ACTA ARITHMETICA
178.1 (2017)

On the factorization of the discriminant of a classical modular equation

by

Mitsusada Nakata (Osaka)

1. Introduction. Let $j(z)$ be the elliptic modular function. For a positive integer N, the set $C(N)$ of matrices is defined by

$$C(N) = \left\{ \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \,\middle|\, ad = N,\ a > 0,\ 0 \le b < d,\ \gcd(a,b,d) = 1 \right\}.$$

We will consider the polynomial in X given by

$$\Phi_N(X, j(z)) = \prod_{\sigma \in C(N)} (X - j(\sigma z)),$$

where $\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) z = (az+b)/d$. It is known that $\Phi_N(X, j(z))$ is the minimal polynomial of $j(Nz)$ over $\mathbb{C}(j(z))$ and a symmetric polynomial in X and $j(z)$ with integer coefficients. We call the equation $\Phi_N(X,Y) = 0$ the *classical modular equation* of level N, and the polynomial $\Phi_N(X,X)$ the *classical modular polynomial* of level N. Classical modular equations have been studied by many mathematicians. For instance, Kaltofen and Yui looked into explicit forms of modular equations (cf. [8], [3]).

In this paper, we will regard $\Phi_p(X,Y) = 0$ as an equation in terms of Y, and consider its discriminant $\operatorname{disc}_Y \Phi_p(X,Y)$ for any odd prime p.

Remark 1.1. $\operatorname{disc}_Y \Phi_p(X,Y) = \operatorname{disc}_Y \Phi_p(Y,X)$.

$\operatorname{disc}_Y \Phi_p(X,Y)$ was studied by Weber. His main result is the following.

Proposition 1.2 (Weber [7, Ch. 119]). *For an odd prime p, $\Phi_p(X,Y)$ has a multiple root if and only if $X = j(\tau_D)$, where τ_D is a root of a primitive quadratic form of negative discriminant D on the upper half-plane, D is coprime to p and there exist integers x, y satisfying $x^2 - Dy^2 = 4p^2$.*

2010 *Mathematics Subject Classification*: Primary 11F03; Secondary 12D05, 14K22.
Key words and phrases: modular equation, discriminant, class polynomial.
Received 28 May 2016; revised 4 August 2016.
Published online 30 January 2017.

DOI: 10.4064/aa8538-8-2016

By Proposition 1.2, Weber determined all roots of the discriminant of the classical modular equation of level p because $\mathrm{disc}_Y \Phi_p(j(\tau_D), Y) = 0$ if and only if $\Phi_p(j(z), Y)$ has a multiple root. We point out that he did not study the multiplicities of those roots.

Let $H_D(X)$ be the minimal polynomial of $j(\tau_D)$ over $\mathbb{Q}$. It is known that $H_D(X)$ has integer coefficients, and we call $H_D(X)$ the *class polynomial* for D. Kaltofen–Yui and Gross–Zagier studied the construction of class polynomials and their discriminants (cf. [4], [2]). It is easy to check that $H_D(X)$ divides $\mathrm{disc}_Y \Phi_p(X, Y)$ if and only if $\Phi_p(j(\tau_D), Y)$ has a multiple root. Hence Weber's result implies that

$$\mathrm{disc}_Y \Phi_p(X, Y) = \text{constant} \times \prod_{D \in S(p)} H_D(X)^{s(D,p)}, \tag{1.1}$$

where the leading coefficient is a nonzero integer, $s(D, p)$ is a positive integer and $S(p)$ is the set defined by

$$\{D \in \mathbb{Z}_{<0} \mid x^2 - Dy^2 = 4p^2,\ \exists x, y \in \mathbb{Z},\ y > 0,\ D \equiv 1, 0 \,(\mathrm{mod}\ 4),\ p \nmid D\}.$$

Remark 1.3. $-3, -4 \in S(p)$ for every odd prime p.

Our main results are the following theorems; the first one is a sharpened version of (1.1).

Theorem 1.4. *For any odd prime p,*

$$\begin{aligned}&\mathrm{disc}_Y \Phi_p(X, Y)\\ &\quad = (-1)^{(p-1)/2} p^p \Big(H_{-3}(X)^{\lceil p/3 \rceil} H_{-4}(X)^{\lceil p/4 \rceil} \prod_{\substack{D \in S(p) \\ D \neq -3,-4}} H_D(X) \Big)^2,\end{aligned}$$

where $\lceil \cdot \rceil$ is the ceiling function.

