<table>
<thead>
<tr>
<th><strong>Title</strong></th>
<th>On some generic expression of Gauss sums (Algebraic Number Theory)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Author(s)</strong></td>
<td>Miki, Hiroo</td>
</tr>
<tr>
<td><strong>Citation</strong></td>
<td>数理解析研究所講究録 (1987), 603: 35-42</td>
</tr>
<tr>
<td><strong>Issue Date</strong></td>
<td>1987-01</td>
</tr>
<tr>
<td><strong>URL</strong></td>
<td><a href="http://hdl.handle.net/2433/99659">http://hdl.handle.net/2433/99659</a></td>
</tr>
<tr>
<td><strong>Type</strong></td>
<td>Departmental Bulletin Paper</td>
</tr>
<tr>
<td><strong>Textversion</strong></td>
<td>publisher</td>
</tr>
</tbody>
</table>

Kyoto University
On some generic expression of Gauss sums

By Hiroo Miki (三木博雄)

Department of Mathematics, Tokyo Metropolitan University

§ Introduction.

Let \( \ell \) be a fixed odd prime number and let \( \zeta_n \) be a primitive \( \ell^n \)-th root of unity such that \( \zeta_n^{\ell^{n+1}} = \zeta_n \) for \( n=1,2,3,\ldots \). Put \( K_n = \mathbb{Q}(\zeta_n) \) for \( n \geq 1 \), where \( \mathbb{Q} \) is the field of rational numbers. Let \( p \) be a prime number different from \( \ell \) and let \( P_n \) be a prime ideal of \( K_n \) for \( n \geq 1 \) satisfying

\[
(p) \subset P_1 \subset P_2 \subset \cdots \subset P_n \subset P_{n+1} \subset \cdots.
\]

We fix such a sequence of prime ideals. Let

\[
\chi_{P_n}(x \mod P_n) = \chi_n(x \mod P_n) = \left( \frac{x}{P_n} \right)
\]

be the \( \ell^n \)-th power residue symbol in \( K_n \) for \( x \in \mathbb{Z}[\zeta_n] \), where \( \mathbb{Z} \) is the ring of rational integers. If \( x \notin P_n \), then \( \chi_n(x \mod P_n) \) is the unique \( \ell^n \)-th root of unity satisfying the congruence

\[
\chi_n(x \mod P_n) \equiv x^{(N_{P_n}/\ell^n - 1)} \pmod{P_n},
\]
where $N_{\mathbb{F}_n}$ is the absolute norm of $\mathbb{F}_n$. If $x \in \mathbb{F}_n$, then $\chi_n(0) = 0$.

Now we state the definition of Gauss sums and Jacobi sums.

Put $\psi_n(x) = \zeta_p^T_n(x)$ for $x \in \mathbb{Z}[\zeta_{\mathbb{F}_n}] / \mathbb{F}_n$, where $T_n : \mathbb{Z}[\zeta_{\mathbb{F}_n}] / \mathbb{F}_n \rightarrow \mathbb{F}_p$ (the field of $p$ elements) is the trace map.

**Definition.** For $a \in \mathbb{Z}$, put

$$g(\chi_n^a) = g_n(a) = g_{\mathbb{F}_n}(\mathbb{F}_n, a) = - \sum_{x \in \mathbb{Z}[\zeta_{\mathbb{F}_n}] / \mathbb{F}_n} \chi_{\mathbb{F}_n}^a(x) \psi_n(x).$$

The sum is called a Gauss sum.

**Definition.** For $a, b \in \mathbb{Z}$, put

$$J_{\mathbb{F}_n}(a, b) = - \sum_{\substack{x, y \in \mathbb{Z}[\zeta_{\mathbb{F}_n}] / \mathbb{F}_n \atop x + y = -1}} \chi_{\mathbb{F}_n}^a(x) \chi_{\mathbb{F}_n}^b(y).$$

The sum is called a Jacobi sum.

As is well known, Gauss sums and Jacobi sums have close relation to each other; the Jacobi sum can be expressed in terms of Gauss sums in the following:

$$J_{\mathbb{F}_n}(a, b) = (N\mathbb{F}_n)^{-1} g_{\mathbb{F}_n}(\mathbb{F}_n, a) g_{\mathbb{F}_n}(\mathbb{F}_n, b) g_{\mathbb{F}_n}(\mathbb{F}_n, c),$$

where $a + b + c \equiv 0 \pmod{\zeta_{\mathbb{F}_n}}$ and $(a, b, c) \neq (0, 0, 0) \pmod{\zeta_{\mathbb{F}_n}}$.

Recently, Y. Ihara ([7], Theorem 7) found a power series which
interpolates \( J^{(a,b)}(\mathcal{P}_n) \) with \( n=1,2,3,\ldots \). Put
\[
\Lambda = Z_\ell[[u,v,w]]/((1+u)(1+v)(1+w)-1) = Z_\ell[[u,v]],
\]
where \( Z_\ell[[u,v,w]] \) is the formal power series ring in three variables \( u, v \) and \( w \) over the ring of \( \ell \)-adic integers \( Z_\ell \).

**Theorem ([7],Theorem 7).** There exists a power series
\[
F_p(u,v,w) \in \Lambda \quad \text{satisfying}
\]
\[
J^{(a,b)}(\mathcal{P}_n) = \prod_{i=0}^{f_n-1} F_p(\zeta_a^{p^i} - 1, \zeta_b^{p^i} - 1, \zeta_c^{p^i} - 1)
\]
for all \( a,b,c \in Z \) such that \( (a,b,c) \not\equiv (0,0,0) \mod \ell \) and \( a+b+c \equiv 0 \mod \ell^n \), and for all \( n \geq 1 \). Here \( f_n \) is the order of \( p \) in \( (Z/\ell^n)^\times \).

