International Mathematical Forum, 4, 2009, no. 8, 367 - 376

N-Systems, Class Polynomials of Double Eta-Quotients and Singular Values of j-Invariant Function

Shunsuke Yoshimura[a], **Aya Comuta**[a], **Noburo Ishii**[b,1]

[a] Graduate School of Science
Osaka Prefecture University
Sakai, Osaka, 599-8531 Japan

[b] Faculty of Liberal arts and Sciences
Osaka Prefecture University
Sakai, Osaka, 599-8531 Japan

Abstract

We study the relation between N-systems, class polynomials of double η-quotients and singular values of the j-invariant function by using normalizers of the group $\Gamma^0(N)$.

Mathematics Subject Classification: 11G15, 11F20

Keywords: class polynomial, eta function

1 Introduction

In elliptic curve cryptosystems, it is important to construct elliptic curves with the number of points required over a finite field. To construct elliptic curves, we often make use of the class polynomials of the j-invariant function J. However these polynomials have the problem on practical use that their coefficients can be very large. Enge and Schertz [2] gave a method to compute singular values of the function J by using class polynomials of double η-quotients and modular equations relating J and double η-quotients. Since double η-quotients are not $\mathrm{SL}_2(\mathbb{Z})$-invariant, they considered N-systems to calculate class polynomials of double η-quotients. It is noted that the class polynomials depend on the choice of N-systems. They obtain a singular value of J as a solution of the

[1]Corresponding author, ishii@las.osakafu-u.ac.jp

equation $\Phi(J)$ which is given by substituting a root of a class polynomial in the modular equation. However in their method, it is necessary to count the number of rational points of elliptic curves over a finite field corresponding to all solutions of the equation, because in advance we can not know which solution corresponds to the singular value. In this article, we shall study the relation between N-systems and class polynomials of double η-quotients by using normalizers of $\Gamma^0(N)$ and give a condition that a singular value of J is a multiple root of the equation $\Phi(J)$. In this situation we may reduce the amount of computation in the process to identify the singular value among solutions. In Section 2, we give some basic results and definitions. In Section 3, we determine the relation between N-systems and class polynomials of double η-quotients. In Section 4, we give a condition that a singular value of J is a multiple root of $\Phi(J)$. In section 5, we give an example.

2 Basic results and definitions

Let $\eta(z) = q^{1/24}\prod_{n=1}^{\infty}(1-q^n)$ $(q = e^{2\pi iz})$ be the Dedekind η-function. For two prime numbers p_1 and p_2, the double η-quotient $\mathfrak{w}_N(z)$ of level $N = p_1p_2$ is defined by

$$\mathfrak{w}_N(z) = \frac{\eta(z/p_1)\eta(z/p_2)}{\eta(z)\eta(z/p_1p_2)}.$$

For $s = 24/\gcd(24, (p_1-1)(p_2-1))$, the function $\mathfrak{w}_N^s(z)$ is invariant under the modular group

$$\Gamma^0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \middle| \, b \equiv 0 \pmod{N} \right\}$$

(see [4]). For a divisor Q of N such that $\gcd(Q, \frac{N}{Q}) = 1$ and $Q \neq N$, put $W_Q = \left(\begin{smallmatrix} -Q & N \\ y & Qx \end{smallmatrix}\right)$, where $x, y \in \mathbb{Z}$ and $\det(W_Q) = Q$. Then we know W_Q is a normalizer of $\Gamma^0(N)$. Further we denote by W_N the Atkin-Lehner involution $\left(\begin{smallmatrix} 0 & N \\ -1 & 0 \end{smallmatrix}\right)$. For N-systems $\mathfrak{N}$, Enge and Schertz [2] defined the class polynomials $H_{\mathfrak{N}}(X)$ of $\mathfrak{w}_N^s(z)$. In the following, we shall recall their results. Let $\mathcal{O}_f$ be the order of conductor f in an imaginary quadratic field K. Let D be the discriminant of $\mathcal{O}_f$ and $\mathfrak{H}_f$ the (proper) ideal class group of $\mathcal{O}_f$. To a proper ideal $\mathfrak{a} = [\beta_1, \beta_2] = \mathbb{Z}\beta_1 + \mathbb{Z}\beta_2, (\mathrm{Im}(\beta_1/\beta_2) > 0)$ of $\mathcal{O}_f$, we associate its basis quotient $\alpha_{\mathfrak{a}} = \beta_1/\beta_2$ and a quadratic form $\mathfrak{q}_{\mathfrak{a}}(X, Y) = N_{K/\mathbb{Q}}(\beta_1 X + \beta_2 Y)/N_{K/\mathbb{Q}}(\mathfrak{a})$. It is noted that the basis quotient $\alpha_{\mathfrak{a}}$ is determined up to $\mathrm{SL}_2(\mathbb{Z})$-equivalence and the form $\mathfrak{q}_{\mathfrak{a}}(X, Y)$ is a primitive quadratic form with integral coefficients of discriminant D. For proper ideals $\mathfrak{a}_1$ and $\mathfrak{a}_2$ of O_f, we write $\mathfrak{a}_1 \sim \mathfrak{a}_2$ if $\mathfrak{a}_1$ and

