

# JACOBI SUMS AND STICKELBERGER'S CONGRUENCE

KEITH CONRAD

ABSTRACT. We present an extension of a classical congruence for Jacobi sums of two characters to a congruence for arbitrary Jacobi sums. This congruence is used to provide what seems to be a new proof of Stickelberger's congruence for Gauss sums, as well as a new explanation for the appearance of base  $p$  digits in Stickelberger's congruence. It is also shown that in fact the Jacobi sum congruence and Stickelberger's congruence are equivalent.

## INTRODUCTION

About a century ago, Stickelberger established a congruence for Gauss sums over a finite field which has had useful implications for the study of cyclotomic fields. A generalized version of a classical congruence for Jacobi sums of two characters will be proven which is ultimately shown to be equivalent to Stickelberger's congruence. In particular, this allows for a new proof of Stickelberger's congruence and a new explanation for the form of the congruence.

Before discussing finite fields, we will need to fix a way of representing these fields and the multiplicative characters on them. Let  $p$  be a positive prime,  $q = p^f$  for  $f$  in  $\mathbf{Z}^+$ . We have the following diagram of number fields and primes, where  $\mathfrak{P}_i$  lies over  $\mathfrak{p}_i$ ,  $g = \varphi(q - 1)/f$ , and  $\zeta_p, \zeta_{q-1} \in \mathbf{C}$  denote roots of unity with respective orders  $p$  and  $q - 1$ :

$$\begin{array}{ccc}
 \mathbf{Q}(\zeta_{q-1}, \zeta_p) & \mathfrak{P}_1^{p-1} \cdots \mathfrak{P}_g^{p-1} & \\
 \downarrow & \downarrow & \\
 \mathbf{Q}(\zeta_{q-1}) & \mathfrak{p}_1 \cdots \mathfrak{p}_g & \\
 \downarrow & \downarrow & \\
 \mathbf{Q} & p &
 \end{array}$$

Fix any prime  $\mathfrak{p}$  in  $\mathbf{Q}(\zeta_{q-1})$  lying over  $p$  and let  $\mathfrak{P}$  be the unique prime in  $\mathbf{Q}(\zeta_{q-1}, \zeta_p)$  lying over  $\mathfrak{p}$ . Then  $\mathbf{Z}[\zeta_{q-1}]/\mathfrak{p}$  is a field of size  $q$ , and from now on  $\mathbf{F}_q$  denotes this field.

Let  $\omega_{\mathfrak{p}}$  denote the Teichmüller character on  $\mathbf{F}_q$ , i.e. for  $\bar{\alpha}$  in  $\mathbf{F}_q$  ( $\alpha \in \mathbf{Z}[\zeta_{q-1}]$ ),  $\omega_{\mathfrak{p}}(\bar{\alpha})$  is the unique complex root of  $X^q - X$  satisfying  $\omega_{\mathfrak{p}}(\bar{\alpha}) \equiv \alpha \pmod{\mathfrak{p}}$ . Taking  $\alpha = \zeta_{q-1}$ , we see that  $\omega_{\mathfrak{p}}$  has order  $q - 1$ , hence generates all multiplicative characters of  $\mathbf{F}_q$ . We will write  $\omega_{\mathfrak{p}}(\alpha)$  instead of  $\omega_{\mathfrak{p}}(\bar{\alpha})$ .

Although  $\mathbf{F}_q$  depends on  $\mathfrak{p}$ , we don't indicate this dependence in the notation. Replacing  $\mathbf{Q}$  by  $\mathbf{Q}_{\mathfrak{p}}$  would give only one prime over  $p$  in each extension field, making our representation of  $\mathbf{F}_q$  and definition of  $\omega_{\mathfrak{p}}$  more canonical, but we will not bother with this.

For  $0 \leq a < q - 1$ , write the base  $p$  expansion of  $a$  as

$$a = a_0 + \cdots + a_{f-1}p^{f-1},$$

where  $0 \leq a_i \leq p - 1$  (not all  $a_i = p - 1$ ).

---

1991 *Mathematics Subject Classification.* 11L05, 11T24.

Supported by an ONR graduate fellowship.

Throughout this paper,  $\zeta_p$  is fixed. The (normalized) Gauss sum of a multiplicative character  $\chi$  of  $\mathbf{F}_q$  is defined by

$$G(\chi) \stackrel{\text{def}}{=} - \sum_{x \in \mathbf{F}_q} \chi(x) \zeta_p^{\text{Tr}_{\mathbf{F}_q/\mathbf{F}_p}(x)}.$$

The (normalized) Jacobi sum of the multiplicative characters  $\chi_1, \dots, \chi_r$  of  $\mathbf{F}_q$  is defined by

$$J(\chi_1, \dots, \chi_r) \stackrel{\text{def}}{=} (-1)^{r-1} \sum_{\substack{x_1, \dots, x_r \in \mathbf{F}_q \\ x_1 + \dots + x_r = 1}} \chi_1(x_1) \cdots \chi_r(x_r).$$

