Sairaiji, F.
Osaka J. Math.
37 (2000), 789–799

ON CONGRUENCES BETWEEN THE COEFFICIENTS OF TWO L-SERIES WHICH ARE RELATED TO A HYPERELLIPTIC CURVE OVER Q

FUMIO SAIRAIJI

(Received February 1, 1999)

1. Introduction

Let $f(x)$ be a monic irreducible polynomial with rational integer coefficients and let p be a prime integer. Reducing the coefficients of $f(x)$ modulo p, we obtain the polynomial $f_p(x)$ with coefficients in $\mathbf{Z}/p\mathbf{Z}$. A rule of the factorization of $f_p(x)$ over $\mathbf{Z}/p\mathbf{Z}$ is called a reciprocity law for $f(x)$ (cf. Wyman [11]). For example, when $f(x)$ is of degree 2, a reciprocity law for $f(x)$ is given by the Legendre symbol (D_f/p) for the discriminant D_f of $f(x)$.

In the case that $f(x)$ is of degree 3, the minimal splitting field K of $f(x)$ over $\mathbf{Q}$ is the Galois extension generated by the coordinates of the two-division points of the elliptic curve $E : y^2 = f(x)$. A reciprocity law for $f(x)$ is given by the Legendre symbol (D_f/p) and the coefficients of the L-series of E over $\mathbf{Q}$, which is the Mellin transform of a modular form of weight two under the Taniyama-Shimura conjecture (the Wiles theorem). Furthermore, in the case that $f(x)$ is of degree 3 and $D_f < 0$, the inverse Mellin transform of the Artin L-function $L(\pi, K/\mathbf{Q}, s)$ attached to the two-dimensional irreducible representation π for the Galois group of K over $\mathbf{Q}$, is a modular form of weight one, by the Weil-Langlands theorem. Thus the Fourier coefficients of the modular form of weight one also gives a reciprocity law for $f(x)$.

In the latter case, we can associate two modular forms with E and the Galois extension generated by the coordinates of its two-division points. Koike [3] obtained congruences between the Fourier coefficients of two modular forms. His congruences describe the relation of the above two reciprocity laws. Naito [6] gave congruences between the coefficients of the L-series of E and those of an Artin L-series attached to the Galois extension generated by the coordinates of the three-division points of E.

In this paper we consider congruences modulo 2 between the coefficients of the L-series of the Jacobian variety of a hyperelliptic curve $y^2 = f(x)$ and those of an Artin L-series which is related to the Galois extension over $\mathbf{Q}$, generated by the coordinates of the two-division points of the same Jacobian variety.

Let $f(x)$ be a polynomial of degree n over $\mathbf{Q}$ with no multiple roots. Let C be a hyperelliptic curve defined by $y^2 = f(x)$. We denote by g the genus of C. We see that either $n = 2g + 1$ or $n = 2g + 2$ holds. We assume that $g \geq 1$ and C has at least one $\mathbf{Q}$-rational point. Then we can choose its Jacobian variety (J, φ) defined over $\mathbf{Q}$.

Let K be the Galois extension over $\mathbf{Q}$, generated by the coordinates of the two-division points of the Jacobian variety J and let G be its Galois group. We assume that $n \neq 1, 2, 4$. Then we can identify G with a suitable subgroup of the permutation group S_n of n letters (See Proposition 2.2). Let π be the restriction of the standard representation of S_n to G. Let ρ_2 be the 2-adic representation of the absolute Galois group of $\mathbf{Q}$ with respect to the 2-adic Tate module of J.

For each odd good prime p of J we put

$$\mathrm{P}_p(u) := \det(I_{n-1} - \pi(\sigma_{\mathfrak{p}})u) \tag{1.1}$$

and

$$\mathrm{Q}_p(u) := \det(I_{2g} - \rho_2(\sigma_{\mathfrak{P}})u), \tag{1.2}$$

where I_m is the unit matrix of size m, $\sigma_{\mathfrak{P}}$ is the Frobenius automorphism for a prime divisor $\mathfrak{P}$ in $\bar{\mathbf{Q}}$, and $\sigma_{\mathfrak{p}}$ is its restriction to K. Then $1/\mathrm{P}_p(p^{-s})$ (resp. $1/\mathrm{Q}_p(p^{-s})$) is the p-factor of Artin L-series $L(\pi, K/\mathbf{Q}, s)$ attached to π (resp. the L-series $L(J/\mathbf{Q}, s)$ of J).

