

## Rédei's Triple Symbols and Modular Forms

Fumiya AMANO, Hisatoshi KODANI, Masanori MORISHITA,  
Takayuki SAKAMOTO and Takafumi YOSHIDA

with Appendix by Takeshi OGASAWARA

*Kyushu University*

(Communicated by M. Kurihara)

**Abstract.** In 1939, L. Rédei introduced a certain triple symbol in order to generalize the Legendre symbol and Gauss' genus theory. Rédei's triple symbol  $[a_1, a_2, p]$  describes the decomposition law of a prime number  $p$  in a certain dihedral extension over  $\mathbf{Q}$  of degree 8 determined by  $a_1$  and  $a_2$ . In this paper, we show that the triple symbol  $[-p_1, p_2, p_3]$  for certain prime numbers  $p_1, p_2$  and  $p_3$  can be expressed as a Fourier coefficient of a modular form of weight one. For this, we employ Hecke's theory on theta series associated to binary quadratic forms and realize an explicit version of the theorem by Weil-Langlands and Deligne-Serre for Rédei's dihedral extensions. A reciprocity law for the Rédei triple symbols yields certain reciprocal relations among Fourier coefficients.

### Introduction

As is well known, the Legendre symbol  $\left(\frac{a}{p}\right)$  describes the decomposition law of a prime number  $p$  in the quadratic extension  $\mathbf{Q}(\sqrt{a})/\mathbf{Q}$ . We may note that  $\left(\frac{a}{p}\right)$  is seen as a Dirichlet character, an "abelian modular form" on  $\mathrm{GL}_1$  over  $\mathbf{Q}$ .

In 1939, L. Rédei ([RÉ]) introduced a certain triple symbol with the intension of a generalization of the Legendre symbol and Gauss' genus theory ([G]). Rédei's triple symbol  $[a_1, a_2, p]$  describes the decomposition law of a prime number  $p$  in a certain dihedral extension over  $\mathbf{Q}$  of degree 8 determined by  $a_1$  and  $a_2$ . In this paper, we show that the triple symbol  $[-p_1, p_2, p_3]$  for certain prime numbers  $p_1, p_2$  and  $p_3$  can be expressed as a Fourier coefficient of a modular form on  $\mathrm{GL}_2$  over  $\mathbf{Q}$  of weight one. For this, we employ Hecke's theory on theta series associated to ideal classes (binary quadratic forms) of the imaginary quadratic field  $\mathbf{Q}(\sqrt{-p_1 p_2})$  ([H]) and realize an explicit and constructive version of the theorem by Weil-Langlands and Deligne-Serre ([Se]). A reciprocity law for the Rédei triple symbol yields certain reciprocal relations among Fourier coefficients.

The Rédei triple symbol may be interpreted as an arithmetic analog of Milnor's triple linking number just as the Legendre symbol is an arithmetic linking number ([Mo]). It is known that there are analytic expressions for Milnor's higher linking numbers (for example,

---

Received June 19, 2012; revised March 5, 2013

2010 *Mathematics Subject Classification*: 11R (Primary), 11F (Secondary)

[Ro]). It was our motivation to get an analytic expression for the Rédei triple symbol. We hope to come back to this problem together with the real quadratic case in the future.

ACKNOWLEDGEMENT. We would like to thank Takuya Konno and C. S. Rajan for useful discussions, and Masanari Kida, Jens Funke and the referee for helpful comments on our preprint. We also thank Dr. Takeshi Ogasawara for explaining to us his result on theta and eta functions. The third author was partially supported by Grants-in-Aids for Scientific Research (B), No. 24340005, Japan Society for the Promotion of Science.

NOTATION. For a number field  $k$  we denote by  $\mathcal{O}_k$  the ring of integers of  $k$ .

### 1. Rédei's dihedral extensions and triple symbols

In this section, we recall the construction of Rédei's dihedral extension over  $\mathbf{Q}$  ([Ré]) for a certain case and give its arithmetic characterization ([Am]). We then introduce the Rédei triple symbol and show a reciprocity law.

Let  $p_1$  and  $p_2$  be distinct primes number satisfying the condition

$$(1.1) \quad p_1 \equiv 3 \pmod{4}, \quad p_2 \equiv 1 \pmod{4}, \quad \left(\frac{p_1}{p_2}\right) = \left(\frac{p_2}{p_1}\right) = 1.$$

We set

$$k_1 := \mathbf{Q}(\sqrt{-p_1}), \quad k_2 := \mathbf{Q}(\sqrt{p_2}) \quad \text{and} \quad k := \mathbf{Q}(\sqrt{-p_1 p_2}).$$

LEMMA 1.2. *There are integers  $x, y, z$  satisfying the following conditions:*

- (1)  $x^2 + p_1 y^2 - p_2 z^2 = 0$ ,
- (2)  $\text{g.c.d.}(x, y, z) = 1$ ,  $y \equiv 0 \pmod{2}$ ,  $x - y \equiv 1 \pmod{4}$ .

*Furthermore, for a given prime ideal  $\mathfrak{p}$  of  $\mathcal{O}_k$  lying over  $p_2$ , we can find integers  $x, y, z$  which satisfy (1), (2) and  $(x + y\sqrt{-p_1}) = \mathfrak{p}^m$  for an odd positive integer  $m$ .*

PROOF. Since  $\left(\frac{-p_1}{p_2}\right) = 1$ ,  $p_2$  is decomposed in  $k_1$ , say  $(p_2) = \mathfrak{p}\bar{\mathfrak{p}}$ . Since  $-p_1 \equiv 1 \pmod{4}$ , the class number, say  $h_1$ , of  $k_1$  is odd by genus theory ([O, 4.7]). Write  $\mathfrak{p}^{h_1} = (\alpha)$  for some  $\alpha = (a + b\sqrt{-p_1})/2$ ,  $a, b \in \mathbf{Z}$ ,  $a \equiv b \pmod{2}$ . Since  $N((\alpha)) = N\mathfrak{p}^{h_1} = p_2^{h_1}$ , we have  $N_{k_1/\mathbf{Q}}(\alpha) = p_2^{h_1} \cdots (\star)$ .

(i) The case  $p_1 \equiv -1 \pmod{8}$ : If  $a \equiv b \equiv 1 \pmod{2}$ ,  $a^2 \equiv b^2 \equiv 1 \pmod{8}$  and so  $a^2 + p_1 b^2 \equiv 0 \pmod{8}$ . Hence  $N_{k_1/\mathbf{Q}}(\alpha) = (a^2 + p_1 b^2)/4 \equiv 0 \pmod{2}$ , which contradicts  $(\star)$ . Therefore we have  $a \equiv b \equiv 0 \pmod{2}$ . Put  $x = a/2$ ,  $y = b/2 \in \mathbf{Z}$ . By  $(\star)$ ,  $N_{k_1/\mathbf{Q}}(\alpha) = x^2 + p_1 y^2 = p_2 z^2$ ,  $z = p_2^{(h_1-1)/2}$ . Therefore  $x^2 + 3y^2 \equiv 1 \pmod{4}$  which yields  $x \equiv 1 \pmod{2}$ ,  $y \equiv 0 \pmod{2}$  and so  $(x, y, z) = 1$ . We can take a suitable sign of  $x$  if necessary so that  $x - y \equiv 1 \pmod{4}$ .

(ii) The case  $p_1 \equiv 3 \pmod 8$ : If  $a \equiv b \equiv 0 \pmod 2$ , we can find  $x, y, z \in \mathbf{Z}$  satisfying (1) and (2) as in the case (i). Now assume that  $a \equiv b \equiv 1 \pmod 2$ . Then we have  $a^2 - 3b^2p_1 \equiv 3a^2 - b^2p_1 \equiv 0 \pmod 8$  and so

$$\alpha^3 = \left( \frac{a + b\sqrt{-p_1}}{2} \right)^3 = \frac{a(a^2 - 3b^2p_1) + b(3a^2 - b^2p_1)\sqrt{-p_1}}{8} = x + y\sqrt{-p_1},$$

where we put  $x = a(a^2 - 3b^2p_1)/8$  and  $y = b(3a^2 - b^2p_1)/8$ . Therefore  $x^2 + p_1y^2 = N_{k_1/\mathbf{Q}}(\alpha^3) = p_2z^2$ ,  $z = p_2^{(3h_1-1)/2}$ . As in the case (i),  $x \equiv 1 \pmod 2$ ,  $y \equiv 0 \pmod 2$  and  $(x, y, z) = 1$ . We can take a suitable sign of  $x$  so that  $x - y \equiv 1 \pmod 4$ .

The latter assertion follows immediately from the above argument.  $\square$

Let  $\mathbf{a} = (x, y, z)$  be a triple of integers satisfying the conditions (1), (2) in Lemma 1.2. We then set

$$K_{\mathbf{a}} := \mathbf{Q}(\sqrt{-p_1}, \sqrt{p_2}, \sqrt{\alpha}), \quad \alpha := x + y\sqrt{-p_1}.$$

The following theorem is due to Rédei ([Ré]). Since Rédei's account was written in a rather classical style, we give here a proof for the sake of readers.