For basic properties of Gauss and Jacobi sums see [6, Chapters 8 and 10]. (Note: We always take  $\chi(0) = 0$ . In contrast to the definitions above, Gauss and Jacobi sums in [6] are *not* normalized by a power of  $-1$ , and the trivial multiplicative character is set equal to 1 at 0. These differences affect no results we use from [6] in any essential way. Actually, our normalizations make some formulas from [6] which we won't use look cleaner.) Using Jacobi sums we will prove

**Theorem 1** (Stickelberger). *Using the same notation as above,*

$$G(\omega_{\mathfrak{p}}^{-a}) \equiv \frac{(\zeta_p - 1)^{a_0 + \dots + a_{f-1}}}{a_0! \cdots a_{f-1}!} \pmod{\mathfrak{P}^{a_0 + \dots + a_{f-1} + 1}}.$$

The original proof of this congruence is in [10, Section 6]. A modern reference for a proof is [7, Chapter 1]. In our proof, we use the following relation between Gauss sums and Jacobi sums in order to introduce the factorials of the base  $p$  digits into Stickelberger's congruence in (essentially) one step:

**Lemma 1.** *If  $\chi_1, \dots, \chi_r$  are multiplicative characters on  $\mathbf{F}_q$  with nontrivial product  $\chi_1 \cdots \chi_r$ , then*

$$G(\chi_1 \cdots \chi_r) = \frac{G(\chi_1) \cdots G(\chi_r)}{J(\chi_1, \dots, \chi_r)}.$$

*Proof.* See [6, Chapter 8, Theorem 3], noting that our weaker hypotheses than those of [6] are sufficient since we assume the trivial character vanishes at 0. □

## PROOF OF STICKELBERGER'S CONGRUENCE VIA JACOBI SUMS

For  $\chi_1, \dots, \chi_r$  multiplicative characters on  $\mathbf{F}_q = \mathbf{Z}[\zeta_{q-1}]/\mathfrak{p}$ , it is easy to check that

$$J(\chi_1, \dots, \chi_r)^{\mathfrak{p}} \equiv J(\chi_1, \dots, \chi_r) \pmod{\mathfrak{p}},$$

so  $J(\chi_1, \dots, \chi_r) \equiv$  rational integer  $\pmod{\mathfrak{p}}$ . We will show below (Theorem 2) that when some  $\chi_i$  is nontrivial, as an integer representative one can take a certain  $r$ -fold multinomial coefficient.

For  $r = 2$  there is the following classical congruence: if  $0 \leq k_1, k_2 < q - 1$  and not both  $k_1, k_2$  are zero, then

$$J(\omega_{\mathfrak{p}}^{-k_1}, \omega_{\mathfrak{p}}^{-k_2}) \equiv \frac{(k_1 + k_2)!}{k_1! k_2!} \pmod{\mathfrak{p}}.$$

References for this congruence are given in the Notes in [6, Chapter 14]. We shall extend this congruence to Jacobi sums of any number of multiplicative characters of  $\mathbf{F}_q$  as follows:

**Theorem 2.** For  $r \geq 1$  and  $0 \leq k_1, \dots, k_r < q - 1$  with some  $k_j > 0$ ,

$$J(\omega_{\mathfrak{p}}^{-k_1}, \dots, \omega_{\mathfrak{p}}^{-k_r}) \equiv \frac{(k_1 + \dots + k_r)!}{k_1! \cdots k_r!} \pmod{\mathfrak{p}}.$$

The simplicity of the statement of this generalization makes it somewhat surprising that it does not seem to appear in the literature (such as that which is mentioned in the Notes in [8, Chapter 5]).

In our proofs of Theorems 1 and 2, we will view multinomial coefficients as special values of polynomials. For  $t \geq 1$  and  $n_1, \dots, n_t \in \mathbf{N}$ , define

$$\binom{X}{n_1, \dots, n_t} = \frac{X(X-1) \cdots (X - n_1 - \dots - n_t + 1)}{n_1! \cdots n_t!}.$$

In particular,  $\binom{X}{0, \dots, 0} = 1$ .

When  $t = 1$ , this reduces (even in notation) to the binomial coefficient polynomial, so whereas many people would write (for  $r \geq 2$  and  $n_1, \dots, n_r \in \mathbf{N}$ )

$$\frac{(n_1 + \dots + n_r)!}{n_1! \cdots n_r!}$$

as  $\binom{n_1 + \dots + n_r}{n_1, \dots, n_r}$ , we write it as  $\binom{n_1 + \dots + n_r}{n_1, \dots, n_{r-1}}$ ; having one less integer in the bottom is convenient, as for binomial coefficients. The main advantage of this notation is that in  $\mathbf{Z}[[X_1, \dots, X_t]]$  one has

$$(1 + X_1 + \dots + X_t)^m = \sum_{n_1, \dots, n_t \geq 0} \binom{m}{n_1, \dots, n_t} X_1^{n_1} \cdots X_t^{n_t}$$

for all integers  $m$ .

Although the following two multinomial coefficient congruences are rather general, they will each be used only once, and in special cases.