Theorem. (i) *If n is odd and $n \neq 1$, the congruence* $\mathrm{P}_p(u) \equiv \mathrm{Q}_p(u) \bmod 2$ *holds for any odd good prime p of J.*
(ii) *If n is even and $n \neq 2, 4$, the congruence* $\mathrm{P}_p(u) \equiv (1-u)\mathrm{Q}_p(u) \bmod 2$ *holds for any odd good prime p of J.*

In the case of $n = 3$, the theorem is that of Koike [3]. Thus our theorem is a generalization of Koike's theorem.

The organization of this paper is as follows. In §2, we construct the reduction $\rho_{2,1}$ of the 2-adic representation ρ_2 modulo 2 by matrices in $\mathrm{GL}(2g, \mathbf{Z}/2\mathbf{Z})$. In §3, we construct the standard representation π^{st} of S_n by matrices in $\mathrm{GL}(n-1, \mathbf{Z})$. By comparing two representations $\rho_{2,1}$ and the restriction π of π^{st}, we prove our theorem in §4. In §5, we give some examples of a reciprocity law for $f(x)$ by using our theorem.

The author would like to express his sincere gratitude to Professor Y. Yamamoto for his valuable advice. The author also wishes to thank Professor H. Naito for his useful suggestion and his warmful encouragement.

2. The field of two-division points of the Jacobian variety of a hyperelliptic curve over Q

Let $f(x)$ be a polynomial over $\mathbf{Q}$ of degree n with no multiple roots and let C be a hyperelliptic curve of genus g defined by $y^2 = f(x)$. We see that either $n = 2g + 1$ or $2g + 2$ holds. When n is even, the hyperelliptic curve C has two points P_∞, P'_∞ at infinity. When n is odd, the hyperelliptic curve C has one point P_∞ at infinity, which is ramified and $\mathbf{Q}$-rational. In the latter case we put $P'_\infty := P_\infty$.

We assume that the hyperelliptic curve C has at least one $\mathbf{Q}$-rational point. Then we can assume that the Jacobian variety (J, φ) is defined over $\mathbf{Q}$.

Let $\mathrm{Pic}^0(C)$ be the divisor class group of C. The canonical mapping φ induces the isomorphism

$$\bar{\varphi} : \mathrm{Pic}^0(C) \to J : \sum P \mapsto \sum \varphi(P). \tag{2.1}$$

The point corresponding to a $\mathbf{Q}$-rational divisor class is $\mathbf{Q}$-rational.

Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be the roots of the equation $f(x) = 0$ and put $P_i := (\alpha_i, 0) \in C$ for $i = 1, 2, \ldots, n$. We see that

$$\mathrm{div}(x - \alpha_i) = 2P_i - P_\infty - P'_\infty \quad \text{for} \quad i = 1, 2, \ldots, n, \tag{2.2}$$

and

$$\mathrm{div}(y) = \begin{cases} P_1 + \cdots + P_{2g+1} - (2g+1)P_\infty & \text{if } n \text{ is odd,} \\ P_1 + \cdots + P_{2g+2} - (g+1)(P_\infty + P'_\infty) & \text{if } n \text{ is even.} \end{cases} \tag{2.3}$$

Let $J[2]$ be the group of two-division points of J. By the equation (2.2) we have that

$$\bar{\varphi}(P_i - P_{2g+1}) \in J[2] \quad \text{for} \quad i = 1, 2, \ldots, 2g. \tag{2.4}$$

Proposition 2.1. $\{\bar{\varphi}(\mathrm{P}_i - \mathrm{P}_{2g+1})\}_{i=1}^{2g}$ *is a basis of* $J[2]$.

For a divisor D on C, we define the set $L(D)$ of rational functions on C over $\bar{\mathbf{Q}}$ by

$$L(D) := \{h : \text{a rational function on } C \mid \mathrm{div}(h) + D \text{ is effective.}\} \cup \{0\}. \tag{2.5}$$

$L(D)$ is a vector space over $\bar{\mathbf{Q}}$.

