IDENTITIES FOR PRODUCTS OF GAUSS SUMS OVER FINITE FIELDS

Autor(en): **Evans, Ronald J.**

Objekttyp: **Article**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **27 (1981)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **26.04.2024**

Persistenter Link: https://doi.org/10.5169/seals-51748

IDENTITIES FOR PRODUCTS OF GAUSS SUMS OVER FINITE FIELDS

by Ronald J. Evans

1. Introduction

In this note, we prove the identities (2)-(5) below for Gauss sums over finite fields of characteristic p. Also, we state conjectures related to (4).

Versions of (2) and (3) for p-adic Gauss sums are stated in [2, p. 368], where they are attributed to Langlands and Dwork, respectively. We allow the case $p = 2$ (note that $p > 2$ in [2], [6]). Also, while l is prime in [2], we do not restrict l to be prime in (2) and (3) (but l is a prime power in (2)).

Identity (4), is a character sum analogue of the case $n = 2$ of the following beautiful formula of Selberg [1, (1.1)]:

$$\int_0^1 \cdots \int_0^1 \Delta_n^z \prod_{i=1}^{n} t_i^{x-1} (1-t_i)^{y-1} \, dt_1 \ldots dt_n \tag{1}$$

$$= n! \prod_{j=0}^{n-1} \frac{\Gamma(jz+z)\,\Gamma(x+jz)\,\Gamma(y+jz)}{\Gamma(z)\,\Gamma(x+y+z(n+j-1))}$$

where

$$\Delta_n = \prod_{1 \leqslant i < j \leqslant n} (t_i - t_j)^2 ,$$

and where

$$x,\ y,\ z + 1/n,\ z + x/(n-1),\ z + y/(n-1)$$

have positive real parts. In §8, we present as conjectures certain formulas which are n-dimensional character sum analogues of (1) and of the following important limiting cases [1, (1.3), (1.2)] of (1):

$$\int_0^\infty \cdots \int_0^\infty \Delta_n^z \prod_{i=1}^{n} t_i^{x-1} e^{-t_i} \, dt_1 \ldots dt_n \tag{1a}$$

$$= n! \prod_{j=0}^{n-1} \frac{\Gamma(jz+z)\,\Gamma(x+jz)}{\Gamma(z)}$$

and

$$\text{(1b)}\qquad \frac{1}{(2\pi)^{n/2}} \int_{-\infty}^{\infty} \cdots \int_{-\infty}^{\infty} e^{-\frac{1}{2}(t_1^2 + \ldots + t_n^2)} \Delta_n^z \, dt_1 \ldots dt_n = n! \prod_{j=0}^{n-1} \frac{\Gamma(jz+z)}{\Gamma(z)}.$$

Identities (4), (4a) and (4b) were discovered and proved by A. Selberg in the early 1940's (unpublished). Also, essentially all of the material in §8 was known to Selberg. We are indebted to him for the ideas provided in [7].

Identity (5) was inspired by the case $n = 2$ of an integral formula of Andrews [1, (4.3)] somewhat similar to (1). It would be interesting to find a higher dimensional analogue.

2. Notation and the identities

Let p be prime and let $\zeta = \exp(2\pi i/p)$. Define the Gauss sum over $GF(p^r)$ by

$$G(\chi) = G_r(\chi) = -\sum_{x \in GF(p^r)} \chi(x) \zeta^{T(x)}$$

(note the minus sign), where T is the trace map from $GF(p^r)$ to $GF(p)$, and χ is any character on the multiplicative group of $GF(p^r)$ (with $\chi(0) = 0$). Fix a prime power $q = p^f$, $f \geqslant 1$.

It is proved in §4 that

$$\text{(2)}\qquad 1 = \frac{\chi^l(l) \, G_f(\chi)}{G_f(\chi^l)} \prod_{j=1}^{e} \prod_{k=1}^{r} \prod_{c=1}^{w^{r-k}} \frac{G_{fn}\left(\chi^{\frac{q^n-1}{q-1}} \psi^{w^{k-1}(cw+ij)}\right)}{G_{fn}\left(\psi^{w^{k-1}(cw+ij)}\right)}$$

where $l = w^r$ for a prime $w \neq p$; n is the order of $q \pmod w$; $e = (w-1)/n$; $i_1, \ldots, i_e$ are coset representatives for the cyclic subgroup $\langle q \rangle$ in the multiplicative group of $GF(w)$; χ is a character on $GF(q^n)$; and ψ is a character of order l on $GF(q^n)$.

