On certain congruences for Gauss sums

Tadashi WASHIO, Asako SHIMAURA and Katsumi SHIRATANI*

Department of Mathematics, Faculty of Education, Nagasaki University, Nagasaki 852, Japan
(Received Mar. 15, 1996)

Abstract

In this note, certain congruences for Gauss sums over the finite field $GF(p^r)$ are studied. Especially, in the case of $r=1$, two deductions for the congruence are given as follows: Let $p$ be any odd prime and $\omega$ be the Teichmüller character of conductor $p$. Let $\zeta_p$ be a fixed primitive $p$-th root of unity. Then for the Gauss sum

$g(\omega^r) = \sum_{x \mod p} \omega^r(x) \zeta_p^s(x)$

with respect to any Dirichlet character $\chi = \omega^r$ with $1 \leq r \leq p-2$, two elementary deductions for a congruence

$g(\omega^r) \equiv - \frac{1}{(p-1-r)!} \varpi^{p-1-r} \pmod{p^{2(p-1-r)}}$

are given by making use of the Stickelberger theorem and by making use of the Kummer congruences together with the Artin–Hasse exponential series, where $\varpi$ means the prime ideal in $\mathbb{Q}_p(\zeta_p)$ and $\varpi$ denotes a prime element in $\mathbb{Q}_p(\zeta_p)$ satisfying $\varpi = p^{-1} \sqrt{-p}$ and $\varpi \equiv \zeta_p - 1 \pmod{\varpi^2}$.

§ 1. Introduction

Let $p$ be any odd prime and $\omega$ be the Teichmüller character of the multiplicative group $GF(q)^\times$ of the finite field $GF(q)$, where we set $q = p^r$. For any multiplicative character $\chi = \omega^r$ with $1 \leq r \leq q-2$ we have the Gauss sum

$g(\omega^r) = \sum_{x \in GF(q)^\times} \omega^r(x) \zeta_p^{s(x)}$

where $x$ runs over $GF(q)^\times$ and $\zeta_p$ denotes a fixed primitive $p$-th root of unity and $s(\cdot)$ denotes the trace with respect to $GF(q)/GF(p)$.

For these Gauss sums we know the Stickelberger theorem [1], and the Gross–Koblitz formula [2], from which we can obtain a congruence

$g(\omega^r) \equiv - \frac{\varpi^{s_p(q-1-r)}}{r_0! r_1! \cdots r_{r-1}!} \pmod{p^{p-1+s_p(q-1-r)}}$.  

* Graduate School of Mathematics, Kyushu University, Fukuoka 812, Japan
Herein \( \wp \) means the prime ideal in the prime cyclotomic field \( \mathbb{Q}_p(\zeta_p) \) over the \( p \)-adic rationals \( \mathbb{Q}_p \), and \( \wp \) denotes a prime element in the field \( \mathbb{Q}_p(\zeta_p) \) satisfying \( \wp = p^{-1} \sqrt{-p} \) and \( \wp \equiv \zeta_p - 1 \pmod{p^2} \). In addition we set \( s_p(q-1-r) = r_0 + r_1 + \cdots + r_{f-1} \) for the canonical \( p \)-adic expansion \( q - 1 - r = r_0 + r_1 p + \cdots + r_{f-1} p^{f-1} \) of \( q - 1 - r \) with \( 0 \leq r_i \leq p-1 \) \( (i=0,1,\cdots,f-1) \).

Especially, if \( f=1 \) then we have

\[
\wp^{p-1-r} \equiv \frac{\wp^{p-1-r}}{(p-1-r)!} \pmod{p^{2(p-1-r)}}.
\]

In this note we shall give two elementary deductions for the congruence above. One is given directly from the Stickelberger theorem. The other is given in the case of \( f=1 \) by making use of the Kummer congruences together with the Artin-Hasse exponential series. We believe that our method is of some interest and gives a few applications.

