Product Formula of the Cubic Gauss Sum Modulo the Product of the Primes

Tsuyoshi Takagi*

NTT Laboratories, Nippon Telegraph and Telephone Corporation,
3-9-11 Midori-Cho, Musashino-Shi, Tokyo 180, Japan

Communicated by A. C. Woods

Received January 4, 1996; revised March 31, 1996

Let \( \omega \) be a prime in the quadratic field \( \mathbb{Q}(e^{2\pi i/3}) \), and let \( G_3(\omega) \) be the cubic Gauss sum. Matthews [Invent. Math. 52 (1979), 163–185; 54 (1979), 23–52] determined the product formula of \( G_3(\omega) \) using Weierstrass’ \( \wp \) function. In this paper, we establish an analogous result for the cubic Gauss sum modulo the product of the primes. © 1997 Academic Press

1. INTRODUCTION

Let \( p \) be a rational prime congruent to 1 modulo 3, and let \( p = e^{2\pi i/3} \). Thus \( p \) splits in the quadratic fields \( \mathbb{Q}(\omega) \). Let \( \omega \) be the prime element of \( \mathbb{Z}[\omega] \) dividing \( p \) and satisfying the congruence \( \omega \equiv 1 \mod (3) \). We call this \( \omega \) the primary prime with this normalization. The definition of the cubic Gauss sum is

\[
G_3(\omega) = \sum_{r=1}^{p-1} \left( \frac{r}{\omega} \right)_3 e^{2\pi i r p},
\]

(1)

where \( \left( \cdot /\omega \right)_3 \) is the cubic residue symbol. We have \( G_3(\omega)^3 = -p\omega \). However, getting information about \( G_3(\omega) \) itself is quite difficult. Matthews [6] proved the following formula which had been conjectured by Cassels [2]:

\[
G_3(\omega) = p^{1/3} \alpha_\omega(S)^{-1} \prod_{s \in S} \phi \left( \frac{s\theta}{\omega} \right).
\]

(2)

Here, \( p^{1/3} \) is the real cube root of \( p \), \( \phi \) is Weierstrass’ \( \wp \) function, which satisfies the differential equation \( \wp'^2 = 4\wp^3 - 1 \), and \( \theta ( > 0) \) is the smallest real period of \( \wp \). \( S \) is a third-set mod \( (\omega) \): that is, \( S \) is a set of \( (p-1)/3 \)

* This work was carried out while the author was at Nagoya University, Japan. E-mail: ttakagi@nittspe.slab.ntt.co.jp.
elements of \( \mathbb{Z}[\rho] \) such that \( S \cup \rho S \cup \rho^2S \) represents the reduced residue class mod \((\omega)\). Moreover, \( \pi(S) \) is the cube root of \(-1\) such that

\[
\prod_{s \in S} s \equiv \pi(S) \mod (\omega).
\] (3)

We can show the existence of \( \pi(S) \) using Wilson's theorem.

In this paper, we prove that Matthews' product formula holds even if we take the modulus of the product of the primes.

Let \( \mu \) be an element in \( \mathbb{Z}[\rho] \) that is not divisible by \( \rho \). The definition of the cubic Gauss sum is

\[
G_3(\mu) = \sum_{r \in \mathbb{Z}[\rho]/\mu \mathbb{Z}} \left( \frac{r}{\mu} \right)_3 e^{2\pi i \bar{z}(z + \bar{z})},
\] (4)

where \( \bar{z} \) is the complex conjugate of \( z \). This definition coincides with the previous Gauss sum \( G_3(\omega) \), when \( \mu \) is the complex prime \( \omega \).