It is proved in §5 that

$$\text{(3)}\qquad 1 = \frac{G_f(\chi^\alpha)}{\chi^\alpha(l) \, G_{fl}(\chi^{\alpha\beta})} \prod_{j=1}^{l-1} G_f(\chi^{j(q-1)/l}),$$

where $l \mid (q-1)$; α is an integer prime to l; β is the integer $(1+q+\ldots+q^{l-1})/l$; and χ is a character on $GF(q^l)$ of order $q^l - 1$. One comparing (3) with the last identity in [2, p. 368] should note that the exponent l on the last line of that page should be deleted; in fact, $(\text{Teich } l)^l \, a(q-1)$ should be corrected to read $(\text{Teich } l)^{a(q-1)}$. We remark that the product over j in (3) equals $q^{(l-1)/2} \, U_0$, where U_0 equals 1 or $i^{(p-1)^2 f/4} (-1)^{f + (q-1)(l-2)/8}$ according as l is odd or even. This

fact is easy to prove for odd l (since $G_f(\psi)\, G_f(\overline{\psi}) = \psi(-1)\, q$ for a nontrivial character ψ on $GF(q)$); for even l, this follows from the classical evaluation of quadratic Gauss sums over $GF(p)$ (extended to $GF(q)$ via (6) below).

It is proved in §6 that

$$\sum_{x,\, y \in GF(q)} \chi_1(xy)\, \chi_2((1-x)(1-y))\, \chi_3^2(x-y) = R(\chi_1, \chi_2, \chi_3) + R(\chi_1, \chi_2, \chi_3\phi), \tag{4}$$

where $\chi_1, \chi_2, \chi_3, \phi$ are characters on $GF(q)$; ϕ has order 2 (so $p > 2$); $\chi_1\, \chi_2\, \chi_3^2$ and $(\chi_1\chi_2\chi_3)^2$ are nontrivial; and

$$R(\chi_1, \chi_2, \chi_3) = \frac{G(\chi_3^2)\, G(\chi_1)\, G(\chi_1\chi_3)\, G(\chi_2)\, G(\chi_2\chi_3)}{G(\chi_3)\, G(\chi_1\chi_2\chi_3)\, G(\chi_1\chi_2\chi_3^2)}.$$

(Cf. (1)). The special case of (4) where $\chi_1 = \chi_2 = \chi_3^2 = \phi$ has been applied in graph theory [4], [9].

Selberg has pointed out that if χ, ψ, and ϕ are characters on $GF(q)$, where ϕ has order 2, then

$$\sum_{x,\, y \in GF(q)} \psi(xy)\, \chi^2(x-y)\, \zeta^{T(x+y)} = \frac{G(\psi)\, G(\chi\psi)\, G(\chi^2)}{G(\chi)} + \frac{G(\psi)\, G(\chi\psi\phi)\, G(\chi^2)}{G(\chi\phi)} \tag{4a}$$

and

$$\frac{1}{G^2(\phi)} \sum_{x,\, y \in GF(q)} \chi^2(x-y)\, \zeta^{\frac{p+1}{2} T(x^2+y^2)} = \frac{G(\chi^2)}{G(\chi)} + \frac{G(\chi^2)}{G(\chi\phi)}. \tag{4b}$$

These are character sum analogues of (1a) and (1b), respectively, for $n = 2$. We omit the proofs, as they are similar to (and easier than) the proof of (4).