$\mathfrak{a}_2$ are in the same ideal class of $\mathcal{O}_f$. The followings are well known (see [1]).

$$\begin{aligned} \mathfrak{a}_1 \sim \mathfrak{a}_2 &\iff \alpha_{\mathfrak{a}_1} \text{ is } \mathrm{SL}_2(\mathbb{Z})\text{-equivalent to } \alpha_{\mathfrak{a}_2} \\ &\iff \mathfrak{q}_{\mathfrak{a}_1}(X,Y) \text{ is proper equivalent to } \mathfrak{q}_{\mathfrak{a}_2}(X,Y). \end{aligned} \tag{1}$$

Further the map $\mathfrak{a} \mapsto \mathfrak{q}_{\mathfrak{a}}(X,Y)$ gives rise to a bijection between $\mathfrak{H}_f$ and the proper equivalent classes of quadratic forms of discriminant D. Since for an ideal $\mathfrak{a}$ the value $J(\alpha_{\mathfrak{a}})$ is independent on the choice of basis quotients $\alpha_{\mathfrak{a}}$, we shall denote by $J(\mathfrak{a})$ the value $J(\alpha_{\mathfrak{a}})$. Hereafter for a triple (A,B,C) of integers such that $A \neq 0$, we shall denote by $[A,B,C]$ a quadratic form $AX^2+BXY+CY^2$. Furthermore, for a quadratic form $\mathfrak{q} = [A,B,C]$ of discriminant D, we put $\mathfrak{a}_{\mathfrak{q}} = [A, \frac{-B+\sqrt{D}}{2}]$ and $\alpha_{\mathfrak{q}} = \frac{-B+\sqrt{D}}{2A}$. Let $h(D)$ be the class number of the order $\mathcal{O}_f$. Then there exist $h(D)$ isomorphic classes of elliptic curves with complex multiplication by $\mathcal{O}_f$. They are represented by the elliptic curves with j-invariants $J(\mathfrak{a}_i)$, where $\mathfrak{a}_i$ $(i = 1, \ldots, h(D))$ are ideals representing all classes of $\mathfrak{H}_f$. Let K_f be the ring class field of K of conductor f. Then the theory of complex multiplication shows $J(\mathfrak{a}_i)$ generates K_f over K for each i and $J(\mathfrak{a}_i)$ $(i = 1, \ldots, h(D))$ are conjugate to each other over $\mathbb{Q}$. To obtain the values $J(\mathfrak{a}_i)$, we use the classical class polynomial $H_D[J](X) = \prod_{i=1}^{h(D)} (X - J(\mathfrak{a}_i))$. However, since this polynomial has large integral coefficient, it is hard to compute the polynomial for large D. Enge and Schertz [2] gave the method of using the double η-quotient to obtain a class polynomial with small integral coefficients. Since double η-quotient is not $\mathrm{SL}_2(\mathbb{Z})$-invariant, the value $\mathfrak{w}_N^{\mathfrak{s}}(\alpha_{\mathfrak{a}})$ depends on the choice of ideals $\mathfrak{a}$ and basis quotients in an ideal class. Therefore we must use N-systems defined by Schertz [5].

Definition 2.1. *Let $\mathfrak{N}$ be a set of $h(D)$ primitive quadratic forms $[A_i,B_i,C_i]$ of discriminant D. We say $\mathfrak{N}$ an N-system for $\mathcal{O}_f$ if forms $[A_i,B_i,C_i]$ satisfy the following conditions:*

1. $\gcd(A_i,N) = 1, B_i \equiv B_j \pmod{2N}$, $N|C_i$ *for every* i,j;
2. *the ideals* $[A_i, \frac{-B_i+\sqrt{D}}{2}]$ *form a representative system of* $\mathfrak{H}_f$.