Theorem 1.5. *For any odd prime p,* $\mathrm{disc}_Y \Phi_p(X, Y)$ *and* $\Phi_{p^2}(X, X)$ *have the same degree and*

$$\begin{aligned}&\mathrm{disc}_Y \Phi_p(X, Y)\\ &\quad = (-1)^{(p+1)/2} p^{p-1} \frac{H_{-3}(X)^{2h(-3p^2)} H_{-4}(X)^{h(-4p^2)}}{H_{-3p^2}(X)^{2h(-3)} H_{-4p^2}(X)^{h(-4)}} \times \Phi_{p^2}(X, X),\end{aligned}$$

where $h(D)$ is the class number of an imaginary quadratic order of discriminant D.

This paper is organized as follows: In Section 2, we calculate $s(D, p)$ for all $D \in S(p)$, and give a proof of Theorem 1.4. In Section 3, we shall prove Theorem 1.5 by comparing the factorizations of $\mathrm{disc}_Y \Phi_p(X, Y)$ and $\Phi_{p^2}(X, X)$.

Throughout this paper, we denote by Γ the full modular group $\mathrm{SL}(2,\mathbb{Z})$, and (D/p) denotes the Legendre symbol for a discriminant D and a prime p.

2. Proof of Theorem 1.4. For τ_D such that $\Phi_p(j(\tau_D),Y)$ has multiple roots, we define a positive integer $r_{D,p}$ to be the multiplicity of the zero of $\operatorname{disc}_Y \Phi_p(X,Y)$ at $j(\tau_D)$. Then it is obvious that $r_{D,p}$ is uniquely determined independent of the choice of τ_D, and it equals $s(D,p)$. Thus it is sufficient to calculate $r_{D,p}$ for

$$\tau_D = \begin{cases} \sqrt{D}/2 & \text{if } D \equiv 0 \pmod 4, \\ (-1+\sqrt{D})/2 & \text{if } D \equiv 1 \pmod 4, \end{cases} \tag{2.1}$$

and we suppose (2.1) from now on.

Since $C(p) = \left\{\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)\right\} \cup \left\{\left(\begin{smallmatrix} 1 & b \\ 0 & p \end{smallmatrix}\right) \,\middle|\, 0 \le b < p\right\}$ by the definition of $C(N)$, we let $\sigma_p = \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)$ and $\sigma_k = \left(\begin{smallmatrix} 1 & k \\ 0 & p \end{smallmatrix}\right)$ for $0 \le k < p$. Then the discriminant of $\Phi_p(j(z),Y)$ as a polynomial in Y can be written

$$\operatorname{disc}_Y \Phi_p(j(z),Y) = \prod_{0 \le i < j \le p} \big(j(\sigma_j z) - j(\sigma_i z)\big)^2.$$

The first step to calculate $r_{D,p}$ $(= s(D,p))$ is to determine all factors $j(\sigma_j z) - j(\sigma_i z)$ that vanish at a point τ_D. For this, Weber also gave the following answer.

Proposition 2.1 (Weber [6, Ch. 91]). *Let p be an odd prime and $D \in S(p)$. Then the following equalities hold, and $j(\sigma_j z) \ne j(\sigma_i z)$ in all other cases.*

(1) *If $D = -3$ and $p = 3$, then*

- $j(\sigma_3\tau_D) = j(\sigma_0\tau_D) = j(\sigma_1\tau_D)$.

(2) *If $D = -3$ and $p \ne 3$, then*

- $j(\sigma_p\tau_D) = j(\sigma_0\tau_D) = j(\sigma_1\tau_D)$,
- $j(\sigma_k\tau_D) = j(\sigma_{k'}\tau_D) = j(\sigma_{k''}\tau_D)$ *whenever* $k' \equiv \frac{1}{1-k}$, $k'' \equiv \frac{1-k}{-k} \pmod p$,
- $j(\sigma_k\tau_D) = j(\sigma_{k'}\tau_D)$ *whenever k, k' are solutions of* $(2x-1)^2 \equiv -3 \pmod p$.

(3) *If $D = -4$, then*

- $j(\sigma_p\tau_D) = j(\sigma_0\tau_D)$,
- $j(\sigma_k\tau_D) = j(\sigma_{k'}\tau_D)$ *whenever* $kk' \equiv -1 \pmod p$,
- $j(\sigma_k\tau_D) = j(\sigma_{k'}\tau_D)$ *whenever k, k' are solutions of* $x^2 \equiv -1 \pmod p$.

