Zeitschrift: L'Enseignement Mathématique

Herausgeber: Commission Internationale de l'Enseignement Mathématique

Band: 27 (1981)

Heft: 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: IDENTITIES FOR PRODUCTS OF GAUSS SUMS OVER FINITE FIELDS

Autor: Evans, Ronald J.

Kapitel: 4. Proof of (2)

DOI: https://doi.org/10.5169/seals-51748

3. Theorems of Stickelberger and Davenport-Hasse

We will make use of the following three classical formulas. First [3, (0.8)],

$$G_{fm}\left(\chi^{\frac{q^m-1}{q-1}}\right) = G_f(\chi)^m, \tag{6}$$

where χ is a character on $GF(q^m)$. Next [3, (0.9)],

$$1 = \frac{\chi^l(l)}{G_f(\chi^l)} \prod_{j=0}^{l-1} \frac{G_f(\chi\psi^j)}{G_f(\psi^j)}, \tag{7}$$

where χ, ψ are characters on $GF(q)$ and ψ has order l. Finally [8], [5, p. 25]

$$\frac{G_f(\chi^\alpha)}{(\zeta-1)^{s(\alpha)}} \equiv \frac{1}{\gamma(\alpha)} \equiv \frac{(\zeta-1)^{\alpha-s(\alpha)}}{\alpha!} \quad (\mathrm{mod}\ P), \tag{8}$$

where α is an integer, $0 \leqslant \alpha < q-1$; $s(\alpha)$ denotes the sum of the p-adic digits of α; $\gamma(\alpha)$ denotes the product of the factorials of the p-adic digits of α; P is a prime ideal above p in the ring $\mathcal{O} = Z[\omega]$, where $\omega = \exp(2\pi i/p(q-1))$; and χ is the character on $\mathcal{O}/P \approx GF(q)$ of order $q-1$ which maps the coset $\omega + P$ to $\bar{\omega}$.

4. Proof of (2)

Let η denote the right side of (2). We must show that $\eta = 1$. Let $\delta = \dfrac{q^n-1}{q-1}$, $\theta = w^{k-1}(cw+i_j)$. Using (6), we have

$$\eta^n = \frac{\chi^{ln}(l)\,G_{fn}(\chi^\delta)}{G_{fn}(\chi^{\delta l})} \prod_{j=1}^{e} \prod_{k=1}^{r} \prod_{c=1}^{w^{r-k}} \frac{G_{fn}^n(\chi^\delta\psi^\theta)}{G_{fn}^n(\psi^\theta)}.$$

Consider a fixed pair j, k. For each $a \in \{1, 2, \ldots, n\}$, $G_{fn}(\psi^\theta) = G_{fn}(\psi^{\theta q^a})$, so

$$\prod_{c=1}^{w^{r-k}} G_{fn}(\psi^\theta) = \prod_{c=1}^{w^{r-k}} G_{fn}\left(\psi^{w^{k-1}(cw+ijq^a)}\right).$$

Similarly,

$$\prod_{c=1}^{w^{r-k}} G_{fn}(\chi^\delta\psi^\theta) = \prod_{c=1}^{w^{r-k}} G_{fn}\left(\chi^\delta\psi^{w^{k-1}(cw+ijq^a)}\right).$$

Thus

$$\eta^n = \frac{\chi^{ln}(l)\, G_{fn}(\chi^\delta)}{G_{fn}(\chi^{\delta l})} \prod_{j=1}^{l-1} \frac{G_{fn}(\chi^\delta \psi^j)}{G_{fn}(\psi^j)}. \tag{9}$$

Since $n \equiv \delta \pmod{q-1}$, $\chi^{ln}(l) = \chi^{\delta l}(l)$. Therefore, by (7), the right side of (9) equals 1, so

$$\eta^n = 1. \tag{10}$$

By the definition of η and of Gauss sums,

$$\eta^l \equiv \frac{\chi^{l^2}(l)\, \overline{\chi}^l(l)\, G_f(\chi^l)}{G_f^l(\chi^l)} \prod_{j=1}^{e} \prod_{k=1}^{r} \prod_{c=1}^{w^{r-k}} \frac{\overline{\chi}^{\delta l}(l)\, G_{fn}(\chi^{\delta l})}{1} \pmod{w},$$

so

$$\eta^l \equiv \frac{\chi^{l^2 - l - l\delta(l-1)/n}(l)\, G_{fn}^{(l-1)/n}(\chi^{\delta l})}{G_f^{l-1}(\chi^l)} \pmod{w}.$$

By (6), $G_{fn}(\chi^{\delta l}) = G_f^n(\chi^l)$; hence

$$\eta^l \equiv 1 \pmod{w}. \tag{11}$$

Thus w divides the norm $N(\eta^l - 1)$. By (10), η^l is an n-th root of unity. Thus if $\eta^l - 1 \neq 0$, then $N(\eta^l - 1)$ divides n, which contradicts the fact that $w \nmid n$. Therefore $\eta^l = 1 = \eta^n$, so since $(l, n) = 1$, $\eta = 1$.

5. Proof of (3)

Let η denote the right side of (3). We assume that $0 < \alpha < q - 1$. To see that this presents no loss of generality, we now show that η is unchanged when α is replaced by $\alpha + (q-1)j$, where j is an integer. Clearly $G_f(\chi^\alpha)$ and $\chi^\alpha(l)$ are unchanged, since the restriction $\chi|_{GF(q)}$ has order $q - 1$. Finally, $G_{fl}(\chi^{\alpha\beta})$ is also unchanged, as

$$G_{fl}(\chi^{\alpha\beta}) = G_{fl}(\chi^{\alpha\beta q^{\alpha_j}}) = G_{fl}(\chi^{\beta(\alpha + j(q-1))}), \tag{12}$$

where α_j is defined by $\alpha_j \alpha \equiv j \pmod{l}$, $\alpha_j \geqslant 0$.

Let $\psi = \chi^{\beta(q-1)}$. Using (6), we have

$$\eta^l = \frac{G_{fl}(\chi^{\alpha\beta l})}{\chi^{\alpha l}(l)\, G_{fl}^l(\chi^{\alpha\beta})} \prod_{j=1}^{l-1} G_{fl}(\psi^j).$$