Proof of Jacobi Sum Congruence Via Stickelberger

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

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

From [3, Chapter IX],

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

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

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

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

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

For $x \in \mathbf{R}$, let $\langle x \rangle$ denote the fractional part of x. For $b \in \mathbf{Z}$, let $b \equiv b' \bmod q - 1$ where $0 \leqslant b' < q - 1$, so that $\left\langle \frac{b}{q-1} \right\rangle = \frac{b'}{q-1}$. 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 $\{b : 0 \leqslant b < q - 1\}$ by $(q - 1)$-periodicity. From [7, p. 10],

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

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

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

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

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

If $b_1 + \cdots + b_r \equiv 0 \bmod m$ *and some* $b_j \not\equiv 0 \bmod m$ *then*

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

Proof. Let $b_j \equiv b_j' \bmod m$, where $0 \leqslant b_j' < m$. Then $b_1' + \cdots + b_r' \geqslant 0$, so since $x \geqslant \langle x \rangle$ for $x \geqslant 0$,

$$\left\langle \frac{b_1}{m} \right\rangle + \cdots + \left\langle \frac{b_r}{m} \right\rangle = \frac{b_1' + \cdots + b_r'}{m} \geqslant \left\langle \frac{b_1' + \cdots + b_r'}{m} \right\rangle = \left\langle \frac{b_1 + \cdots + b_r}{m} \right\rangle .$$

If $b_1 + \cdots + b_r \equiv 0 \bmod m$ then $(b_1' + \cdots + b_r')/m \in \mathbf{N}$. If some $b_j \not\equiv 0 \bmod m$ then $b_j' > 0$, so $(b_1' + \cdots + b_r')/m \in \mathbf{Z}^+$, hence is $\geqslant 1$. □

COROLLARY 1. *Let* $0 \leqslant k_1, \ldots, k_r < q - 1$ *with* $k_1 + \cdots + k_r \geqslant q - 1$, *so* $r \geqslant 2$ *and at least two* $k_j > 0$. *Then*

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

Proof. From above,

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

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

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

If $k_1 + \cdots + k_r \equiv 0 \bmod q - 1$ then by Lemma 2 each addend is $\geqslant 1$, with strict inequality when $i = 0$ if $k_1 + \cdots + k_r > q - 1$. □

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* $k_1, \ldots, k_r \in \mathbf{Z}$ *with some* $k_j \not\equiv 0 \bmod q-1$,

$$J(\omega_{\mathfrak{p}}^{-k_1}, \ldots, \omega_{\mathfrak{p}}^{-k_r}) = \begin{cases} \dfrac{G(\omega_{\mathfrak{p}}^{-k_1}) \cdot \ldots \cdot G(\omega_{\mathfrak{p}}^{-k_r})}{G(\omega_{\mathfrak{p}}^{-(k_1+\cdots+k_r)})} & \text{if } k_1+\cdots+k_r \not\equiv 0 \bmod q-1 \\ \dfrac{1}{q}\, G(\omega_{\mathfrak{p}}^{-k_1}) \cdot \ldots \cdot G(\omega_{\mathfrak{p}}^{-k_r}) & \text{if } k_1+\cdots+k_r \equiv 0 \bmod q-1. \end{cases}$$

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. □

Proof that Theorem 1 implies Theorem 2. We have $0 \leqslant k_1, \ldots, k_r < q-1$ with some $k_j > 0$, so if the second case of Lemma 3 holds, then $r \geqslant 2$ 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

$$\frac{(k_1 + \cdots + k_r)!}{k_1! \cdot \ldots \cdot k_r!} \equiv 0 \bmod p\,. \qquad (*)$$

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

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

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

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 $\mathrm{ord}_{\mathfrak{P}}(J(\omega_{\mathfrak{p}}^{-k_1}, \ldots, \omega_{\mathfrak{p}}^{-k_r})) > 0$. By both Stickelberger's congruence and Lemma 3,

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

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 $u \equiv 1 \bmod (\zeta_p - 1)$, hence $u \equiv 1 \bmod \mathfrak{P}$.