Let \( \mu = \omega_1 \omega_2 \cdots \omega_n \) where \( \omega_i \) \((i = 1, 2, \ldots, n)\) are the distinct primary primes. Let \( \Gamma \) be a third-set mod \((\mu)\). When we consider the ordered prime factors \( \omega_1, \omega_2, \ldots, \omega_s \) \((s = 1, 2, \ldots, n)\) of \( \mu \), where \( \{i_1, i_2, \ldots, i_s\} \subseteq \{1, 2, \ldots, n\} \), \((i_1 < i_2 < \cdots < i_s)\), we can divide the disjoint \( 2^n - 1 \) sets of \( \Gamma \),

\[
\Gamma_{i_1, i_2, \ldots, i_s} := \{ \gamma \in \Gamma | \omega_{i_1}, \omega_{i_2}, \ldots, \omega_{i_s}, \gamma, \omega_{j} | \gamma \neq i_1, \ldots, i_s \}. \] (5)

Then we define \( \tau(\Gamma) \) as follows:

For \( \Gamma_{i_1, i_2, \ldots, i_s} \), we multiply each element in \( \Gamma_{i_1, i_2, \ldots, i_s} \)

\[
\prod_{\gamma \in \Gamma_{i_1, i_2, \ldots, i_s}} \gamma \equiv \pi(\Gamma_{i_1, i_2, \ldots, i_s}) \mod (\omega_1 \omega_2 \cdots \omega_s),
\] (6)

where

\[
\pi(\Gamma_s)^3 = -1 \quad (s = 1)
\]

\[
\pi(\Gamma_{i_1, i_2, \ldots, i_s})^3 = 1 \quad (s \geq 2). \] (7)

The existence of \( \Gamma_{i_1, i_2, \ldots, i_s} \) follows from Wilson's Theorem in the first case \((s = 1)\) and the second case \((s \geq 2)\) is shown here in the lemma. Then we put

\[
\pi(\Gamma) := \prod_{s = 1}^{n} \pi(\Gamma_{i_1, i_2, \ldots, i_s}).
\]
Theorem. Let \( \omega_i \ (i = 1, 2, \ldots, n) \) be distinct primary primes, \( \mu = \omega_1 \omega_2 \cdots \omega_n \), and \( N(\mu) = m \). Then we have

\[
G_3(\mu) = m^{1/3} \mu z(\Gamma)^{-1} \prod_{\gamma \in \Gamma} \varphi \left( \frac{r\theta}{\mu} \right),
\]
where \( \Gamma \) is a third-set mod \( (\mu) \) and \( m^{1/3} \) is the real cube root of \( m \).

Remark. For the quartic Gauss sum over field \( \mathbb{Q}(\sqrt{-1}) \), we can also prove an extension of Matthews' results modulo the product of the primes.

2. WEIERSTRASS' \( \wp \) FUNCTION AND THE CUBIC RESIDUE SYMBOL

We introduce Weierstrass' \( \wp \) function that has a differential equation such that \( \wp'^2 = 4\wp^3 - 1 \). The periodic lattice is \( \mathbb{Z}[\wp] \theta \ (\theta > 0) \). This function satisfies

\[
\wp(\rho z) = \rho \wp(z).
\]
And we have \( \mu \) times the formula of the \( \wp \) function

\[
\wp(\mu z \theta) = \prod_{r \bmod \mu} \wp \left( z\theta + \frac{r\theta}{\mu} \right),
\]
where \( \mu \) is a mixed number in \( \mathbb{Z}[\wp] \) whose prime factors are normalized by \( 1 \bmod (3) \). (See, for example, [4, 6]).

Next, we look at Gauss' lemma. Let \( \mu \) and \( \nu \) be coprime mixed numbers not divisible by \( 1 - \rho \). Let \( N(\mu) = m \) and \( N(\nu) = n \). The third-set mod \( (\mu) \) is defined by

\[
\mathbb{Z}[\wp]/(\mu) = \{ 0 \} \sqcup \Gamma_{\mu} \sqcup \rho \Gamma_{\mu} \sqcup \rho^2 \Gamma_{\mu}.
\]

The number of elements in \( \Gamma_{\mu} \) is \((m - 1)/3\). For \( \gamma \in \Gamma_{\mu} \), we can choose the cube root of unity \( \zeta_{\alpha, \gamma} \) and \( \tilde{\gamma} \in \Gamma_{\mu} \) such that

\[
\gamma \equiv \zeta_{\alpha, \gamma} \tilde{\gamma} \pmod{(\mu)}.
\]