**THEOREM 1.3.** (1) *The extension  $K_{\mathbf{a}}/\mathbf{Q}$  is a Galois extension whose Galois group is the dihedral group  $D_8$  of order 8.*

(2) *All prime numbers ramified in  $K_{\mathbf{a}}/\mathbf{Q}$  are only  $p_1$  and  $p_2$  with ramification index 2.*

**PROOF.** (1) Let  $K_f$  be the splitting field over  $\mathbf{Q}$  of  $f(T) := T^4 - 2xT^2 + p_2z^2 = (T - \sqrt{\alpha})(T + \sqrt{\alpha})(T - \sqrt{\alpha})(T + \sqrt{\alpha}) \in \mathbf{Z}[T]$ , where  $\alpha := x - y\sqrt{-p_1}$ . Since  $\alpha^2 = x + y\sqrt{-p_1}$  and  $\sqrt{\alpha}\sqrt{\alpha} = z\sqrt{p_2}$ , we have  $K_{\mathbf{a}} = K_f$  and so  $K_{\mathbf{a}}$  is a Galois extension over  $\mathbf{Q}$ . Define  $s, t \in \text{Gal}(K_{\mathbf{a}}/\mathbf{Q})$  by

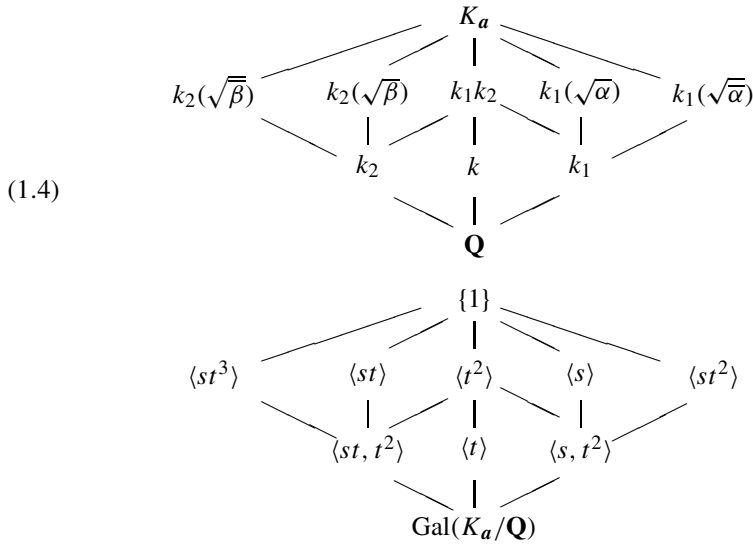
$$\begin{aligned} s(\sqrt{-p_1}) &= \sqrt{-p_1}, & s(\sqrt{p_2}) &= -\sqrt{p_2}, & s(\sqrt{\alpha}) &= \sqrt{\alpha}, \\ t(\sqrt{-p_1}) &= -\sqrt{-p_1}, & t(\sqrt{p_2}) &= -\sqrt{p_2}, & t(\sqrt{\alpha}) &= -\sqrt{\alpha}. \end{aligned}$$

Then we easily see that

$$s^2 = t^4 = 1, \quad sts = t^{-1}$$

and so  $s, t$  generate the dihedral group  $D_8$  of order 8. Since it is easy to see  $[K_{\mathbf{a}} : \mathbf{Q}] = 8$ , we conclude  $\text{Gal}(K_{\mathbf{a}}/\mathbf{Q}) = D_8$ .

Putting  $\beta := (\sqrt{\alpha} + \sqrt{\alpha})^2 = 2(x + z\sqrt{p_2})$ , all subfields of  $K_{\mathbf{a}}/\mathbf{Q}$  and the corresponding subgroups of  $\text{Gal}(K_{\mathbf{a}}/\mathbf{Q})$  are illustrated as follows.



(2) By the condition (1.1),  $p_i$  is the only ramified prime number in  $k_i/\mathbf{Q}$  ( $i = 1, 2$ ) and that  $p_1$  (resp.  $p_2$ ) splits in  $k_2/\mathbf{Q}$  (resp.  $k_1/\mathbf{Q}$ ). So, looking at the diagram (1.4), it suffices to show that the only one prime of  $k_1$  lying over  $p_2$  is ramified in  $k_1(\sqrt{\alpha})/k_1$ . First we note that  $\lambda := (1 + \sqrt{\alpha})/2 \in \mathcal{O}_{k_1(\sqrt{\alpha})}$ , since  $\lambda$  satisfies  $\lambda^2 + \lambda + (1 - \alpha)/4 = 0$  and  $(1 - \alpha)/4 \in \mathcal{O}_{k_1}$  by  $x - y \equiv 1 \pmod{4}$ . Since the relative discriminant of  $\lambda$  in  $k_1(\sqrt{\alpha})/k_1$  is

$$d(\lambda, k_1(\sqrt{\alpha})/k_1) = \begin{vmatrix} 1 & \lambda \\ 1 & \bar{\lambda} \end{vmatrix}^2 = \alpha,$$

where  $\bar{\lambda} := (1 - \sqrt{\alpha})/2$ , and  $(\alpha)$  is prime to 2, any prime of  $k_1$  lying over 2 is unramified in  $k_1(\sqrt{\alpha})/k_1$ . Next let

$$(\alpha) = \mathfrak{p}^e \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r}$$

be the decomposition of  $(\alpha)$  into the product of positive powers of distinct prime ideals  $\mathfrak{p}, \mathfrak{q}_1, \dots, \mathfrak{q}_r$  of  $\mathcal{O}_{k_1}$ . Since  $N_{k_1/\mathbf{Q}}(\alpha) = p_2 z^2$ , we can take  $\mathfrak{p}$  to be one of primes lying over  $p_2$  and  $e$  to be odd. We claim that all  $e_i$ 's are even. Suppose that there is an odd  $e_j$ . Let  $q_j$  be the prime number lying below  $\mathfrak{q}_j$ . If  $(q_j)$  splits to  $\mathfrak{q}_j \bar{\mathfrak{q}}_j$  in  $k_1$ , we have  $\alpha \in \bar{\mathfrak{q}}_j$  by  $N_{k_1/\mathbf{Q}}(\alpha) = p_2 z^2$ . Then  $\alpha, \bar{\alpha} \in \mathfrak{q}_j \bar{\mathfrak{q}}_j = (q_j)$  and so  $2x, 2y \in (q_j)$ . This contradicts  $(x, y, z) = 1$ . If  $q_j$  is inert in  $k_1/\mathbf{Q}$ ,  $\alpha, \bar{\alpha} \in (q_j)$  and so  $2x, 2y \in (q_j)$  again, which is a contradiction. If  $(q_j) = \mathfrak{q}_j^2$  in  $k_1$ ,  $q_j$  must be  $p_1$ . So  $N\mathfrak{q}_j^{e_j} = p_1^{e_j}$ , which contradicts  $N_{k_1/\mathbf{Q}}(\alpha) = p_2 z^2$ . Thus we have the decomposition

$$(\alpha) = \mathfrak{p}^e \mathfrak{a}^2, \quad (\mathfrak{p}, \mathfrak{a}) = 1, \quad e \text{ is odd.}$$

By the ramification theory in a Kummer extension ([F, Ch.4, Theorem 2.1, Lemma 2.1]),  $\mathfrak{p}$  is the unique prime ideal of  $\mathcal{O}_{k_1}$  which is ramified in  $k_1(\sqrt{\alpha})/k_1$ .  $\square$

The following theorem shows that the properties (1), (2) in Proposition 1.3 characterize Rédei's extension  $K_a/\mathbf{Q}$ .

**THEOREM 1.5.** *Let  $p_1$  and  $p_2$  be prime numbers satisfying the condition (1.1). Suppose that an extension  $K/\mathbf{Q}$  satisfies the following properties:*

- (1)  *$K/\mathbf{Q}$  is a Galois extension whose Galois group is the dihedral group  $D_8$  of order 8.*
- (2) *All prime numbers ramified in  $K/\mathbf{Q}$  are only  $p_1$  and  $p_2$  with ramification index 2. Then  $K$  is uniquely determined.*

**PROOF.** By the properties (1) and (2),  $K$  contains quadratic fields  $k_1, k_2$  and  $k$ , and  $K/k$  is an unramified cyclic extension of degree 4. Since the 2-primary part of the ideal class group of  $k$  is cyclic by genus theory ([O, 4.7]), the unramified cyclic extension  $K/k$  of degree 4 must be unique by class field theory. □

By Theorem 1.5, the extension  $K_a/\mathbf{Q}$  is independent of a choice of  $a$ .

**DEFINITION 1.6.** We denote  $K_a$  by  $K_{\{-p_1, p_2\}}$  the field and call  $K_{\{-p_1, p_2\}}$  the Rédei extension over  $\mathbf{Q}$  associated to prime numbers  $p_1$  and  $p_2$  satisfying the condition (1.1).

The following corollary will be used later. Let  $H_k$  denote the ideal class group of  $k$  with  $h_k := \#H_k$ , the class number of  $k$ , and let  $H_k(2)$  denote the 2-primary part of  $H_k$  with  $h_k(2) := \#H_k(2)$ , the 2-class number of  $k$ .

**COROLLARY 1.7.** *Notations being as above,*

- (1)  *$K_{\{-p_1, p_2\}}$  is an unramified cyclic extension over  $k$  of order 4.*
- (2)  *$H_k(2)$  is a cyclic group of order  $2^m$ ,  $m \geq 2$ .*
- (3) *Let  $\mathfrak{p}_i$  be the prime ideal of  $\mathcal{O}_k$  lying over  $p_i$ . Then the class  $[\mathfrak{p}_i]$  has order 2 in  $H_k$  for  $i = 1, 2$  and the Frobenius automorphism of  $\mathfrak{p}_i$  in  $K/k$  is given by*

$$\left(\frac{K/k}{\mathfrak{p}_i}\right) = \begin{cases} 1 & \text{if } h_k(2) \geq 8, \\ t^2 & \text{if } h_k(2) = 4. \end{cases}$$

**PROOF.** (1) and (2) were shown in the proof of Theorem 1.5. For (3), suppose that  $\mathfrak{p}_i = (x + y\omega)$  with  $x, y \in \mathbf{Z}$ ,  $\omega := (1 + \sqrt{-p_1 p_2})/2$ . Then we have  $(2x + y)^2 + p_1 p_2 y^2 = 4p_i$ . This never occurs. Hence  $[\mathfrak{p}_i]$  has order 2 and the Frobenius automorphism  $\left(\frac{K/k}{\mathfrak{p}_i}\right)$  is  $t^{h_k(2)/2}$  by class field theory. So the last assertion follows. □

Finally, we introduce the Rédei triple symbol and show a reciprocity law. Let  $p_1, p_2$  and  $p_3$  be distinct prime numbers satisfying the condition

$$(1.8) \quad p_1 \equiv 3 \pmod{4}, \quad p_i \equiv 1 \pmod{4} \ (i = 2, 3), \quad \left(\frac{p_i}{p_j}\right) = 1 \quad (1 \leq i \neq j \leq 3).$$

DEFINITION 1.9. We define the Rédei triple symbol by

$$[-p_1, p_2, p_3] := \begin{cases} 1 & \text{if } p_3 \text{ is completely decomposed in } K_{\{-p_1, p_2\}}/\mathbf{Q}, \\ -1 & \text{otherwise.} \end{cases}$$