(4) *If* $D \in S(p) \setminus \{-4, -3\}$ *and* $D \equiv 0 \pmod 4$, *then*

- $j(\sigma_k \tau_D) = j(\sigma_{k'} \tau_D)$ *whenever* k, k' *are solutions of* $x^2 - D/4 \equiv 0 \pmod p$.

(5) *If* $D \in S(p) \setminus \{-4, -3\}$ *and* $D \equiv 1 \pmod 4$, *then*

- $j(\sigma_k \tau_D) = j(\sigma_{k'} \tau_D)$ *whenever* k, k' *are solutions of*
$$x^2 - x + (1 + D)/4 \equiv 0 \pmod p.$$

The next step is to calculate the multiplicity of the zero of $j(\sigma_j z) - j(\sigma_i z)$ at τ_D. We denote by $\mathrm{ord}_\tau(f)$ the multiplicity of the zero of a function f at a point τ.

Proposition 2.2. *Let* p *be an odd prime and* $D \in S(p)$. *Suppose that* $j(\sigma_k \tau_D) - j(\sigma_{k'} \tau_D) = 0$ *for* $k \neq k'$. *Then*

$$\mathrm{ord}_{\tau_D}(j(\sigma_k z) - j(\sigma_{k'} z)) = \begin{cases} 3 & \textit{if } D = -3 \textit{ and } k, k' \textit{ are solutions of } x^2 - x + 1 \equiv 0 \pmod p, \\ 2 & \textit{if } D = -4 \textit{ and } k, k' \textit{ are solutions of } x^2 + 1 \equiv 0 \pmod p, \\ 1 & \textit{otherwise.} \end{cases}$$

Proof. We will need following two lemmas.

Lemma 2.3 ([1, Section 11]). *For* τ *in the upper half-plane, we have* $j'(\tau) \neq 0$, *except in the following cases:*

- $\tau = \gamma i$, $\gamma \in \Gamma$, *where* $j'(\tau) = 0$, $j''(\tau) \neq 0$,
- $\tau = \gamma \omega$, $\gamma \in \Gamma$, *where* $j'(\tau) = 0$, $j''(\tau) = 0$, $j'''(\tau) \neq 0$,

where $i = \tau_{-4}$ *and* $\omega = \tau_{-3}$.

Lemma 2.4. *Let* p *be an odd prime and* $D \in S(p)$. *Then*

$$\sigma_k \tau_D \overset{\Gamma}{\sim} \omega \;\Leftrightarrow\; \tau_D = \omega \textit{ and } k^2 - k + 1 \equiv 0 \pmod p,$$
$$\sigma_k \tau_D \overset{\Gamma}{\sim} i \;\Leftrightarrow\; \tau_D = i \textit{ and } k^2 + 1 \equiv 0 \pmod p,$$

where $\overset{\Gamma}{\sim}$ *means lying in the same orbit of the action of* Γ.

Proof. First it is easily seen that if $\sigma_k \tau_D \overset{\Gamma}{\sim} \omega$, then $\tau_D = \omega$ and $k \neq p$. Hence we suppose that $\sigma_k \omega = \gamma \omega$ for some $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$. This implies $\mathfrak{p} = [p, \omega + k]$ is an ideal of an imaginary quadratic field $K = \mathbb{Q}(\omega)$. Furthermore we see that $\mathcal{O}_K \supsetneq \mathfrak{p} \supsetneq p\mathcal{O}_K$, where $\mathcal{O}_K$ is the ring of integers in K. Hence k satisfies $k^2 - k + 1 = 0 \pmod p$ because

$$p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}} = [p, \omega + k][p, \bar{\omega} + k] = [p^2, p(k - 1 - \omega), p(k + \omega), k^2 - k - 1].$$

Conversely, if $\tau_D = \omega$ and k satisfies $k^2 - k + 1 = 0 \pmod p$, then $\mathfrak{p} = p\mathcal{O}_K + (\omega + k)\mathcal{O}_K = [p, \omega + k]$ is the prime ideal of K such that $p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$ (see [1, Section 5]). Since the class number of K equals one, we see that