Then the cubic residue symbol is

\[
\prod_{\gamma \in \Gamma_{\mu}} \zeta_{\alpha, \gamma} = \left( \frac{\nu}{\mu} \right)_3.
\]
We take $\mu$ and $v$ having distinct and primary primes factors. Then from Eqs. (9) and (10), we get the equation

$$\left( \frac{\gamma}{\mu} \right)_3 = \prod_{\gamma \in \Gamma_\mu} \varphi \left( \frac{\gamma \theta + \gamma' \theta}{\mu + \gamma' \theta} \right) \varphi \left( \frac{\gamma \theta + \rho \gamma' \theta}{\mu + \rho \gamma' \theta} \right), \quad (11)$$

where $\Gamma_\mu$ and $\Gamma_v$ are the third-set mod ($\mu$) and ($v$). We have the reciprocity law of the cubic residue symbol

$$\left( \frac{\gamma}{\mu} \right)_3^* = \left( \frac{\gamma}{v} \right)_3^*, \quad (12)$$

where $\mu$ and $v$ are ($\mu, v) = (\mu, 1 - \rho) = (v, 1 - \rho) = 1$ and have only the distinct primary primes. (See [4]).

**Lemma.** Let $\omega_i (i = 1, 2, \ldots, n), (n \geq 2)$ be any sets of primary primes in $\mathbb{Z}[p]$ that are all different. Let $\mu = \omega_1 \omega_2 \cdots \omega_k$ and $v = \omega_{k+1} \omega_{k+2} \cdots \omega_n$. Let $\Gamma_\mu$ and $\Gamma_v$ be the third-set mod ($\mu$) and ($v$) respectively

$$\left( \frac{\gamma}{\mu} \right)_3 = \alpha(\Gamma_\mu)^{-1} \prod_{\gamma \in \Gamma_\mu} \varphi \left( \frac{\gamma \theta}{\mu + \gamma \theta} \right)^{\gamma' \theta} \mod (\mu v). \quad (13)$$

Here, $\alpha(\Gamma_\mu)$ is a cube root of unity depending on $\Gamma_\mu$, and is defined as

$$\alpha(\Gamma_\mu) \equiv \prod_{\gamma \in \Gamma_\mu} \gamma \mod (\mu v).$$

**Proof.** From Eq. (11),

$$\left( \frac{\mu}{\gamma} \right)_3 = \prod_{\gamma \in \Gamma_\mu} \varphi \left( \frac{\gamma \theta + \rho \gamma' \theta}{\mu + \rho \gamma' \theta} \right).$$

We define

$$\Gamma' := \{ \gamma \mu + \rho \gamma' v \mid \gamma \mu \in \Gamma_\mu, \gamma' \in \Gamma_v, \gamma, \gamma' = 0, 1, 2 \}. \quad (14)$$

Here, $\Gamma'$ is the subset of the special third-set mod ($\mu v$), which is not divisible by both $\mu$ and $v$. Each element of this set from the elements of $\Gamma_\mu$
only by being multiplied by the cube root of unity. Let \( N = (N^2 - 1) / 3 \). For each element \( r_b (b = 1, \ldots, N) \) in \( T \), we have a corresponding element \( r_b \rho^b \) in \( T_{\rho} \). Therefore,

\[
\left\lfloor \frac{\mu}{\nu} \right\rfloor = \left\lfloor \left( \prod_{b=1}^{N} \rho^b \right) \prod_{\gamma \in T_{\nu}} \varphi(\frac{\varphi(\gamma \rho^b)}{\mu \nu}) \right\rfloor
\]

\[\prod_{\gamma \in T} \gamma' \equiv \alpha(T_{\mu}) \mod (\mu \nu).\]

All we have to do is to check \( \prod_{\gamma \in T} \gamma' \). In fact, we have

\[\prod_{\gamma \in T} \gamma' \equiv 1 \mod (\mu \nu). \tag{15}\]

