

Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 41 (1995)
Heft: 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: JACOBI SUMS AND STICKELBERGER'S CONGRUENCE
Autor: Conrad, Keith
Kapitel: Proof of Stickelberger's Congruence Via Jacobi Sums
DOI: <https://doi.org/10.5169/seals-61822>

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. [Siehe Rechtliche Hinweise.](#)

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. [Voir Informations légales.](#)

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. [See Legal notice.](#)

Download PDF: 06.02.2025

ETH-Bibliothek Zürich, E-Periodica, <https://www.e-periodica.ch>

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 χ_1, \dots, χ_r are multiplicative characters on \mathbf{F}_q with nontrivial product $\chi_1 \cdot \dots \cdot \chi_r$, then*

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

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. \square

PROOF OF STICKELBERGER'S CONGRUENCE VIA JACOBI SUMS

For χ_1, \dots, χ_r multiplicative characters on $\mathbf{F}_q = \mathbf{Z}[\zeta_{q-1}]/\mathfrak{p}$, it is easy to check that

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

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

In the case $r = 2$ 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

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

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 $k_j > 0$,*

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

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

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

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 $n_1, \dots, n_r \in \mathbf{N}$)

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

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

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

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

$$m_0 = c_0 + c_1p + \dots + c_dp^d, \quad 0 \leq c_i \leq p-1 \quad \text{for } i < d;$$

$$m_j = c_{0j} + c_{1j}p + \dots + c_{dj}p^d, \quad 0 \leq c_{ij} \leq p-1 \quad \text{for } i < d \text{ and } 1 \leq j \leq t,$$

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

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

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 coefficient of $X_1^{m_1} \cdot \dots \cdot X_t^{m_t}$ 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 χ , $J(\chi) = 1$, 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

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

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

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

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

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

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 ω_p^{-1} , not of ω_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

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

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

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

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 $\omega_p^{-a}, \omega_p^{-a_i p^i}$ are nontrivial.

Then by Lemma 1,

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

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

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

$$G(\omega_p^{-a_0}) \cdot \dots \cdot G(\omega_p^{-a_{f-1}}) \equiv \frac{(\zeta_p - 1)^{a_0 + \dots + a_{f-1}}}{a_0! \cdot \dots \cdot a_{f-1}!} \pmod{\mathfrak{P}^{a_0 + \dots + a_{f-1} + 1}}.$$

By Theorem 2 and C2,

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

Therefore

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

so we are done. \square

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

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

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

$$n = c_0 + c_1 p + \cdots + c_d p^d, \quad 0 \leq c_i \leq p - 1.$$

From [3, Chapter IX],

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

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

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

and note neither of these definitions 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

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