**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:** 1. Introduction

**DOI:** 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)]:

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

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

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):

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

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

and

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

Identities (4), (4a) and (4b) were discovered and proved by A. Selberg in the early 1940's (unpublished).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 $\chi$ 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

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

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 $GF(w)$; $\chi$ is a character on $GF(q^n)$; and $\psi$ is a character of order $l$ on $GF(q^n)$.

It is proved in §5 that

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

where $l \mid (q-1)$; $\alpha$ is an integer prime to $l$; $\beta$ is the integer $(1+q+\ldots+q^{l-1})/l$; and $\chi$ 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