$\mathfrak{p}$ and $\mathcal{O}_K$ belong to the same class in the ideal class group $Cl(\mathcal{O}_K)$. This implies $\sigma_k\tau_D \overset{\Gamma}{\sim} \omega$. By a similar argument the second assertion is proved. ■

First we prove the assertion of Proposition 2.2 when $D = -3$ and k, k' are solutions of $x^2 - x + 1 \equiv 0 \pmod{p}$. Then we can take $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, $\gamma' = \left(\begin{smallmatrix} a' & b' \\ c' & d' \end{smallmatrix}\right) \in \Gamma$ such that $\sigma_k\omega = \gamma\omega$, $\sigma_{k'}\omega = \gamma'\sigma_k\omega$ by Lemma 2.4 and the assumption. This implies

$$\begin{gathered} j'(\sigma_k\omega) = 0, \quad j''(\sigma_k\omega) = 0, \quad j'''(\sigma_k\omega) \neq 0, \\ j'(\sigma_{k'}\omega) = 0, \quad j''(\sigma_{k'}\omega) = 0, \quad j'''(\sigma_{k'}\omega) \neq 0, \end{gathered}$$

by Lemma 2.3. Moreover since the third derivative of $j(\gamma z)$ is

$$j'''(\gamma z) = (cz+d)^6 j'''(z) + 6c(cz+d)^5 j''(z) + 6c^2(cz+d)^4 j'(z),$$

we see that $j'''(\sigma_{k'}\omega) = j'''(\gamma'\sigma_k\omega) = (c'\sigma_k\omega + d')^6 j'''(\sigma_k\omega)$. Thus it is sufficient to show that $1 \neq (c'\sigma_k\omega + d')^6$ because

$$\begin{aligned} \lim_{z\to\omega} \frac{j(\sigma_k z) - j(\sigma_{k'} z)}{(z-\omega)^3} &= \lim_{z\to\omega} \left\{ \frac{j(\sigma_k z) - j(\sigma_k\omega)}{(z-\omega)^3} - \frac{j(\sigma_{k'} z) - j(\sigma_{k'}\omega)}{(z-\omega)^3} \right\} \\ &= \frac{j'''(\sigma_k\omega)}{6p^3} - \frac{j'''(\sigma_{k'}\omega)}{6p^3} \\ &= \{1 - (c'\sigma_k\omega + d')^6\} \frac{j'''(\sigma_k\omega)}{6p^3}. \end{aligned}$$

If $1 = (c'\sigma_k\omega + d')^6$, it is easy to check that γ' is one of

$$\begin{pmatrix} \pm1 & r \\ 0 & \pm1 \end{pmatrix}, \quad \begin{pmatrix} s & t \\ \pm p & \mp k \end{pmatrix}, \quad \begin{pmatrix} u & v \\ \pm p & \mp(1-k) \end{pmatrix}.$$

The first case implies $\sigma_{k'}\omega = \gamma'\sigma_k\omega = \sigma_k\omega + r$, and r must be zero because $0 < k, k' < p$. This contradicts the assumption $k \neq k'$. In the second case, since $\sigma_{k'}\omega = \gamma'\sigma_k\omega = (s+1+\omega)/p$, we obtain $k' = s+1$. Moreover $s = k-1$ because $sk \equiv -1 \pmod{p}$. This implies $k' = k$, a contradiction. In the last case, since $\sigma_{k'}\omega = \gamma'\sigma_k\omega = (u+\omega)/p$ and $u(k-1) \equiv -1 \pmod{p}$, we obtain $k' = u = k$, a contradiction. Consequently, $1 \neq (c'\sigma_k\omega + d')^6$, as desired.

The proof of the other assertions is reduced to showing $1 \neq (c'\sigma_k i + d')^4$ and $1 \neq (c'\sigma_k\tau_D + d')^2$, and these are proved in a similar way. ■

For $D \in S(p)$, τ_D is a zero of both $j(z) - j(\tau_D)$ and $\operatorname{disc}_Y \Phi_p(j(z), Y)$. Let $m_{D,p}$ and $n_{D,p}$ be the respective multiplicities of these zeros. Note that $x^2 - x + 1 \equiv 0 \pmod{p}$ has a solution if and only if $(-3/p) = 1$, and $x^2 + 1 \equiv 0 \pmod{p}$ has a solution if and only if $(-4/p) = 1$. Then the following assertions follow immediately from Proposition 2.1, Proposition 2.2 and Lemma 2.3:

- If $D = -3$, then $m_{D,p} = 3$ and $n_{D,p} = \begin{cases} 6 & \text{if } p = 3, \\ 2p + 3 + (-3/p) & \text{if } p \neq 3. \end{cases}$

- If $D = -4$, then $m_{D,p} = 2$ and $n_{D,p} = p + 2 + (-4/p)$.
- If $D \neq -4, -3$, then $m_{D,p} = 1$ and $n_{D,p} = 2$.

