

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 Jacobi Sum Congruence Via Stickelberger
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>

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

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

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

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

If $b_1 + \dots + b_r \equiv 0 \pmod m$ and some $b_j \not\equiv 0 \pmod m$ then

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

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

$$\begin{aligned} \left\langle \frac{b_1}{m} \right\rangle + \dots + \left\langle \frac{b_r}{m} \right\rangle &= \frac{b'_1 + \dots + b'_r}{m} \geq \left\langle \frac{b'_1 + \dots + b'_r}{m} \right\rangle \\ &= \left\langle \frac{b_1 + \dots + b_r}{m} \right\rangle. \end{aligned}$$

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

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

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

Proof. From above,

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

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

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

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

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

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

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

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

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

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

So

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

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

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

Since

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

we see

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

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

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

REFERENCES

- [1] COLEMAN, R. The Gross-Koblitz Formula. In: *Galois Representations and Arithmetic Algebraic Geometry*. North-Holland, New York, 1987, 21-52.
- [2] DICKSON, L.E. 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] ——— *History of the Theory of Numbers*, vol. 1. Chelsea Publishing Company, Bronx, New York, 1971.
- [4] FINE, N.J. Binomial coefficients modulo a prime. *Amer. Math. Monthly* 54 (1947), 589-592.
- [5] GROSS, B.H. and N. KOBLITZ. Gauss sums and the p -adic Γ -function. *Ann. of Math.* 109 (1979), 569-581.
- [6] IRELAND, K. and M. ROSEN. *A Classical Introduction to Modern Number Theory*, 2nd ed. Springer-Verlag, New York, 1990.
- [7] LANG, S. *Cyclotomic Fields I and II*. Springer-Verlag, New York, 1990.
- [8] LIDL, R. and H. NIEDERREITER. *Finite Fields*, Encyclopedia of Mathematics and Its Applications, vol. 20. Addison-Wesley, Reading, Massachusetts, 1983.