**C1.** For  $t \geq 1$ , choose  $n_1, \dots, n_t \in \mathbf{N}$  and  $d \in \mathbf{N}$  with each  $n_i < p^d$ . For  $b \in \mathbf{Z}$ ,

$$\binom{b + p^d}{n_1, \dots, n_t} \equiv \binom{b}{n_1, \dots, n_t} \pmod{p}.$$

**C2.** For  $d \geq 0$ ,  $t \geq 1$ , and  $m_0, \dots, m_t \geq 0$  write

$$\begin{aligned} m_0 &= c_0 + c_1 p + \dots + c_d p^d, \quad 0 \leq c_i \leq p - 1 \text{ for } i < d; \\ m_j &= c_{0j} + c_{1j} p + \dots + c_{dj} p^d, \quad 0 \leq c_{ij} \leq p - 1 \text{ for } i < d \text{ and } 1 \leq j \leq t, \end{aligned}$$

where  $c_d, c_{dj} \geq 0$ . Then

$$\binom{m_0}{m_1, \dots, m_t} \equiv \binom{c_0}{c_{01}, \dots, c_{0t}} \cdots \binom{c_d}{c_{d1}, \dots, c_{dt}} \pmod{p}.$$

To prove **C1**, work in  $\mathbf{F}_p[[X_1, \dots, X_t]]$  and use the equation

$$(1 + X_1 + \dots + X_t)^{b+p^d} = (1 + X_1 + \dots + X_t)^b (1 + X_1^{p^d} + \dots + X_t^{p^d}).$$

To prove **C2**, the condition on the leading “digits”  $c_d, c_{d1}, \dots, c_{dt}$  just being nonnegative reduces the proof to the case  $d = 1$ . Now look at the coefficients of  $X_1^{m_1} \cdots X_t^{m_t}$  on both sides of the equation

$$(1 + X_1 + \dots + X_t)^{m_0} = (1 + X_1 + \dots + X_t)^{c_0} (1 + X_1^p + \dots + X_t^p)^{c_1}$$

in  $\mathbf{F}_p[[X_1, \dots, X_t]]$ . In the binomial case ( $t = 1$ ), **C2** is originally due to Lucas [9], and is also in [4]. The general result ( $t > 1$ ) is due to Dickson [2, p. 76].

*Proof of Theorem 2.* For any  $\chi$ ,  $J(\chi) = 1$ , so we can assume  $r > 1$ . Since some  $k_j > 0$  and a Jacobi sum is a symmetric function of its arguments, we choose  $k_r > 0$ . We will let  $\alpha_1, \dots, \alpha_{r-1}$  each run independently through representatives for the nonzero classes of  $\mathbf{F}_q = \mathbf{Z}[\zeta_{q-1}]/\mathfrak{p}$ , say the complex roots of  $X^{q-1} - 1$ . For  $s$  in  $\mathbf{Z}$ ,  $\omega_{\mathfrak{p}}^s(\alpha) \equiv \alpha^s \pmod{\mathfrak{p}}$  if  $\alpha \not\equiv 0 \pmod{\mathfrak{p}}$  or  $s \geq 0$  (we set  $0^0 = 1$ ), so

$$\begin{aligned} J(\omega_{\mathfrak{p}}^{-k_1}, \dots, \omega_{\mathfrak{p}}^{-k_r}) &= \\ &(-1)^{r-1} \sum_{\alpha_j} \omega_{\mathfrak{p}}^{-k_1}(\alpha_1) \cdots \omega_{\mathfrak{p}}^{-k_{r-1}}(\alpha_{r-1}) \omega_{\mathfrak{p}}(1 - \alpha_1 - \cdots - \alpha_{r-1})^{q-1-k_r} \\ &\equiv (-1)^{r-1} \sum_{\alpha_j} \alpha_1^{-k_1} \cdots \alpha_{r-1}^{-k_{r-1}} (1 - \alpha_1 - \cdots - \alpha_{r-1})^{q-1-k_r} \pmod{\mathfrak{p}} \\ &\equiv \sum_{\substack{n_j \geq 0 \\ n_1 + \cdots + n_{r-1} \leq q-1-k_r}} \binom{q-1-k_r}{n_1, \dots, n_{r-1}} (-1)^{r-1+n_1+\cdots+n_{r-1}} \prod_{1 \leq i \leq r-1} \left( \sum_{\alpha_i} \alpha_i^{n_i-k_i} \right). \end{aligned}$$