Proof. Since $J[2]$ is a $\mathbf{Z}/2\mathbf{Z}$-module of rank $2g$, it is enough to show that $\bar{\varphi}(\mathrm{P}_i - \mathrm{P}_{2g+1})$ $(i = 1, 2, \ldots, 2g)$ are linearly independent. Suppose

$$\sum_{i=1}^{2g} a_i \; \bar{\varphi}(P_i - P_{2g+1}) = 0 \quad \text{for} \quad a_1, \ldots, a_{2g} \in \{0, 1\}. \tag{2.6}$$

Then there exists a rational function h on C such that

$$\mathrm{div}(h) = \sum_{i=1}^{2g} a_i(P_i - P_{2g+1}). \tag{2.7}$$

We put $a_{2g+1} := a_1+\cdots+a_{2g}$. For the largest integer m less than or equal to $(a_{2g+1}+1)/2$, we put $h_1 := (x-\alpha_{2g+1})^m h$. We have

$$\operatorname{div}(h_1) = \sum_{i=1}^{2g} a_i P_i + (2m - a_{2g+1})P_{2g+1} - m(P_\infty + P'_\infty). \tag{2.8}$$

Since $a_{2g+1} = \sum_{i=1}^{2g+1} a_i \le 2g$, $m \le g$. Thus h_1 is contained in $L(g(P_\infty + P'_\infty))$. By the Riemann-Roch theorem, h_1 is a linear combination of $1, x, \dots, x^g$. Together with the fact P_i is ramified for $i = 1, \dots, 2g+1$, the order of h_1 at P_i is even for $i = 1, \dots, 2g+1$. Since $a_1, \dots, a_{2g} = 0, 1$, we have $a_1, \dots, a_{2g} = 0$. Thus $a_{2g+1} = a_1 + \cdots + a_{2g} = 0$. This completes the proof. □

Let K be the Galois extension over $\mathbf{Q}$ generated by the coordinates of the points of $J[2]$. Since φ is a rational function defined over $\mathbf{Q}$, $\varphi(P_i)$ is defined over $\mathbf{Q}(\alpha_i)$ for each i. We note that the addition on J are also defined over $\mathbf{Q}$. Thus the point $\bar{\varphi}(P_i - P_{2g+1}) = \varphi(P_i) - \varphi(P_{2g+1})$ is defined over $\mathbf{Q}(\alpha_i, \alpha_{2g+1})$. Hence K is a subfield of the minimal splitting field $\mathbf{Q}(f) = \mathbf{Q}(\alpha_1, \dots, \alpha_n)$ of f over $\mathbf{Q}$.

Proposition 2.2. (i) *If $n \ne 1, 2, 4$, then $K = \mathbf{Q}(f)$.*
(ii) *If $n = 4$, then K is the minimal splitting field of the decomposition cubic of f over $\mathbf{Q}$.*

For the proof of Proposition 2.2, we need the following two lemmas.

Lemma 2.3. *Assume that $n \ne 1, 2, 4$. If $\bar{\varphi}(P_i - P_j) = \bar{\varphi}(P_k - P_l)$ for $i \ne j$ and $k \ne l$, then $\{P_i, P_j\} = \{P_k, P_l\}$.*

Proof. Assume that $n = 3$. Then $g = 1$. We have

$$\bar{\varphi}(P_1 - P_2) = \bar{\varphi}(P_1 - P_3) + \bar{\varphi}(P_2 - P_3). \tag{2.9}$$

Since it follows from Proposition 2.1 that

$$\bar{\varphi}(P_1 - P_3),\ \bar{\varphi}(P_2 - P_3),\ \bar{\varphi}(P_1 - P_2) \tag{2.10}$$

are distinct, our assertion follows in this case.