We shall prove this. Let \( T_{\mu} \) be the third-set mod \( (\mu \nu) \). We take the \( 2^k - 1 \) prime factors of \( \mu \) such that \( \omega_{i_1}, \omega_{i_2}, \ldots, \omega_{i_k} \) (\( s = 1, 2, \ldots, k \)), where \( \{i_1, i_2, \ldots, i_k\} \subseteq \{1, 2, \ldots, k\} \) (\( i_1 < i_2 < \cdots < i_k \)), and \( 2^k - 1 \) prime factors of \( \nu \) such that \( \omega_{j_1}, \omega_{j_2}, \ldots, \omega_{j_k} \) (\( t = 1, 2, \ldots, n - k \)), where \( \{j_1, j_2, \ldots, j_k\} \subseteq \{k + 1, k + 2, \ldots, n\} \) (\( j_1 < j_2 < \cdots < j_k \)). Then we can decompose \( T_{\mu} \) into subsets defined in Eq. (5), such that

\[
\Gamma_{i_1, i_2, \ldots, i_k} = \{ \gamma \in \Gamma | \omega_{i_1} \gamma, \omega_{i_2} \gamma, \ldots, \omega_{i_k} \gamma \ (j \neq i_1, \ldots, i_k) \}
\]

\[
\Gamma_{j_1, j_2, \ldots, j_l} = \{ \gamma \in \Gamma | \omega_{j_1} \gamma, \omega_{j_2} \gamma, \ldots, \omega_{j_k} \gamma \ (j \neq j_1, \ldots, j_k) \}.
\]

Let \( N_{\omega_{i_1} \omega_{i_2} \cdots \omega_{i_k}} \) be the third-set mod \( (\omega_{i_1} \omega_{i_2} \cdots \omega_{i_k}) \). And let \( \mu/((\omega_{j_1} \omega_{j_2} \cdots \omega_{j_k})) = \mu_{i_1, i_2, \ldots, i_k} \) and \( \nu/((\omega_{j_1} \omega_{j_2} \cdots \omega_{j_k})) = \nu_{j_1, j_2, \ldots, j_k} \). Then we can choose the special third-set \( \Gamma_{\omega_{i_1} \omega_{i_2} \cdots \omega_{i_k}} \) which satisfies \( T_{\rho} \geq \nu_{j_1, j_2, \ldots, j_k} \times \Gamma_{\omega_{i_1} \omega_{i_2} \cdots \omega_{i_k}} \) and \( \Gamma_{\omega_{i_1} \omega_{i_2} \cdots \omega_{i_k}} \) which satisfies \( T_{\rho} \geq \mu_{i_1, i_2, \ldots, i_k} \Gamma_{\omega_{i_1} \omega_{i_2} \cdots \omega_{i_k}} \). Then we have

\[
\Gamma_{i_1, i_2, \ldots, i_k} = \nu_{j_1, j_2, \ldots, j_k} \mu_{i_1, i_2, \ldots, i_k} \Gamma_{\omega_{i_1} \omega_{i_2} \cdots \omega_{i_k}}, \quad \Gamma_{j_1, j_2, \ldots, j_l} = \mu_{i_1, i_2, \ldots, i_k} \Gamma_{\omega_{i_1} \omega_{i_2} \cdots \omega_{i_k}} \tag{16}\]

From this, we can also decompose the product \( \prod_{\gamma' \in R} \gamma' \).

\[
\prod_{r_{\gamma} \in T} \{ r_{\gamma} \mu + \rho r_{\gamma} \nu \} = \prod_{i_1 < j_1 < \cdots < i_k} \prod_{j_1 < j_2 < \cdots < j_l} \prod_{s=1}^{k} \prod_{t=k+1}^{n} \prod_{\gamma \in \Gamma_{\omega_{i_s} \omega_{i_{s+1}} \cdots \omega_{i_k}}} \{ r_{\gamma} \nu_{j_1, j_2, \ldots, j_l} (\mu + \rho r_{\gamma} \mu_{i_1, i_2, \ldots, i_k}) \}
\]

\[
\times \prod_{r_{\gamma} \in T} \{ r_{\gamma} \nu_{j_1, j_2, \ldots, j_l} (\mu + \rho r_{\gamma} \mu_{i_1, i_2, \ldots, i_k}) \}
\]

\[
\times \prod_{r_{\gamma} \in T} \{ r_{\gamma} \nu_{j_1, j_2, \ldots, j_l} (\mu + \rho r_{\gamma} \mu_{i_1, i_2, \ldots, i_k}) \}
\]
This shows that in the product we can reduce mod (μ) and mod (ν) to mod (ω1, ω2, ..., ωk) and mod (ωk+1, ωk+2, ..., ωn). Therefore, we shall check the product modulo one prime number such that

