Functiones et Approximatio
49.1 (2013), 103–109
doi: 10.7169/facm/2013.49.1.7

OCTAHEDRAL NEWFORMS OF WEIGHT ONE ASSOCIATED TO THREE-DIVISION POINTS OF ELLIPTIC CURVES

Takeshi Ogasawara

Abstract: In this paper, we give an explicit formula for computing Fourier coefficients of octahedral newforms of weight one associated to three-division points of elliptic curves.

Keywords: modular form, Galois representation, elliptic curve.

1. Introduction

Let $G_{\mathbb{Q}}$ be the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ of rational numbers $\mathbb{Q}$. A two-dimensional representation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{C})$ which is continuous and irreducible is classified into four cases by its projective image in $\mathrm{PGL}_2(\mathbb{C})$: dihedral group, alternating group A_4 (tetrahedral case), symmetric group S_4 (octahedral case), or alternating group A_5 (icosahedral case). We assume that ρ is odd, i.e. $\det\rho(c) = -1$ for the complex conjugation c. The modularity of such Galois representations was known in the cases of dihedral, tetrahedral and octahedral by the results of Hecke and Langlands-Tunnell. Recently, Serre's modularity conjecture has been proven by C. Khare and J. P. Wintenberger giving modularity in the icosahedral case as well (cf. [5], [6], [7]). Therefore, for any ρ which is odd and irreducible, there exists a newform f of weight one such that two L-functions $L(s, \rho)$ and $L(s, f)$ coincide. According to the projective image of ρ, we call the associated f dihedral, tetrahedral, octahedral, or icosahedral. It is important to know the Fourier coefficients of the newform f in the context of describing reciprocity law for the Galois extension corresponding to the kernel of ρ.

There are many examples of Fourier expansions for dihedral newforms, because suitable linear combinations of theta series of binary quadratic forms are dihedral newforms. However, there are few examples for Fourier expansion of other type

This research is partly supported by Grant-in-Aid for JSPS Fellows (23·3076).
2010 Mathematics Subject Classification: primary: 11F30; secondary: 11F80, 11G05

newforms. In [3], for some newforms of such type, Fourier coefficients a_n for small n are computed by studying how primes split in the field fixed by the kernel of ρ.

In this paper, we consider octahedral newforms related to mod 3 Galois representations arising from the action of $G_{\mathbb{Q}}$ on three-division points of given elliptic curves. Our main result describes a method for computing the Fourier coefficients of such octahedral newform in terms of Fourier coefficients of the newform of weight 2 associated to the elliptic curve and some dihedral newform of weight one (Theorem 3.1).

2. Elliptic curves and octahedral Galois representations

In this section, we review how we obtain an octahedral Galois representation from a mod 3 Galois representation.

2.1. The group $\mathrm{GL}_2(\mathbb{F}_3)$

The group $\mathrm{GL}_2(\mathbb{F}_3)$ has eight conjugacy classes, and their representatives are

$$e=\begin{pmatrix}1&0\\0&1\end{pmatrix},\qquad t=\begin{pmatrix}-1&0\\0&-1\end{pmatrix},\qquad u=\begin{pmatrix}0&1\\-1&0\end{pmatrix},$$
$$v_0=\begin{pmatrix}1&0\\1&1\end{pmatrix},\qquad v=\begin{pmatrix}-1&0\\-1&-1\end{pmatrix},\qquad w_0=\begin{pmatrix}1&0\\0&-1\end{pmatrix},$$
$$w_1=\begin{pmatrix}1&-1\\1&1\end{pmatrix},\qquad w_2=\begin{pmatrix}-1&1\\-1&-1\end{pmatrix}$$

(see, for example, [4]). For corresponding conjugacy classes, we denote by C_e, C_t, C_u, C_{v_0}, and so on.

