Aequationes Mathematicae 30 (1986) 134–141
University of Waterloo

0001-9054/86/001134-8$1.50+0.20/0

The triplication formula for Gauss sums

JOHN GREENE AND DENNIS STANTON

Abstract. A new proof of the triplication formula for Gauss sums is given. It mimics an old proof of the analogous result for gamma functions. The techniques are formal and rely upon the character properties of fields. A new character sum evaluation is given.

1. Introduction

The analogy between Gauss sums and the gamma function has been pointed out at various times [9], [6; p. 144], [14, Sec. 2]. Given the field $GF(q)$ (or $\mathbb{R}$), Gauss sums (the gamma function) can be defined as the Fourier transform of a multiplicative character. Many properties of Gauss sums and gamma functions have identical proofs using only formal character properties, the Fourier inversion formula, and a convolution. For example, the Jacobi sum evaluation [8, p. 93]

$$J(\chi_1, \chi_2) = \frac{G(\chi_1)G(\chi_2)}{G(\chi_1\chi_2)} \tag{1.1}$$

and the beta function evaluation [5, eq. 1.5(5), p. 9]

$$B(x, y) = \frac{\Gamma(x)\Gamma(y)}{\Gamma(x+y)} \tag{1.2}$$

follow from taking the Fourier transform of a convolution of two multiplicative characters. Gauss's evaluation of the modulus of a Gauss sum

AMS (1980) subject classification: Primary 10G05, 33A15.

Manuscript received August 15, 1983.

$$G(\chi)G(\bar{\chi}) = \chi(-1)q \tag{1.3}$$

and the reflection formula for the gamma function

$$\Gamma(x)\Gamma(1-x) = \frac{\pi}{\sin \pi x} \tag{1.4}$$

follow from the Fourier inversion formula.

There is another pair of formulas which are completely analogous. The multiplication formula for the gamma function is [5, 1.2(11), p. 4]

$$\Gamma(nx)\Gamma(1/n) \dots \Gamma((n-1)/n) = n^{nx-1}\Gamma(x)\Gamma(x+1/2) \dots \Gamma(x+(n-1)/n). \tag{1.5}$$

The Hasse-Davenport formula for Gauss sums is [14, Eq. (2.2)], [2],

$$G(\chi^n)G(\varphi)G(\varphi^2) \dots G(\varphi^{n-1}) = \chi^n(n)G(\chi)G(\chi\varphi) \dots G(\chi\varphi^{n-1}), \tag{1.6}$$

where φ is a multiplicative character of $GF(q)$ such that $\varphi^n = 1$. As far as we know, there is no simple formal proof for (1.5) and (1.6) simultaneously. Guided by a proof of (1.5), in this note we shall prove (1.6) for $n = 3$ and $q = p$, a prime.

There are two interesting features of our proof. First, we use a transformation for a generalized hypergeometric series ${}_3F_2$ to establish the appropriate congruence relation. We have not seen an application of these series to Gauss sums. Also we will explicitly evaluate some character sums in Proposition 3.2.

2. Liouville's proof of (1.5)

In [4, p. 175] one can find Liouville's proof [12] of (1.5). His idea was to represent the right-hand-side of (1.5) as a multiple integral, change variables, and evaluate all but one integral to obtain the left-hand-side of (1.5). For (1.6) and Gauss sums we let $n = 3$ and $3 | p-1$ so that there is a multiplicative character φ such that $\varphi^3 = 1$. Then, if $\rho = \exp(2\pi i/p)$,

$$G(\chi)G(\chi\varphi)G(\chi\varphi^2) = \sum_{\substack{a,b,c \in GF(p) \\ \neq 0}} \rho^{a+b+c}\chi(abc)\varphi(bc^2) \tag{2.1}$$

Liouville then proceeds to change variables $a = d^3/bc$ in the triple integral. However, for (2.1) it is not true that abc is always a cube so we put $a = d/bc$ and get

$$G(\chi)G(\chi\varphi)G(\chi\varphi^2) = \sum_{\substack{b,c,d\in GF(p)\\ \neq 0}} \rho^{b+c+d/bc}\chi(d)\varphi(bc^2). \tag{2.2}$$

Next we will see that the change of variables $a = d^3/bc$ was proper in (2.1) because we will show that the right-hand-side of (2.2) is zero unless d is a cube:

$$f(d) = \sum_{\substack{b,c\in GF(p)\\ \neq 0}} \rho^{b+c+d/bc}\varphi(bc^2) = 0 \text{ if } \varphi(d) \neq 1. \tag{2.3}$$

The substitution $e = d/bc$ shows that

$$f(d) = \varphi(d)f(d) \tag{2.4}$$

so $f(d) = 0$ if $\varphi(d) \neq 1$. Thus we can replace d by d^3 in (2.2) and divide by 3.