The only time  $\sum_{\alpha_i} \alpha_i^{n_i-k_i}$  isn't zero is when  $q-1 \mid n_i - k_i$ , when the sum is  $q-1 \equiv -1 \pmod{\mathfrak{p}}$ . From  $0 \leq k_i < q-1$  and

$$-(q-1) < -k_i \leq n_i - k_i \leq n_i \leq q-1 - k_r < q-1,$$

we see that  $q-1 \mid n_i - k_i \iff n_i = k_i$ . Thus, if  $k_1 + \cdots + k_{r-1} > q-1 - k_r$ , we have  $J(\omega_{\mathfrak{p}}^{-k_1}, \dots, \omega_{\mathfrak{p}}^{-k_r}) \equiv 0 \pmod{\mathfrak{p}}$ , while if  $k_1 + \cdots + k_{r-1} \leq q-1 - k_r$ ,

$$\begin{aligned} J(\omega_{\mathfrak{p}}^{-k_1}, \dots, \omega_{\mathfrak{p}}^{-k_r}) &\equiv \binom{q-1-k_r}{k_1, \dots, k_{r-1}} (-1)^{r-1+k_1+\cdots+k_{r-1}} (-1)^{r-1} \pmod{\mathfrak{p}} \\ &= \binom{q-1-k_r}{k_1, \dots, k_{r-1}} (-1)^{k_1+\cdots+k_{r-1}} \\ &= \binom{k_1 + \cdots + k_{r-1} - q}{k_1, \dots, k_{r-1}}. \end{aligned}$$

If  $k_1 + \cdots + k_{r-1} > q-1 - k_r$ , this last expression equals 0, so regardless of the value of  $k_1 + \cdots + k_{r-1}$ , we have by **C1** that

$$\begin{aligned} J(\omega_{\mathfrak{p}}^{-k_1}, \dots, \omega_{\mathfrak{p}}^{-k_r}) &\equiv \binom{k_1 + \cdots + k_r}{k_1, \dots, k_{r-1}} \pmod{\mathfrak{p}} \\ &= \frac{(k_1 + \cdots + k_r)!}{k_1! \cdots k_r!}. \end{aligned}$$

□

*Remarks.* 1. Theorem 2 is not true in general when all  $k_j = 0$ , since the Jacobi sum of the trivial character on  $\mathbf{F}_q$  taken  $r$  times is  $(1 - (1 - q)^r)/q \equiv r \pmod{p}$ .

2. It is reasonable to ask if Theorem 2 can be proven in general if it is just known for  $r = 2$ . After all, there are recursion formulas relating a multinomial coefficient to a product of binomial coefficients and a Jacobi sum of several characters to a product of Jacobi sums of two characters. However, this latter relation depends on hypotheses of nontriviality of certain characters which are not part of the hypotheses of Theorem 2 (for example,  $J(\chi_1, \chi_2, \chi_3) = J(\chi_1, \chi_2)J(\chi_1\chi_2, \chi_3)$  precisely when  $\chi_1\chi_2$  is nontrivial). Thus it would likely be cumbersome to use this approach to prove Theorem 2.

*Proof of Theorem 1.* It is obvious for  $a = 0$ , and see [11, pp. 96-97] for the case  $a = 1$  (whose proof shows why one should expect the theorem to hold for positive powers of  $\omega_{\mathfrak{p}}^{-1}$ , not of  $\omega_{\mathfrak{p}}$ :  $p^f - 1 = \#\mathbf{F}_q^\times$  is more closely related to  $p^d - 1$  than to  $p^d + 1$ ). Now we may assume  $q > 3$ . For  $0 < a < q - 2$ , we have by Lemma 1 that

$$G(\omega_{\mathfrak{p}}^{-(a+1)}) = \frac{G(\omega_{\mathfrak{p}}^{-a})G(\omega_{\mathfrak{p}}^{-1})}{J(\omega_{\mathfrak{p}}^{-a}, \omega_{\mathfrak{p}}^{-1})},$$

and  $J(\omega_{\mathfrak{p}}^{-a}, \omega_{\mathfrak{p}}^{-1}) \equiv a + 1 \pmod{\mathfrak{p}}$  (hence also  $\pmod{\mathfrak{P}}$ ) by Theorem 2, so by induction and the equation  $\text{ord}_{\mathfrak{P}}(\zeta_p - 1) = 1$ ,

$$G(\omega_{\mathfrak{p}}^{-a}) \equiv \frac{(\zeta_p - 1)^a}{a!} \pmod{\mathfrak{P}^{a+1}}$$

for  $0 \leq a \leq p - 1$  (or  $a < p - 1$  if  $q = p$ ). If  $q = p$  we're done, so assume  $q > p$ , i.e.  $f \geq 2$ . Going from  $a = p - 1$  to  $a = p$  is a problem because  $\mathfrak{P} \mid p$  and we don't want to divide by  $p$  in our congruence modulo a power of  $\mathfrak{P}$ . We circumvent this with Jacobi sums.

For  $1 \leq a < q - 1$ , some digit  $a_i$  is  $> 0$ , so  $\omega_{\mathfrak{p}}^{-a}$ ,  $\omega_{\mathfrak{p}}^{-a_i p^i}$  are nontrivial. Then by Lemma 1,

$$\begin{aligned} G(\omega_{\mathfrak{p}}^{-a}) &= G(\omega_{\mathfrak{p}}^{-a_0} \cdots \omega_{\mathfrak{p}}^{-a_{f-1} p^{f-1}}) \\ &= \frac{G(\omega_{\mathfrak{p}}^{-a_0}) \cdots G(\omega_{\mathfrak{p}}^{-a_{f-1} p^{f-1}})}{J(\omega_{\mathfrak{p}}^{-a_0}, \dots, \omega_{\mathfrak{p}}^{-a_{f-1} p^{f-1}})} \\ &= \frac{G(\omega_{\mathfrak{p}}^{-a_0}) \cdots G(\omega_{\mathfrak{p}}^{-a_{f-1}})}{J(\omega_{\mathfrak{p}}^{-a_0}, \dots, \omega_{\mathfrak{p}}^{-a_{f-1} p^{f-1}})}, \end{aligned}$$

the last equation holding since  $G(\chi^p) = G(\chi)$  (see [7, p. 5]).