\[ \prod_{r \in S_i} \{ r \cdot v \cdot \mu + p^r \cdot r \cdot \mu \cdot v \} \equiv 1 \mod (\mu \cdot \nu), \]

where \( i = 1, 2, ..., k \) and \( j = k+1, k+2, ..., n \). We note \( S_i = I_{\omega_i}^r \) (\( i = 1, 2, ..., n \)), this corresponds to the case \( s = 1 \) in Eq. (7). Here, \( S_i \) and \( S_j \) do not depend on the representation of mod (ω1) and mod (ωj). We take \( \{ 1, 2, ..., N(0|2) = p_j \} \) and \( \{ 1, 2, ..., N(0|1) = p_j \} \) as the representation of mod (ω1) and mod (ωj). From the definition of the cubic residue symbol, we reduce mod (ωj),

\[ \prod_{r \in S_i} \{ r \cdot v \cdot \mu + p^r \cdot r \cdot \mu \cdot v \} \equiv \left( \prod_{r \in S_i} r^3 \right)^{(p_j - 1)/3} \left( \frac{\mu \cdot v}{\omega_j} \right)^{p_j - 1} \mod (\omega_j) \]

\[ \equiv (p_j - 1)^{p_j - 1/3} \mod (\omega_j) \]

\( p_j \) is a rational prime which is 1 mod 3, and by Wilson’s theorem, this is 1 mod (ωj). In the same manner it is 1 mod (ωj). Therefore, the lemma holds.

**Remark.** From Eq. (15), we have

\[ \alpha(\Gamma_{\mu}) \equiv \prod_{b = 1}^{\infty} \rho^b \mod (\mu \cdot \nu). \]

This shows the existence of Eq. (7).

3. PROOF OF THE THEOREM

We have the basic properties of the Gauss sum \( G_3(\mu) \) in Eq. (4), modulo a mixed number \( \mu \) which is not divided by \( 1 - \rho \). For coprime numbers \( \mu_1 \) and \( \mu_2 \), the Gauss sum \( G_3(\mu_1, \mu_2) \) decomposes

\[ G_3(\mu_1, \mu_2) = \left( \frac{\mu_2}{\mu_1} \right) \left( \frac{\mu_1}{\mu_2} \right) G_3(\mu_1) G_3(\mu_2). \]  

(See, for example, [5]). Then, the Gauss sum \( G_3 \) modulo the power of a prime is trivial, such that

\[ G_3(\rho^k) = 0, \]
where $\mathcal{P}$ is a prime. (See, for example, [5]). From this fact, it is enough to only calculate the Gauss sum modulo the product of different primes. For one complex prime in $\mathbb{Z}[\rho]$, we have the result of Matthews Eq. (2). And for a rational prime in $\mathbb{Z}[\rho]$,

\[ G_3(q_1 q_2 \cdots q_n) = q_1 q_2 \cdots q_n, \]

holds, where $q_i$ ($i = 1, 2, \ldots, n$) are different rational primes. (See, for example, [2]). Therefore, to determine the Gauss sum modulo the mixed number, we need only check the Gauss sum modulo different split primes i.e., $G_3(\omega_1 \omega_2 \cdots \omega_n)$.

We prove the theorem by induction. Assume the theorem is true up to $k$.

\[ G_3(\omega_1 \cdots \omega_k) = (p_1 \cdots p_k)^{1/3} (\omega_1 \cdots \omega_k) \]

\[ \times \left\{ \alpha(\Gamma_0) \alpha(\Gamma_1) \cdots \alpha(\Gamma_k) \right\}^{-1} \prod_{\gamma \in \Gamma} \phi \left( \frac{\gamma \theta}{\omega_1 \cdots \omega_k} \right), \]

where $\Gamma$ is the third-set mod $(\omega_1 \cdots \omega_k)$, and

\[ \Gamma_i = \{ \gamma \in \Gamma | \omega_i/\gamma, \omega_j/\gamma, (i \neq j) \} \quad (i = 1, 2, \ldots, k), \]

and $\Gamma_0$ is the subset of $\Gamma$, which is the part of the product of $s \geq 2$ in Eq. (7), and $\alpha(\Gamma_0)$ is the cube root of unity. From Eq. (17), we decompose the Gauss sum.