Let  $\mathfrak{p}_2$  (resp.  $\mathfrak{p}_3$ ) be one of the prime ideals of  $k_1$  lying over  $p_2$  (resp.  $p_3$ ). Then there is a triple of integers  $(x_2, y_2, z_2)$  with  $\alpha_{12} = x_2 + y_2\sqrt{-p_1}$  (resp.  $(x_3, y_3, z_3)$  with  $\alpha_{13} = x_3 + y_3\sqrt{-p_1}$ ) satisfying the conditions (1), (2) in Lemma 1.1 with respect to the pair  $(p_1, p_2)$  (resp.  $(p_1, p_3)$ ) such that

$$(\alpha_{12}) = \mathfrak{p}_2^{m_2}, \quad (\alpha_{13}) = \mathfrak{p}_3^{m_3} \quad (m_2, m_3 \text{ being odd integers}), \\ K_{\{-p_1, p_2\}} = \mathbf{Q}(\sqrt{-p_1}, \sqrt{p_2}, \sqrt{\alpha_{12}}), \quad K_{\{-p_1, p_3\}} = \mathbf{Q}(\sqrt{-p_1}, \sqrt{p_3}, \sqrt{\alpha_{13}}).$$

Since  $\mathfrak{p}_3$  is unramified in  $k_1(\sqrt{\alpha_{12}})/k_1$  by Theorem 1.2 (2), we have the Frobenius automorphism  $\left(\frac{k_1(\sqrt{\alpha_{12}})/k_1}{\mathfrak{p}_3}\right) \in \text{Gal}(k_1(\sqrt{\alpha_{12}})/k_1)$ . We note that the Rédei triple symbol is rewritten as

$$(1.10) \quad [-p_1, p_2, p_3] = \begin{cases} 1 & \text{if } \left(\frac{k_1(\sqrt{\alpha_{12}})/k_1}{\mathfrak{p}_3}\right) = \text{id}_{k_1(\sqrt{\alpha_{12}})}, \\ -1 & \text{otherwise.} \end{cases}$$

For a prime  $\mathfrak{p}$  of  $k_1$ , we denote by  $\left(\frac{\cdot}{\mathfrak{p}}\right)$  the Hilbert symbol in the local field  $k_{1\mathfrak{p}}$  ( $:=$  the completion of  $k_1$  at  $\mathfrak{p}$ ), namely,

$$(a, k_{1\mathfrak{p}}(\sqrt{b})/k_{1\mathfrak{p}})\sqrt{b} = \left(\frac{a, b}{\mathfrak{p}}\right)\sqrt{b} \quad (a, b \in k_{1\mathfrak{p}}^\times),$$

where  $(\cdot, k_{1\mathfrak{p}}(\sqrt{b})/k_{1\mathfrak{p}}) : k_{1\mathfrak{p}}^\times \rightarrow \text{Gal}(k_{1\mathfrak{p}}(\sqrt{b})/k_{1\mathfrak{p}})$  is the norm residue symbol of local class field theory.

LEMMA 1.11. We have

$$[-p_1, p_2, p_3] = \left(\frac{\alpha_{12}, \alpha_{13}}{\mathfrak{p}_3}\right), \quad [-p_1, p_3, p_2] = \left(\frac{\alpha_{12}, \alpha_{13}}{\mathfrak{p}_2}\right).$$

PROOF. Let  $\pi$  be a prime element of  $k_{1\mathfrak{p}_3}$  and  $U_{\mathfrak{p}_3}$  denote the unit group in  $k_{1\mathfrak{p}_3}^\times$ . We write  $\alpha_{13} = u\pi^{m_3}$ ,  $u \in U_{\mathfrak{p}_3}$ . Noting that  $u, \alpha_{12} \in U_{\mathfrak{p}_3}$  and  $m_3$  is odd, we have

$$\begin{aligned} \left(\frac{\alpha_{12}, \alpha_{13}}{\mathfrak{p}_3}\right) &= \left(\frac{\alpha_{12}, \alpha_{13}}{\mathfrak{p}_3}\right) \\ &= \left(\frac{u, \alpha_{12}}{\mathfrak{p}_3}\right) \left(\frac{\pi^{m_3}, \alpha_{12}}{\mathfrak{p}_3}\right) \\ &= \left(\frac{\pi, \alpha_{12}}{\mathfrak{p}_3}\right) \end{aligned}$$

$$\begin{aligned} &= \frac{(\pi, k_{1p_3}(\sqrt{\alpha_{12}})/k_{1p_3})\sqrt{\alpha_{12}}}{\sqrt{\alpha_{12}}} \\ &= \left(\frac{k_1(\sqrt{\alpha_{12}})/k_1}{p_3}\right)(\sqrt{\alpha_{12}})/\sqrt{\alpha_{12}} \\ &= [-p_1, p_2, p_3] \quad ((1.10)). \end{aligned}$$

Similarly, we can show  $\left(\frac{\alpha_{12}, \alpha_{13}}{p_2}\right) = [-p_1, p_3, p_2]$ . □

Finally, we show a reciprocity law for the Rédei symbol.

**THEOREM 1.12.** *We have*

$$[-p_1, p_2, p_3] = [-p_1, p_3, p_2].$$

*In particular,  $p_3$  is completely decomposed in  $K_{\{-p_1, p_2\}}/\mathbf{Q}$  if and only if  $p_2$  is completely decomposed in  $K_{\{-p_1, p_3\}}/\mathbf{Q}$ .*

**PROOF.** By Lemma 1.11 and the product formula for the Hilbert symbol

$$\prod_p \left(\frac{\alpha_{12}, \alpha_{13}}{p}\right) = 1 \quad (p \text{ runs over all primes of } k_1),$$

we have only to prove

$$\prod_{p \neq p_2, p_3} \left(\frac{\alpha_{12}, \alpha_{13}}{p}\right) = 1.$$

If  $p$  is prime to 2 or  $\infty$  (the infinite prime of  $k_1$ ), we have

$$\left(\frac{\alpha_{12}, \alpha_{13}}{p}\right) = 1,$$

since  $\alpha_{12}, \alpha_{13} \in U_p$ . Since  $\infty$  is the complex prime, it is obvious that  $\left(\frac{\alpha_{12}, \alpha_{13}}{\infty}\right) = 1$ . Let  $\mathfrak{P}$  be a prime ideal of  $k_1$  lying over 2. Noting that 2 is unramified in  $k_1/\mathbf{Q}$  and that  $\alpha_{12}, \alpha_{13} \in 1 + \mathfrak{P}^2$  by the condition (2) of Lemma 1.2, we have  $\left(\frac{\alpha_{12}, \alpha_{13}}{\mathfrak{P}}\right) = 1$  ([Sa, Theorem 10.29]). This completes the proof. The latter assertion just follows from Definition (1.9). □

## 2. Galois representations and Artin $L$ -functions

In this section, we interpret the Rédei triple symbol in terms of a two dimensional Galois representation, and consider the associated Artin  $L$ -function to relate the triple symbol with modular forms in the subsequent sections. We keep the same notations as in Section 1.

Let  $p_1$  and  $p_2$  be prime numbers satisfying the condition (1.1), and let  $K_{\{-p_1, p_2\}}$  be the Rédei dihedral extension over  $\mathbf{Q}$  in Definition 1.6. In this section, we denote  $K_{\{-p_1, p_2\}}$  by  $K$  for simplicity.

We let

$$\rho : \text{Gal}(K/\mathbf{Q}) \longrightarrow \text{GL}(V(\rho)), \quad V(\rho) = \mathbf{C}^2$$

be the two dimensional complex representation of the Galois group  $\text{Gal}(K/\mathbf{Q}) = \langle s, t \mid s^2 = t^4 = 1, sts = t^{-1} \rangle$  defined by

$$(2.1) \quad \rho(s) = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \rho(t) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

We note that  $\rho$  is irreducible and odd ( $\det(\rho(\text{complex conjugate})) = -1$ ).

First, we have the following

LEMMA 2.2. *For a prime number  $p_3$  satisfying the condition (1.8), we have*

$$[-p_1, p_2, p_3] = \frac{1}{2} \text{tr}(\rho(\sigma_{\mathfrak{P}}))$$

where  $\sigma_{\mathfrak{P}}$  is the Frobenius automorphism of a prime  $\mathfrak{P}$  of  $K$  lying over  $p_3$ .

PROOF. The assertion follows immediately from (1.10) and  $\rho(t^2) = -I_2$ . □

Next, we consider the Artin  $L$ -function associated to  $\rho$ , which is defined by

$$(2.3) \quad \begin{cases} L(\rho, s) := \prod_p L_p(\rho, s) \quad (p \text{ runs over all prime numbers, } \text{Re}(s) > 1), \\ L_p(\rho, s) := \det(I_2 - \rho(\sigma_{\mathfrak{P}}) p^{-s} | V(\rho)^{I_{\mathfrak{P}}})^{-1}, \end{cases}$$

where  $I_{\mathfrak{P}}$  denotes the inertia group of a prime  $\mathfrak{P}$  of  $K$  lying over  $p$  and  $\sigma_{\mathfrak{P}} \bmod I_{\mathfrak{P}}$  is the Frobenius automorphism.

LEMMA 2.4. *We have*

$$L_p(\rho, s) = \begin{cases} (1 - p^{-s})^{-1} & \text{if } p = p_1 \text{ or } p_2 \text{ and } h_k(2) \geq 8, \\ (1 + p^{-s})^{-1} & \text{if } p = p_1 \text{ or } p_2 \text{ and } h_k(2) = 4, \\ \left(1 - \text{tr}(\rho(\sigma_{\mathfrak{P}})) p^{-s} + \left(\frac{-p_1 p_2}{p}\right) p^{-2s}\right)^{-1} & \text{if } p \neq p_1, p_2. \end{cases}$$

PROOF. If  $p = p_1$  or  $p_2$ ,  $V(\rho)^{I_{\mathfrak{P}}}$  is one dimensional and, by Corollary 1.7, (3),  $\sigma_{\mathfrak{P}} \bmod I_{\mathfrak{P}} \equiv 1 \bmod I_{\mathfrak{P}}$  or  $t^2 \bmod I_{\mathfrak{P}}$  according to  $h_k(2) \geq 8$  or  $h_k(2) = 4$ . Since  $\rho(t^2) = -I_2$ , the assertion follows. If  $p \neq p_1, p_2$ ,  $I_{\mathfrak{P}} = \{1\}$  by Theorem 1.3, (2) and so  $L_p(\rho, s) = (1 - \text{tr}(\rho(\sigma_{\mathfrak{P}})) p^{-s} + \det(\rho(\sigma_{\mathfrak{P}})) p^{-2s})^{-1}$ . Since  $\det \circ \rho$  is a non-trivial character  $\text{Gal}(k/\mathbf{Q}) \rightarrow \mathbf{C}^\times$ , the assertion follows. □

By Lemmas 2.2 and 2.4, we have the following.