Since  $\text{ord}_{\mathfrak{P}}(a_i!) = 0$ ,

$$G(\omega_{\mathfrak{p}}^{-a_0}) \cdots G(\omega_{\mathfrak{p}}^{-a_{f-1}}) \equiv \frac{(\zeta_p - 1)^{a_0 + \cdots + a_{f-1}}}{a_0! \cdots a_{f-1}!} \pmod{\mathfrak{P}^{a_0 + \cdots + a_{f-1} + 1}}.$$

By Theorem 2 and **C2**,

$$\begin{aligned} J(\omega_{\mathfrak{p}}^{-a_0}, \dots, \omega_{\mathfrak{p}}^{-a_{f-1} p^{f-1}}) &\equiv \binom{a_0 + \cdots + a_{f-1} p^{f-1}}{a_0, \dots, a_{f-2} p^{f-2}} \pmod{\mathfrak{p}} \\ &\equiv \binom{a_0}{a_0, 0, \dots, 0} \binom{a_1}{0, a_1, \dots, 0} \cdots \binom{a_{f-1}}{0, \dots, 0} \\ &= 1. \end{aligned}$$

Therefore

$$J(\omega_{\mathfrak{p}}^{-a_0}, \dots, \omega_{\mathfrak{p}}^{-a_{f-1} p^{f-1}}) \equiv 1 \pmod{\mathfrak{P}},$$

so we are done. □

Our method of proof shows that writing Stickelberger's congruence as

$$G(\omega_{\mathfrak{p}}^{-a}) \equiv \prod_{0 \leq i \leq f-1} \frac{(\zeta_p - 1)^{a_i}}{a_i!} \pmod{\mathfrak{P}^{a_0 + \cdots + a_{f-1} + 1}}$$

isolates terms in analogy with Lemma 1. This gives a new explanation for the appearance of base  $p$  digits in the denominator in Stickelberger's congruence. There are more sophisticated explanations, cf. the proof of Stickelberger's congruence via the Gross-Koblitz formula in

[7, Chapter 15]. (Although both the original proof of the Gross-Koblitz formula in [5] and the proof in [7] are only done for finite fields of odd characteristic, the formula is also valid for characteristic 2 since Lemma 1.1 (ii) in [7, p. 333] is valid for all  $\delta > 0$ , not just for  $\delta \geq 1/(p-1)$ . Alternatively, in [1] Coleman gives a simple proof which he explicitly points out is valid in all characteristics. Thus a proof of Stickelberger's congruence for all finite fields via the Gross-Koblitz formula is justified.)

### PROOF OF JACOBI SUM CONGRUENCE VIA STICKELBERGER

We now want to show that not only does Theorem 1 follow from Theorem 2, but Theorem 2 follows from Theorem 1, so the two theorems are equivalent. Some preliminary results will be required before the (tedious) proof is presented.

For  $n \in \mathbf{N}$ , write

$$n = c_0 + c_1p + \cdots + c_dp^d, \quad 0 \leq c_i \leq p-1.$$

From [3, Chapter IX],

$$\text{ord}_p n! = \frac{n - (c_0 + \cdots + c_d)}{p-1}, \quad \frac{n!}{(-p)^{\text{ord}_p n!}} \equiv c_0! \cdots c_d! \pmod{p}.$$

Note neither equation requires  $c_d \neq 0$ . We define

$$S_p(n) \stackrel{\text{def}}{=} c_0 + \cdots + c_d, \quad H_p(n) \stackrel{\text{def}}{=} c_0! \cdots c_d!,$$

and note neither of these expressions requires  $c_d \neq 0$ . One sees easily that for any  $n \in \mathbf{N}$ ,  $n \equiv S_p(n) \pmod{p-1}$ , and for  $n_1, \dots, n_t \in \mathbf{N}$ ,

$$\text{ord}_p \left( \frac{(n_1 + \cdots + n_t)!}{n_1! \cdots n_t!} \right) = \frac{S_p(n_1) + \cdots + S_p(n_t) - S_p(n_1 + \cdots + n_t)}{p-1}.$$