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

$$\frac{J(\omega_\mathfrak{p}^{-k_1}, \ldots, \omega_\mathfrak{p}^{-k_r})}{(\zeta_p - 1)^{s_q(k_1) + \cdots + s_q(k_r)}} \cdot q \equiv \frac{1}{h_q(k_1)} \cdot \ldots \cdot \frac{1}{h_q(k_r)} \bmod \mathfrak{P}$$

$$\equiv \frac{1}{H_p(k_1)} \cdot \ldots \cdot \frac{1}{H_p(k_r)} \bmod \mathfrak{P} \text{ since } 0 \leqslant k_i < q-1$$

$$\equiv \frac{(-p)^{\operatorname{ord}_p(k_1!) + \cdots + \operatorname{ord}_p(k_r!)}}{k_1! \cdot \ldots \cdot k_r!} \bmod \mathfrak{P}\ .$$

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

$$(\zeta_p - 1)^{s_q(k_1) + \cdots + s_q(k_r)} = (\zeta_p - 1)^{k_1 + \cdots + k_r - (p-1)\left(\operatorname{ord}_p(k_1!) + \cdots + \operatorname{ord}_p(k_r!)\right)}$$

$$= (\zeta_p - 1)^{(p-1)\left(\frac{q-1}{p-1} - \left(\operatorname{ord}_p(k_1!) + \cdots + \operatorname{ord}_p(k_r!)\right)\right)}$$

$$= (-pu)^{\frac{q-1}{p-1} - \operatorname{ord}_p(k_1! \cdot \ldots \cdot k_r!)}\ .$$

So

$$\frac{J(\omega_\mathfrak{p}^{-k_1}, \ldots, \omega_\mathfrak{p}^{-k_r})\, q (-pu)^{\operatorname{ord}_p(k_1! \cdot \ldots \cdot k_r!)}}{(-pu)^{\frac{q-1}{p-1}}} \equiv \frac{(-p)^{\operatorname{ord}_p(k_1! \cdot \ldots \cdot k_r!)}}{k_1! \cdot \ldots \cdot k_r!} \bmod \mathfrak{P}\ ,$$

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

$$J(\omega_\mathfrak{p}^{-k_1}, \ldots, \omega_\mathfrak{p}^{-k_r}) \frac{q!}{(-p)^{\frac{q-1}{p-1}}} (-p)^{\operatorname{ord}_p(k_1! \cdot \ldots \cdot k_r!)} \equiv$$

$$\frac{(k_1 + \cdots + k_r)!}{k_1! \cdot \ldots \cdot k_r!} (-p)^{\operatorname{ord}_p(k_1! \cdot \ldots \cdot k_r!)} \bmod \mathfrak{P}^{1 + (p-1)\operatorname{ord}_p((q-1)!)}\ .$$

Since

$$1 + (p-1)\operatorname{ord}_p((q-1)!) - (p-1)\operatorname{ord}_p(k_1! \cdot \ldots \cdot k_r!)$$
$$= 1 + q - 1 - S_p(q-1) - k_1 - \cdots - k_r + S_p(k_1) + \cdots + S_p(k_r)$$
$$= 1 - f(p-1) + s_q(k_1) + \cdots + s_q(k_r) \text{ since } 0 \leqslant k_i < q-1$$
$$\geqslant 1 \text{ by Corollary 1,}$$

we see

$$J(\omega_{\mathfrak{p}}^{-k_1}, \ldots, \omega_{\mathfrak{p}}^{-k_r}) \cdot \frac{q!}{(-p)^{\frac{q-1}{p-1}}} \equiv \frac{(k_1 + \cdots + k_r)!}{k_1! \cdot \ldots \cdot k_r!} \bmod \mathfrak{P},$$

so the congruence

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

settles Case 3.

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

$$\frac{J(\omega_{\mathfrak{p}}^{-k_1}, \ldots, \omega_{\mathfrak{p}}^{-k_r})}{(\zeta_p - 1)^{s_q(k_1) + \cdots + s_q(k_r) - s_q(k_1 + \cdots + k_r)}} \equiv \frac{h_q(k_1 + \cdots + k_r)}{h_q(k_1) \cdot \ldots \cdot h_q(k_r)} \bmod \mathfrak{P},$$

so

$$\frac{J(\omega_{\mathfrak{p}}^{-k_1}, \ldots, \omega_{\mathfrak{p}}^{-k_r})}{(\zeta_p - 1)^{(p-1)\mathrm{ord}_p\left(\frac{(k_1 + \cdots + k_r)!}{k_1! \cdot \ldots \cdot k_r!}\right)}} \equiv \frac{(k_1 + \cdots + k_r)!}{k_1! \cdot \ldots \cdot k_r!} \cdot \frac{1}{(-p)^{\mathrm{ord}_p\left(\frac{(k_1 + \cdots + k_r)!}{k_1! \cdot \ldots \cdot k_r!}\right)}} \bmod \mathfrak{P},$$

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

$$J(\omega_{\mathfrak{p}}^{-k_1}, \ldots, \omega_{\mathfrak{p}}^{-k_r}) \equiv \frac{(k_1 + \cdots + k_r)!}{k_1! \cdot \ldots \cdot k_r!} \bmod \mathfrak{P}. \quad \square$$

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.