By Theorems 3.1, 3.2 of [2], we have

Theorem 2.2. *Assume prime numbers p_1 and p_2 satisfy the following conditions:*

1. *If* $p_1 \neq p_2$, *then* $\left(\frac{D}{p_1}\right), \left(\frac{D}{p_2}\right) \neq -1$,
2. *if* $p_1 = p_2 = p$, *then either* $\left(\frac{D}{p}\right) = 1$ *or* $p|f$.

Then there exists an N-system $\mathfrak{N} = \{\mathfrak{q}_i\}$ for $\mathcal{O}_f$. Further $\mathfrak{w}_N^s(\alpha_{\mathfrak{q}_i}) \in K_f$ for every i and $\mathfrak{w}_N^s(\alpha_{\mathfrak{q}_i})$ are conjugate to each other over K.

Now the class polynomial of $\mathfrak{w}_N^s$ related to the N-system $\mathfrak{N}$ is defined by

$$H_{\mathfrak{N}}(X) = \prod_{i=1}^{h(D)} \left(X - \mathfrak{w}_N^s(\alpha_{\mathfrak{q}_i})\right).$$

By Theorem 2.2, we have $H_{\mathfrak{N}}(X) \in K[X]$. Further Corollary 3.1 of [2] gives

Corollary 2.3. *Suppose that following conditions hold:*

1. *If $p_1 \neq p_2$, then $\left(\frac{D}{p_1}\right), \left(\frac{D}{p_2}\right) \neq -1$, and $p_1, p_2 \nmid f$;*
2. *if $p_1 = p_2 = p \neq 2$, then $\left(\frac{D}{p}\right) = 1$ or $p|f$;*
3. *if $p_1 = p_2 = 2$, then $\left(\frac{D}{2}\right) = 1$, or $2|f$, but $D \not\equiv 4 \pmod{32}$.*

Then $H_{\mathfrak{N}}(X) \in \mathbb{Z}[X]$.

To relate $J(\mathfrak{a}_{\mathfrak{q}})$ and $\mathfrak{w}_N^s(\alpha_{\mathfrak{q}})$, the modular equation $\Phi_N(X, J)$ relating J and $\mathfrak{w}_N^s$ is used,which is defined by

$$\Phi_N(X, J) = \prod_{\sigma} (X - \mathfrak{w}_N^s(\sigma(z))),$$

where σ runs over a representative system of the coset decomposition $\mathrm{SL}_2(\mathbb{Z})$ modulo $\Gamma^0(N)$. We know that $\Phi_N(X, J) \in \mathbb{Z}[X, J]$ by Theorems 7 and 8 of [3]. To obtain elliptic curves with complex multiplication by $\mathcal{O}_f$ over the finite field $\mathbb{F}_q$ of q-elements, Enge and Schertz use the polynomials $H_{\mathfrak{N}}(X)$ and $\Phi_N(X, J)$ as follows. Assume that q is a prime number which splits completely in K_f. Then $H_{\mathfrak{N}}(X)$ splits completely in distinct linear factors over $\mathbb{F}_q$. Let α be a root of $H_{\mathfrak{N}}(X) \bmod q$. Then for some i $J(\mathfrak{a}_i) \bmod q$ is a $\mathbb{F}_q$-rational solution of $\Phi_N(\alpha, J) \equiv 0 \bmod q$. To identify $J(\mathfrak{a}_i) \bmod q$ among the rational solutions j_k, it is necessary to count the number of $\mathbb{F}_q$-rational points of each elliptic curve E_k with the j-invariant j_k. But,in the case $\Phi_N(\alpha, J) \bmod q$ has the degree 2 in J and a multiple root, we can save the process of counting the number of rational points. In section 4, we shall consider the condition that $\Phi(\alpha, J)$ has $J(\mathfrak{a}_i) \bmod q$ as a multiple root.

3 N-systems and class polynomials

In this section, we study the relation between N-systems and class polynomials.