COROLLARY 2.5. *For a prime number  $p_3$  satisfying the condition (1.8), we have*

$$L_{p_3}(\rho, s) = \left(1 - 2[-p_1, p_2, p_3] p_3^{-s} + \left(\frac{-p_1 p_2}{p_3}\right) p_3^{-2s}\right)^{-1}.$$



Now, let  $k = \mathbf{Q}(\sqrt{-p_1 p_2})$  as in Section 1 and let

$$\chi : \text{Gal}(K/k) \longrightarrow \mathbf{C}^\times$$

be the character defined by

$$(2.6) \quad \chi(t) = \sqrt{-1}.$$

We let

$$\text{Ind}(\chi) : \text{Gal}(K/\mathbf{Q}) \longrightarrow \text{GL}_2(\mathbf{C})$$

be the induced representation of  $\chi$ .

LEMMA 2.7. *The representation  $\rho$  is equivalent to  $\text{Ind}(\chi)$ .*

PROOF. The induced representation  $\text{Ind}(\chi)$  is given by

$$\text{Ind}(\chi)(s) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \text{Ind}(\chi)(t) = \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix}.$$

Since  $P\rho(g) = \text{Ind}(\chi)(g) \cdot P$  for  $g = s, t$  with  $P = \begin{pmatrix} 1 & \sqrt{-1} \\ -1 & \sqrt{-1} \end{pmatrix}$ , the assertion follows.  $\square$

By Lemma 2.7, we have

$$(2.8) \quad L(\rho, s) = L(\chi, s),$$

where  $L(\chi, s)$  is the abelian Artin  $L$ -function defined by

$$(2.9) \quad L(\chi, s) = \prod_{\mathfrak{p}} (1 - \chi(\sigma_{\mathfrak{p}}) N_{\mathfrak{p}}^{-s})^{-1} \quad (\mathfrak{p} \text{ runs over all prime ideals of } \mathcal{O}_k).$$

Since  $K/k$  is an unramified abelian extension (Theorem 1.3), we have the Artin reciprocity homomorphism

$$\left( \frac{K/k}{\cdot} \right) : H_k \longrightarrow \text{Gal}(K/k); [\mathfrak{a}] \mapsto \left( \frac{K/k}{\mathfrak{a}} \right) = \sigma_{\mathfrak{a}}$$

Let  $\chi$  be the Hecke character on  $H_k$  obtained as the composite of  $\left( \frac{K/k}{\cdot} \right)$  with  $\chi$ :

$$(2.10) \quad \chi := \chi \circ \left( \frac{K/k}{\cdot} \right) : H_k \longrightarrow \mathbf{C}^\times$$

and let  $L(\chi, s)$  be the Hecke  $L$ -function defined by

$$(2.11) \quad L(\chi, s) = \prod_{\mathfrak{p}} (1 - \chi([\mathfrak{p}]) N_{\mathfrak{p}}^{-s})^{-1} = \sum_{\mathfrak{a}} \chi([\mathfrak{a}]) N_{\mathfrak{a}}^{-s}$$

where  $\mathfrak{a}$  runs over all integral ideals of  $k$  and  $\text{Re}(s) > 1$ .

Getting (2.8)  $\sim$  (2.11) together, we have the following

PROPOSITION 2.1. *We have*

$$L(\rho, s) = L(\chi, s).$$

**3. Ideal classes and quadratic forms**

In this section, we express the Hecke  $L$ -function  $L(\chi, s)$  in terms of the binary quadratic forms corresponding to ideal classes of  $k$ . We also show some formulas on the numbers of integral representations by these quadratic forms, which will be used in the next section. We keep the same notations as in the previous sections.

Let  $k$  be the imaginary quadratic field  $\mathbf{Q}(\sqrt{-p_1 p_2})$  for prime numbers  $p_1, p_2$  satisfying the condition (1.1). Let  $H_k$  be the ideal class group of  $k$  with class number  $h_k = \#H_k$ . We write

$$H_k = \{C_0, C_1, \dots, C_{h_k-1}\}, \quad C_0 = [\mathcal{O}_k].$$

Let  $Q_i = Q_i(x, y)$  be a representative of the  $\mathrm{SL}_2(\mathbf{Z})$ -equivalence class of binary quadratic forms corresponding to the ideal class  $C_i$  for  $i = 0, \dots, h_k-1$  ([O, Notes D]). For a positive integer  $n$ , we set

$$(3.1) \quad \begin{aligned} A(C_i, n) &:= \{(x, y) \in \mathbf{Z}^2 \mid Q_i(x, y) = n\}, \\ a(C_i, n) &:= \#A(C_i, n), \quad \text{and} \\ B(C_i, n) &:= \{\mathfrak{a} \in C_i^{-1} \mid \mathfrak{a} \subset \mathcal{O}_k, N\mathfrak{a} = n\}, \\ b(C_i, n) &:= \#B(C_i, n). \end{aligned}$$

LEMMA 3.2. *There is a surjective and two to one map*

$$A(C_i, n) \longrightarrow B(C_i, n).$$

*In particular, we have  $a(C_i, n) = 2b(C_i, n)$ .*

PROOF. Take an integral ideal  $\mathfrak{b} = \mathbf{Z}\mu + \mathbf{Z}\nu \in C_i$  where  $\{\mu, \nu\}$  is a well ordered basis of  $\mathfrak{b}$  ([O, Notes D]). We define the map  $\varphi : A(C_i, n) \rightarrow B(C_i, n)$  by  $\varphi((x, y)) := (x\mu + y\nu)\mathfrak{b}^{-1}$ . Since  $(N\mathfrak{b})^{-1}N_{k/\mathbf{Q}}(x\mu + y\nu) = Q_i(x, y)$ ,  $\varphi$  is well defined. For any  $\mathfrak{a} \in B(C_i, n)$ ,  $\mathfrak{a} \cdot \mathfrak{b} \in C_i^{-1} \cdot C_i = C_0$  and so  $\mathfrak{a}\mathfrak{b} = (z)$  for some  $z \in \mathcal{O}_k$ . Since  $z \in \mathfrak{b}$ , we can write  $z = x\mu + y\nu$  so that  $\varphi((x, y)) = \mathfrak{a}$ , hence  $\varphi$  is surjective. Further, we have  $\varphi((x, y)) = \varphi((x', y')) \Leftrightarrow (x\mu + y\nu) = (x'\mu + y'\nu) \Leftrightarrow x'\mu + y'\nu = \pm(x\mu + y\nu)$  because  $\mathcal{O}_k^\times = \{\pm 1\}$ . Hence  $\varphi$  is two to one.  $\square$

Let  $\chi : H_k \rightarrow \mathbf{C}^\times$  be the Hecke character defined in (2.10). For a positive integer  $n$ , we set

$$(3.3) \quad a_\chi(n) := \frac{1}{2} \sum_{i=0}^{h_k-1} \chi(C_i) a(C_i, n) = \sum_{i=0}^{h_k-1} \chi(C_i) b(C_i, n).$$

PROPOSITION 3.4. *Let  $I$  be the set of indices  $i$  ( $0 \leq i \leq h_k - 1$ ) such that  $\chi(C_i) \in \{\pm 1\}$ . Then we have*

$$a_\chi(n) = \frac{1}{2} \sum_{i \in I} \chi(C_i) a(C_i, n)$$

and

$$L(\chi, s) = \sum_{n=1}^{\infty} a_\chi(n) n^{-s}.$$

PROOF. By Lemma 3.2, we have

$$\begin{aligned} L(\chi, s) &= \sum_{i=0}^{h_k-1} \chi(C_i^{-1}) \sum_{\substack{\mathfrak{a} \in C_i^{-1} \\ \mathfrak{a} \subset \mathcal{O}_k}} N\mathfrak{a}^{-s} \\ &= \sum_{i=0}^{h_k-1} \chi(C_i^{-1}) \sum_{n=1}^{\infty} b(C_i, n) n^{-s} \\ &= \sum_{n=1}^{\infty} \left( \frac{1}{2} \sum_{i=0}^{h_k-1} \chi(C_i^{-1}) a(C_i, n) \right) n^{-s}. \end{aligned}$$

Since  $L(\chi, s) = L(\rho, s)$  by Proposition 2.12 and  $\text{Im}(\rho) \subset \text{GL}_2(\mathbf{Z})$  by (2.1), the coefficients  $a_\chi(n)$  should be in  $\mathbf{Z}$ . Since  $\text{Im}\chi \subset \{\pm 1, \pm\sqrt{-1}\}$  by (2.6) and (2.10), and  $a(C_i, n) \in \mathbf{Z}$ , we have

$$\frac{1}{2} \sum_{i=0}^{h_k-1} \chi(C_i^{-1}) a(C_i, n) = \frac{1}{2} \sum_{i \in I} \chi(C_i) a(C_i, n) = a_\chi(n)$$

and hence

$$L(\chi, s) = \sum_{n=1}^{\infty} a_\chi(n) n^{-s}. \quad \square$$

Here are some properties about the integer coefficients  $a_\chi(n)$  which will be used in the next section. Similar results were stated in [HM, 2.3].

PROPOSITION 3.5. (1) *If  $(m, n) = 1$ , then  $a_\chi(mn) = a_\chi(m)a_\chi(n)$ .*  
 (2) *If  $p$  is a prime number different from  $p_1$  and  $p_2$ , then we have*

$$a_\chi(p^{r+1}) - a_\chi(p)a_\chi(p^r) + \left(\frac{-p_1 p_2}{p}\right) a_\chi(p^{r-1}) = 0 \quad \text{for } r \geq 1.$$

Here we mean  $\left(\frac{-p_1 p_2}{2}\right) = 1$  or  $-1$  according as 2 is decomposed or inert in  $k/\mathbf{Q}$ , respectively.