It is proved in §7 that

$$\sum_{\substack{x,\, y \in GF(q) \\ x,\, y \neq 0}} \chi_1\, \chi_3\left(\frac{1+x}{y}\right) \chi_2\, \chi_3\left(\frac{1+y}{x}\right) \chi_1\, \chi_2(y-x) = D(\chi_1, \chi_2, \chi_3) + D(\chi_1\phi, \chi_2\phi, \chi_3\phi), \tag{5}$$

where $\chi_1, \chi_2, \chi_3, \phi$ are characters on $GF(q)$; ϕ has order 2 (so $p > 2$); $\chi_1^2, \chi_2^2, \chi_3^2, \chi_1\chi_2, \chi_1\chi_3$, and $\chi_2\, \chi_3$ are nontrivial; and

$$D(\chi_1, \chi_2, \chi_3) = \frac{q^2 \chi_2(-1)\, G(\chi_1\chi_2\chi_3)}{G(\chi_1)\, G(\chi_2)\, G(\chi_3)}.$$

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]

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

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

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

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

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

and

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

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),

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

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

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

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

$$u\eta \equiv \frac{1}{\alpha!}\, l^{\alpha}(\zeta-1)^{M} \prod_{i=1}^{l} \left(\frac{q-1}{l} L(-i\alpha)\right)! \prod_{j=1}^{\alpha} \left(1 + \frac{q-1}{l}(l-j)\right)$$

$$\equiv (\zeta-1)^{M} \prod_{i=1}^{l} \left(\frac{q-1}{l} L(-i\alpha)\right)! \pmod{P}.$$

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

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

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 $\eta \equiv 1 \pmod{P}$ in the case $0 < \alpha < l$.

Finally, suppose that $l < \alpha < q - 1$. We suppose as induction hypothesis that $\eta' \equiv 1 \pmod{P}$, 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

$$\eta \equiv \eta/\eta' \equiv \frac{1}{\alpha!}(\zeta-1)^{N}(\alpha-l)!\, l^{l} \prod_{i=1}^{l} c_i$$

$$= \frac{1}{\alpha!}(\zeta-1)^{N}(\alpha-l)! \prod_{i=1}^{l} \{l\varepsilon_i + \alpha - L(\alpha) + (q-1)\,L(-i\alpha)\} \pmod{P}.$$

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 $\eta \equiv 1 \pmod{P}$.

6. Proof of (4)

For characters $\psi_1, ..., \psi_m$ on $GF(q)$, define the Jacobi sum

$$J(\psi_1, ..., \psi_m) = (-1)^{m+1} \sum_{\substack{x_1, ..., x_m \in GF(q) \\ x_1 + ... + x_m = 1}} \psi_1(x_1) ... \psi_m(x_m).$$

We will use the well-known fact that if $\psi_1 \psi_2 ... \psi_m$ is nontrivial, then

$$J(\psi_1, ..., \psi_m) = G(\psi_1 ... \psi_m)^{-1} \prod_{i=1}^{m} G(\psi_i). \tag{18}$$

Let S denote the left side of (4). If χ_1, χ_2, or χ_3^2 is trivial, then it is easy to verify (4) directly, with use of (18) and (26) below. Thus assume that χ_1, χ_2, and χ_3^2 are nontrivial. With the change of variables

$$u = xy, \qquad v = x + y,$$

we have

$$S = \sum_{u, v \in GF(q)} \chi_1(u) \chi_2(1+u-v) \chi_3(v^2-4u) \{1 + \phi(v^2-4u)\}.$$

It therefore remains to show that

$$S_1 = \sum_{u, v} \chi_1(u) \chi_2(1+u-v) \chi_3(v^2-4u) = R(\chi_1, \chi_2, \chi_3\phi). \tag{19}$$

Replace v by $u + 1 - v$ to get

$$S_1 = \sum_{u, v} \chi_1(u) \chi_2(v) \chi_3(1+u^2+v^2-2u-2v-2uv). \tag{20}$$

Replace u by u/t, and v by v/t, to get

$$S_2 = -S_1 G(\chi_1\chi_2\chi_3^2) \tag{21}$$

$$= \sum_{t \neq 0} \sum_{u, v} \chi_1(u) \chi_2(v) \chi_3(t^2+u^2+v^2-2ut-2vt-2uv) \zeta^{T(t)}.$$