§ 2. Stickelberger theorem and general cases

Let \( \mathfrak{p} \) be such a prime ideal in the field \( \mathbb{Q}(\zeta_{q-1}, \zeta_p) \) that divides the prime ideal \( \wp \) on \( p \) in the field \( \mathbb{Q}(\zeta_{q-1}) \). Then the Stickelberger congruence is known as follows:

Following the Davenport-Hasse arguments [1], the Gauss sum \( g(\omega^r) \) is an integer in the field \( \mathbb{Q}(\zeta_{q-1}, \zeta_p) \) and satisfies the congruence

\[
g(\omega^r) \equiv \frac{\zeta_p^{p(q-1-r)} - 1}{r_0! r_1! \cdots r_{f-1}!} \pmod{\mathfrak{p}^{q-1-r} + 1}.
\]

If we embed \( g(\omega^r) \) into the completion \( \mathbb{Q}(\zeta_{q-1}, \zeta_p)_{\mathfrak{p}} \) and take the prime element \( \wp \) in \( \mathbb{Q}_p(\zeta_p) \), then we have

\[
g(\omega^r) \equiv \frac{\wp^{p(q-1-r)}}{r_0! r_1! \cdots r_{f-1}!} \pmod{\mathfrak{p}^{q-1-r} + 1}.
\]

This follows from the fact that the Gauss sum \( g(\omega^r) \) is left fixed by any element of the Galois group \( G(\mathbb{Q}(\zeta_{q-1}, \zeta_p)_{\mathfrak{p}}/\mathbb{Q}_p(\zeta_p)) \), hence we see that \( g(\omega^r) \) lies in \( \mathbb{Q}_p(\zeta_p) \).

By the way, let \( \rho : \zeta_p \rightarrow \zeta_p^t \) be any element in the Galois group \( G(\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p) \). Then we see immediately \( g(\omega)^n = \omega^{-t}(t) g(\omega) \) and

\[
\wp^{s_p(q-1-r)n} \equiv (\zeta_p^t - 1)^{s_p(q-1-r)} \equiv t^{s_p(q-1-r)} \wp^{s_p(q-1-r)} \pmod{p^n}.
\]

Here we remark that \( \omega(t) \) is a \( (p-1) \)-th root of unity, because \( t \) is in \( \mathbb{Z} \). Thus we have \( \wp^{s_p(q-1-r)n} = \omega^{-t}(t) \wp^{s_p(q-1-r)} \).

Therefore we get the following

Theorem 1. For \( 1 \leq r \leq q-2 \) we have in the field \( \mathbb{Q}_p(\zeta_p) \)

\[
g(\omega^r) \equiv \frac{\wp^{s_p(q-1-r)}}{r_0! r_1! \cdots r_{f-1}!} \pmod{p^{s_p(q-1-r)}}.
\]

But, this congruence is a direct consequence of the Gross-Koblitz formula [2]. In the subsequent section we treat the case of \( f=1 \).
§ 3. Several lemmas

First we have

\[ g(\omega^r) = \sum_{x=0}^{p-1} \omega^r(x) \xi_p^x \]
\[ = \sum_{x=0}^{p-1} \omega^r(x) \sum_{j=0}^{p-1} \binom{x}{j} (\zeta_p - 1)^j \]
\[ = \sum_{j=1}^{p-1} \omega^r(x) \frac{(x)_j}{j!} (\zeta_p - 1)^j \]
\[ = \sum_{j=1}^{p-1} \frac{(\zeta_p - 1)^j}{j!} \sum_{x=0}^{p-1} \omega^r(x) (x)_j, \]

because \( \sum_{x=0}^{p-1} \omega^r(x) = 0 \), and \((x)_j\) denotes the Jordan factorial notation \((x)_j = x(x-1) \cdots (x-j+1)\), \((x)_0 = 1\).