(3) Suppose  $p = p_1$  or  $p_2$ . If the 2-class number  $h_k(2) \geq 8$ , then we have  $a_\chi(p^r) = 1$  for  $r \geq 0$ . If  $h_k(2) = 4$ , we have

$$a_\chi(p^r) = \begin{cases} 1 & \text{if } r \equiv 0 \pmod{2}, \\ -1 & \text{if } r \equiv 1 \pmod{2}. \end{cases}$$

PROOF. (1) Let  $m, n$  be coprime positive integers. It is easy to set that the map

$$\bigsqcup_{C_{i_1} C_{i_2} = C_i} (B(C_{i_1}, m) \times B(C_{i_2}, n)) \longrightarrow B(C_i, mn); \quad (\mathfrak{a}_1, \mathfrak{a}_2) \mapsto \mathfrak{a}_1 \mathfrak{a}_2$$

is bijective and so, by Lemma 3.2, we have

$$a(C_i, mn) = \frac{1}{2} \sum_{C_{i_1} C_{i_2} = C_i} a(C_{i_1}, m) a(C_{i_2}, n).$$

Therefore by (3.3) we have

$$\begin{aligned} a_\chi(mn) &= \frac{1}{2} \sum_{i=0}^{h_k-1} \chi(C_i) a(C_i, mn) \\ &= \left( \frac{1}{2} \sum_{i_1} \chi(C_{i_1}) a(C_{i_1}, m) \right) \left( \frac{1}{2} \sum_{i_2} \chi(C_{i_2}) a(C_{i_2}, n) \right) \\ &= a_\chi(m) a_\chi(n) \end{aligned}$$

(2) (i) The case  $p$  is inert in  $k/\mathbf{Q}$ ,  $(p) = \mathfrak{p}$ : Then  $\left(\frac{-p_1 p_2}{p}\right) = -1$  and so we have to prove

$$(3.5.1) \quad a_\chi(p^{r+1}) - a_\chi(p) a_\chi(p^r) - a_\chi(p^{r-1}) = 0 \quad (r \geq 1).$$

First, since  $N\mathfrak{p} = p^2$ ,  $a(C_i, p) = 0$  for any  $i$  and so we have  $a_\chi(p) = 0$ . Next, since  $[\mathfrak{p}] = C_0$ , we note that the map

$$B(C_i, p^{r-1}) \longrightarrow B(C_i, p^{r+1}); \quad \mathfrak{a} \mapsto \mathfrak{a}\mathfrak{p}$$

is a bijection for any  $i$ . By Lemma 3.2 and (3.3), we have  $a_\chi(p^{r+1}) = a_\chi(p^r)$ . This proves (3.5.1).

(ii) The case  $p$  splits in  $k/\mathbf{Q}$ ,  $(p) = \mathfrak{p}\bar{\mathfrak{p}}$ : Then  $\left(\frac{-p_1 p_2}{p}\right) = 1$  and so we need to prove

$$(3.5.2) \quad a_\chi(p^{r+1}) - a_\chi(p) a_\chi(p^r) + a_\chi(p^{r-1}) = 0 \quad (r \geq 1).$$

(ii)<sub>1</sub>. Suppose  $[\mathfrak{p}] = [\bar{\mathfrak{p}}]$ . By (3.1) and Lemma 3.2, we have

$$a(C_i, p) = \begin{cases} 4 & \text{if } C_i^{-1} = [\mathfrak{p}] = [\bar{\mathfrak{p}}], \\ 0 & \text{otherwise.} \end{cases}$$

Therefore we have

$$(3.5.3) \quad a_{\chi}(p) = \frac{1}{2} \sum_{i=0}^{h_k-1} \chi(C_i) a(C_i, p) = 2\chi([\mathfrak{p}]).$$

Note that the map

$$B(C_i[\mathfrak{p}], p^r) \longrightarrow B(C_i, p^{r+1}) \setminus \{\bar{\mathfrak{p}}^{r+1}\}; \quad \mathfrak{a} \mapsto \mathfrak{a}\mathfrak{p}$$

is a bijection for each  $i$  and so, by Lemma 3.2, we have

$$a(C_i[\mathfrak{p}], p^r) = \begin{cases} a(C_i, p^{r+1}) & \text{if } C_i \neq [\mathfrak{p}]^{r+1}, \\ a(C_i, p^{r+1}) - 2 & \text{if } C_i = [\mathfrak{p}]^{r+1}. \end{cases}$$

Therefore we have, for  $r \geq 0$ ,

$$(3.5.4) \quad \begin{aligned} a_{\chi}(p^{r+1}) &= \frac{1}{2} \sum_{i=0}^{h_k-1} \chi(C_i) a(C_i, p^{r+1}) \\ &= \frac{1}{2} \sum_{i=0}^{h_k-1} \chi(C_i) a(C_i[\mathfrak{p}], p^r) - \chi([\mathfrak{p}])^{r+1} \\ &= \chi([\mathfrak{p}]) a_{\chi}(p^r) - \chi([\mathfrak{p}])^{r+1} \quad ([\mathfrak{p}]^{-1} = [\mathfrak{p}]). \end{aligned}$$

By (3.5.3) and (3.5.4), we get

$$\begin{aligned} a_{\chi}(p^{r+1}) - a_{\chi}(p) a_{\chi}(p^r) + a_{\chi}(p^{r-1}) \\ = (\chi([\mathfrak{p}]) a_{\chi}(p^r) - \chi([\mathfrak{p}])^{r+1}) - 2\chi([\mathfrak{p}]) a_{\chi}(p^r) + (\chi([\mathfrak{p}]) a_{\chi}(p^r) + \chi([\mathfrak{p}])^{r+1}) \\ = 0. \end{aligned}$$

(ii)<sub>2</sub>. Suppose  $[\mathfrak{p}] \neq [\bar{\mathfrak{p}}]$ . By (3.1) and Lemma 3.2, we have

$$a(C_i, p) = \begin{cases} 2 & \text{if } C_i^{-1} = [\mathfrak{p}] \text{ or } [\bar{\mathfrak{p}}], \\ 0 & \text{otherwise.} \end{cases}$$

Therefore we have

$$(3.5.5) \quad a_{\chi}(p) = \frac{1}{2} \sum_{i=0}^{h_k-1} \chi(C_i) a(C_i, p) = \chi([\mathfrak{p}]) + \chi([\bar{\mathfrak{p}}]).$$

Note that the map

$$B(C_i[\mathfrak{p}], p^r) \longrightarrow B(C_i, p^{r+1}) \setminus \{\bar{\mathfrak{p}}^{r+1}\}; \quad \mathfrak{a} \mapsto \mathfrak{a}\mathfrak{p}$$

is a bijection for each  $i$ . Therefore, noting  $[\mathfrak{p}]^{-1} = [\bar{\mathfrak{p}}]$ , the argument similar to the case (ii)<sub>1</sub> shows

$$(3.5.6) \quad a_{\chi}(p^{r+1}) = \chi([\bar{\mathfrak{p}}]) a_{\chi}(p^r) - \chi([\mathfrak{p}])^{r+1} \quad (r \geq 0).$$

Since the map  $B(C_i[\bar{p}], p^r) \rightarrow B(C_i, p^{r+1}) \setminus \{p^{r+1}\}$ ;  $\alpha \mapsto \alpha\bar{p}$  is also bijective for each  $i$ , we obtain similarly

$$(3.5.7) \quad a_{\chi}(p^{r+1}) = \chi([\mathfrak{p}])a_{\chi}(p^r) - \chi([\bar{\mathfrak{p}}])^{r+1} \quad (r \geq 0).$$

By (3.5.5), (3.5.6) and (3.5.7), we get

$$\begin{aligned} & a_{\chi}(p^{r+1}) - a_{\chi}(p)a_{\chi}(p^r) + a_{\chi}(p^{r-1}) \\ &= (\chi([\mathfrak{p}])a_{\chi}(p^r) - \chi([\bar{\mathfrak{p}}])^{r+1}) - (\chi([\mathfrak{p}]) + \chi([\bar{\mathfrak{p}}]))a_{\chi}(p^r) + (\chi([\mathfrak{p}])a_{\chi}(p^r) + \chi([\mathfrak{p}])^{r+1}) \\ &= \chi([\mathfrak{p}])a_{\chi}(p^r) - \chi([\bar{\mathfrak{p}}])^{r+1} - (\chi([\bar{\mathfrak{p}}])a_{\chi}(p^r) - \chi([\mathfrak{p}])^{r+1}) \\ &= 0. \end{aligned}$$

(3) Let  $p = p_1$  or  $p_2$  so that  $(p) = \mathfrak{p}^2$ ,  $N\mathfrak{p} = p$ . Since  $[\mathfrak{p}]$  has order 2 in  $H_k$  by Corollary 1.7,(3), we have

$$a(C_i, p^r) = 2b(C_i, p^r) = 0 \quad \text{unless } C_i = C_0 \text{ or } [\mathfrak{p}]$$

and

$$a(C_0, p^r) = 2b(C_0, p^r) = \begin{cases} 2 & \text{if } r \equiv 0 \pmod{2}, \\ 0 & \text{if } r \equiv 1 \pmod{2}, \end{cases}$$

$$a([\mathfrak{p}], p^r) = 2b([\mathfrak{p}], p^r) = \begin{cases} 0 & \text{if } r \equiv 0 \pmod{2}, \\ 2 & \text{if } r \equiv 1 \pmod{2}. \end{cases}$$

Further,  $\chi(C_0) = 1$ , and by Corollary 1.7,(3),

$$\chi([\mathfrak{p}]) = \begin{cases} 1 & \text{if } h_k(2) \geq 8, \\ -1 & \text{if } h_k(2) = 4. \end{cases}$$

Hence, if  $h_k(2) \geq 8$ , we have

$$a_{\chi}(p^r) = \frac{1}{2}(a(C_0, p^r) + a([\mathfrak{p}], p^r)) = 1,$$

and if  $h_k(2) = 4$ ,

$$a_{\chi}(p^r) = \frac{1}{2}(a(C_0, p^r) - a([\mathfrak{p}], p^r)) = \begin{cases} 1 & \text{if } r \equiv 0 \pmod{2}, \\ -1 & \text{if } r \equiv 1 \pmod{2}. \end{cases} \quad \square$$

#### 4. Theta series and reciprocity laws

In this section, we express the Artin  $L$ -function in Section 2 as the  $L$ -function of a modular form associated to binary quadratic forms in Section 3. This may be seen as an explicit and constructive version of the theorem by Weil-Langlands and Deligne-Serre ([Se]) for the Rédei extension. In particular, the Rédei triple symbol is expressed as a Fourier coefficient of

a modular form which is given in terms of the numbers of integral representations of binary quadratic forms. A reciprocity law for the triple symbol yields certain reciprocal relations among Fourier coefficients.