Since $\chi_1\chi_2\chi_3^2$ is nontrivial, the restriction $t \neq 0$ may be dropped. Then replace t by $t + u + v$ to get

$$S_2 = \sum_{t, u, v} \chi_1(u) \chi_2(v) \chi_3(t^2-4uv) \zeta^{T(t+u+v)}.$$

Replace u by ua and v by vb to get

$$S_3 = S_2 \overline{G(\chi_1)}\ \overline{G(\chi_2)} \tag{22}$$

$$= \sum_{t} \sum_{a, b, u, v \neq 0} \chi_1(u) \chi_2(v) \chi_3(t^2-4uvab) \zeta^{T(t+a(u-1)+b(v-1))}.$$

Replace a by $a/(4uvb)$ to get

$$S_3 = \sum_t \sum_{a,\,b,\,u,\,v\neq 0} \chi_1(u)\,\chi_2(v)\,\chi_3(t^2-a)\,\zeta^{T\left(t+b(v-1)+\frac{a(u-1)}{4uvb}\right)}.$$

Since χ_1 is nontrivial, the restriction $a \neq 0$ may be dropped. Then replace a by $t^2 - a$ to get

$$S_3 = \sum_{a,\,t} \sum_{b,\,u,\,v\neq 0} \chi_1(u)\,\chi_2(v)\,\chi_3(a)\,\zeta^{T\left(t+b(v-1)+\frac{(1-u)(a-t^2)}{4uvb}\right)}$$

$$= -G(\chi_3) \sum_{u\neq 0,\,1} \sum_{b,\,v\neq 0} \chi_1(u)\,\chi_2(v)\,\chi_3\left(\frac{4uvb}{1-u}\right)\zeta^{T(b(v-1))} \sum_t \zeta^{T\left(t+\frac{t^2(u-1)}{4uvb}\right)}.$$

The inner sum on t equals $-\zeta^{T\left(\frac{uvb}{1-u}\right)}\,\phi\left(\frac{4uvb}{u-1}\right)G(\phi)$.

Hence

$$S_4 = S_3\left(G(\chi_3)\,G(\phi)\,\chi_3(-1)\right)^{-1} \tag{23}$$

$$= \sum_{u\neq 0,\,1} \sum_{b,\,v\neq 0} \chi_1(u)\,\chi_2(v)\,\chi_3\phi\left(\frac{4uvb}{u-1}\right)\zeta^{T\left(b(v-1)+\frac{uvb}{1-u}\right)}.$$

Therefore,

$$S_4 = \sum_{u\neq 0,\,1} \sum_{v\neq 0} \chi_1\chi_3\phi(u)\,\chi_2\chi_3\phi(v)\,\bar{\chi}_3\phi\left(\frac{u-1}{4}\right)\sum_b \chi_3\phi(b)\,\zeta^{T\left(b(v-1)+\frac{buv}{1-u}\right)}.$$

Since χ_2 and $\chi_3\phi$ are nontrivial,

$$S_4 = -G(\chi_3\phi)\sum_{u,\,v} \chi_1\chi_3\phi(u)\,\chi_2\chi_3\phi(v)\,\bar{\chi}_3\phi\left(\frac{1-u-v}{4}\right),$$

so

$$S_4 = -\chi_3(4)\,G(\chi_3\phi)\,J(\chi_1\chi_3\phi,\,\chi_2\chi_3\phi,\,\bar{\chi}_3\phi). \tag{24}$$

Combining (21)-(24), we get

$$S_1 = \frac{\chi_3(-4)\,G(\chi_3)\,G(\phi)\,G(\chi_3\phi)\,J(\chi_1\chi_3\phi,\,\chi_2\chi_3\phi,\,\bar{\chi}_3\phi)}{G(\chi_1\chi_2\chi_3^2)\,\overline{G(\chi_1)}\,\overline{G(\chi_2)}}. \tag{25}$$

Applying (7) with $l = 2$, we find that for any character χ_3,

$$\chi_3(-4)\,G(\chi_3)\,G(\phi)\,G(\chi_3\phi) = \chi_3\phi(-1)\,qG(\chi_3^2). \tag{26}$$

Since χ_1 and χ_2 are nontrivial, it follows from (25) and (26) that

$$S_1 = \frac{\chi_3\phi(-1)\,G(\chi_3^2)\,G(\chi_1)\,G(\chi_2)\,J(\chi_1\chi_3\phi,\,\chi_2\chi_3\phi,\,\bar{\chi}_3\phi)}{q\,G(\chi_1\chi_2\chi_3^2)}. \tag{27}$$

Since $\chi_1\chi_2\chi_3\phi$ and $\chi_3\phi$ are nontrivial, (19) now follows from (18) and (27).