Now we recall the definitions and some basic properties of the Stirling numbers \( S(j, \ell) \) of the first kind and the Stirling numbers \( \ominus(\ell, j) \) of the second kind. They are defined by

\[ (x)_j = \sum_{j=0}^{\ell} S(j, \ell) x^j, \]
\[ x^j = \sum_{j=0}^{\ell} \ominus(\ell, j) (x)_j. \]

It is known that

\[ S(j, \ell) = \sum_{P(j, \ell)} \frac{(-1)^{\ell-j}}{a_1! a_2! \cdots a_r!} \frac{1}{1^{a_1} 2^{a_2} \cdots r^{a_r}}, \]
\[ \ominus(\ell, j) = \sum_{P(\ell, j)} \frac{\ell!}{a_1! a_2! \cdots a_r!} \frac{1}{(1!)^{a_1} (2!)^{a_2} \cdots (\ell!)^{a_r}}, \]

where the summation in the first one is taken over all the partitions \( P(j, \ell) : a_1 + a_2 + \cdots + a_r = \ell, \quad a_1 + 2a_2 + \cdots + ja_j = j, \quad a_i \geq 0 \) and the second one is also taken similarly.

Moreover we have \( \ominus(\ell, j) = \frac{1}{\ell!} A^0 \delta = \frac{1}{\ell!} \sum_{k=0}^{\ell} (-1)^{\ell-k} \binom{\ell}{k} k! \) and the orthogonality relations

\[ \sum_{k=1}^{\ell} S(j, k) \ominus(k, \ell) = \delta_{j, \ell}, \quad \sum_{k=1}^{\ell} \ominus(j, k) S(k, \ell) = \delta_{j, \ell} \]

where \( \delta_{j, \ell} \) means the Kronecker delta symbol.

Hence we see

\[ g(\omega^r) = \sum_{j=1}^{p-1} \frac{1}{j!} (\zeta_p - 1)^j \sum_{x=0}^{p-1} \omega^r(x) S(j, \ell) x^j \]
\[ + \sum_{j=p-1-r}^{p-1} \frac{1}{j!} (\zeta_p - 1)^j \sum_{x=0}^{p-1} \omega^r(x) S(j, \ell) x^j. \]

Lemma 1. We have \( \sum_{x=1}^{p-1} \omega^r(x) x^j \equiv -\delta_{r+1, p-1} \pmod{p} \).

Proof. This is clear from \( \omega^r(x) \equiv x^r \pmod{p} \).

Lemma 2. For \( 1 \leq \ell \leq 2(p-1)-r-1 \) we have
\[
\sum_{x=1}^{p-1} \omega(x)x^t \equiv (1-r)pB_{r+t} + rpB_{r+t+p-1} \quad (\text{mod } p^2).
\]

Here we denote the \(i\)-th Bernoulli number by \(B_i\), which is defined by \(\frac{te^t}{e^t-1} = \sum_{i=0}^{\infty} \frac{1}{i!} B_i t^i\).

Proof. Let \(q_x = \frac{1}{p}(x^{p-1} - 1)\) be the Fermat quotient of \(x \in \mathbb{Z}\) prime to \(p\). Then we know \(\omega(x) = x(1 + pq_x)^{-\frac{1}{p}}\) in \(\mathbb{Z}_p\) [2]. Therefore we see

\[
\sum_{x=1}^{p-1} \omega(x)x^t \equiv \sum_{x=1}^{p-1} x^{r+t} (1 + rpq_x) \quad (\text{mod } p^2)
\]

\[
= (1-r) \sum_{x=1}^{p-1} x^{r+t} + r \sum_{x=1}^{p-1} x^{r+t+p-1} \quad (\text{mod } p^2)
\]

\[
= (1-r) \sum_{x=1}^{p-1} x^{r+t} + r \sum_{x=1}^{p-1} x^{r+t+p-1} \quad (\text{mod } p^2),
\]

because \(r + \ell \geq 2\) by the assumption on \(r, \ell\).