Let  $\mathfrak{H}$  be the upper half plane in  $\mathbf{C}$ . Let  $M_w(\Gamma_0(N), \varepsilon)$  be the space of holomorphic modular forms on  $\mathfrak{H}$  of weight  $w$  and character  $\varepsilon \pmod N$  with respect to  $\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z}) \mid c \equiv 0 \pmod N \right\}$  on which the Hecke operators  $T(m)$  ( $m \in \mathbf{Z} > 0$ ) act. Each modular form  $f \in M_w(\Gamma_0(N), \varepsilon)$  has the Fourier expansion

$$f(z) = \sum_{n=0}^{\infty} a_n q^n, \quad q := \exp(2\pi\sqrt{-1}z) \quad (z \in \mathfrak{H}),$$

and the action of the Hecke operator  $T(m)$  is defined by

$$(4.1) \quad (f|T(m))(z) = \sum_{n=0}^{\infty} b_n q^n, \quad b_n = \sum_{0 < d|(m,n)} \varepsilon(d) d^{\omega-1} a_{mn/d^2},$$

where we understand that  $b_n = a_{mn}$  if  $m$  divides  $N$ .

Let  $S_w(\Gamma_0(N), \varepsilon)$  be the subspace of  $M_w(\Gamma_0(N), \varepsilon)$  consisting of cusp forms  $f(z)$  (i.e.,  $a_0 = 0$ ) which is stable under the action of Hecke operators  $T(m)$  ( $m \in \mathbf{Z} > 0$ ). A cusp form in  $S_w(\Gamma_0(N), \varepsilon)$  is called a Hecke eigenform if it is a common eigenfunction of all Hecke operators  $T(m)$ 's.

Now, let us be back in the situation of the previous sections. We consider the following theta series. For  $z \in \mathfrak{H}$ , we let

$$(4.2) \quad \begin{cases} \theta(C_i, z) := \frac{1}{2} \sum_{n=0}^{\infty} a(C_i, n) q^n = \frac{1}{2} \sum_{x,y \in \mathbf{Z}} q^{Q_i(x,y)} \quad (0 \leq i \leq h_k - 1), \\ \Theta_{\chi}(z) := \sum_{n=0}^{\infty} a_{\chi}(n) q^n = \sum_{i=0}^{h_k-1} \chi(C_i) \theta(C_i, z). \end{cases}$$

Here we set  $a(C_i, 0) = 1$  for all  $i$  and  $a_{\chi}(0) = \sum_{i=0}^{h_k-1} \chi(C_i) = 0$ . The following theorem is due to E. Hecke ([H]).

- THEOREM 4.3.** (1)  $\theta(C_i, z) \in M_1(\Gamma_0(p_1 p_2), \left(\frac{-p_1 p_2}{\cdot}\right))$ .  
 (2)  $\Theta_{\chi}(z) \in S_1(\Gamma_0(p_1 p_2), \left(\frac{-p_1 p_2}{\cdot}\right))$  and it is a Hecke eigenform.

**PROOF.** (1) We refer to [Mi, Corollary 4.9.5].

(2) Since  $\chi$  is not a genus character (i.e., a character of order 2),  $\Theta_{\chi}(z)$  is a cusp form ([Z, 4.3], [Mi, Theorem 4.8.2]). Further, by proposition 3.5, the Dirichlet series associated to

$\Theta_{\chi}(z)$  is written as

$$(4.4) \quad \sum_{n=1}^{\infty} a_{\chi}(n)n^{-s} = \prod_p (1 - a_{\chi}(p)p^{-s} + \left(\frac{-p_1 p_2}{p}\right) p^{-2s})^{-1}$$

where  $p$  runs over all prime numbers and we set  $\left(\frac{-p_1 p_2}{p}\right) = 0$  if  $p = p_1$  or  $p_2$ . This implies that  $\Theta_{\chi}(z)$  is a Hecke eigenform ([Mi, Theorem 4.5.16]).  $\square$

Let  $L(\Theta_{\chi}, s)$  denote the  $L$ -function of the modular form  $\Theta_{\chi}(z)$ , namely, the Dirichlet series

$$(4.5) \quad L(\Theta_{\chi}, s) := \sum_{n=1}^{\infty} a_{\chi}(n)n^{-s}.$$

By (4.4), we have

$$\begin{cases} L(\Theta_{\chi}, s) = \prod_p L_p(\Theta_{\chi}, s) \quad (p \text{ runs over all prime numbers}), \\ L_p(\Theta_{\chi}, s) = \left(1 - a_{\chi}(p)p^{-s} + \left(\frac{-p_1 p_2}{p}\right) p^{-2s}\right)^{-1}. \end{cases}$$

By Proposition 3.5, (3), we note

$$L_p(\Theta_{\chi}, s) = \begin{cases} (1 - p^{-s})^{-1} & \text{if } p = p_1 \text{ or } p_2 \text{ and } h_k(2) \geq 8, \\ (1 + p^{-s})^{-1} & \text{if } p = p_1 \text{ or } p_2 \text{ and } h_k(2) = 4. \end{cases}$$

The following theorem may be regarded as an explicit and constructive version of the theorem of Weil-Langlands and Deligne-Serre ([Se]).

**THEOREM 4.6.** *We have*

$$L(\rho, s) = L(\Theta_{\chi}, s).$$

*For a prime number  $p \neq p_1, p_2$ , we have*

$$\text{tr}(\rho(\sigma_{\mathfrak{p}})) = a_{\chi}(p)$$

*where  $\sigma_{\mathfrak{p}}$  is the Frobenius automorphism of a prime of  $K$  lying over  $p$ .*

**PROOF.** The first assertion follows from Propositions 2.12, 3.4 and (4.5). The second one follows from Lemma 2.4 and (4.4).  $\square$

Let  $p_1, p_2$  and  $p_3$  be prime numbers satisfying the condition (1.8). The following corollary gives a relation between the Rédei triple symbol and modular form.

**COROLLARY 4.7.** *We have*

$$[-p_1, p_2, p_3] = \frac{1}{2} a_{\chi}(p_3).$$



In particular,  $p_3$  is completely decomposed in the Rédei extension  $K_{\{-p_1, p_2\}}/\mathbf{Q}$  if and only if  $a_\chi(p_3) = 2$ .

PROOF. This follows from Lemma 2.2 and Theorem 4.6. □

Now we write  $k_{12}$  and  $\chi_{12} : H_{k_{12}} \rightarrow \mathbf{C}^\times$  for  $k = \mathbf{Q}(\sqrt{-p_1 p_2})$  and  $\chi$  in the previous sections, and we let  $k_{13} := \mathbf{Q}(\sqrt{-p_1 p_3})$  and denote by  $\chi_{13}$  the Hecke character  $H_{k_{13}} \rightarrow \mathbf{C}^\times$  defined in the similar manner to the case of  $\chi_{12}$ . The reciprocity law for the triple symbol yields the following

THEOREM 4.8. *Notations being as above, we have*

$$a_{\chi_{12}}(p_3) = a_{\chi_{13}}(p_2).$$

PROOF. It follows from Theorem 1.12 and Corollary 4.7. □

### 5. Numerical examples

In this section, we discuss numerical examples. We keep the same notations as in the previous sections.

EXAMPLE 5.1. Let  $p_1 = 11$  and  $p_2 = 5$ . The associated Rédei extension is given by

$$K_{\{-11, 5\}} = \mathbf{Q}(\sqrt{-p_1}, \sqrt{p_2}, \sqrt{\alpha}), \quad \alpha = 3 + 2\sqrt{5}.$$

Let  $\rho : \text{Gal}(K_{\{-11, 5\}}/\mathbf{Q}) \rightarrow \text{GL}_2(\mathbf{C})$  be the representation defined in (2.1). The ideal class group  $H_k$  of  $k = \mathbf{Q}(\sqrt{-55})$  is a cyclic group of order 4:

$$H_k = \{C_0 = [\mathcal{O}_k], C_1 = [\mathfrak{p}_2], C_2 = C_1^2 = [\mathfrak{p}_5], C_3 = C_1^3 = [\overline{\mathfrak{p}_2}]\}$$

where  $\mathcal{O}_k = [1, \omega]$ ,  $\mathfrak{p}_2 = [2, \omega]$ ,  $\mathfrak{p}_5 = [5, 2 + \omega]$ ,  $\overline{\mathfrak{p}_2} = [2, 1 + \omega]$ . ( $\omega = (1 + \sqrt{-55})/2$ ), and the corresponding binary quadratic forms are given respectively by

$$\begin{aligned} Q_0 &= X^2 + XY + 14Y^2, & Q_1 &= 2X^2 + XY + 7Y^2, \\ Q_2 &= 5X^2 + 5XY + 4Y^2, & Q_3 &= 2X^2 + 3XY + 8Y^2. \end{aligned}$$

Note that  $K_{\{-11, 5\}}$  is the Hilbert class field of  $k$ . For a positive integer  $n$ ,  $a(C_i, n) := \#\{(x, y) \in \mathbf{Z} \mid Q_i(x, y) = n\}$  ( $0 \leq i \leq 3$ ). Since the character  $\chi : H_k \rightarrow \mathbf{C}^\times$  in (2.10) is given by  $\chi(C_i) = (\pm\sqrt{-1})^i$  ( $0 \leq i \leq 3$ ), we have

$$a_\chi(n) = \frac{1}{2}(a(C_0, n) - a(C_2, n))$$

and

$$\Theta_\chi(z) = \sum_{n=1}^{\infty} a_\chi(n)q^n = \frac{1}{2} \left( \sum_{x, y \in \mathbf{Z}} q^{x^2 + xy + 14y^2} - \sum_{x, y \in \mathbf{Z}} q^{5x^2 + 5xy + 4y^2} \right)$$

$$= q - q^4 - q^5 + q^9 - q^{11} + q^{16} + \dots$$

Theorem 4.6 reads:

$$\begin{cases} L(\rho, s) = L(\Theta_\chi, s), \\ \text{tr}(\rho(\sigma_{\mathfrak{p}_3})) = a_\chi(p) \text{ for a prime number } p \neq 5, 11. \end{cases}$$