Hence $r_{D,p} = n_{D,p}/m_{D,p}$ because

$$\begin{aligned}\lim_{X\to j(\tau_D)} \frac{\mathrm{disc}_Y\, \Phi_p(X,Y)}{(X - j(\tau_D))^{n_D/m_D}} &= \lim_{z\to\tau_D} \frac{\mathrm{disc}_Y\, \Phi_p(j(z),Y)}{(j(z) - j(\tau_D))^{n_D/m_D}} \\ &= \lim_{z\to\tau_D} \frac{\mathrm{disc}_Y\, \Phi_p(j(z),Y)}{(z-\tau_D)^{n_D}} \frac{(z-\tau_D)^{n_D}}{(j(z) - j(\tau_D))^{n_D/m_D}} \neq 0.\end{aligned}$$

As a consequence, $r_{D,p}$ $(= s(D,p))$ can be written as

$$r_{D,p} = \frac{n_{D,p}}{m_{D,p}} = \begin{cases} 6/3 = 2\lceil p/3\rceil & \text{if } D = -3 \text{ and } p = 3, \\ \frac{2p+3+(-3/p)}{3} = 2\lceil p/3\rceil & \text{if } D = -3 \text{ and } p \neq 3, \\ \frac{p+2+(-4/p)}{2} = 2\lceil p/4\rceil & \text{if } D = -4, \\ 2 & \text{if } D \neq -4, -3. \end{cases}$$

Finally, we calculate the coefficient of the most negative term of q in the q-expansion of $\mathrm{disc}_Y\, \Phi_p(j(z),Y)$ to calculate the leading coefficient of the discriminant of $\Phi_p(X,Y)$. By the definition of $\mathrm{disc}_Y\, \Phi_p(j(z),Y)$,

$$\begin{aligned}(2.2)\qquad &\prod_{0\le i<j\le p} (j(\sigma_j z) - j(\sigma_i z))^2 \\ &= (-1)^{p(p+1)/2} \prod_{0\le i<j\le p} (j(\sigma_i z) - j(\sigma_j z)) \prod_{0\le i<j\le p} (j(\sigma_j z) - j(\sigma_i z)) \\ &= (-1)^{(p+1)/2} \prod_{j=0}^{p} \prod_{\substack{i\neq j \\ 0\le i\le p}} (j(\sigma_j z) - j(\sigma_i z)).\end{aligned}$$

Furthermore the q-expansion of $j(\sigma_k z)$ is of the form (see [1, Section 11])

$$j(\sigma_k z) = \begin{cases} \zeta_p^{-k}/q^{1/p} + \sum_{n=0}^{\infty} c_n \zeta_p^{kn} (q^{1/p})^n,\ c_n \in \mathbb{C}, & \text{if } 0 \le k < p, \\ 1/q^p + \sum_{n=0}^{\infty} c_n q^{pn},\ c_n \in \mathbb{C}, & \text{if } k = p. \end{cases}$$

Thus the most negative term in the q-expansion of (2.2) is

$$\begin{aligned}\frac{(-1)^{(p+1)/2}}{q^{p^2}} \prod_{j=0}^{p-1} \frac{-1}{q^p} \prod_{\substack{i\neq j \\ 0\le i<p}} (\zeta_p^j - \zeta_p^i) q^{1/p} &= \frac{(-1)^{(p-1)/2}}{q^{2p^2+p-1}} \prod_{j=0}^{p-1} \prod_{\substack{i\neq j \\ 0\le i<p}} (\zeta_p^j - \zeta_p^i) \\ &= \frac{(-1)^{(p-1)/2}}{q^{2p^2+p-1}} \prod_{1\le i<p} (1 - \zeta_p^i)^p = \frac{(-1)^{(p-1)/2} p^p}{q^{2p^2+p-1}}.\end{aligned}$$

This implies that $\mathrm{disc}_Y\, \Phi_p(j(z),Y)$ is a polynomial in $j(z)$ whose degree is $2p^2 + p - 1$ and leading coefficient is $(-1)^{(p-1)/2} p^p$ by Hasse's q-expansion principle. This completes our proof.