Remark. We evaluated S (the left side of (4)) only under the assumption that $\chi_1\chi_2\chi_3^2$ and $(\chi_1\chi_2\chi_3)^2$ were nontrivial. We now indicate how S can be simply evaluated in terms of Gauss sums when this assumption is dropped. If χ_1, χ_2, or χ_3^2 is trivial, one can easily evaluate S directly from its definition. If $\chi_1\chi_2\chi_3^2$ is trivial, then one can evaluate S_1 (and hence S) from (20), by first replacing u by u^{-1}, then replacing v by vu^{-1}, to obtain

$$S_1 = \sum_{u,\,v} \bar{\chi}_1\bar{\chi}_2\bar{\chi}_3^2(u)\,\chi_3(1+u^2+v^2-2u-2v-2uv)\,\chi_2(v).$$

Finally, suppose that χ_1, χ_2, χ_3^2, and $\chi_1\chi_2\chi_3^2$ are nontrivial. Then S_1 can be evaluated from (27).

7. Proof of (5)

Let E denote the left side of (5). Since $\chi_1\chi_2$ is nontrivial,

$$E + 1 + \chi_1\chi_2(-1) = \sum_{\substack{x,\,y\neq 0\\ x+y\neq -1}} \chi_1\chi_3\left(\frac{1+x}{y}\right)\chi_2\chi_3\left(\frac{1+y}{x}\right)\chi_1\chi_2(y-x).$$

Set $t = \dfrac{1+x}{y}$, $u = \dfrac{1+y}{x}$, so

$$x = \frac{t+1}{ut-1}, \qquad y = \frac{u+1}{ut-1}.$$

Then

$$E + 1 + \chi_1\chi_2(-1) = \sum_{\substack{u,\,t\neq -1\\ ut\neq 1}} \chi_1\chi_3(t)\,\chi_2\chi_3(u)\,\chi_1\chi_2\left(\frac{t-u}{1-ut}\right)$$

$$= \sum_{u,\,t\neq -1} \chi_1\chi_3(t)\,\chi_2\chi_3(u)\,\chi_1\chi_2(t-u)\,\bar{\chi}_1\bar{\chi}_2(1-ut).$$

Since $\chi_1\chi_3$ and $\chi_2\chi_3$ are nontrivial,

$$E = \sum_{u,\,t\neq 0} \chi_1\chi_3(t)\,\chi_2\chi_3(u)\,\chi_1\chi_2(t-u)\,\bar{\chi}_1\bar{\chi}_2(1-ut).$$

Replace t by t/u to obtain

$$E = \sum_{u,\,t\neq 0} \chi_1\chi_3(t)\,\bar{\chi}_1^2(u)\,\chi_1\chi_2(t-u^2)\,\bar{\chi}_1\bar{\chi}_2(1-t)$$

$$= \sum_{u,\,t\neq 0} \chi_1\chi_3(t)\,\bar{\chi}_1\bar{\chi}_2(1-t)\,\bar{\chi}_1(u)\,\chi_1\chi_2(t-u)\{1+\phi(u)\}.$$

Now replace u by tu to get

$$(28)\qquad E = \sum_{u,\,t} \chi_1\chi_2\chi_3(t)\,\bar{\chi}_1\bar{\chi}_2(1-t)\,\bar{\chi}_1(u)\,\chi_1\chi_2(1-u)\{1+\phi(ut)\}$$

$$= J(\chi_1\chi_2\chi_3, \bar{\chi}_1\bar{\chi}_2)\,J(\bar{\chi}_1, \chi_1\chi_2) + J(\chi_1\chi_2\chi_3\phi, \bar{\chi}_1\bar{\chi}_2)\,J(\bar{\chi}_1\phi, \chi_1\chi_2),$$

where the Jacobi sums J are defined above (18). Since χ_1^2, χ_2^2, χ_3^2, and $\chi_1\chi_2$ are nontrivial, (5) now follows from (18).