By the way we see from the summation formula

\[
\sum_{x=1}^{p-1} x^{r+t} = \frac{1}{r + \ell + 1}(B + p)^{r+t+1} - B^{r+t+1}
\]

\[
= pB_{r+t} + \sum_{i=1}^{r+t+1} \left( \frac{r + \ell}{i} \right) \frac{1}{i} B_i p^{r+t+1-i} + \frac{1}{r + \ell + 1} B_0 p^{r+t+1}
\]

\[
= pB_{r+t} + \left( \frac{r + \ell}{2} \right) \frac{1}{r + \ell + 1} B_{r+t+1} p^2 \quad (\text{mod } p^2),
\]

Herein we have used \(2 \leq r + \ell \leq 2p - 3 < p^2\) and \(\frac{1}{i} B_i\) has \(p^2\) at most as its denominator, which is the von Staudt-Clausen theorem. Similarly we have

\[
\sum_{x=1}^{p-1} x^{r+t+p-1} = pB_{r+t+p-1} + \binom{r + \ell + p - 1}{2} \frac{1}{r + \ell + p - 2} B_{r+t+p-2} p^2 \quad (\text{mod } p^2).
\]

The condition \(r + \ell - 1 = 0 \quad (\text{mod } p-1)\) occurs only when \(r + \ell = p\) or \(r + \ell = 2p - 1\) in the given range of \(r\) and \(\ell\) in the above. If \(1 \leq \ell \leq j \leq 2(p-1) - r - 1\), then \(r + \ell - 1 \equiv 0 \quad (\text{mod } p-1)\) is just equivalent to \(r + \ell = p\). Thus we obtain the congruence in our assertion.

Next we consider two cases separately.

If \(r + \ell \neq p - 1\), then we have a congruence of Kummer

\[
\frac{1}{r + \ell + p - 1} B_{r+t+p-1} = \frac{1}{r + \ell} B_{r+t} \quad (\text{mod } p),
\]

therefrom we have

\[
rpB_{r+t+p-1} \equiv rpB_{r+t} - \frac{rp}{r + \ell} B_{r+t} \quad (\text{mod } p^2).
\]

Thus we obtain

**Lemma 3.** For \(1 \leq \ell \leq 2(p-1) - r - 1\), \(r + \ell \neq p - 1\) we have
On certain congruences for Gauss sums

\[ \sum_{x=1}^{p-1} \omega^r(x)x^t \equiv p \frac{\ell}{r+\ell} B_{r+t} \pmod{p^2}. \]

If \( r + \ell = p - 1 \), then we set \( pB_{p-1} = -1 + p\alpha_p \) with \( \alpha_p \in \mathbb{Z}_p \). We see \( B_{2(p-1)}\equiv 1 - \frac{1}{p} + i(a_p - 1) \pmod{p} \) for \( p \geq 5, i \geq 1 \). Especially we have

\[ pB_{2(p-1)} = -1 + p + 2p(a_p - 1) \pmod{p^2}. \]

Hence we see from Lemma 2

\[ \sum_{x=1}^{p-1} \omega^r(x)x^t \equiv (1 - r)( -1 + p\alpha_p) + r(p - 1 + 2p\alpha_p - 2p) \pmod{p^2} \]

\[ \equiv -1 + p\alpha_p + rp(a_p - 1) \pmod{p^2} \]

\[ \equiv pB_{p-1} + (\ell + 1)(1 - a_p)p \pmod{p^2} \]

\[ \equiv -1 - (1 + pB_{p-1})\ell + (\ell + 1)p \pmod{p^2}. \]

We state this result in the following

**Lemma 4.** For \( 1 \leq \ell \leq 2(p-1) - r - 1, r + \ell = p - 1 \) we have

\[ \sum_{x=1}^{p-1} \omega^r(x)x^t \equiv -1 - (1 + pB_{p-1})\ell + (\ell + 1)p \pmod{p^2}. \]

However we do not use this congruence in the sequel. In the first summation in (1) the term with \( r + \ell = p - 1 \) vanishes, because we have necessarily \( S(j, p - 1 - r) = 0 \) for \( 1 \leq j \leq p - 1 - r - 1 \).