Lemma 3.1. *Let* $\{[A_i, B_i, C_i]\}$ *and* $\{[A'_i, B'_i, C'_i]\}$ *be* N*-systems for* $\mathcal{O}_f$*. Suppose that* $[A_i, B_i, C_i]$ *and* $[A'_i, B'_i, C'_i]$ *are proper equivalent for every* i*. Then* $\alpha_i = \frac{-B_i+\sqrt{D}}{2A_i}$ *is* $\Gamma^0(N)$*-equivalent to* $\alpha'_i = \frac{-B'_i+\sqrt{D}}{2A'_i}$ *if and only if* $B_i \equiv B'_i \pmod{2N}$*. In particular, if* $B_i \equiv B'_i \pmod{2N}$*, then* $\mathfrak{w}_N^s(\alpha_i) = \mathfrak{w}_N^s(\alpha'_i)$*.*

Proof. Since $[A_i, B_i, C_i]$ and $[A'_i, B'_i, C'_i]$ are proper equivalent, there exists a matrix $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ such that $\alpha_i = M(\alpha'_i)$. We have only to show $M \in \Gamma^0(N)$ if and only if $B_i \equiv B'_i \pmod{2N}$. Since we have

$$\begin{aligned} B_iB'_ic - 2A'_iB_id + Dc &= -2A_iB'_ia + 4A_iA'_ib, &(2)\\ -B_ic - B'_ic + 2A'_id &= 2A_ia, &(3)\end{aligned}$$

by substituting (3) into (2), we obtain

$$a(B'_i - B_i) - 2C_ic = 2A'_ib.$$

Since $\gcd(A'_i, N) = 1$ and $N|C_i$, we have $a(B'_i - B_i) \equiv 2A'_ib \pmod{2N}$. Therefore $M \in \Gamma^0(N)$ if and only if $B_i \equiv B'_i \pmod{2N}$. □

The following result is deduced from Proposition 3 of [5].

Proposition 3.2. *Let* $[A, B, C]$ *be a primitive quadratic form of discriminant* D *such that* $A > 0, \gcd(A, N) = 1$ *and* $N|C$*. Then there exists an* N*-system* $\mathfrak{N}$ *for* $\mathcal{O}_f$ *containing* $[A, B, C]$*. In particular, for an integer* B *such that* $B^2 \equiv D \pmod{4N}$*, there exists an* N*-system* $\mathfrak{N}$ *for* $\mathcal{O}_f$ *containing* $[1, B, (B^2 - D)/4]$*.*

By Proposition 3.2 and Lemma 3.1, we know the class polynomials of double η-quotient related to N-systems depend only on integers B, considered mod $2N$, such that $B^2 \equiv D \pmod{4N}$. In the following, we shall fix an N-system containing $[1, B, (B^2 - D)/4]$ and shall denote it by $\mathfrak{N}_B$ and by $H_{B,N}(X)$ the class polynomial $H_{\mathfrak{N}_B}(X)$ related to the N-system $\mathfrak{N}_B$.

Lemma 3.3. *Assume that* p_1 *and* p_2 *are odd primes. Let* $N(D)$ *be the number of integers* $B \bmod 2N$ *such that* $B^2 \equiv D \pmod{4N}$*. Then*

$$N(D) = \begin{cases} 4 & if \quad \left(\frac{D}{p_1}\right) = 1 \quad and \quad \left(\frac{D}{p_2}\right) = 1, \\ 2 & if \quad \left(\frac{D}{p_1}\right) = 1 \quad and \quad \left(\frac{D}{p_2}\right) = 0. \end{cases}$$

Proof. Let us consider the case $\left(\frac{D}{p_1}\right) = 1$ and $\left(\frac{D}{p_2}\right) = 1$. Then there exists an integer a_i such that $a_i^2 \equiv D \pmod{p_i}$ for $i = 1, 2$. By Chinese reminder theorem, we see $B^2 \equiv D \pmod{4N}$ if and only if

$$B \equiv D \pmod 2, \quad B \equiv \pm\alpha_i \pmod{p_i} \quad (i = 1, 2).$$

This shows $N(D) = 4$. The remaining case can be treated similarly. □

If N is odd, then we obtain at most $N(D)$ distinct class polynomials of the double η-quotient.