\[ G_3((\omega_1 \omega_2 \cdots \omega_k) \omega_{k+1}) \]

\[ = \left( \frac{\omega_{k+1}}{\omega_1 \omega_2 \cdots \omega_k} \right)^2 (p_1 p_2 \cdots p_k)^{1/3} (\omega_1 \omega_2 \cdots \omega_k) \]

\[ \times \left\{ \alpha(\Gamma_0) \alpha(\Gamma_1) \cdots \alpha(\Gamma_k) \right\}^{-1} \prod_{\gamma \in \Gamma} \phi \left( \frac{\gamma \theta}{\omega_1 \cdots \omega_k} \right) \]

\[ \times \prod_{\gamma \in \Gamma} \phi \left( \frac{\gamma \theta}{\omega_1 \cdots \omega_k} \right) p_k^{1/3} \omega_{k+1} \alpha(S_{k+1})^{-1} \prod_{s_k+1 \neq s_{k+1}} \phi \left( \frac{s_{k+1} \theta}{\omega_{k+1}} \right). \]

Let $\hat{\Gamma}$ be the third-set mod $(\omega_1 \omega_2 \cdots \omega_k \omega_{k+1})$. We define

\[ \hat{\Gamma}_0 := \{ \gamma \in \hat{\Gamma} | \omega_1 \cdots \omega_k / \gamma, \omega_{k+1} / \gamma \} \]

\[ \hat{\Gamma}_0 := \frac{1}{3} (p_1 \cdots p_k - 1)(p_k + 1 - 1) \]

\[ \hat{\Gamma}_{1, \ldots, k} := \{ \gamma \in \hat{\Gamma} | \omega_{k+1} / \gamma \} \]

\[ \hat{\Gamma}_{1, \ldots, k} := \frac{1}{3} (p_1 \cdots p_k - 1) \]

\[ \hat{\Gamma}_{k+1} := \{ \gamma \in \hat{\Gamma} | \omega_i (i = 1, \ldots, k), \omega_{k+1} / \gamma \} \]

\[ \hat{\Gamma}_{k+1} := \frac{1}{3} (p_k + 1 - 1). \]
Then $\tilde{\Gamma}$ decomposes into the disjoint subset so that $\tilde{\Gamma} = \tilde{\Gamma}_0 \sqcup \tilde{\Gamma}_{1, \ldots, k} \sqcup \tilde{\Gamma}_{k+1}$.

From Eq. (16), we choose $\Gamma$ and $S_{k+1}$ such that $\tilde{\Gamma} \supset \omega_{k+1} \Gamma$ and $\tilde{\Gamma} \supset \omega_1 \cdots \omega_k S_{k+1}$. We have

$$\tilde{\Gamma}_{1, \ldots, k} = \omega_{k+1} \Gamma$$
$$\tilde{\Gamma}_{k+1} = \omega_1 \cdots \omega_k S_{k+1}.$$  

By the definition of the cubic residue symbol,

$$\varepsilon(\tilde{\Gamma}_{k+1}) = \left( \frac{\omega_1 \cdots \omega_k}{\omega_{k+1}} \right) \varepsilon(S_{k+1}).$$

We also define the subset of $\tilde{\Gamma}$

$$\tilde{\Gamma}_i = \{ \gamma \in \tilde{\Gamma} \mid \omega_i | \omega_j | \gamma (i \neq j) \} \quad (i = 1, \ldots, k),$$

From $\tilde{\Gamma} \supset \omega_{k+1} \Gamma \supset \omega_{k+1} \Gamma_i$, we have

$$\tilde{\Gamma}_i = \omega_{k+1} \Gamma_i$$
$$\varepsilon(\tilde{\Gamma}_i) = \left( \frac{\omega_{k+1}}{\omega_i} \right) \varepsilon(\Gamma_i) \quad (i = 1, \ldots, k)$$