Thus, for the first sum in (1), we have by Lemma 3

\[ \sum_{j=1}^{p-2} \frac{1}{j!}(\zeta_p - 1)^j \sum_{x=1}^{p-1} S(j, \ell) \sum_{x=1}^{p-1} \omega^r(x)x^t \]

\[ \equiv \sum_{j=1}^{p-2} \frac{1}{j!}(\zeta_p - 1)^j \sum_{x=1}^{p-1} S(j, \ell)p \frac{\ell}{r+\ell} B_{r+t} \pmod{p^{2(p-1)}}. \]

§ 4. The congruence

Let \( \omega = p^{-1/\sqrt{-p}} \) be a prime element in \( \mathbb{Q}(\zeta_p) \) such that \( \omega \equiv \zeta_p - 1 \pmod{\wp^2} \) holds.

Then by making use of the Artin–Hasse exponential series \( E(X) = e^{L(X)} \) with \( L(X) = \sum_{r=0}^{\omega-1} \frac{X^r}{r!} X^t \) we have a congruence [3]

\[ \omega \equiv \sum_{r=0}^{p-1} (-1)^{r-1} e^{p^{p^r}} \pmod{p^{p^r}}, \]

\[ \omega = E(\omega) \pmod{p^{p^r}} \]

\[ = \sum_{r=0}^{p-1} \frac{1}{r!} \omega^r - \left( 1 + \frac{1}{(p-1)!} \right) \omega \pmod{p^{p^r}}. \]

Set \( 1 + \frac{1}{(p-1)!} = p\beta_p \) with \( \beta_p \in \mathbb{Z}_p \). From these congruences we have for \( 1 \leq j \leq p - 1 \)

\[ \frac{1}{j!}(\zeta_p - 1)^j \equiv \sum_{r=0}^{2(p-1) - r - 1} \frac{1}{t!}(t, j) \omega^t \pmod{p^{2(p-1) - r}}. \]
As for the first sum in (1) we have from the congruence \( \frac{1}{j!}(\xi_p - 1) \equiv \sum_{j=0}^{p-1} \frac{1}{j!} \xi(t, j) \xi^t \pmod{p^r} \)

\[
(2) \quad \sum_{j=0}^{p-1} \frac{1}{j!} \sum_{t=0}^{p-1} \xi(t, j) \xi^t \lbrack \xi^p - 1 \rbrack \equiv - \sum_{j=1}^{p-2} \frac{1}{j!} \sum_{t=1}^{p-1} \xi(t, j) \xi^t \pmod{p^r},
\]

Now, together with Lemma 1, the second sum in (1) becomes

\[
- \sum_{j=p-r}^{p-1} \frac{1}{j!} \sum_{t=p-r}^{p-1} \xi(t, j) \xi^t \pmod{p^r}.
\]

Here we need the following

**Lemma 5.** For \( p \leq j \leq 2(p-1) - r - 1 \) we have

\[
\frac{1}{j!} S(j, p-1-r) \equiv \frac{1}{j!} \sum_{i=1}^{j-1} \sum_{l=1}^{p-1} \xi(t, j) \xi^t \pmod{p},
\]

where \( j_0 = j - p \), so \( 0 \leq j_0 \leq p - r - 3 \).