Lemma 3.4. *Let B be an integer such that $B^2 \equiv D \pmod{4N}$. Then $H_{-B,N}(X) = H_{B,N}(X)$.*

Proof. We know the q-expansion $\mathfrak{w}_N^s(z) = \sum a_n q^n$ is rational, thus $a_n \in \mathbb{Q}$ (see section 3 of [3]). Therefore we have $\overline{\mathfrak{w}_N^s(z)} = \sum a_n \overline{q}^n = \mathfrak{w}_N^s(-\overline{z})$. Since $-(\overline{\frac{-B+\sqrt{D}}{2A}}) = \frac{B+\sqrt{D}}{2A}$ and $H_{B,N}(X) \in \mathbb{Z}[X]$, we have $H_{B,N}(X) = \overline{H_{B,N}(X)} = H_{-B,N}(X)$. □

Theorem 3.5. *Let $N(H_D)$ be the number of distinct class polynomials $H_{B,N}(X)$. Then*

$$N(H_D) = \begin{cases} 1,2 & if \quad \left(\frac{D}{p_1}\right) = 1 \quad and \quad \left(\frac{D}{p_2}\right) = 1, \\ 1 & if \quad \left(\frac{D}{p_1}\right) = 1 \quad and \quad \left(\frac{D}{p_2}\right) = 0. \end{cases}$$

Proof. Lemmas 3.3 and 3.4 imply that $N(H_D) \le N(D)/2$. Thus we have the assertion. □

In the case $N(H_D) = 2$, we have two class polynomials $H_{B,N}(X)$ and $H_{B',N}(X)$, where B, B' are integers such that $B^2 \equiv D \pmod{4N}$, $B' \equiv B \pmod{p_1}$, $B' \equiv -B \pmod{p_2}$. We shall show $H_{B',N}(X)$ is obtainable from $H_{B,N}(X)$ by a simple transformation. We shall use the following transformation formula of the Dedekind η-function (see Theorem 1 of [3]).

Theorem 3.6. *Let $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ be normalized such that $c \ge 0$, and $d > 0$ if $c = 0$. Write $c = \gamma 2^\lambda$ with γ odd; by convention, $\gamma = \lambda = 1$ if $c = 0$. Then*

$$\eta(Mz) = \epsilon(M)\sqrt{cz+d}\,\eta(z)$$

with $\Re(\sqrt{cz+d}) > 0$, $\quad \epsilon(M) = \left(\frac{a}{\gamma}\right)\zeta_{24}^{ab+c(d(1-a^2)-a)+3\gamma(a-1)+\frac{3}{2}\lambda(a^2-1)}$.

Lemma 3.7. *Let $W_{p_1} = \left(\begin{smallmatrix} -p_1 & N \\ y & -p_1 x \end{smallmatrix}\right)$ with $y > 0$, $y \equiv 1 \pmod 2$ and $p_1 x - p_2 y = 1$. Then*

$$\mathfrak{w}_N^s(z)\mathfrak{w}_N^s(W_{p_1}(z)) = \left(\frac{p_1}{p_2}\right)^s.$$

Proof. By Theorem 3.6,

$$\begin{aligned} \mathfrak{w}_N(W_{p_1}(z)) &= \mathfrak{w}_N\left(\frac{-p_1 z + N}{yz - p_1 x}\right) = \frac{\eta(\frac{-z+p_2}{yz-p_1x})\eta(\frac{-p_1(z/N)+1}{p_2y(z/N)-x})}{\eta(\frac{-p_1(z/p_1)+p_2}{y(z/p_1)-x})\eta(\frac{-(z/p_2)+1}{p_2y(z/p_2)-p_1x})} \\ &= \left(\frac{p_1}{p_2}\right)\zeta_{24}^{(1-p_2)(1-p_1)(1+4y-xy(p_1+1))}\mathfrak{w}_N(z)^{-1}. \end{aligned}$$

Since $s(p_1-1)(p_2-1) \equiv 0 \pmod{24}$, we have our assertion. □

Proposition 3.8. *Suppose that* $\left(\frac{D}{p_1}\right) = \left(\frac{D}{p_2}\right) = 1$. *Then*

$$H_{B',N}(X) = \frac{X^{h(D)}}{H_{B,N}(0)} H_{B,N}(\left(\frac{p_1}{p_2}\right)^s / X).$$