For  $x \in \mathbf{R}$ , let  $\langle x \rangle$  denote the fractional part of  $x$ . For  $b \in \mathbf{Z}$ , let  $b \equiv b' \pmod{q-1}$  where  $0 \leq b' < q-1$ , so that  $\langle \frac{b}{q-1} \rangle = \frac{b'}{q-1}$ . Define

$$s_q(b) = S_p(b'), \quad h_q(b) = H_p(b'),$$

so  $s_q$  and  $h_q$  are just the extensions of  $S_p$  and  $H_p$  from  $\{b : 0 \leq b < q-1\}$  by  $(q-1)$ -periodicity. From [7, p. 10],

$$s_q(b) = (p-1) \sum_{0 \leq i \leq f-1} \left\langle \frac{p^i b}{q-1} \right\rangle.$$

Since  $\text{ord}_{\mathfrak{P}}(\zeta_p - 1) = 1$ , Stickelberger's congruence can be written for all  $a$  in  $\mathbf{Z}$  as

$$\frac{G(\omega_{\mathfrak{P}}^{-a})}{(\zeta_p - 1)^{s_q(a)}} \equiv \frac{1}{h_q(a)} \pmod{\mathfrak{P}}.$$

**Lemma 2.** For  $r, m \in \mathbf{Z}^+$ , and  $b_1, \dots, b_r \in \mathbf{Z}$ ,

$$\left\langle \frac{b_1}{m} \right\rangle + \cdots + \left\langle \frac{b_r}{m} \right\rangle \geq \left\langle \frac{b_1 + \cdots + b_r}{m} \right\rangle.$$

If  $b_1 + \cdots + b_r \equiv 0 \pmod{m}$  and some  $b_j \not\equiv 0 \pmod{m}$  then

$$\left\langle \frac{b_1}{m} \right\rangle + \cdots + \left\langle \frac{b_r}{m} \right\rangle \geq 1.$$

*Proof.* Let  $b_j \equiv b'_j \pmod{m}$ , where  $0 \leq b'_j < m$ . Then  $b'_1 + \cdots + b'_r \geq 0$ , so since  $x \geq \langle x \rangle$  for  $x \geq 0$ ,

$$\left\langle \frac{b_1}{m} \right\rangle + \cdots + \left\langle \frac{b_r}{m} \right\rangle = \frac{b'_1 + \cdots + b'_r}{m} \geq \left\langle \frac{b'_1 + \cdots + b'_r}{m} \right\rangle = \left\langle \frac{b_1 + \cdots + b_r}{m} \right\rangle.$$

If  $b_1 + \cdots + b_r \equiv 0 \pmod{m}$  then  $b'_1 + \cdots + b'_r \equiv 0 \pmod{m}$ , so  $(b'_1 + \cdots + b'_r)/m \in \mathbf{N}$ . If some  $b_j \not\equiv 0 \pmod{m}$  then  $b'_j > 0$ , so  $(b'_1 + \cdots + b'_r)/m \in \mathbf{Z}^+$ , hence is  $\geq 1$ .  $\square$

**Corollary 1.** *Let  $0 \leq k_1, \dots, k_r < q - 1$  with  $k_1 + \cdots + k_r \geq q - 1$  (so  $r \geq 2$  and at least two  $k_j > 0$ ). Then*

$$s_q(k_1) + \cdots + s_q(k_r) \begin{cases} > s_q(k_1 + \cdots + k_r) & \text{if } k_1 + \cdots + k_r \not\equiv 0 \pmod{q-1} \\ > f(p-1) & \text{if } k_1 + \cdots + k_r \equiv 0 \pmod{q-1}, > q-1 \\ \geq f(p-1) & \text{if } k_1 + \cdots + k_r = q-1. \end{cases}$$

*Proof.* From above,

$$s_q(k_1) + \cdots + s_q(k_r) = (p-1) \sum_{0 \leq i \leq f-1} \left( \left\langle \frac{p^i k_1}{q-1} \right\rangle + \cdots + \left\langle \frac{p^i k_r}{q-1} \right\rangle \right).$$

If  $k_1 + \cdots + k_r \not\equiv 0 \pmod{q-1}$ , applying Lemma 2 to  $p^i k_1, \dots, p^i k_r$  shows that each addend is  $\geq \left\langle \frac{p^i(k_1 + \cdots + k_r)}{q-1} \right\rangle$ , with strict inequality when  $i = 0$  by hypothesis, since

$$\left\langle \frac{k_1}{q-1} \right\rangle + \cdots + \left\langle \frac{k_r}{q-1} \right\rangle = \frac{k_1 + \cdots + k_r}{q-1} > 1 \geq \left\langle \frac{k_1 + \cdots + k_r}{q-1} \right\rangle.$$

If  $k_1 + \cdots + k_r \equiv 0 \pmod{q-1}$  then by Lemma 2 each addend is  $\geq 1$ , with strict inequality when  $i = 0$  if  $k_1 + \cdots + k_r > q - 1$ .  $\square$

We now state a more general version of Lemma 1, with a different notation that will be better suited for what follows.