We assume that $n \ge 5$. Then $g \ge 2$. Suppose that $\bar{\varphi}(P_i - P_j) = \bar{\varphi}(P_k - P_l)$. Then there exists a function h satisfying $\operatorname{div}(h) = P_i + P_j + P_k + P_l - 2(P_\infty + P'_\infty)$. Thus h is contained in $L(2(P_\infty + P'_\infty))$, which is spanned by $1, x, x^2$ by the Riemann-Roch theorem, and h has zero at P_i and P_j. Since $i \ne j$, h is equal to $(x-\alpha_i)(x-\alpha_j)$ up to a constant, that is, $\operatorname{div}(h) = 2P_i + 2P_j - 2(P_\infty + P'_\infty)$. Thus we have that $\{P_i, P_j\} = \{P_k, P_l\}$. □

Lemma 2.4. *When* $n = 4$,

$$\bar{\varphi}(P_1 - P_3) = \bar{\varphi}(P_2 - P_4), \ \bar{\varphi}(P_2 - P_3) = \bar{\varphi}(P_1 - P_4), \tag{2.11}$$

and

$$\bar{\varphi}(P_1 - P_3) + \bar{\varphi}(P_2 - P_3) = \bar{\varphi}(P_1 - P_2) = \bar{\varphi}(P_3 - P_4). \tag{2.12}$$

Proof. These equations follow from (2.2) and (2.3). □

Proof of Proposition 2.2. (i) Let σ be an element of the Galois group of $\mathbf{Q}(f)$ over $\mathbf{Q}$. Suppose that σ fixes all elements in K. Then $\sigma\bar{\varphi}(P_i - P_{2g+1}) = \bar{\varphi}(\sigma(P_i) - \sigma(P_{2g+1})) = \bar{\varphi}(P_i - P_{2g+1})$ for $i = 1, \dots, 2g$. By Lemma 2.3, we have that $\{\sigma(P_i), \sigma(P_{2g+1})\} = \{P_i, P_{2g+1}\}$ for $i = 1, \dots, 2g$. Thus we have $\sigma(P_i) = P_i$, that is, $\sigma(\alpha_i) = \alpha_i$ for $i = 1, 2, \dots, 2g+1$. Hence σ is the identity element. Thus our assertion (i) follows.
(ii) Suppose that $\sigma\bar{\varphi}(P_i - P_3) = \bar{\varphi}(P_i - P_3)$ for $i = 1, 2$. By Lemma 2.4 we have that $\{\sigma(P_i), \sigma(P_3)\} = \{P_i, P_3\}$, or $\{P_{3-i}, P_4\}$ for $i = 1, 2$. Equivalently, σ fixes $(\alpha_1+\alpha_3)(\alpha_2+\alpha_4)$, $(\alpha_2+\alpha_3)(\alpha_1+\alpha_4)$, and $(\alpha_1+\alpha_2)(\alpha_3+\alpha_4)$, Since these 3 elements are all roots of the decomposition cubic of f over $\mathbf{Q}$, K is its minimal splitting field. □

In the following we always assume $n \neq 1, 2, 4$. Let S_n be the permutation group of n letters $\{1, 2, \dots, n\}$. The group S_n acts on the set $\{\alpha_i\}_{i=1}^n$ of the roots of $f(x) = 0$ by

$$\sigma\alpha_i = \alpha_{\sigma(i)} \text{ for } i = 1, 2, \dots, n. \tag{2.13}$$

The group S_n acts on $J[2]$ from the left hand side by

$$\sigma\bar{\varphi}(P_i - P_{2g+1}) = \bar{\varphi}(P_{\sigma(i)} - P_{\sigma(2g+1)}) \text{ for } i = 1, 2, \dots, 2g. \tag{2.14}$$

We take a basis $\{w_i\}_{i=1}^{2g}$ as follows:

$$w_i := \bar{\varphi}(P_i - P_{2g+1}) \ (1 \leq i \leq 2g). \tag{2.15}$$

For $i = 1, 2, \dots, n$, let $\sigma_j := (j, 2g+1)$ be the transposition.