The group $\mathrm{GL}_2(\mathbb{F}_3)$ has a two-dimensional irreducible character ϕ whose character table is given by

	e	t	u	v_0	v	w_0	w_1	w_2
ϕ	2	-2	0	-1	1	0	$\sqrt{-2}$	$-\sqrt{-2}$

We can take a realization Φ of ϕ given by

$$\Phi\left(\begin{pmatrix}-1&1\\-1&0\end{pmatrix}\right)=\begin{pmatrix}-1&1\\-1&0\end{pmatrix},\qquad \Phi\left(\begin{pmatrix}1&-1\\1&1\end{pmatrix}\right)=\begin{pmatrix}1&-1\\-\sqrt{-2}&-1+\sqrt{-2}\end{pmatrix}.$$

Here, $\begin{pmatrix}-1&1\\-1&0\end{pmatrix}$ and $\begin{pmatrix}1&-1\\1&1\end{pmatrix}$ are generators of $\mathrm{GL}_2(\mathbb{F}_3)$, and the assignment Φ defines the homomorphism from $\mathrm{GL}_2(\mathbb{F}_3)$ to $\mathrm{GL}_2(\mathbb{Z}[\sqrt{-2}])\subset\mathrm{GL}_2(\mathbb{C})$. Note that Φ is injective, and that for the prime ideal $(1+\sqrt{-2})$ dividing 3 in $\mathbb{Z}[\sqrt{-2}]$, we have

$$\Phi(\sigma)\equiv\sigma\ (\mathrm{mod}\ (1+\sqrt{-2})) \tag{2.1}$$

for all $\sigma\in\mathrm{GL}_2(\mathbb{F}_3)$.

We know $|\mathrm{GL}_2(\mathbb{F}_3)|=48$, and hence $|\mathrm{PGL}_2(\mathbb{F}_3)|=24$. Since $\mathrm{PGL}_2(\mathbb{F}_3)$ acts on $\mathbb{P}^1(\mathbb{F}_3)$ faithfully, $\mathrm{PGL}_2(\mathbb{F}_3)$ is isomorphic to the symmetric group S_4, and hence $\mathrm{PSL}_2(\mathbb{F}_3)$ is isomorphic to the alternating group A_4.

2.2. Octahedral Galois representations

Let E be an elliptic curve over $\mathbb{Q}$ and Δ_E be the discriminant of E. Since $G_{\mathbb{Q}}$ acts on the $\mathbb{F}_3$-module $E[3]$ of rank 2 consisting of three-division points of E, we obtain a mod 3 Galois representation $\overline{\rho}_{E,3} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_3)$. Considering the Weil pairing, by class field theory, the determinant of $\overline{\rho}_{E,3}$ is regarded as the quadratic character $\left(\frac{-3}{\cdot}\right)$. Let L be the fixed field of the kernel of $\overline{\rho}_{E,3}$, which is the field generated over $\mathbb{Q}$ by coordinates of elements of $E[3]$. Throughout this paper, we consider the case when $\overline{\rho}_{E,3}$ is surjective, i.e. $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{F}_3)$. This situation occurs when the third division polynomial of E is irreducible over $\mathbb{Q}$ and Δ_E is not a cube (cf [9], Theorem 2.3). Then, we obtain an octahedral Galois representation

$$\rho_{E,3} := \Phi \circ \overline{\rho}_{E,3} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{C}). \tag{2.2}$$

For simplicity, we put $\rho := \rho_{E,3}$. Note that $\det\rho(c) = -1$ for the complex conjugation c. By Langlands-Tunnell's theorem, there exists a newform f of weight one such that $L(s, f) = L(s, \rho)$.

2.3. Main subfields of $L = \mathbb{Q}(E[3])$

Let Z be the center of $\mathrm{GL}_2(\mathbb{F}_3)$, i.e. $Z = \left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$, and let M be the subfield of L fixed by Z. As mentioned above, we have $\mathrm{Gal}(M/\mathbb{Q}) \cong \mathrm{PGL}_2(\mathbb{F}_3) \cong S_4$. The field M is generated by x-coordinates of points in $E[3]$. Since $\det\rho = \left(\frac{-3}{\cdot}\right)$, the field fixed by $\mathrm{SL}_2(\mathbb{F}_3)$ is the quadratic field $\mathbb{Q}(\sqrt{-3})$. Let V' be the normal subgroup of $\mathrm{PSL}_2(\mathbb{F}_3)$ such that $\mathrm{PSL}_2(\mathbb{F}_3)/V'$ is cyclic of order 3, and let V be the lifting of V' to $\mathrm{GL}_2(\mathbb{F}_3)$. If N is the field fixed by V, then $N/\mathbb{Q}$ is a Galois extension and we have $\mathrm{Gal}(N/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{F}_3)/V \cong S_3$. In fact, N is generated by $\sqrt{-3}$ and $\sqrt[3]{\Delta_E}$; $N = \mathbb{Q}(\sqrt{-3}, \sqrt[3]{\Delta_E})$ (cf. [10], p.305).