**Lemma 3.** *For  $k_1, \dots, k_r \in \mathbf{Z}$  with some  $k_j \not\equiv 0 \pmod{q-1}$ ,*

$$J(\omega_p^{-k_1}, \dots, \omega_p^{-k_r}) = \begin{cases} \frac{G(\omega_p^{-k_1}) \cdots G(\omega_p^{-k_r})}{G(\omega_p^{-(k_1 + \cdots + k_r)})} & \text{if } k_1 + \cdots + k_r \not\equiv 0 \pmod{q-1} \\ \frac{1}{q} G(\omega_p^{-k_1}) \cdots G(\omega_p^{-k_r}) & \text{if } k_1 + \cdots + k_r \equiv 0 \pmod{q-1}. \end{cases}$$

*Proof.* Use [6, Chapter 8, Theorem 3] and its corollaries, keeping in mind the differences mentioned between that book and this paper on various definitions.  $\square$

*Proof that Theorem 1 implies Theorem 2.* We have  $0 \leq k_1, \dots, k_r < q - 1$  with some  $k_j > 0$ , so if the second case of Lemma 3 holds, then  $r \geq 2$  and at least two  $k_j$  are  $> 0$ . From the multinomial coefficient manipulations at the end of the proof of Theorem 2, if  $k_1 + \cdots + k_r > q - 1$  then

$$\frac{(k_1 + \cdots + k_r)!}{k_1! \cdots k_r!} \equiv 0 \pmod{p}. \quad (*)$$

Thus to prove Theorem 1 implies Theorem 2 we are led to the following four cases:

Case 1:  $k_1 + \cdots + k_r > q - 1$ ,  $k_1 + \cdots + k_r \not\equiv 0 \pmod{q-1}$

Case 2:  $k_1 + \cdots + k_r > q - 1$ ,  $k_1 + \cdots + k_r \equiv 0 \pmod{q-1}$

Case 3:  $k_1 + \cdots + k_r = q - 1$

Case 4:  $0 < k_1 + \cdots + k_r < q - 1$ .

We will prove Theorem 2 from Theorem 1 by establishing the congruence of Theorem 2 modulo  $\mathfrak{P}$ , since Theorem 1 involves a Gauss sum, which lies in  $\mathbf{Z}[\zeta_{q-1}, \zeta_p]$  but not usually in  $\mathbf{Z}[\zeta_{q-1}]$ .

In Cases 1 and 2, by (\*) we want to prove  $\text{ord}_{\mathfrak{P}}(J(\omega_p^{-k_1}, \dots, \omega_p^{-k_r})) > 0$ . By both Stickelberger's congruence and Lemma 3,

$$\text{ord}_{\mathfrak{P}}(J(\omega_p^{-k_1}, \dots, \omega_p^{-k_r})) = \begin{cases} s_q(k_1) + \dots + s_q(k_r) - s_q(k_1 + \dots + k_r) & \text{in Case 1} \\ s_q(k_1) + \dots + s_q(k_r) - f(p-1) & \text{in Case 2,} \end{cases}$$

and in both cases the expression on the right is  $> 0$  by the corollary to Lemma 2. To prove Cases 3 and 4, note  $(\zeta_p - 1)^{p-1} = -pu$ , where  $u \equiv 1 \pmod{(\zeta_p - 1)}$  [11, p. 324], hence  $u \equiv 1 \pmod{\mathfrak{P}}$ .

In Case 3, Stickelberger's congruence and Lemma 3 yield

$$\begin{aligned} \frac{J(\omega_p^{-k_1}, \dots, \omega_p^{-k_r})}{(\zeta_p - 1)^{s_q(k_1) + \dots + s_q(k_r)}} \cdot q &\equiv \frac{1}{h_q(k_1)} \cdots \frac{1}{h_q(k_r)} \pmod{\mathfrak{P}} \\ &\equiv \frac{1}{H_p(k_1)} \cdots \frac{1}{H_p(k_r)} \pmod{\mathfrak{P}} \text{ since } 0 \leq k_i < q-1 \\ &\equiv \frac{(-p)^{\text{ord}_p(k_1!) + \dots + \text{ord}_p(k_r!)}}{k_1! \cdots k_r!} \pmod{\mathfrak{P}}. \end{aligned}$$

Since  $s_q(k_i) = S_p(k_i)$ ,

$$\begin{aligned} (\zeta_p - 1)^{s_q(k_1) + \dots + s_q(k_r)} &= (\zeta_p - 1)^{k_1 + \dots + k_r - (p-1)(\text{ord}_p(k_1!) + \dots + \text{ord}_p(k_r!))} \\ &= (\zeta_p - 1)^{(p-1)(\frac{q-1}{p-1} - (\text{ord}_p(k_1!) + \dots + \text{ord}_p(k_r!)))} \\ &= (-pu)^{\frac{q-1}{p-1} - \text{ord}_p(k_1! \cdots k_r!)}. \end{aligned}$$