Proposition 2.5. (i) *When* $n = 2g+1$ *and* $n \neq 1$,

$$\sigma_j w_i = \begin{cases} w_i & \text{if either } j = 2g+1 \text{ or } i = j, \\ w_i + w_j & \text{if } j \neq 2g+1 \text{ and } i \neq j. \end{cases} \tag{2.16}$$

(ii) *When $n = 2g+2$ and $n \neq 2,4$,*

$$\sigma_j w_i = \begin{cases} w_i & \text{if } j = 2g+1, \\ & \text{or if } j \neq 2g+1, 2g+2, \text{ and } i = j, \\ w_i + w_j & \text{if } j \neq 2g+1, 2g+2 \text{ and } i \neq j, \\ w_1 + w_2 + \cdots + w_{2g} + w_i & \text{if } j = 2g+2. \end{cases} \tag{2.17}$$

Let G be the Galois group of K over $\mathbf{Q}$. By Proposition 2.2, for any element $\sigma \in G$, there exists the unique element τ in S_n such that

$$\sigma(\alpha_1, \alpha_2, \ldots, \alpha_n) = (\alpha_{\tau(1)}, \alpha_{\tau(2)}, \ldots, \alpha_{\tau(n)}). \tag{2.18}$$

We can identify G with a suitable subgroup of S_n through the inclusion $G \to S_n : \sigma \mapsto \tau$.

We define the representation $\rho_{2,1} : G \to \mathrm{GL}(2g, \mathbf{Z}/2\mathbf{Z})$ by

$$\sigma(w_1, w_2, \ldots, w_{2g}) = (w_1, w_2, \ldots, w_{2g})\rho_{2,1}(\sigma) \text{ for } \sigma \in G. \tag{2.19}$$

The representation $\rho_{2,1}$ is the restriction to G of the representation of S_n defined by (2.14).

Let $T_2(J)$ be the 2-adic Tate module of J. $T_2(J)$ is a free $\mathbf{Z}_2$-module of rank $2g$, where $\mathbf{Z}_2$ is the 2-adic integer ring. Taking a basis $T_2(J)$, we get a representation ρ_2 of the absolute Galois group $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ of $\mathbf{Q}$ by matrices in $\mathrm{GL}(2g, \mathbf{Z}_2)$. We can take a basis of $T_2(J)$ satisfying

$$\rho_{2,1}(\sigma') \equiv \rho_2(\sigma) \bmod 2 \text{ for all } \sigma \in \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}), \tag{2.20}$$

where σ' is the restriction of σ to K. We call the representation ρ_2 is the *2-adic representation of* $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ *with respect to* $T_2(J)$ and we call the representation $\rho_{2,1}$ the *reduction modulo* 2 *of* ρ_2.

3. Standard representation of S_n

Let S_n be the permutation group of n letters $\{1, 2, \ldots, n\}$. Let V^{pr} be an n-dimensional vector space over $\mathbf{Q}$ with basis $\{\varepsilon_i\}_{i=1}^n$. The group S_n acts on the vector space V^{pr} from the left hand side by

$$\sigma\varepsilon_i := \varepsilon_{\sigma(i)} \text{ for } i = 1, 2, \ldots, n, \text{ and } \sigma \in S_n. \tag{3.1}$$

The vector space V^{pr} is called the *permutation representation* of S_n. The permutation representation V^{pr} of S_n is decomposed into the direct sum of two irreducible representations of S_n. Namely, the 1-dimensional subspace V^{tr} spanned by $\varepsilon_1 + \cdots + \varepsilon_n$ and the $(n-1)$-dimensional subspace V^{st} with basis $\{\varepsilon_i - \varepsilon_n\}_{i=1}^{n-1}$. The representations V^{tr}

and V^{st} are called the *trivial representation* and the *standard representation*, respectively.

In this section, we investigate the standard representation V^{st} of S_n. As a matter of convenience, we denote by g the largest integer less than or equal to $(n-1)/2$. Then either $n = 2g+1$ or $n = 2g+2$ holds.

We take a basis $\{v_i\}_{i=1}^{n-1}$ of V^{st} as follows:

When $n = 2g+1$,

$$v_i := \varepsilon_i - \varepsilon_{2g+1} \ \text{ if } 1 \le i \le 2g; \tag{3.2}$$

When $n = 2g+2$,

$$v_i := \begin{cases} \varepsilon_i - \varepsilon_{2g+1} & \text{if } 1 \le i \le 2g, \\ \varepsilon_1 - \varepsilon_2 + \varepsilon_3 - \varepsilon_4 + \cdots + \varepsilon_{2g+1} - \varepsilon_{2g+2} & \text{if } i = 2g+1. \end{cases} \tag{3.3}$$

We define the matrix representation π^{st} of S_n by

$$\sigma(v_1, v_2, \ldots, v_{n-1}) = (v_1, v_2, \ldots, v_{n-1})\pi^{st}(\sigma). \tag{3.4}$$

For $j = 1, 2, \ldots, n$, let $\sigma_j := (j, 2g+1)$ be the transposition in S_n.