3. Proof of Theorem 1.5. The basic idea of the proof is to compare the factorizations of $\operatorname{disc}_Y \Phi_p(X,Y)$ and $\Phi_{p^2}(X,X)$. We now give the factorization of the latter.

PROPOSITION 3.1. *For any odd prime p,*

$$\Phi_{p^2}(X,X) = -pH_{-3}(X)^u H_{-4}(X)^v H_{-3p^2}(X)^2 H_{-4p^2}(X) \prod_{\substack{D\in S(p)\\ D\neq -3,-4}} H_D(X)^2,$$

where

$$u = \begin{cases} 0 & \text{if } p=3,\\ 1+(-3/p) & \text{if } p\neq 3,\end{cases} \qquad v = 1+(-4/p).$$

Proof. Let $w(D)$ denote the number of elements of the unit group of an imaginary quadratic order $\mathcal{O}$ with negative discriminant D. We define a polynomial $\mathcal{H}_D(X)$ by

$$\mathcal{H}_D(X) = \prod_{r^2\mid D} H_{D/r^2}(X)^{2/w(D/r^2)}.$$

Then $\deg_X(\Phi_{p^2}(X,X)) = 2p^2+p-1$ and

$$\Phi_{p^2}(X,X) = \text{constant} \times \frac{\prod_{t^2<4p^2} \mathcal{H}_{t^2-4p^2}(X)}{\mathcal{H}_{-3}(X)^2\mathcal{H}_{-4}(X)} \tag{3.1}$$

(see [9]). Let $\mathcal{N}_{D,p}$ denote

$$\#\{(x,y)\in\mathbb{Z}^2 \mid x^2-Dy^2 = 4p^2,\ y>0\}.$$

Then $\Phi_{p^2}(X,X)$ can be written as

$$\text{constant} \times H_{-3p^2}(X)^{s^*(-3p^2,p)} H_{-4p^2}(X)^{s^*(-4p^2,p)} \prod_{D\in S(p)} H_D(X)^{s^*(D,p)},$$

where

$$s^*(D,p) = \begin{cases} (\mathcal{N}_{D,p}-2)/3 & \text{if } D=-3,\\ (\mathcal{N}_{D,p}-1)/2 & \text{if } D=-4,\\ \mathcal{N}_{D,p} & \text{otherwise.}\end{cases}$$

It is obvious that $s^*(-3p^2,p)=2$ and $s^*(-4p^2,p)=1$ by (3.1). Moreover because $x^2+4y^2=4p^2 \Leftrightarrow (x/2)^2+y^2=p^2$ and $x^2+3y^2=4p^2 \Leftrightarrow \left(\frac{x+y}{2}\right)^2 - \left(\frac{x+y}{2}\right)y + y^2 = p^2$, we have

$$\begin{aligned}\mathcal{N}_{-3,p} &= \#\{(x,y)\in\mathbb{Z}^2 \mid x^2-xy+y^2=p^2,\ y>0\}\\ &= \begin{cases} 2 & \text{if } p=3,\\ 5+3(-3/p) & \text{if } p\neq 3,\end{cases}\\ \mathcal{N}_{-4,p} &= \#\{(x,y)\in\mathbb{Z}^2 \mid x^2+y^2=p^2,\ y>0\}\\ &= 3+2(-4/p)\end{aligned}$$

(see [5, Section 3]). This implies $s^*(-3,-3)=0$, $s^*(-3,p)=1+(-3/p)$ and $s^*(-4,p)=1+(-4/p)$ for any prime $p>3$.

Lemma 3.2. *For an odd prime p,*

$$\begin{aligned}&\deg_X\bigl(H_{-3}(X)^{s(-3,p)}H_{-4}(X)^{s(-4,p)}\bigr)\\&\quad=\deg_X\bigl(H_{-3}(X)^{s^*(-3,p)}H_{-4}(X)^{s^*(-3,p)}H_{-3p^2}(X)^{s^*(-3,p)}H_{-4p^2}(X)^{s^*(-3,p)}\bigr).\end{aligned}$$

Proof. It is well known that $h(-3)=h(-4)=1$. By the class number formula, we obtain

$$h(-3p^2)=\frac{p}{3}\left(1-\left(\frac{-3}{p}\right)\frac{1}{p}\right)\quad\text{and}\quad h(-4p^2)=\frac{p}{2}\left(1-\left(\frac{-4}{p}\right)\frac{1}{p}\right)$$