By Corollary 4.7, for a prime number  $p_3$  satisfying (1.8), i.e.,  $p_3 \equiv 1 \pmod{4}$ ,  $\left(\frac{11}{p_3}\right) = \left(\frac{5}{p_3}\right) = 1$ , we have

$$[-11, 5, p_3] = \frac{1}{2}a_\chi(p_3).$$

For example, let  $p_3 = 89$  satisfying (1.8). To distinguish the notations, we write  $k_{12}$ ,  $Q_{12,i}$  and  $\chi_{12}$  for the above  $k$ ,  $Q_i$  and  $\chi$ , and let  $k_{13} := \mathbf{Q}(\sqrt{-11 \cdot 89}) = \mathbf{Q}(\sqrt{-979})$ . The ideal class group  $H_{k_{13}}$  of  $k_{13}$  is a cyclic group of order 8 consisting of  $C_{13,0}, C_{13,i} = (C_{13,1})^i$  ( $1 \leq i \leq 7$ ):

$$\begin{aligned} C_{13,0} &= [X^2 + XY + 245Y^2], & C_{13,1} &= [7X^2 + XY + 35Y^2], \\ C_{13,2} &= [5X^2 + 9XY + 53Y^2], & C_{13,3} &= [13X^2 + 23XY + 29Y^2], \\ C_{13,4} &= [11X^2 + 11XY + 25Y^2], & C_{13,5} &= [13X^2 + 35XY + 29Y^2], \\ C_{13,6} &= [5X^2 + XY + 49Y^2], & C_{13,7} &= [7X^2 + 13XY + 41Y^2]. \end{aligned}$$

We set  $a(C_{13,i}, n) := \#\{(x, y) \in \mathbf{Z} \mid Q_{13,i}(x, y) = n\}$ . Since the character  $\chi_{13} : H_{k_{13}} \rightarrow \mathbf{C}^\times$  in (2.10) is given by  $\chi_{13}(C_{13,i}) = (\pm\sqrt{-1})^i$  ( $0 \leq i \leq 7$ ), we have

$$a_{\chi_{13}}(n) = \frac{1}{2}(a(C_{13,0}, n) - a(C_{13,2}, n) + a(C_{13,4}, n) - a(C_{13,6}, n)).$$

The reciprocity law of Theorem 4.8 then reads

$$a_{\chi_{12}}(89) = a_{\chi_{13}}(5).$$

In fact, we can easily see  $a_{\chi_{13}}(5) = -2$ . So the above reciprocity tells us  $a_{\chi_{12}}(89) = -2$ . Therefore 89 is decomposed as  $(89) = \mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3\mathfrak{P}_4, N\mathfrak{P}_i = 89^2$  in  $K_{\{-11,5\}}$ .

EXAMPLE 5.2. Let  $p_1 = 3$  and  $p_2 = 73$ . The associated Rédei extension is then given by

$$K_{\{-3,73\}} = \mathbf{Q}(\sqrt{-p_1}, \sqrt{p_2}, \sqrt{\alpha}), \quad \alpha = -17 + 2\sqrt{73}.$$

Let  $\rho : \text{Gal}(K_{\{-3,73\}}/\mathbf{Q}) \rightarrow \text{GL}_2(\mathbf{C})$  be the representation defined in (2.1). The ideal class group  $H_k$  of  $k = \mathbf{Q}(\sqrt{-219})$  is a cyclic group of order 4:

$$H_k = \{C_0 = [\mathcal{O}_k], C_1 = [\mathfrak{p}_5], C_2 = C_1^2 = [\mathfrak{p}_3], C_3 = C_1^3 = [\overline{\mathfrak{p}_5}]\}$$

where  $\mathcal{O}_k = [1, \omega]$ ,  $\mathfrak{p}_5 = [5, \omega]$ ,  $\mathfrak{p}_3 = [3, 1 + \omega]$ ,  $\overline{\mathfrak{p}}_5 = [1, 4 + \omega]$ . ( $\omega = (1 + \sqrt{-219})/2$ ), and the corresponding binary quadratic forms are given respectively by

$$\begin{aligned} Q_0 &= X^2 + XY + 55Y^2, & Q_1 &= 5X^2 + XY + 11Y^2, \\ Q_2 &= 3X^2 + 3XY + 19Y^2, & Q_3 &= 5X^2 + 9XY + 15Y^2. \end{aligned}$$

Note that  $K_{\{-3,73\}}$  is the Hilbert class field of  $k$ . For a positive integer  $n$ ,  $a(C_i, n) := \#\{(x, y) \in \mathbf{Z} \mid Q_i(x, y) = n\}$  ( $0 \leq i \leq 3$ ). Since the character  $\chi : H_k \rightarrow \mathbf{C}^\times$  in (2.10) is given by  $\chi(C_i) = (\pm\sqrt{-1})^i$  ( $0 \leq i \leq 3$ ), we have

$$a_\chi(n) = \frac{1}{2}(a(C_0, n) - a(C_2, n))$$

and

$$\begin{aligned} \Theta_\chi(z) &= \sum_{n=1}^\infty a_\chi(n)q^n = \frac{1}{2} \left( \sum_{x,y \in \mathbf{Z}} q^{x^2+xy+55y^2} - \sum_{x,y \in \mathbf{Z}} q^{3x^2+3xy+19y^2} \right) \\ &= q - q^3 + q^4 + q^9 - q^{12} + q^{16} - \dots \end{aligned}$$

Theorem 4.6 reads:

$$\begin{cases} L(\rho, s) = L(\Theta_\chi, s), \\ \text{tr}(\rho(\sigma_{\mathfrak{p}_3})) = a_\chi(p) \quad \text{for a prime number } p \neq 3, 73. \end{cases}$$

By Corollary 4.7, for a prime number  $p_3$  satisfying (1.8), i.e.,  $p_3 \equiv 1 \pmod{4}$ ,  $\left(\frac{3}{p_3}\right) = \left(\frac{73}{p_3}\right) = 1$ , we have

$$[-3, 73, p_3] = \frac{1}{2}a_\chi(p_3).$$

For example, let  $p_3 = 97$ . To distinguish the notations, we write  $k_{12}$ ,  $Q_{12,i}$  and  $\chi_{12}$  for the above  $k$ ,  $Q_i$  and  $\chi$ , and let  $k_{13} := \mathbf{Q}(\sqrt{-3 \cdot 97}) = \mathbf{Q}(\sqrt{-291})$ . According to the table of [WS], the triple of prime numbers  $\{3, 73, 97\}$  is an example such that (1.8) is satisfied and the ideal class groups of  $k_{12}$  and  $k_{13}$  are both cyclic group of order 4. In fact, the ideal class group  $H_{k_{13}}$  of  $k_{13}$  consists of  $C_{13,0}, C_{13,i} = (C_{13,1})^i$  ( $1 \leq i \leq 3$ ):

$$\begin{aligned} C_{13,0} &= [X^2 + XY + 73Y^2], & C_{13,1} &= [5X^2 + 7XY + 17Y^2], \\ C_{13,2} &= [3X^2 + 3XY + 25Y^2], & C_{13,3} &= [5X^2 + 3XY + 15Y^2]. \end{aligned}$$

So  $K_{\{-3,97\}}$  is also the Hilbert class field of  $k_{13}$ . We set  $a(C_{13,i}, n) := \#\{(x, y) \in \mathbf{Z} \mid Q_{13,i}(x, y) = n\}$ . Since the Hecke character  $\chi_{13} : H_{k_{13}} \rightarrow \mathbf{C}^\times$  in (2.10) is given by  $\chi_{13}(C_{13,i}) = (\pm\sqrt{-1})^i$  ( $0 \leq i \leq 3$ ), we have

$$a_{\chi_{13}}(n) = \frac{1}{2}(a(C_{13,0}, n) - a(C_{13,2}, n)).$$

The reciprocity law of Theorem 4.8 reads

$$a_{\chi_{12}}(97) = a_{\chi_{13}}(73).$$

In fact, we can easily see  $a_{\chi_{12}}(97) = a_{\chi_{13}}(73) = 2$ . So 97 (resp. 73) is completely decomposed in  $K_{\{-3,73\}}/\mathbf{Q}$  (resp.  $K_{\{-3,97\}}/\mathbf{Q}$ ).

REMARK 5.3. In Appendix, a neat formula for  $a_{\chi}(n)$  is presented in the case that  $k = \mathbf{Q}(\sqrt{-p_1 p_2})$  has the class number 4, equivalently, the Rédei extension  $K_{\{-p_1, p_2\}}$  is the Hilbert class field of  $k$ . According to the table of [WS], there are 21 pairs of  $(p_1, p_2)$  in the range  $p_1 p_2 < 10000$  such that the condition (1.1) satisfied and the class number of  $k$  is 4, namely,  $(p_1, p_2) = (3, 13), (11, 5), (31, 5), (7, 29), (3, 73), (7, 37), (3, 97), (19, 17), (71, 5), (23, 29), (3, 241), (7, 109), (191, 5), (59, 17), (79, 13), (3, 409), (11, 113), (19, 73), (83, 17), (11, 137), (311, 5)$ .<sup>1</sup> Among these, the triples of  $(p_1, p_2, p_3)$  such that the condition (1.8) is satisfied are given by  $(3, 73, 97), (3, 97, 241), (7, 29, 109)$ .

#### Appendix by Takeshi Ogasawara

In this appendix, we express the modular form  $\Theta_{\chi}(z) = \sum_{n=1}^{\infty} a_{\chi}(n)q^n$  defined in (4.2) in terms of eta quotients, when  $k = \mathbf{Q}(\sqrt{-p_1 p_2})$  has the class number 4 so that the Rédei extension  $K_{\{-p_1, p_2\}}$  is the Hilbert class field of  $k$ . From this, we obtain a formula for the Fourier coefficient  $a_{\chi}(n)$  and hence for the Rédei symbol  $[-p_1, p_2, p_3]$  in this case. We keep the same notations as in the previous sections.