So

$$\frac{J(\omega_p^{-k_1}, \dots, \omega_p^{-k_r}) q (-pu)^{\text{ord}_p(k_1! \cdots k_r!)}}{(-pu)^{\frac{q-1}{p-1}}} \equiv \frac{(-p)^{\text{ord}_p(k_1! \cdots k_r!)}}{k_1! \cdots k_r!} \pmod{\mathfrak{P}},$$

which implies by the congruence  $u \equiv 1 \pmod{\mathfrak{P}}$  and by multiplication by  $(q-1)! = (k_1 + \dots + k_r)!$  that

$$\begin{aligned} J(\omega_p^{-k_1}, \dots, \omega_p^{-k_r}) \frac{q!}{(-p)^{\frac{q-1}{p-1}}} (-p)^{\text{ord}_p(k_1! \cdots k_r!)} &\equiv \\ \frac{(k_1 + \dots + k_r)!}{k_1! \cdots k_r!} (-p)^{\text{ord}_p(k_1! \cdots k_r!)} &\pmod{\mathfrak{P}^{1+(p-1)\text{ord}_p((q-1)!)}}. \end{aligned}$$

Since

$$\begin{aligned} &1 + (p-1)\text{ord}_p((q-1)!) - (p-1)\text{ord}_p(k_1! \cdots k_r!) \\ &= 1 + q - 1 - S_p(q-1) - k_1 - \dots - k_r + S_p(k_1) + \dots + S_p(k_r) \\ &= 1 - f(p-1) + s_q(k_1) + \dots + s_q(k_r) \text{ since } 0 \leq k_i < q-1 \\ &\geq 1 \text{ by the corollary to Lemma 2,} \end{aligned}$$

we see

$$J(\omega_p^{-k_1}, \dots, \omega_p^{-k_r}) \cdot \frac{q!}{(-p)^{\frac{q-1}{p-1}}} \equiv \frac{(k_1 + \dots + k_r)!}{k_1! \cdots k_r!} \pmod{\mathfrak{P}},$$

so the congruence

$$\frac{q!}{(-p)^{\frac{q-1}{p-1}}} = \frac{q!}{(-p)^{\text{ord}_p(q!)}} \equiv H_p(q) = 1 \pmod{p}$$

settles Case 3.

Finally, in Case 4, Stickelberger's congruence and Lemma 3 imply that



$$\frac{J(\omega_p^{-k_1}, \dots, \omega_p^{-k_r})}{(\zeta_p - 1)^{s_q(k_1) + \dots + s_q(k_r) - s_q(k_1 + \dots + k_r)}} \equiv \frac{h_q(k_1 + \dots + k_r)}{h_q(k_1) \cdot \dots \cdot h_q(k_r)} \pmod{\mathfrak{P}},$$

so

$$\frac{J(\omega_p^{-k_1}, \dots, \omega_p^{-k_r})}{(\zeta_p - 1)^{(p-1)\text{ord}_p\left(\frac{(k_1 + \dots + k_r)!}{k_1! \cdot \dots \cdot k_r!}\right)}} \equiv \frac{(k_1 + \dots + k_r)!}{k_1! \cdot \dots \cdot k_r!} \cdot \frac{1}{(-p)^{\text{ord}_p\left(\frac{(k_1 + \dots + k_r)!}{k_1! \cdot \dots \cdot k_r!}\right)}} \pmod{\mathfrak{P}},$$

since  $s_q(k_i) = S_p(k_i)$  and  $s_q(k_1 + \dots + k_r) = S_p(k_1 + \dots + k_r)$ . Thus

$$J(\omega_p^{-k_1}, \dots, \omega_p^{-k_r}) \equiv \frac{(k_1 + \dots + k_r)!}{k_1! \cdot \dots \cdot k_r!} \pmod{\mathfrak{P}}.$$

□

### REFERENCES

- [1] R. Coleman, *The Gross-Koblitz Formula*, in: Galois Representations and Arithmetic Algebraic Geometry, North-Holland, New York, 1987, 21-52.
- [2] L.E. Dickson, *The Analytic Representation of Substitutions of a Prime Number of Letters with a Discussion of the Linear Group*, Ann. of Math. (1) 11 (1896-1897), 65-120.
- [3] L.E. Dickson, *History of the Theory of Numbers*, vol. 1, Chelsea Publishing Company, Bronx, New York, 1971.
- [4] N.J. Fine, *Binomial coefficients modulo a prime*, Amer. Math. Monthly 54 (1947), 589-592.
- [5] B.H. Gross and N. Koblitz, *Gauss sums and the p-adic  $\Gamma$ -function*, Ann. of Math. 109 (1979), 569-581.
- [6] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd ed., Springer-Verlag, New York, 1990.
- [7] S. Lang, *Cyclotomic Fields I and II*, Springer-Verlag, New York, 1990.
- [8] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and Its Applications, vol. 20, Addison-Wesley, Reading, Massachusetts, 1983.
- [9] E. Lucas, *Sur les congruences des nombres eulériens et des coefficients différentiels des fonctions trigonométriques, suivant un module premier*, Bull. Soc. Math. France 6 (1877-1878), 49-54.
- [10] L. Stickelberger, *Über eine Verallgemeinerung der Kreistheilung*, Math. Ann. 37 (1890), 321-367.
- [11] L. Washington, *Introduction to Cyclotomic Fields*, Springer-Verlag, New York, 1982.

DEPARTMENT OF MATHEMATICS, HARVARD UNIVERSITY, CAMBRIDGE, MA 02138