**Proof.** For \( j \geq p \) we see first

\[
0 = \sum_{j=1}^{p-1} x^r(x) = \frac{1}{j!} \sum_{j=1}^{p-1} S(j, \ell) \xi^r \xi^t \pmod{p^r}.
\]

In fact, \( p \leq j \leq 2(p-1) - r - 1 \) yields \( S(j, p-1-r) \equiv 0 \pmod{p} \), because

\[
S(j, p-1-r) = S(j_0, p-r-2) \equiv 0 \pmod{p},
\]

On the other hand we have for \( j \geq p \)

\[
S(j, \ell) \equiv - S(j_0, \ell - 1) \pmod{p} \text{ if } 1 \leq \ell \leq p - 1,
\]

\[
S(j, \ell) \equiv S(j_0, \ell - p) \pmod{p} \text{ if } p \leq \ell \leq j.
\]

Therefore we see for \( p \leq j \leq 2(p-1) - r - 1 \)

\[
\frac{1}{j!} S(j, p-1-r) = \frac{1}{j!} \sum_{j=1}^{p-1} S(j, \ell) \xi^r \xi^t + \frac{1}{j!} \sum_{j=1}^{p-1} S(j, \ell) \xi^r \xi^t \pmod{p},
\]

\[
= \frac{1}{j!} \sum_{j=1}^{p-1} S(j_0, \ell - 1)(-pB_{r+t}) + \frac{1}{j!} \sum_{j=1}^{p-1} S(j_0, \ell - p) pB_{r+t} \pmod{p},
\]

\[
= - \frac{1}{j!} \sum_{j=1}^{p-1} S(j_0, \ell - 1)(pB_{r+t} - pB_{r+t+p-1}) \pmod{p},
\]

\[
= \frac{1}{j!} \sum_{j=1}^{p-1} S(j_0, \ell - 1)(pB_{r+t+p-1} - pB_{r+t}) \pmod{p}.
\]
Consequently a congruence of Kummer $B_{r+t+p-1} \equiv B_{r+t} - \frac{1}{r + \ell} B_{r+t}$ (mod $p$) gives the desired congruence in our assertion.

Thus the second sum in question becomes

$$-\sum_{t=1-r}^{2(p-1)-r-1} \sum_{j=1-r}^{p-1} \frac{1}{t!} \xi(t, j) S(j, p-1-r) \zeta^t$$

$$\equiv - \frac{1}{(p-1-r)!} \zeta^{p-1-r}$$

$$- \sum_{t=1-r}^{2(p-1)-r-1} \sum_{j=1-r}^{p-1} \xi(t, j) S(j, \ell) \frac{p}{r + \ell} B_{r+t} (\text{mod } p^{2(p-1)-r}).$$

If we set $t = h + p - 1$ with $1 \leq h \leq p - 1 - r - 1$, we have $\xi(t, j) \equiv \xi(h, j) \pmod{p}$ and thus we see

$$-\sum_{t=1-r}^{2(p-1)-r-1} \sum_{j=1-r}^{p-1} \frac{1}{t!} \xi(t, j) S(j, p-1-r) \zeta^t$$

$$\equiv - \frac{1}{(p-1-r)!} \zeta^{p-1-r}$$

$$- \sum_{t=1-r}^{2(p-1)-r-1} \sum_{j=1-r}^{p-1} \xi(t, j) S(j, \ell) \frac{p}{r + \ell} B_{r+t} \zeta^{t+p-1} (\text{mod } p^{2(p-1)-r}).$$

By virtue of the congruence $(h + p - 1)! \equiv -(h - 1)! \cdot p \pmod{p^2}$ we have finally

$$(3) \quad \sum_{j=p-1-r}^{p-1} \frac{1}{j!} (\zeta^p - 1)^j \sum_{x=1}^{p-1} \omega^p(x)(x) \frac{p}{r + h} B_{r+t} \zeta^{t+p-1} (\text{mod } p^{2(p-1)-r}).$$

Finally we obtain from the formulas $(2), (3)$ the following special case of Theorem 1.

**Theorem 1'.** For $1 \leq r \leq p - 2$ we have

$$g(\omega^r) \equiv - \frac{1}{(p-1-r)!} \zeta^{p-1-r} \pmod{p^{2(p-1)-r}}.$$
References