Proof. Let $\mathfrak{q} = [A, B, C]$ be a form of the N-system $\mathfrak{N}_B$. Put $W_{p_1}(\alpha_\mathfrak{q}) = \frac{-B'+\sqrt{D}}{2A'}$. Then we see easily that $B' \equiv B \pmod{p_1}$, $B' \equiv -B \pmod{p_2}$ and $C' = (B'^2 - D)/4A' \equiv 0 \pmod{N}$. If $\gcd(A', N) > 1$, then we shall show there exists an element $\gamma \in \Gamma^0(N)$ such that the first coefficient A'' of the quadratic form $[A'', B'', C'']$ corresponding to $\gamma W_{p_1}(\alpha_\mathfrak{q})$ is prime to N. It is noted by the proof of Lemma 3.1 that $B' \equiv B'' \pmod{2N}$ and $N|C''$. Since $\mathfrak{w}_N^s(\gamma W_{p_1}(\alpha_\mathfrak{q})) = \mathfrak{w}_N^s(W_{p_1}(\alpha_\mathfrak{q}))$, we have $H_{B',N}(X) = \prod_{\mathfrak{q} \in \mathfrak{N}_B} (X - \mathfrak{w}_N^s(W_{p_1}(\alpha_\mathfrak{q})))$. By Lemma 3.7, we have our result. Assume that A' is not prime to N. Put $\gamma = \begin{pmatrix} r & N \\ t & 1 \end{pmatrix}$, for integers r, t. Then

$$\gamma W_{p_1}(\alpha_\mathfrak{q}) = \frac{(-rB' - tB'N + 2A'N + 2rtC') + \sqrt{D}}{2(-tB' + A' + t^2C')}.$$

Therefore we have $A'' = -tB' + A' + t^2C'$. Since $N|C'$, we know $\gcd(A'', N) = 1$ if and only if $\gcd(-tB' + A', N) = 1$. Assume $N|A'$. Then $\gcd(D, N) = 1$ implies $\gcd(B', N) = 1$. Hence we can take $r = N + 1$, $t = 1$. Next assume $p_i|A'$ and $p_j \nmid A'$. Then we have $p_i \nmid B'$. Therefore we can take $r = p_jN + 1$, $t = p_j$. This completes our proof. □

4 Multiple roots of modular equation

In this section, we assume the conditions in Corollary 2.3. We shall give a condition that for singular values α of double η-quotients the polynomial $\Phi_N(\alpha, J)$ of J has a multiple root.

Proposition 4.1. *The polynomial* $\Phi_N(X, J)$ *has degree* $(p_1 + 1)(p_2 + 1)$ *as a polynomial of* X *and has degree* $s(p_1 - 1)(p_2 - 1)/12$ *as a polynomial of* J. *For* $\tau \in \mathbb{C}$,$\mathrm{Im}\tau > 0$, *the equation* $\Phi_N(\mathfrak{w}_N^s(\tau), J) = 0$ *has two roots* $J(\tau)$ *and* $J(W_N(\tau))$. *In particular, if* $J(\tau) = J(W_N(\tau))$, *then the equation has a multiple root.*

Proof. The assertion concerning the degree follows from Theorem 9 of [3]. The equation $\Phi_N(\mathfrak{w}_N^s(\tau), J) = 0$ obviously has the root $J(\tau)$. Similarly, $J(W_N(\tau))$ is a root of $\Phi_N(\mathfrak{w}_N^s(W_N(\tau)), J) = 0$. By Theorem 2 of [3], we have $\mathfrak{w}_N^s(W_N(\tau)) = \mathfrak{w}_N^s(\tau)$. Therefore $J(W_N(\tau))$ is a root of $\Phi_N(\mathfrak{w}_N^s(\tau), J) = 0$. □

In the following, we consider a fixed N-system $\mathfrak{N}_B$. Let $\mathfrak{q} = [A, B, C] \in \mathfrak{N}_B$. Since $W_N(\alpha_\mathfrak{q}) = \frac{B+\sqrt{D}}{2(\frac{C}{N})}$, the action of W_N on the ideal $\mathfrak{a}_\mathfrak{q}$ is given by $W_N(\mathfrak{a}_\mathfrak{q}) = [\frac{C}{N}, \frac{B+\sqrt{D}}{2}]$.

Lemma 4.2. *If we set* $\mathfrak{a}_B = [N, \frac{-B+\sqrt{D}}{2}]$, *then* $W_N(\mathfrak{a}_\mathfrak{q}) \sim \mathfrak{a}_\mathfrak{q}\mathfrak{a}_B$.

