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: 5. Proof of (3)

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

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. 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. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Mehr erfahren

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. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. En savoir plus

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. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. Find out more

Download PDF: 05.12.2025

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

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

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

For each $j \in \{0, 1, ..., l-1\}$, we have, by (12),

$$G_{fl}(\chi^{\alpha\beta}) = G_{fl}(\chi^{\alpha\beta}\psi^j).$$

Thus,

$$\eta^l = \frac{G_{fl}(\chi^{\alpha\beta l})}{\chi^{\alpha l}(l)} \prod_{j=0}^{l-1} \frac{G_{fl}(\psi^j)}{G_{fl}(\chi^{\alpha\beta}\psi^j)}. \tag{13}$$

Since $\chi^{\alpha l}(l) = \chi^{\alpha\beta l}(l)$, the right side of (13) equals 1 by (7), so

$$\eta^l = 1. \tag{14}$$

Let P be the prime ideal above p in $\mathcal{O} = Z[\omega]$, where

$$\omega = \exp(2\pi i/p(q^l - 1),$$

with P chosen such that χ is the character of order $q^l - 1$ on $\mathcal{O}/P \approx GF(q^l)$ which maps the coset $\omega + P$ to $\bar{\omega}$. To show that $\eta = 1$, it suffices to show that $\eta \equiv 1 \pmod{P}$. For, if $\eta \neq 1$, then by (14), the norm $N(\eta - 1)$ divides l; but if also $\eta \equiv 1 \pmod{P}$, then $p \mid N(\eta - 1)$, which yields the contradiction $p \mid l$.

For any integer x, let $L(x)$ denote the least nonnegative residue of $x \pmod{l}$. For integers $i \geqslant 0$, define

$$\varepsilon_i = \begin{matrix} 1, & \text{if } 1 \leqslant L(i\alpha) \leqslant L(\alpha) \\ 0, & \text{otherwise}, \end{matrix}$$

and

$$c_i = \varepsilon_i + l^{-1}\big(\alpha - L(\alpha) + (q-1)L(-i\alpha)\big).$$

Note that each c_i is an integer with $0 \leqslant c_i \leqslant q - 1$. We have

$$l\alpha\beta - l\sum_{i=1}^{l} c_i q^{i-1} = \sum_{i=1}^{l} q^{i-1}(\alpha - lc_i)$$

$$= \sum_{i=1}^{l} q^{i-1}\{-l\varepsilon_i + L(\alpha) - L((1-i)\alpha) + L(-i\alpha)\}.$$

The expressions in braces are easily seen to vanish. Thus we have the following explicit expansion of $\alpha\beta$ in base q:

$$\alpha\beta = \sum_{i=1}^{l} c_i q^{i-1}. \tag{15}$$

By (8), (14), and the definition of η,

$$\eta \equiv (u\gamma(\alpha))^{-1} l^{\alpha}\gamma(\alpha\beta) \pmod{P}, \tag{16}$$

where

$$u = \prod_{j=1}^{l-1} \gamma\left(j\,(q-1)/l\right).$$

By (15) and (16),

$$\eta \equiv \left(u\gamma(\alpha)\right)^{-1} l^{\alpha} \prod_{i=1}^{l} \gamma(c_i) \qquad (\text{mod } P).$$

Thus by the second congruence in (8), there is an integer M such that

$$u\eta \equiv \frac{1}{\alpha!} l^{\alpha} (\zeta-1)^{M} \prod_{i=1}^{l} c_i! \qquad (\text{mod } P). \tag{17}$$

First suppose that $0 < \alpha < l$. Then by (17) and the definition of c_i,

$$\begin{aligned} u\eta &\equiv \frac{1}{\alpha!} l^{\alpha} (\zeta-1)^{M} \prod_{i=1}^{l} \left(\frac{q-1}{l} L(-i\alpha)\right)! \prod_{j=1}^{\alpha} \left(1 + \frac{q-1}{l}(l-j)\right) \\ &\equiv (\zeta-1)^{M} \prod_{i=1}^{l} \left(\frac{q-1}{l} L(-i\alpha)\right)! \qquad (\text{mod } P). \end{aligned}$$

By (14), η is a unit, so again applying the second congruence in (8), we find that

$$u\eta \equiv \prod_{i=1}^{l} \gamma\left(\frac{q-1}{l} L(-i\alpha)\right) \qquad (\text{mod } P).$$

Since α is prime to l, the numbers $L(-i\alpha)$ run through a complete residue system (mod l) as i runs from 1 to l. Thus, be the definition of u following (16), we obtain the desired result $\eta \equiv 1$ (mod P) in the case $0 < \alpha < l$.

Finally, suppose that $l < \alpha < q - 1$. We suppose as induction hypothesis that $\eta' \equiv 1$ (mod P), where η' is obtained from η by replacing α by $\alpha - l$. Then by (17) and the definition of c_i, there is an integer N such that

$$\begin{aligned} \eta \equiv \eta/\eta' &\equiv \frac{1}{\alpha!} (\zeta-1)^{N} (\alpha-l)!\, l^{l} \prod_{i=1}^{l} c_i \\ &= \frac{1}{\alpha!} (\zeta-1)^{N} (\alpha-l)! \prod_{i=1}^{l} \{l\varepsilon_i + \alpha - L(\alpha) + (q-1)\, L(-i\alpha)\} \qquad (\text{mod } P). \end{aligned}$$

Since the numbers $\{l\varepsilon_i - L(-i\alpha) + \alpha - L(\alpha)\}$ run through the l numbers $\alpha, \ldots, \alpha - l + 1$ as i runs from 1 to l, we see that $N = 0$ and $\eta \equiv 1$ (mod P).