$$\begin{array}{ccc}
L & \qquad & \{1\} \\
| & & | \\
M & & Z \\
| & & | \\
N & & V \\
| & & | \\
\mathbb{Q}(\sqrt{-3}) & & \mathrm{SL}_2(\mathbb{F}_3) \\
| & & | \\
\mathbb{Q} & & \mathrm{GL}_2(\mathbb{F}_3)
\end{array}$$

3. Main results

Throughout, we assume the notation as in Section 2.

Since $\mathrm{Gal}(N/\mathbb{Q}) \cong S_3$ and S_3 has an embedding to $\mathrm{GL}_2(\mathbb{C})$ given by

$$(2\ 3) \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad (1\ 2\ 3) \mapsto \begin{pmatrix} \zeta_3 & 0 \\ 0 & \zeta_3^2 \end{pmatrix}, \qquad \zeta_3 = e^{2\pi i/3},$$

we obtain a dihedral Galois representation $\psi : \mathrm{Gal}(N/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{C})$. Let

$$h(\tau) = \sum_{n=1}^{\infty} c_n q^n, \qquad (q = e^{2\pi i \tau})$$

be the newform of weight one corresponding to ψ. Then, for primes p with $p \nmid 3\Delta_E$, the p-th Fourier coefficients of h are

$$c_p = \begin{cases} 2 & \text{if } p \text{ splits completely in } N \text{ and } p \equiv 1 \pmod 3, \\ -1 & \text{if } p \text{ does not split completely in } N \text{ and } p \equiv 1 \pmod 3, \\ 0 & \text{if } p \equiv 2 \pmod 3. \end{cases} \tag{3.1}$$

Moreover, let

$$g(\tau) = \sum_{n=1}^{\infty} b_n q^n$$

be the newform of weight 2 corresponding to the elliptic curve E.

Now we are ready to state our main theorem.

Theorem 3.1. *Let E be an elliptic curve over $\mathbb{Q}$. Suppose the mod 3 Galois representation $\overline{\rho}_{E,3}$ is surjective. Suppose $f(\tau) = \sum_{n=1}^{\infty} a_n q^n$ is the newform of weight one associated to the octahedral Galois representation ρ defined by (2.2). Then, for all primes p with $p \nmid 3\Delta_E$, we have*

$$a_p = \begin{cases} 0 & \text{if } b_p \equiv 0 \pmod 3, \\ 1 & \text{if } b_p \equiv 1 \pmod 3 \text{ and } c_p = -1, \\ -2 & \text{if } b_p \equiv 1 \pmod 3 \text{ and } c_p = 2, \\ -\sqrt{-2} & \text{if } b_p \equiv 1 \pmod 3 \text{ and } c_p = 0, \\ -1 & \text{if } b_p \equiv 2 \pmod 3 \text{ and } c_p = -1, \\ 2 & \text{if } b_p \equiv 2 \pmod 3 \text{ and } c_p = 2, \\ \sqrt{-2} & \text{if } b_p \equiv 2 \pmod 3 \text{ and } c_p = 0. \end{cases}$$

From this theorem, we obtain an explicit formula for Fourier coefficients a_p;

Corollary 3.2. *For all primes p with $p \nmid 3\Delta_E$, we have*

$$a_p = \left(\frac{-b_p}{3}\right)\left(c_p + \sqrt{(c_p+1)(c_p-2)}\right),$$

where $\left(\frac{\cdot}{3}\right)$ is the Legendre symbol and we take a branch of square root such that $\sqrt{1} = 1$.