Remark. If $\chi_1\chi_2$, $\chi_1\chi_3$, or $\chi_2\chi_3$ is trivial, we can easily evaluate E directly from its definition. Otherwise, E can be evaluated simply from (28).

8. Character sum analogues of (1), (1a) and (1b)

Let $\chi_1, \chi_2, \chi_3, \phi$ be characters on $GF(q)$, where ϕ has order 2, $p > 2$. Set $t_0 = 1$. The discriminant of the polynomial

$$F(y) = \sum_{i=0}^{n} t_i\, y^{n-i}$$

is a polynomial in $t_1, \ldots, t_n$ which shall be denoted by D_n. Write

$$E_n = \sum_{i=0}^{n} (-1)^i\, t_i\,.$$

We conjecture that the following analogues of (1), (1a), (1b) hold for each $n \geqslant 1$:

$$(29)\qquad \sum_{t_1,\ldots,t_n \in GF(q)} \chi_1(t_n)\,\chi_2(E_n)\,\chi_3\phi(D_n) = \prod_{j=0}^{n-1} \frac{-G(\chi_3^{j+1})\,G(\chi_1\chi_3^j)\,G(\chi_2\chi_3^j)}{G(\chi_3)\,G(\chi_1\chi_2\chi_3^{n+j-1})},$$

provided that the n characters $\chi_1\chi_2\chi_3^{n+j-1}$ $(0 \leqslant j \leqslant n-1)$ are all nontrivial;

$$(29a)\qquad \sum_{t_1,\ldots,t_n \in GF(q)} \chi_1(t_n)\,\chi_3\phi(D_n)\,\zeta^{T(t_1)} = \prod_{j=0}^{n-1} \frac{-G(\chi_3^{j+1})\,G(\chi_1\chi_3^j)}{G(\chi_3)}$$

for all χ_1, χ_3; and

$$(29b)\qquad \sum_{t_1,\ldots,t_n \in GF(q)} \chi_3\phi(D_n)\,\zeta^{\frac{p+1}{2}T(t_1^2-2t_2)} = \prod_{j=0}^{n-1} \frac{-\phi(2)\,G(\phi)\,G(\chi_3^{j+1})}{G(\chi_3)}$$

for all χ_3.

Formulas (29), (29a), and (29b) have been verified by computer for some small primes q with $n = 3, 4$. Of course the formulas are well known for $n = 1$. For

$n = 2$, (29a) and (29b) are not hard to prove, and (29) follows from the proof of (4). (For example, if χ_3 in (29) is trivial, one makes use of (19) and (21)-(23).)

For $n = 3$, we can prove (29b), but not (29) or (29a). The *ad hoc* proof given below appears to shed little light on the general case.

THEOREM. For $n = 3$, (29b) holds.

Proof. All rational fractions below are to be interpreted as integers (mod p); for example, $\frac{1}{2}$ equals $(p+1)/2$. We must show that

$$(30) \qquad A = \sum_{t,u,v} \chi\phi(D_3)\,\zeta^{T\left(\frac{v^2}{2}-u\right)} = -\frac{\phi(2)\,G^3(\phi)\,G(\chi^3)\,G(\chi^2)}{G^2(\chi)}$$

for any character χ on $GF(q)$, where

$$D_3 = u^2v^2 - 4u^3 - 4tv^3 - 27t^2 + 18tuv\,.$$

First suppose that $p = 3$. Then

$$\begin{aligned} A &= \sum_{t,u,v} \chi\phi(u^2v^2 - u^3 - tv^3)\,\zeta^{T\left(\frac{v^2}{2}-u\right)} \\ &= \sum_{v\neq 0}\sum_{u} \zeta^{T\left(\frac{v^2}{2}-u\right)} \sum_{t} \chi\phi(u^2v^2 - u^3 - t) + \sum_{t,u} \phi\chi^3(-u)\,\zeta^{T(-u)} \\ &= 0 - q\,G(\phi\chi^3) = -q\,G(\chi\phi)\,, \end{aligned}$$

since $G(\psi^p) = G(\psi)$ for any character ψ. Now (30) follows with the aid of (26).