Proof. Put $\omega = (B + \sqrt{D})/2$. Since $\gcd(A, B, C) = 1$,

$$\begin{aligned}\overline{\mathfrak{a}_\mathfrak{q}} W_N(\mathfrak{a}_\mathfrak{q}) &= [A, \omega][C/N, \omega] = [AC/N, (C/N)\omega, A\omega, B\omega] \\ &= [AC/N, \omega] = (\omega/N)[N, (-B + \sqrt{D})/2] \sim \mathfrak{a}_B.\end{aligned}$$

Since $\overline{\mathfrak{a}_\mathfrak{q}}\mathfrak{a}_\mathfrak{q} \sim 1$, this shows the assertion. □

Proposition 4.3. *Let* $\mathfrak{q} = [A, B, C] \in \mathfrak{N}_B$. *Then* $J(W_N(\alpha_\mathfrak{q})) = J(\alpha_\mathfrak{q})$ *if and only if there exist* $u, v \in \mathbb{Z}$ *such that*

$$u^2 - Dv^2 = 4N, \quad u - Bv \equiv 0 \pmod{2N}. \tag{4}$$

Proof. By (1) and Lemma 4.2, we have

$$J(W_N(\mathfrak{a}_\mathfrak{q})) = J(\mathfrak{a}_\mathfrak{q}) \quad \Leftrightarrow \quad W_N(\mathfrak{a}_\mathfrak{q}) \sim \mathfrak{a}_\mathfrak{q} \quad \Leftrightarrow \quad \mathfrak{a}_B \sim 1.$$

Further we know the condition $\mathfrak{a}_B \sim 1$ is equivalent to the existence of an element $\begin{pmatrix} x & y \\ z & w \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ such that

$$\frac{-B + \sqrt{D}}{2N} = \frac{x(\frac{-B+\sqrt{D}}{2}) + y}{z(\frac{-B+\sqrt{D}}{2}) + w}. \tag{5}$$

Let us assume (5). Then we have

$$zB^2 + zD - 2wB = -2xNB + 4Ny, \quad w = xN + zB. \tag{6}$$

From (6), we have $y = -A\frac{C}{N}z$. Therefore, from $xw - yz = 1$, we obtain $(Bz + 2xN)^2 - Dz^2 = 4N$. Now, we put $u = Bz + 2Nx$, $v = z$. Then we have $u^2 - Dv^2 = 4N$ and $x = \frac{u-Bv}{2N}$. Further, since $x \in \mathbb{Z}$, we have $u - Bv \equiv 0 \pmod{2N}$. Conversely, let u, v be integers satisfying (4). Put $x = \frac{u-Bv}{2N}$, $y = -A\frac{C}{N}v$, $z = v$ and $w = xN + zB$. Then we have $xw - zy = 1$ and (5). □

Immediately from Proposition 4.3, we obtain

Corollary 4.4. *If* $J(W_N(\mathfrak{a}_\mathfrak{q})) = J(\mathfrak{a}_\mathfrak{q})$, *then* $N > -D/4$.

Proof. The condition (4) shows $D = \frac{u^2-4N}{v^2} > -4N$. □

Proposition 4.5. *Assume there exist u, $v \in \mathbb{Z}$ satisfying* (4). *Then the equation $\Phi_N(\mathfrak{w}_N^s(\alpha_\mathfrak{q}), J) = 0$ has a multiple root $J(\mathfrak{a}_\mathfrak{q})$.*

Proof. The assertion is obvious. □

Theorem 4.6. *Let $\mathfrak{a}_{\mathfrak{q}_i}$ $(i = 1, \ldots, h(D))$ be the ideals associated with the quadratic forms $\mathfrak{q}_i = [A_i, B_i, C_i]$ of $\mathfrak{N}_B$. Then*

$$J(\mathfrak{a}_{\mathfrak{q}_1}) = J(W_N(\mathfrak{a}_{\mathfrak{q}_1})) \Leftrightarrow J(\mathfrak{a}_{\mathfrak{q}_i}) = J(W_N(\mathfrak{a}_{\mathfrak{q}_i})) \quad (i = 1, \ldots, h(D)).$$

Proof. Since $B_1 \equiv B_i \pmod{2N}$, our assertion follows from Proposition 4.3. □

Corollary 4.7. *Let ℓ be a prime number which splits completely in K_f. Let B be an integer such that there exist integers u and v satisfying* (4). *Then for any $\mathfrak{q} \in \mathfrak{N}_B$, $\Phi_N(\mathfrak{w}_N^s(\alpha_\mathfrak{q}), J)$ has a multiple root $J(\mathfrak{a}_\mathfrak{q})$ over $\mathbb{F}_\ell$.*