Let  $\eta(z)$  be the Dedekind eta function defined by

$$\eta(z) := q^{1/24} \prod_{n=1}^{\infty} (1 - q^n)$$

and consider the eta quotient (Jacobi's product expansion of the theta function)

$$\vartheta(z) := \frac{\eta(2z)^5}{\eta(z)^2 \eta(4z)^2} = \sum_{n \in \mathbf{Z}} q^{n^2}.$$

Let  $p_1$  and  $p_2$  be prime numbers satisfying the condition (1.1). We note that the following eta quotients

$$\vartheta(z)\vartheta(p_1 p_2 z) = \sum_{x, y \in \mathbf{Z}} q^{x^2 + p_1 p_2 y^2}, \quad \vartheta(p_1 z)\vartheta(p_2 z) = \sum_{x, y \in \mathbf{Z}} q^{p_1 x^2 + p_2 y^2}$$

<sup>1</sup>We are grateful to Masanari Kida and the referee for kindly telling us the references [Ar] and [Wat], by which this list of 21 pairs is proved to be complete.

belong to  $M_1(\Gamma_0(4p_1p_2), (\frac{-p_1p_2}{\cdot}))$  on which the operator  $T(m)$  acts by (4.1). For an integer  $n \geq 0$ , we set

$$\begin{aligned} a_n^1 &:= \#\{(x, y) \in \mathbf{Z}^2 \mid x^2 + p_1p_2y^2 = n\}, \\ a_n^2 &:= \#\{(x, y) \in \mathbf{Z}^2 \mid p_1x^2 + p_2y^2 = n\}, \\ a_{\{p_1, p_2\}}(n) &:= \frac{1}{2}(a_{4n}^1 - a_{4n}^2). \end{aligned}$$

**THEOREM A1.** *Notations being as above, assume that the class number of  $k = \mathbf{Q}(\sqrt{-p_1p_2})$  is 4. Then we have*

$$\Theta_\chi(z) = \frac{1}{2}(\vartheta(z)\vartheta(p_1p_2z) - \vartheta(p_1z)\vartheta(p_2z))|T(4),$$

and

$$a_\chi(n) = a_{\{p_1, p_2\}}(n).$$

**PROOF.** We note by the assumption that the ideal class group  $H_k$  of  $k$  is a cyclic group of order 4:

$$H_k = \{C_0, C_1, C_2, C_3\}, \quad C_i = (C_1)^i \quad (0 \leq i \leq 3).$$

Since  $\vartheta(z)\vartheta(p_1p_2z) = \sum_{x,y \in \mathbf{Z}} q^{x^2+p_1p_2y^2} = \sum_{n=0}^\infty a_n^1q^n$ , we have

$$\begin{aligned} (\vartheta(z)\vartheta(p_1p_2z))|T(4) &= \sum_{n=0}^\infty a_{4n}^1q^n \quad \text{by (4.1)} \\ &= \sum_{\substack{x,y \in \mathbf{Z} \\ x^2+p_1p_2y^2 \equiv 0 \pmod{4}}} q^{(x^2+p_1p_2y^2)/4} \\ &= \sum_{\substack{x,y \in \mathbf{Z} \\ x \equiv y \pmod{2}}} q^{(x^2+p_1p_2y^2)/4} \\ &= \sum_{\alpha \in \mathcal{O}_k} q^{N_k/\mathbf{Q}(\alpha)} \\ &= \sum_{x,y \in \mathbf{Z}} q^{Q_0(x,y)} \\ &= 2\theta(C_0, z) \quad \text{by (4.2)}. \end{aligned}$$

Similarly, since  $\vartheta(p_1z)\vartheta(p_2z) = \sum_{x,y \in \mathbf{Z}} q^{p_1x^2+p_2y^2} = \sum_{n=0}^\infty a_n^2q^n$ , we have

$$(\vartheta(p_1z)\vartheta(p_2z))|T(4) = \sum_{n=0}^\infty a_{4n}^2q^n \quad \text{by (4.1)}$$

$$\begin{aligned}
 &= \sum_{\substack{x, y \in \mathbf{Z} \\ p_1x^2 + p_2y^2 \equiv 0 \pmod{4}}} q^{(p_1x^2 + p_2y^2)/4} \\
 &= \sum_{\substack{x, y \in \mathbf{Z} \\ x \equiv y \pmod{2}}} q^{(p_1x^2 + p_2y^2)/4} \\
 &= \sum_{\substack{x, y \in \mathbf{Z} \\ x \equiv y \pmod{2}}} q^{((p_1x)^2 + p_1p_2y^2)/4p_1} \\
 &= \sum_{\alpha \in \mathfrak{p}_1} q^{N_{k/\mathbf{Q}}(\alpha)/N\mathfrak{p}_1}.
 \end{aligned}$$

Here  $\mathfrak{p}_1 = \{(p_1x + y\sqrt{-p_1p_2})/2 \mid x \equiv y \pmod{2}\}$  is the prime ideal of  $\mathcal{O}_k$  lying over  $p_1$ . Since  $[\mathfrak{p}_1]$  has the order 2 in  $H_k$  by Corollary 1.7, (3),  $[\mathfrak{p}_1] = C_2$  and so the above series is nothing but  $2\theta(C_2, z)$  by (4.2).

Since  $\chi(C_0) = 1$ ,  $\chi(C_1) = \pm\sqrt{-1}$ ,  $\chi(C_2) = -1$  and  $\chi(C_3) = \mp\sqrt{-1}$ , by Proposition 3.4 and (4.2), we have

$$\Theta_\chi(z) = \frac{1}{2}(\vartheta(z)\vartheta(p_1p_2z) - \vartheta(p_1z)\vartheta(p_2z))|T(4).$$

Comparing the Fourier coefficients of both sides, we have

$$\begin{aligned}
 a_\chi(n) &= \frac{1}{2}(a_{4n}^1 - a_{4n}^2) \\
 &= a_{\{p_1, p_2\}}(n). \quad \square
 \end{aligned}$$

By Theorem A1 together with Corollary 4.7 and Theorem 4.8, we get the following

**COROLLARY A2.** *Let  $p_1, p_2$  and  $p_3$  be prime numbers satisfying the condition (1.8) and assume that the class number of  $\mathbf{Q}(\sqrt{-p_1p_2})$  is 4. Then we have*

$$\begin{aligned}
 [-p_1, p_2, p_3] &= \frac{1}{2}a_{\{p_1, p_2\}}(p_3) \\
 &= \begin{cases} 1 & \text{if there are integers } x, y \text{ satisfying } x^2 + p_1p_2y^2 = 4p_3, \\ -1 & \text{otherwise.} \end{cases}
 \end{aligned}$$

Further, we assume that the class number of  $\mathbf{Q}(\sqrt{-p_1p_3})$  is 4. Then we have

$$a_{\{p_1, p_2\}}(p_3) = a_{\{p_1, p_3\}}(p_2).$$

### References

[Am] F. AMANO, On certain nilpotent extensions and multiple residue symbols, Master thesis, Kyushu University, 2012.

- [Ar] S. ARNO, The imaginary quadratic fields of class number 4, *Acta Arith.* **60** (1992), no. 4, 321–334.
- [F] G. FUJISAKI, *Introduction to Algebraic Number Theory* (Japanese), Shokabo, 1975.
- [H] E. HECKE, Zur Theorie der elliptischen Modulfunktionen, *Math. Ann.* **97** (1927), no. 1, 210–242.
- [HM] T. HIRAMATSU and Y. MIMURA, The modular equation and modular forms of weight one, *Nagoya Math. J.* **100** (1985), 145–162.
- [Mi] T. MIYAKE, *Modular Forms*, Springer Monographs in Mathematics, Springer, 2006.
- [Mo] M. MORISHITA, On certain analogies between knots and primes, *J. Reine Angew. Math.* **550** (2002), 141–167.
- [O] T. ONO, *An introduction to algebraic number theory*, The University Series in Mathematics, Plenum Press, New York, 1990.
- [Sa] S. SAITO, *Number Theory* (Japanese), Kyoritsu, 1997.
- [Se] J.-P. SERRE, Modular forms of weight one and Galois representations, In: *Algebraic number fields: L-functions and Galois properties* (Proc. Sympos., Univ. Durham, Durham, 1975), Academic Press, London, 193–268.
- [Ré] L. RÉDEI, Ein neues zahlentheoretisches Symbol mit Anwendungen auf die Theorie der quadratischen Zahlkörper I, *J. Reine Angew. Math.* **180** (1939), 1–43.
- [Ro] L. ROZANSKY, Reshetikhin's formula for the Jones polynomial of a link: Feynman diagrams and Milnor's linking numbers, *Topology and physics, J. Math. Phys.* **35** (1994), no. 10, 5219–5246.
- [WS] H. WADA and M. SAITO, A Table of Ideal Class Groups of Imaginary Quadratic Fields, *Sophia Kôkyûroku in Mathematics* **28** (1988).
- [Wat] M. WATKINS, Class numbers of imaginary quadratic fields, *Math. Comp.* **73** (2004), no. 246, 907–938.
- [Z] D. ZAGIER, Elliptic modular forms and their application, In: *The 1-2-3 of Modular Forms*, Universitext, Springer, 1–103.

*Present Addresses:*

FACULTY OF MATHEMATICS,  
 KYUSHU UNIVERSITY,  
 744, MOTOOKA, NISHI-KU, FUKUOKA, 819–0395 JAPAN.

FUMIYA AMANO  
*e-mail:* f-amano@math.kyushu-u.ac.jp

HISATOSHI KODANI  
*e-mail:* ma212018@math.kyushu-u.ac.jp

MASANORI MORISHITA  
*e-mail:* morisita@math.kyushu-u.ac.jp

TAKAYUKI SAKAMOTO  
*e-mail:* t-sakamoto@math.kyushu-u.ac.jp

TAKAFUMI YOSHIDA  
*e-mail:* ma212046@math.kyushu-u.ac.jp

TAKESHI OGASAWARA  
 DEPARTMENT OF GENERAL EDUCATION,  
 OYAMA NATIONAL COLLEGE OF TECHNOLOGY,  
 771, NAKAKUKI, OYAMA CITY, TOCHIGI,  
 323–0806 JAPAN.  
*e-mail:* t-ogasawara@oyama-ct.ac.jp