Next, suppose that $p > 3$. Completing the square in t, one has

$$D_3/27 = c - \left(t + \frac{2v^3}{27} - \frac{uv}{3}\right)^2,$$

where $c = \frac{4}{27}\left(\frac{v^2}{3} - u\right)^3$. Thus

$$\begin{aligned} \bar{\chi}\phi(27)\,A &= \sum_{t,u,v} \chi\phi(c - t^2)\,\zeta^{T\left(\frac{v^2}{2}-u\right)} \\ &= \sum_{u,v} \zeta^{T\left(\frac{v^2}{2}-u\right)} \sum_{t} \chi\phi(c-t)\cdot\{1 + \phi(t)\} \\ &= \sum_{u,v} \zeta^{T\left(\frac{v^2}{2}-u\right)} \sum_{t} \chi\phi(c-t)\,\phi(t) \\ &= K \sum_{\substack{u,v \\ c=0}} \zeta^{T\left(\frac{v^2}{2}-u\right)} + J \sum_{u,v} \chi(c)\,\zeta^{T\left(\frac{v^2}{2}-u\right)}, \end{aligned}$$

where $K = \chi\phi(-1)\sum_t \chi(t)$ and $J = \sum_t \chi\phi(1-t)\,\phi(t)$.

Thus

$$\bar{\chi}\phi(27)\,A = K\sum_v \zeta^{T\left(\frac{v^2}{6}\right)} + \chi\left(\frac{4}{27}\right) J \sum_{u,v} \chi^3\left(\frac{v^2}{3} - u\right)\zeta^{T\left(\frac{v^2}{2}-u\right)}.$$

Replace u by $u + \dfrac{v^2}{3}$ to obtain

$$\begin{aligned}\bar{\chi}\phi(27)\,A &= -K\phi(6)\,G(\phi) + \chi\left(\frac{4}{27}\right) J \sum_{u,v} \chi^3(-u)\,\zeta^{T\left(\frac{v^2}{6}-u\right)} \\ &= \phi(6)\,G(\phi)\left\{-K + \chi\left(\frac{4}{27}\right) JG(\chi^3)\right\}.\end{aligned}$$

If χ is trivial, then $K = \phi(-1)(q-1)$, $J = -\phi(-1)$, and $G(\chi^3) = 1$, and the desired result (30) follows. If χ is nontrivial, then $K = 0$ and

$$J = -G(\chi\phi)\,G(\phi)/G(\chi)$$

by (18), and (30) follows with the aid of (26).

REFERENCES

[1] ASKEY, R. Some basic hypergeometric extensions of integrals of Selberg and Andrews. *SIAM J. Math. Anal. 11* (1980), 938-951,

[2] BOYARSKY, M. p-adic gamma functions and Dwork cohomology. *Trans. Amer. Math. Soc. 257* (1980), 359-369.

[3] DAVENPORT, H. und H. HASSE. Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen. *J. Reine Angew. Math. 172* (1934), 151-182.

[4] EVANS, R., J. PULHAM and J. SHEEHAN. On the number of complete subgraphs contained in certain graphs. *J. Combinatorial Theory* (to appear).

[5] GRAS, G. Sommes de Gauss sur les corps finis. *Publ. Math. Besançon 1* (1977-1978), 1-71.

[6] GROSS, B. and N. KOBLITZ. Gauss sums and the p-adic Γ-function. *Annals of Math. 109* (1979), 569-581.

[7] SELBERG, A. Private correspondence, Summer, 1980.

[8] STICKELBERGER, L. Über eine Verallgemeinerung der Kreistheilung. *Math. Ann. 37* (1890), 321-367.

[9] THOMASON, A. Ph.D. Thesis, Cambridge University, 1979.

(Reçu le 18 septembre 1980)

Ronald J. Evans

Department of Mathematics
University of California, San Diego
La Jolla, CA 92093