Remark 3.3. By the theory of ring class fields, the newform h can be written as a linear combination of theta series of binary quadratic forms, cf. [1].

Example 3.4. Let E be the elliptic curve defined by $y^2 + y = x^3 - x^2$. Then $\Delta_E = -11, N = \mathbb{Q}(\sqrt{-3}, \sqrt[3]{11})$ and $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{F}_3)$. The newform $g(\tau)$ of weight 2 corresponding to E is $\eta(\tau)^2\eta(11\tau)^2$, where $\eta(\tau)$ is the Dedekind eta function: $\eta(\tau) = q^{1/24}\prod_{n=1}^{\infty}(1-q^n)$, and the newform $h(\tau)$ corresponding to $N/\mathbb{Q}$ is a linear combination of theta series of binary quadratic forms with discriminant $-3^3 \cdot 11^2$ (cf. [2], Illustration 17.31.);

$$\begin{aligned}
g(\tau) &= \eta(\tau)^2\eta(11\tau)^2 \\
&= q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 - 2q^9 - 2q^{10} + q^{11} - 2q^{12} + 4q^{13} \\
&\quad + 4q^{14} - q^{15} - 4q^{16} - 2q^{17} + 4q^{18} + 2q^{20} + 2q^{21} - 2q^{22} - q^{23} + \cdots, \\
h(\tau) &= \frac{1}{2}\left(\sum_{x,y\in\mathbb{Z}} q^{x^2+xy+817y^2} + \sum_{x,y\in\mathbb{Z}} q^{27x^2+27xy+37y^2} + 2\sum_{x,y\in\mathbb{Z}} q^{19x^2+xy+43y^2}\right. \\
&\quad - \sum_{x,y\in\mathbb{Z}} q^{27x^2+9xy+31y^2} - \sum_{x,y\in\mathbb{Z}} q^{7x^2+3xy+117y^2} \\
&\quad \left. - \sum_{x,y\in\mathbb{Z}} q^{9x^2+3xy+91y^2} - \sum_{x,y\in\mathbb{Z}} q^{13x^2+3xy+63y^2}\right) \\
&= q + q^4 - q^7 - q^{13} + q^{16} + 2q^{19} + q^{25} - q^{28} - q^{31} + 2q^{37} + 2q^{43} - q^{52} + \cdots.
\end{aligned}$$

From these q-expansions, we obtain $a_2 = -\sqrt{-2}$, $a_5 = -\sqrt{-2}$, $a_7 = 1$, $a_{13} = 1$, $a_{17} = -\sqrt{-2}$, $a_{23} = \sqrt{-2}$, ...

4. Proof of Theorem 3.1

Since the mod 3 representation $\overline{\rho}_{E,3}$ is isomorphic to the mod 3 reduction of 3-adic representation $\rho_3 : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}_3)$ coming from the 3-adic Tate module of E, the congruence (2.1) implies that $a_p \equiv b_p \pmod{(1+\sqrt{-2})}$ for all primes p with $p \nmid 3\Delta_E$. Therefore, by the character table of ϕ, we see that

$$\begin{aligned}
b_p \equiv 0 \pmod 3 &\iff a_p \equiv 0 \pmod{(1+\sqrt{-2})} \\
&\iff a_p = 0 \\
&\iff \mathrm{Frob}_{p,\rho} = C_u \text{ or } C_{w_0}, \\
b_p \equiv 1 \pmod 3 &\iff a_p \equiv 1 \pmod{(1+\sqrt{-2})} \\
&\iff a_p = 1, -2 \text{ or } -\sqrt{-2} \\
&\iff \mathrm{Frob}_{p,\rho} = C_v, C_t, \text{ or } C_{w_2}, \\
b_p \equiv 2 \pmod 3 &\iff a_p \equiv 2 \pmod{(1+\sqrt{-2})} \\
&\iff a_p = -1, 2 \text{ or } \sqrt{-2} \\
&\iff \mathrm{Frob}_{p,\rho} = C_{v_0}, C_e, \text{ or } C_{w_1},
\end{aligned} \tag{4.1}$$

where $\mathrm{Frob}_{p,\rho}$ denotes the image by ρ of the conjugacy class of the Frobenius automorphism of p. Since w_0, w_1 and w_2 are not in $\mathrm{SL}_2(\mathbb{F}_3)$, we have

$$\begin{aligned} p \equiv 2 \pmod 3 &\Longleftrightarrow \mathrm{Frob}_{p,\rho} = C_{w_0}, C_{w_1}, \text{ or } C_{w_2} \\ &\Longleftrightarrow c_p = 0. \end{aligned} \tag{4.2}$$