(see [1, Section 7]). Thus the assertion follows immediately from $\deg_X H_D(X)=h(D)$. ■

By using $\deg(\mathrm{disc}_Y\,\varPhi_p(X,Y))=\deg(\varPhi_{p^2}(X,X))$ and Lemma 3.1, it follows that

$$\sum_{\substack{D\in S(p)\\D\neq-3,-4}}h(D)s^*(D,p)=\sum_{\substack{D\in S(p)\\D\neq-3,-4}}h(D)s(D,p)=\sum_{\substack{D\in S(p)\\D\neq-3,-4}}2h(D).$$

Hence $s^*(D,p)=2$ for all $D\in S(p)\setminus\{-3,-4\}$ because $s^*(D,p)\ge 2$ if $D\in S(p)\setminus\{-3,-4\}$. Finally, we calculate the leading coefficient of $\varPhi_{p^2}(X,X)$. By the definition of $C(N)$, we see that

$$C(p^2)=\bigl\{\bigl(\begin{smallmatrix}p^2&0\\0&1\end{smallmatrix}\bigr)\bigr\}\cup\bigl\{\bigl(\begin{smallmatrix}p&k\\0&p\end{smallmatrix}\bigr)\bigm|1<k<p\bigr\}\cup\bigl\{\bigl(\begin{smallmatrix}1&k\\0&p^2\end{smallmatrix}\bigr)\bigm|0\le k<p^2\bigr\}.$$

Hence

$$\begin{aligned}&\varPhi_{p^2}(j(z),j(z))\\&\quad=(j(z)-j(p^2z))\prod_{u=1}^{p-1}\left(j(z)-j\left(z+\frac{u}{p}\right)\right)\prod_{v=0}^{p^2-1}\left(j(z)-j\left(\frac{z+v}{p^2}\right)\right).\end{aligned}$$

This implies that the most negative term in the q-expansion of $\varPhi_{p^2}(j(z),j(z))$ equals $(-1)\prod_{k=1}^{p-1}(1-\zeta_p^k)=-p$, and this is the leading coefficient of $\varPhi_{p^2}(X,X)$. ■

Now we have the factorizations of both $\mathrm{disc}_Y\,\varPhi_p(X,Y)$ and $\varPhi_{p^2}(X,X)$ by Theorem 1.4 and Proposition 3.1. Moreover we see that

$$\begin{aligned}s(-3,p)-s^*(-3,p)&=2\frac{p-(-3/p)}{3}=2h(-3p^2),\\s(-4,p)-s^*(-4,p)&=\frac{p-(-4/p)}{2}=h(-4p^2),\end{aligned}$$

for any odd prime p. Thus Theorem 1.5 is proved by comparing two polynomials.

References

[1] D. A. Cox, *Primes of the Form* $x^2 + ny^2$, Wiley, New York, 1989.

[2] B. H. Gross and D. B. Zagier, *On singular moduli*, J. Reine Angew. Math. 355 (1985), 191–220.

[3] E. Kaltofen and N. Yui, *On the modular equation of order 11*, in: Third MACSYMA Users' Conference, General Electric, 1984, 472–485.

[4] E. Kaltofen and N. Yui, *Explicit construction of the Hilbert class fields of imaginary quadratic fields by integer lattice reduction*, in: Number Theory, Springer, 1991, 149–202.

[5] I. Niven, H. S. Zuckerman and H. L. Montgomery, *An Introduction to the Theory of Numbers*, Wiley, 1991.

[6] H. Weber, *Elliptische Functionen und algebraische Zahlen*, Vieweg, Braunschweig, 1891.

[7] H. Weber, *Lehrbuch der Algebra: Vol. 3*, Vieweg, 1908.

[8] N. Yui, *Explicit form of the modular equation*, J. Reine Angew. Math. 299/300 (1978), 185–200; Correction, ibid. 302 (1978), 70.

[9] D. Zagier, *Traces of singular moduli*, in: Motives, Polylogarithms and Hodge Theory, Part I (Irvine, CA, 1998), Int. Press, Somerville, MA, 2002, 211–244.

Mitsusada Nakata
9-2-5, Karita, Sumiyoshi-ku
Osaka-shi, Osaka, Japan
E-mail: n32sada@gmail.com