-(k-1)}\Gamma(k-1)D(k-1,f,h),\quad ([\mathrm{Sh76},(2.3)]).\end{aligned}$$

On the other hand, we can write

$$\mathrm{Tr}(hE^*_{\lambda,N})(z) = \sum_{f\in\mathcal{P}(k)}c(f)f(z)\quad (c(f)\in\mathbb{C}).$$

Then the orthogonality between elements of $\mathcal{P}(k)$ with respect to the Petersson inner product implies

$$\langle f, \mathrm{Tr}(hE^*_{\lambda,N})\rangle = c(f)\langle f, f\rangle. \tag{5.2}$$

Therefore we have by (5.1)

$$\begin{aligned}\mathrm{Tr}(hE^*_{\lambda,N}) &= \sum_{f\in\mathcal{P}(k)} \frac{\langle f, \mathrm{Tr}(hE^*_{\lambda,N})\rangle}{\langle f, f\rangle} f(z)\\ &= 3\cdot 4^{-(k-1)}\Gamma(k-1)\sum_{f\in\mathcal{P}(k)} \frac{D(k-1,f,h)}{\pi^k\langle f, f\rangle} f(z).\end{aligned}$$

□

Theorem 3.1(a) is obtained by applying Theorem 5.1 to $h(z) = g(z)^\mu E^*_{\lambda,N}(z)^{\mu-1}$.

□

The proof of Theorem 3.3. Suppose $k \equiv 0 \mod 4$ and put

$$G_k(z) := \frac{2}{\zeta(1-k)} E_k(z).$$

Since in general we have

$$D(s, f_k, E_\ell) = \frac{L(s, f_k)L(s+1-\ell, f_k)}{\zeta(2s+2-k-\ell)}, \quad (\text{[Sh76, Lemma 1]}),$$

we see

$$D(k-1, f_k, E_{k/2}) = \frac{L(k-1, f_k)L(k/2, f_k)}{\zeta(k/2)}.$$

Since $L(k-1, f_k) \neq 0$, we have

$$\begin{aligned}L(k/2, f_k) = 0 \ &\textit{if and only if } D(k-1, f_k, E_{k/2}) = 0\\ &\textit{if and only if } D(k-1, f_k, G_{k/2}) = 0.\end{aligned}$$

On the other hand, since $E^*_{k/2,1}(z) = G_{k/2}(z)$ ([Mi89, (7.1.30)]), we have by (5.1)

$$(4\pi)^{-(k-1)}\Gamma(k-1)D(k-1, f_k, G_{k/2}) = \frac{\pi}{3}\langle f_k, G^2_{k/2}\rangle,$$

thus

$$L(k/2, f_k) = 0 \textit{ if and only if } \langle f_k, G^2_{k/2}\rangle = 0.$$

Now assume that (H_a) holds for $\mathcal{S}_k$ and take and fix an element $f_k \in \mathcal{P}(k)$, then we have

$$G^2_{k/2}(z) = G_k(z) + \sum_{\sigma\in G(f_k)} c_\sigma f^\sigma_k(z) \quad (c_\sigma \in \mathbb{C}).$$

In particular,

$$\langle f_k, G_{k/2}^2 \rangle = c_{\mathrm{id}} \langle f_k, f_k \rangle.$$

Since $G_{k/2}(z)$ and $G_k(z)$ have rational Fourier expansions, we have for any $\tau \in \mathrm{Aut}(\mathbb{C})$

$$G_{k/2}^2(z) = G_k(z) + \sum_{\sigma \in G(f_k)} c_\sigma^\tau f_k^{\sigma\tau}(z),$$

thus the uniqueness of the expression implies

$$c_\sigma^\tau = c_{\sigma\tau}.$$

In particular, $c_\sigma = c_{\mathrm{id}}^\sigma$. Thus if $c_{\mathrm{id}} = 0$, then all $c_\sigma = 0$, namely, $G_{k/2}^2(z) = G_k(z)$, which holds only for $k = 8$. Since $k \geq 12$, we get a contradiction if $L(k/2, f_k) = 0$. $\square$

References

[A08] S. Ahlgren, On the irreducibility of Hecke polynomials, Math. Comp. **77**(2008), 1725-1731.

[BM03] S. Baba and M. R. Murty, Irreducibility of Hecke polynomials, Math. Res. Lett. **10**(2003), 709-715.

[BJX11] J. Beyerl, K. James and H. Xue, Divisibility of an eigenform by an eigenform, Proc. Amer. Math. Soc. **142**(2014), 29-38.

[B96] K. Buzzard, On the eigenvalues of the Hecke operator T_2, J. Number theory **57**(1996), 130-132.

[CF99] J.B. Conrey and D.W. Farmer, Hecke operators and the nonvanishing of L-functions, in *Topics in Number Theory* (University Park, PA, 1997), Math. Appl. **467**, 143-150, Kluwer Acad. Publ., Dordrecht, 1999.

[CFW00] J. B. Conrey, D. W. Farmer and P. J. Wallace, Factoring Hecke polynomials modulo a prime, Pacific J. Math. **196**(2000), 123-130.

[DT12] L. Dieulefait and P. Tsaknias, Possible connection between Maeda and local types – short note, preprint 2013.

[DHM84] K. Doi, H. Hida and Y. Maeda, The transformation equations and the special values of Shimura's zeta functions, Hokkaido Math. J. **13**(1984), 347-361.

[FJ01] D. W. Farmer and K. James, The irreducibility of some level 1 Hecke polynomials, Math. Comp. **71**(2001), 1263-1270.

[GM12] A. Ghitza and A. McAndrew, Experimental evidence for Maeda's conjecture on modular forms, Tbil. Math. J. **5**(2012), 55-69.

[HM97] H. Hida and Y. Maeda, Non-abelian base change for totally real fields, Pacific J. Math. Special Issue(1997), Olga Taussky-Todd, 189-217.

[JO98] K. James and K. Ono, A note on the irreducibility of Hecke polynomials, J. Number Theory **73**(1998), 527-532.

[K04] S. Kleinerman, Some computations in support of Maeda's conjecture, preprint 2004 (available at: http://modular.math.washington.edu/edu/Fall2003/252/final_project).

[LH95] H.-C. Lee and W.-H. Hung, Galois groups of Hecke eigenforms, Chinese J. Math. **23**(1995), 329-342.

[L05] C.-W. Lim, Decomposition of cusp forms over Q, and variants of partial Nim, ProQuest LLC, Ann Arbor, MI, 2005. Thesis(Ph.D.)- University of California, Berkeley.

[Mi89] T. Miyake, Modular forms, Springer, 1989.

[Sh71] G. Shimura, On elliptic curves with complex multiplication as factors of the Jacobians of modular function fields, Nagoya Math. J. **43**(1971), 199-208.

[Sh76] G. Shimura, The special values of the zeta functions associated with cusp forms, Comm. Pure Appl. Math. **29**(1976), 783-804.

[T12] P. Tsaknias, A possible generalization of Maeda's conjecture, in *Computations with Modular Forms* (Proceedings of a Summer School and Conference, Heidelberg, August/September 2011), Contributions in Mathematical and Computational Sciences 6 (Springer International Publishing, Switzerland 2014), 317-329.

[W12] G. Wiese, An application of Maeda's conjecture to the inverse Galois problem, Math. Res. Lett. **20**(2013), 985-993.

[Y12] S. Yokoyama, On Hecke Algebra Discriminants; Prototype, in Tables/Codes, http://www2.math.kyushu-u.ac.jp/∼s-yokoyama.