To prove our theorem, when $p \equiv 1 \pmod 3$, we need to study a condition to determine the conjugacy class $\mathrm{Frob}_{p,\rho}$.

For a subset S of $\mathrm{GL}_2(\mathbb{F}_3)$, denote the projective image in $\mathrm{PGL}_2(\mathbb{F}_3)$ by $\overline{S}$. The key lemma is the following;

Lemma 4.1. *If we put $H := C_u \cup Z$, then $V' = \overline{H}$, therefore $V = H$.*

Proof. By direct computation, we have

$$C_u = \left\{ \pm u = \pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \pm \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}, \pm \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \right\},$$

therefore

$$\overline{H} = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \right\}.$$

By direct computation again, we see that $\overline{H}$ is a subgroup of $\mathrm{PGL}_2(\mathbb{F}_3)$ and $\overline{H} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and since $\overline{H} \subset \mathrm{PSL}_2(\mathbb{F}_3) \cong A_4$, the lemma follows. ■

From this lemma and subsection 2.3, we see that p splits completely in N if and only if $\mathrm{Frob}_{p,\rho} = C_u, C_e$, or C_t. Therefore, from (3.1), (4.1) and (4.2), we have

$$\begin{aligned} a_p = 1 &\Longleftrightarrow b_p \equiv 1 \pmod 3 \text{ and } c_p = -1, \\ a_p = -2 &\Longleftrightarrow b_p \equiv 1 \pmod 3 \text{ and } c_p = 2, \\ a_p = -1 &\Longleftrightarrow b_p \equiv 2 \pmod 3 \text{ and } c_p = -1, \\ a_p = 2 &\Longleftrightarrow b_p \equiv 2 \pmod 3 \text{ and } c_p = 2. \end{aligned}$$

This completes the proof of the theorem.

References

[1] J. Antoniadis, *Diedergruppe und Reziprozitätsgesetz*, J. Reine Angew. Math. **377** (1987), 197–209.
[2] H. Cohn, *A classical invitation to algebraic numbers and class fields*, Springer-Verlag, New York-Heidelberg, 1978.
[3] T. Crespo, *Galois representations, embedding problems and modular forms*, Collectanea Math. **48** (1997), 63–83.
[4] L. Dornhoff, *Group representation theory, Part A*, New York, Dekker, 1971.
[5] C. Khare, *Remarks on mod p forms of weight one*, Internat. Math. Res. Notices (1997), no. 3, 127–133.

[6] C. Khare, J.P. Wintenberger, *Serre's modularity conjecture (I)*, Invent. Math. **178** (2009), 485–504.

[7] C. Khare, J.P. Wintenberger, *Serre's modularity conjecture (II)*, Invent. Math. **178** (2009), 505–586.

[8] R. Langlands, *Base change for* GL(2), Annals of Mathematics Studies **96**, Princeton University Press, 1980.

[9] A. Reverter, N. Vila, *Image of mod p Galois representations associated to elliptic curves*, Canad. Math. Bull. **44** (2001), no. 3, 313–322.

[10] J.P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259–331.

[11] J. Tunnell, *Artin's conjecture for representations of octahedral type*, Bull. Amer. Math. Soc. **5** (1981), no. 2, 173–175.

Address: Takeshi Ogasawara: Faculty of Mathematics, Kyushu University, 744 Motooka, Nishi-ku, Fukuoka, 819-0395, Japan.

E-mail: t-ogasawara@math.kyushu-u.ac.jp

Received: 24 May 2012