By the reciprocity law of the cubic residue symbol,

$$\left( \frac{\omega_{k+1}}{\omega_1 \cdots \omega_k} \right)^2 \left( \frac{\omega_1 \cdots \omega_k}{\omega_{k+1}} \right) \left( \frac{\omega_{k+1}}{\omega_1} \right) \left( \frac{\omega_1}{\omega_2} \right) \cdots \left( \frac{\omega_k}{\omega_{k+1}} \right) = \left( \frac{\omega_1 \cdots \omega_k}{\omega_{k+1}} \right)^3.$$

Therefore,

$$G_i(\omega_1 \cdots \omega_k \omega_{k+1})$$
$$= (p_1 \cdots p_{k+1} \omega_{k+1})^{1/3} (p_1 \cdots p_k \omega_{k+1}) \varepsilon(\tilde{\Gamma}_1) \cdots \varepsilon(\tilde{\Gamma}_k) \varepsilon(\tilde{\Gamma}_{k+1}) \left( \frac{s_{k+1} \theta}{\omega_{k+1}} \right)^{-1}$$
$$\cdot \left( \frac{\omega_1 \cdots \omega_k}{\omega_{k+1}} \right)^3 \prod_{\gamma \in \tilde{\Gamma}} \varphi \left( \frac{\gamma \theta}{\omega_1 \cdots \omega_k} \right) \prod_{\gamma \in \tilde{\Gamma}} \varphi \left( \frac{s_{k+1} \theta}{\omega_{k+1}} \right). \quad (18)$$

From the lemma, if we take $\mu = \omega_1 \omega_2 \cdots \omega_k$ and $v = \omega_{k+1}$, then we have

$$\left( \frac{\omega_1 \cdots \omega_k}{\omega_{k+1}} \right)^3 = \varepsilon(\tilde{\Gamma}_0) \prod_{\gamma \in \tilde{\Gamma}_k} \varphi \left( \frac{\gamma \theta}{\omega_1 \cdots \omega_k \omega_{k+1}} \right). \quad (19)$$
Here, \( \alpha(\vec{r}_0) \) is the cube root of unity depending on \( \vec{r} \) and is defined as
\[
\alpha(\vec{r}_0) = \prod_{\gamma \in \vec{r}_0} \gamma \mod (\omega_1 \cdots \omega_{k+1}) \quad \text{s.t.} \quad \alpha(\vec{r}_0)^3 = 1.
\]
\( \alpha(\vec{r}_0) \) is all the products in Eq. (8) such that \( s \geq 2 \). Therefore, we write the cubic residue symbol \( \varphi \) function, and change the product to the subset of \( \vec{r} \):
\[
\prod_{\gamma \in \vec{r}_s} \varphi\left(\frac{\gamma \theta}{\omega_1 \cdots \omega_{k+1}}\right) = \prod_{\gamma \in \vec{r}_s} \varphi\left(\frac{\gamma \theta}{\omega_1 \cdots \omega_{k+1}}\right) \quad (20)
\]
\[
\prod_{s_1 = 1}^{s_k + 1} \varphi\left(\frac{s_{k+1} \theta}{\omega_{k+1}}\right) = \prod_{s_1 = 1}^{s_k + 1} \varphi\left(\frac{s_{k+1} \theta}{\omega_{k+1}}\right) \quad (21)
\]
From Eqs. (19), (20), and (21), we have
\[
\left(\frac{\omega_1 \cdots \omega_k}{\omega_{k+1}}\right) \prod_{\gamma \in \vec{r}_s} \varphi\left(\frac{\gamma \theta}{\omega_1 \cdots \omega_{k+1}}\right) \prod_{s_1 = 1}^{s_k + 1} \varphi\left(\frac{s_{k+1} \theta}{\omega_{k+1}}\right) = \alpha(\vec{r}_0)^{-1} \prod_{\gamma \in \vec{r}_s} \varphi\left(\frac{\gamma \theta}{\omega_1 \cdots \omega_{k+1}}\right).
\]
This equation is the last part of Eq. (18). Consequently the theorem is proved by induction.

ACKNOWLEDGMENT

I thank Professor H. Ito for his mathematical advice.

REFERENCES