Proposition 3.1. (i) *When $n = 2g+1$, we have*

$$\sigma_j v_i = \begin{cases} v_i & \textit{if } j = 2g+1, \\ -v_i & \textit{if } i = j \textit{ and } j \ne 2g+1, \\ v_i - v_j & \textit{if } i \ne j \textit{ and } j \ne 2g+1. \end{cases} \tag{3.5}$$

(ii) *When $n = 2g+2$, we have*

$$\sigma_j v_i = \begin{cases} v_i & \textit{if } j = 2g+1, \\ -v_i & \textit{if } i \ne 2g+1,\ j \ne 2g+1,\ 2g+2 \\ & \qquad \textit{and } i = j, \\ v_i - v_j & \textit{if } i \ne 2g+1,\ j \ne 2g+1,\ 2g+2 \\ & \qquad \textit{and } i \ne j, \\ \displaystyle\sum_{m=1}^{2g}(-1)^m v_m + v_i + v_{2g+1} & \textit{if } i \ne 2g+1 \textit{ and } j = 2g+2, \\ v_{2g+1} & \textit{if } i = 2g+1 \textit{ and } j \textit{ is odd}, \\ v_{2g+1} + 2v_j & \textit{if } i = 2g+1 \textit{ and } j \ne 2g+2 \textit{ is even}, \\ -v_{2g+1} + 2\displaystyle\sum_{m=1}^{2g}(-1)^{m-1} v_m & \textit{if } i = 2g+1 \textit{ and } j = 2g+2. \end{cases} \tag{3.6}$$

Since σ_j's generate S_n, it follows from Proposition 3.1 that $\pi^{st}(\sigma)$ is a matrix in $\mathrm{GL}(n-1,\mathbf{Z})$. Thus we can consider the reduction of the representation π^{st} modulo 2.

Proposition 3.2. (i) *When $n = 2g+1$, we have*

$$\sigma_j v_i \equiv \begin{cases} v_i & \bmod 2 \text{ if either } j = 2g+1 \text{ or } i = j, \\ v_i + v_j & \bmod 2 \text{ if } i \neq j \text{ and } j \neq 2g+1. \end{cases} \tag{3.7}$$

(ii) *When $n = 2g+2$,*

$$\sigma_j v_i \equiv \begin{cases} v_i & \bmod 2 \text{ if } i \neq 2g+1,\ j = 2g+1, \\ & \qquad \text{or if } i \neq 2g+1,\ i = j, \\ v_i + v_j & \bmod 2 \text{ if } i \neq 2g+1,\ j \neq 2g+1,\ 2g+2, \\ & \qquad \text{and } i \neq j, \\ \displaystyle\sum_{m=1}^{2g} v_m + v_i + v_{2g+1} & \bmod 2 \text{ if } i \neq 2g+1 \text{ and } j = 2g+2, \\ v_{2g+1} & \bmod 2 \text{ if } i = 2g+1. \end{cases} \tag{3.8}$$

Proof. Proposition 3.2 follows from (3.5) and (3.6). □

The conjugate classes of S_n correspond to partitions of n bijectively. We call an element σ in S_n of *type* $(n_1, n_2, \dots, n_r)$ if σ belongs to the conjugacy class corresponding to the partition $(n_1, n_2, \dots, n_r)$. The following is well-known.

Proposition 3.3. *Let σ be an element in S_n of type $(n_1, n_2, \dots, n_r)$. Then the characteristic polynomial of σ in S_n for π^{st} is given by*

$$\det(\mathrm{I}_{n-1} - \pi^{st}(\sigma)u) = \frac{1}{1-u} \prod_{i=1}^{r} (1 - u^{n_i}), \tag{3.9}$$

where I_{n-1} is the unit matrix of size $n-1$

Proof. We note that $V^{pr} = V^{st} \oplus V^{tr}$. Our assertion follows from direct computations. □

4. Proof of Theorem

Let the notation be the same as in §1. We note that any odd good prime is unramified in K.