Proof. Our assertion follows from Proposition 4.3 and Theorem 4.6. □

5 Example

We give an example for the result given in Corollary 4.7. Let $D = -56$ and $N = 39$. The integer $B = 10$ satisfies $B^2 \equiv D \pmod{4N}$ and for $u = 10, v = 1$ the condition (4) holds true. By routine computation, we have $H_{10,39}(X) = X^4 - 2X^3 - X^2 + 2X - 1$ and $\Phi_{39}(X, J) = X^{56} + \sum_{i=0}^{55} a_i X^i$, where coefficients a_i are given in the following table:

i	a_i	i	a_i	i	a_i
55	$704 - J$	54	$168568 + 39J$	53	$14498520 - 663J$
52	$187807764 + 6331J$	51	$744637296 - 35763J$	50	$-6562036 + 106392J$
49	$-3840625568 - 18070J$	48	$1058251610 - 1082016J$		
47	$10302034600 + 3516903J$	46	$4510900472 - 1278901J$		
45	$-34331690432 - 18277116J$	44	$-7097865034 + 40532700J$		
43	$84188024320 + 11574823J$	42	$546780176 - 161476962J$		
41	$-154959173464 + 168751479J$	40	$-12359340101 + 230086922J$		
39	$327081484064 - 617987682J$	38	$-49301838300 + 137626281J$		
37	$-576339027576 + 928366231J$	36	$284363953068 - 959457720J$		
35	$735938431592 - 477589944J$	34	$-558265224452 + 1429130144J$		
33	$-890017323520 - 466517064J$	32	$977815434427 - 963208272J$		
31	$966995235128 + 909996295J$	30	$-1755072840368 + 158515461J$		
29	$-345165085024 - 607329720J$	28	$2218368968890 + 197238236J$		
27	$-911733108784 + 179445279J$	26	$-1540031876048 - 140684622J$		
25	$1628026178168 - 6888479J$	24	$261124933147 + 37909092J$		
23	$-1229692547200 - 8835450J$	22	$462040501468 - 4070053J$		
21	$441029439032 + 1885689J$	20	$-422841966612 + 44928J$		
19	$-7261052136 - 111436J$	18	$163453863300 + 9516J$		
17	$-59787354976 + 740J$	16	$-26470898021 - 1486J + J^2$		
15	$24009911816 - 49J$	14	$-1731574864 + 29J$		

13	$-3926472080+246J$	12	$1333660406-364J$	11	$158103088-221J$
10	$-172600168+650J$	9	$25597000-221J$	8	$5195450-364J$
7	$-2155088+247J$	6	$177164+26J$	5	$39936-52J$
4	$-9996+13J$	3	$600-J$	2	88
1	-16	0	1		

It is noted the degree of the $\Phi_{39}(X,J)$ in J is 2. We take a prime number $\ell = 3593$, which splits completely in K_1. Then we have $H_{10,39}(X) \equiv (X - 607)(X - 166)(X - 3428)(X - 2987) \pmod{3593}$. By substituting the roots of $H_{10,39}(X)$ into $\Phi_{39}(X,J)$, we have modulo 3593

$$\Phi_{39}(607,J) \equiv (J-229)^2, \qquad \Phi_{39}(166,J) \equiv (J-2979)^2,$$
$$\Phi_{39}(3428,J) \equiv (J-2874)^2, \qquad \Phi_{39}(2987,J) \equiv (J-2696)^2.$$

On the other hand, the discriminant of $\Phi_{39}(X,J)$ as a polynomial in J is divided by $H_{10,39}(X)$. This means that the polynomial $\Phi_{39}(\mathfrak{w}_N^s(\alpha_{\mathfrak{q}_i}),J)$ has a multiple root for every form $\mathfrak{q}_i \in \mathfrak{N}_B$, thus, we have $J(\mathfrak{a}_{\mathfrak{q}_i}) = J(W_{39}(\mathfrak{a}_{\mathfrak{q}_i}))$ for every i.

References

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

[2] A. Enge and R. Schertz, Constructing elliptic curves over finite fields using double eta-quotients, *J. Théor. Nombres de Bordeaux*, **16** (2004), 555–568.

[3] A. Enge and R. Schertz, Modular Curves of Composite Level, *Acta Arith.*, **118.2** (2005), 129–141.

[4] M. Newman, Construction and application of a class of modular functions (II), *Proc. London Math. Soc.*, **9** (1959), 373–387.

[5] R. Schertz, Weber's class invariants revisited, *J. Théor. Nombres de Bordeaux*, **14(1)** (2002), 325–343.

Received: July, 2008