Note that Ihara([7],Theorem 7) gives a more general result than the above statement.

For the proof, Ihara [7] uses the \( \ell \)-adic Tate module of the Jacobian variety of the Fermat curve of degree \( \ell^n \) in the limit as \( n \rightarrow \infty \), and studies its Galois module structure; the module is a free \( \Lambda \)-module of rank 1 and the action of Frobenius over \( p \) on the module corresponds to the above Ihara's power series \( F_p(u,v,w) \).

At the Kyoto conference Oct.1985, G. Anderson stated that he found a power series of one variable interpolating Gauss sums into which Ihara's power series can be factored (see [1]). Using Deligne's
theory [5] on absolute Hodge cycles, he develops the theory of hyperadelic gamma functions and beta functions, and relates Ihara's power series to Anderson's adelic beta function.

In the present paper, we shall consider the following purely local problem.

**Problem (purely local).** For a given sequence of local $\ell$-units $u_1, u_2, \ldots, u_n, \ldots$, find a necessary and sufficient condition for $u_1, u_2, \ldots, u_n, \ldots$ to be interpolated as in the above Ihara's Theorem.

In the following, we shall give a partial answer to the problem and obtain another proof of the special case of Anderson's result.

§1 Interpolation of local units in $\mathbb{Q}_\ell(\zeta_p)$.

Put $K'_i = \mathbb{Q}_\ell(\zeta_{p^i})$ for $i=1, 2, 3, \ldots$, where $\mathbb{Q}_\ell$ is the field of $\ell$-adic numbers.

**Theorem 1.** Let $u_1, u_2, \ldots, u_n, \ldots$ be a sequence of principal units of $K'_1$. Then there exists a power series $F(T) \in \mathbb{Z}[\zeta_p][[T]]$, $F(T) \equiv 1 \pmod{T}$, satisfying $N_{K'_i/K'_1}(F(\zeta_{p^i}^{-1})) = u_i$ for all $i \geq 1$, if and only if the following two conditions (i) and (ii) are satisfied for all $i \geq 1$.

(i) $N_{K'_i/\mathbb{Q}_\ell}(u_i) \equiv 1 \pmod{\ell^i}$. 
(ii) \( u_{i+1} \equiv u_i^\tau \pmod {l^i} \), where \( \tau \in G(Q(\zeta_\infty)/Q_\ell(\zeta_\infty)) \) is the Frobenius automorphism.

The proof is rather complicated and technical. We use local class field theory and the analysis of elements of norm 1, in particular, Hasse's classical result on the relation between the norms and the Hasse function (cf. e.g. Serre [14]), but we do not use algebraic geometry.

We also note that the above Theorem 1 has a similarity to the Coleman power series [2](see also Theorem 13.38 of Washington [16]).

§2 Congruence for Gauss sums.

Let \( \overline{\mathbb{Q}} \) (resp. \( \overline{\mathbb{Q}}_\ell \)) be an algebraic closure of \( \mathbb{Q} \) (resp. \( \mathbb{Q}_\ell \)). By a fixed imbedding, we consider \( \overline{\mathbb{Q}} \) as a subfield of \( \overline{\mathbb{Q}}_\ell \).

Theorem 2. Let \( M \) be the decomposition field of \( p \) in \( Q(\zeta_{\infty})/Q(\zeta_p) \) and let \( \mathcal{O}_{MQ_\ell} \) be the ring of integers of \( MQ_\ell \).

Let \( \tau \) be as in Theorem 1. Then the following (i),(ii) and (iii) hold for all \( i \geq 1 \).

(i) \( g(\chi_1^a) \in M \).

(ii) \( g(\chi_{i+1}^a) \equiv g(\chi_i^a)^\tau \pmod {\left[ Q(\zeta_{i+1}, p \mathbb{M}) : M \mathbb{M} \right] \mathcal{O}_{MQ_\ell}} \).
(iii) $N_{MQ_\ell/Q_\ell}(g(\chi_i^a)) \equiv 1 \pmod{\ell^iZ_\ell}$.

§3 Interpolation of Gauss sums.

As an application of Theorems 1 and 2, we obtain another proof of the special case of Anderson's result([1]).

Theorem 3. Assume $\ell \mid (p-1)$, i.e., the exact power of $\ell$ dividing $(p-1)$ is $\ell$. Then there exists a power series $F(T) \in Z_\ell[[T]]$ satisfying the following (i) and (ii):

(i) $F(T) \equiv 1 \pmod{T}$.

(ii) $g(\chi_n^a) = \prod_{i=0}^{f_n-1} F(\zeta_n^{ap_i} - 1)$ for all $a \not\equiv 0 \pmod{\ell}$ and for all $n \geq 1$, where $f_n (=\ell^{n-1})$ is the order of $p \pmod{\ell^n}$ in $(\mathbb{Z}/\ell^n)^\times$.

References


[9] Y. Ihara, On Galois representations arising from towers of coverings of $\mathbb{P}^1 \setminus \{0,1,\infty\}$, General constructions, Preprint.


to Weil's Grössencharacter, in preparation.


[15] T. Uehara, On cyclotomic units connected with p-adic characters,

[16] L. Washington, Introduction to Cyclotomic Fields, GTM 83,

[17] A. Weil, Number of solutions of equations in finite fields,

    Soc. 73 (1952), 487-495.

    1974, Nr.1, 14 pp.

Department of Mathematics
Faculty of Science
Tokyo Metropolitan University
Setagaya-ku, Tokyo 158
Japan