Let $\rho_{2,1} : G \to \mathrm{GL}(2g, \mathbf{Z}/2\mathbf{Z})$ be the representation defined by (2.19). It follows from (2.20) that

$$\mathrm{Q}_p(u) = \det(I_{2g} - \rho_2(\sigma_{\mathfrak{P}})u) \equiv \det(I_{2g} - \rho_{2,1}(\sigma_{\mathfrak{p}})u) \mod 2. \tag{4.1}$$

We can take $\pi^{st} : S_n \to \mathrm{GL}(n-1, \mathbf{Z})$ defined by (3.4) in §4 as the standard representation of S_n. Compared with (2.16), (2.17) and (3.7), (3.8), we have

$$\pi(\sigma) \equiv \rho_{2,1}(\sigma) \quad \left(\text{resp. } \pi(\sigma) \equiv \begin{pmatrix} \rho_{2,1}(\sigma) & 0 \\ * & 1 \end{pmatrix}\right) \mod 2 \qquad \text{for all } \sigma \in G, \tag{4.2}$$

if n is odd and $n \neq 1$ (resp. if n is even and $n \neq 2, 4$). Thus we have

$$\mathrm{P}_p(u) \equiv \mathrm{Q}_p(u) \ (\text{resp. } \mathrm{P}_p(u) \equiv (1-u)\mathrm{Q}_p(u)) \mod 2. \tag{4.3}$$

5. Numerical examples

Let the notation be the same as in §1. We assume that $f(x)$ is a monic polynomial with rational integer coefficients. We denote by $f_p(x)$ the reduction of $f(x)$ modulo p. The type of the factorization of $f_p(x)$ corresponds to that of the conjugate class of the Frobenius automorphism $\sigma_{\mathfrak{p}}$. By Proposition 3.3 and by our Theorem, we have:

Proposition 5.1. (i) *If $f_p(x) = g_1(x)g_2(x)\cdots g_r(x)$ in $\mathbf{Z}/p\mathbf{Z}[x]$ for some irreducible polynomials $g_i(x)$ of degree n_i, then*

$$\mathrm{Q}_p(u) \equiv \frac{1}{(1-u)^{\varepsilon}} \prod_{i=1}^{r} (1-u^{n_i}) \mod 2, \tag{5.1}$$

where $\varepsilon = 1$ (resp. $\varepsilon = 2$) if n is odd and $n \neq 1$ (resp. if n is even and $n \neq 2, 4$).
(ii) *The signature of $\sigma_{\mathfrak{p}}$ in S_n is equal to the Legendre symbol (D_f/p).*

In the following we give three examples, which describe the law of decomposition of primes in terms of $\mathrm{Q}_p(u) \mod 2$ and (D_f/p), in the case of $g = 2$. We note that an odd prime integer q is a good prime of J if q is prime to the discriminant D_f of $f(x)$.

EXAMPLE 1. We put $f(x) := x^5 - x - 1$. Then $D_f = 2869 = 19 \cdot 151$ and $G = S_5$ (cf. [4], p. 121). For any $p \neq 2, 19, 151$ we have the following:

$Q_p(u) \bmod 2$	$\left(\frac{2869}{p}\right)$	degrees of irreducible factors of f_p	example of p
$(1-u)^4$	1	1, 1, 1, 1, 1	1973, 3769, 5101
		1, 2, 2	67, 71
	-1	1, 1, 1, 2	163, 193, 227
		1, 4	23, 29, 31, 61, 97
$(1-u)^2(1+u+u^2)$	1	1, 1, 3	17, 41, 43, 47, 53
	-1	2, 3	7, 13, 37, 59, 73, 83
$1+u+u^2+u^3+u^4$	1	5	3, 5, 11, 79, 89

EXAMPLE 2. We put $f(x) := x^6-4x^5-12x^4+2x^3+8x^2+8x-7$. Then $D_f = 2^{12}29^5$ and the hyperelliptic curve C is the modular curve $X_0(29)$ (cf. [5]). We can check that the endomorphism algebra of J is $\mathbf{Q}(\sqrt{2})$. By choosing suitable indices of roots of f, $G = \langle(1,2,3)(4,5,6),\ (1,2)(4,5),\ (1,4)(2,5)(3,6)\rangle$, which is isomorphic to the dihedral group of order 12 (cf. [8]). For any $p \neq 2, 29$ we have the following:

$Q_p(u) \bmod 2$	$\left(\frac{29}{p}\right)$	degrees of irreducible factors of f_p	example of p
$(1-u)^4$	1	1, 1, 1, 1, 1, 1	173, 197, 277
		1, 1, 2, 2	7, 23, 59, 67, 71, 83
	-1	2, 2, 2	17, 19, 37, 41, 61, 73, 89, 97
$(1+u+u^2)^2$	1	3, 3	5, 13, 53
	-1	6	3, 11, 31, 43, 47, 79

In this example, by using the fact that K contains $\mathbf{Q}(\sqrt{-1})$, we can distinguish the first row and the second row by the Legendre symbol $(-1/p)$. And also the fourth row and the fifth row.

EXAMPLE 3. We put $f(x) := x^6-4x^5+6x^4-6x^3+9x^2-14x+9$. Then $D_f = 2^{12}67^2$ and the hyperelliptic curve C is the modular curve $X_0^*(67)$ (cf. [5]). Then we can checked that the endomorphism algebra of J is $\mathbf{Q}(\sqrt{5})$. By choosing suitable indices of roots of f, $G = \langle(1,2,6)(3,5,4),\ (1,2,3,4,5),\ (2,5)(3,4)\rangle$, which is isomorphic to the alternative group of degree 5 (cf. [8]). For any $p \neq 2, 67$ we have the following:

$Q_p(u) \bmod 2$	degrees of irreducible factors of f_p	example of p
$(1-u)^4$	1, 1, 1, 1, 1, 1	311, 1163, 1453
	1, 1, 2, 2	17, 59, 73
$(1+u+u^2)^2$	3, 3	5, 11, 23
$1+u+u^2+u^3+u^4$	1, 5	3, 7, 13

In Example 2 and in Example 3, there exist modular forms h_1, h_2 of weight two with respect to a congruence subgroup such that $L(J/\mathbf{Q}, s)$ and the product $L(h_1, s)L(h_2, s)$ of their Mellin transforms are essentially same as in Shimura's sense (cf. [7]). Thus by our theorem, we can consider congruences between the coefficients of the Artin L-series $L(\pi, K/\mathbf{Q}, s)$ and the Fourier coefficients of the modular forms h_1, h_2 of weight two in those examples.

References

[1] P. Deligne and J. -P. Serre: *Formes modulaires de poids* 1, Ann. Sci. E.N.S. **4** (1974), 507–530.
[2] W. Fulton and J. Harris: Representation theory, Springer-Verlag, New-York, 1991.
[3] M. Koike: *Higher reciprocity law, modular forms of weight 1 and elliptic curves*, Nagoya Math. J. **98** (1985), 109–115.
[4] S. Lang: Algebraic Number Theory, Springer-Verlag, 1986.
[5] N. Murabayashi: *On normal forms of modular curves of genus* 2, Osaka J. Math. **29** (1992), 405–418.
[6] H. Naito: *A congruence between the coefficients of the L-series which are related to an elliptic curve and algebraic number field generated by its* 3*-division points*, Mem. Fac. Edu. Kagawa Univ. **37** (1987), 43–45.
[7] G. Shimura: Introduction to the arithmetic theory of automorphic functions, Iwanami Shoten, Publishers and Princeton Univ. Press, Tokyo, 1971.
[8] R.P. Stauduhar: *The determination of Galois groups*, Math. Comp. **124** (1973), 981–996.
[9] A. Weil: Variété abéliennes et courbes algébriques, Hermann, Paris, 1948.
[10] A. Wiles: *Modular elliptic curves and Fermat's Last Theorem*, Ann. of Math. **141** (1995), 443–551.
[11] B.F. Wyman: *What is a reciprocity law?*, Amer. Math. Monthly, **79** (1972), 571–586.

Department of Mathematics
Graduate School of Science
Osaka University
Toyonaka, Osaka 560-0043, Japan
e-mail: sairaiji@mathsun01.math.sci.osaka-u.ac.jp