Then Liouville evaluates [4, p. 173–175], [12],

$$\int_0^\infty \int_0^\infty e^{-b-c-d^3/bc} b^{-2/3} c^{-1/3} db\,dc = 2\pi e^{-3d}/\sqrt{3} = e^{-3d}\Gamma\left(\frac{1}{3}\right)\Gamma\left(\frac{2}{3}\right). \tag{2.5}$$

The Gauss sum analog of (2.5) that we will prove is

$$\sum_{\substack{b,c\in GF(p)\\ \neq 0}} \rho^{b+c+d^3/bc}\varphi(bc^2) = p(\rho^{3d} + \rho^{3rd} + \rho^{3r^2d}) \tag{2.6}$$

where r is a primitive cube root of 1.

Assuming (2.6) we see that

$$G(\chi)G(\chi\varphi)G(\chi\varphi^2) = \frac{p}{3}\sum_{\substack{d\in GF(p)\\ \neq 0}} \chi^3(d)[\rho^{3d} + \rho^{3rd} + \rho^{3r^2d}] = p\bar{\chi}^3(3)G(\chi^3) \tag{2.7}$$

This is the $n = 3$ case of (1.6) because $G(\varphi)G(\varphi^2) = p$.

3. Proof of (2.6)

Note that the change of variables $b \to bd$ and $c \to cd$ shows that it is sufficient to prove (2.6) for $d = 1$ and any non-trivial pth-root of unity ρ. In this case the substitutions $b \to bc$, $c \to 1/c$ allow (2.6) to be rewritten as

$$\sum_{\substack{b,c\in GF(p)\\ \neq 0}} \rho^{b+c+1/bc}\varphi(bc^2) = \sum_{x\in GF(p)} \rho^x \sum_{\substack{b,c\in GF(p),\neq 0\\ b^2+(1-xc)b+c^3=0}} \varphi(b). \tag{3.1}$$

Thus (2.6) (for $d = 1$) will follow from the following proposition.

PROPOSITION 3.2. *Let p be a prime such that $3|p-1$. Let $r\in\mathbb{Z}_p$ be a primitive cube root of unity and let φ be a cubic residue character, $\varphi^3 = 1$. Then*

$$\sum_{\substack{b,c\in GF(p),\neq 0\\ b^2+(1-xc)b+c^3=0}} \varphi(b) = \begin{cases} p-3 & x = 3,\ 3r,\ 3r^2 \\ -3 & \text{otherwise.} \end{cases}$$

We prove directly that Proposition 3.2 holds for $x = 3$, $3r$, and $3r^2$ by showing that each solution b is a cube, and that there are $p-3$ solutions. For each $c \neq 0$, there is a solution b to $b^2+(1-xc)b+c^3 = 0$ if and only if $(1-xc)^2-4c^3$ is a square. However, for $x = 3$, $3r$, and $3r^2$ $(1-xc)^2-4c^3$ has a repeated root, e.g. $(1-3c)^2-4c^3 = (1-c)^2(1-4c)$. In this case we can put $1-4c = \alpha^2$ so that $2b = 3(1-\alpha^2)/4 - 1 \pm \alpha(3+\alpha^2)/4$ are the solutions. This implies that $8b = (\mp\alpha-1)^3$, so that b is always a cube. Two values of c ($c = 1/4, 1$) allow one b, while the remaining $(p-1)/2-2$ values of c allow 2 distinct b's. Thus the number of solutions is $2[(p-1)/2-2]+2 = p-3$, all of which have $\varphi(b) = 1$.

There is also a similar argument for $x = 0$ in Proposition 3.2. Instead we give a lemma that applies to all x.

LEMMA 3.3. *In Proposition* 3.2,

$$f(x) = \sum_{\substack{b,c\in GF(p),\neq 0\\ b^2+(1-xc)b+c^3=0}} \varphi(b) \equiv -3 \pmod{p} \text{ for all } x.$$

Note that Lemma 3.3 makes sense. If b_1 and b_2 are two distinct roots of the quadratic equation for b, then $b_1b_2 = c^3$ so $\varphi(b_1)+\varphi(b_2)$ is an integer. To see that Lemma 3.3 implies Proposition 3.2, clearly

$$\sum_{x\in GF(p)} f(x) = 0$$

and

$$f(3) = f(3r) = f(3r^2) = p-3.$$

So $f(x) \geqq -p-2$ shows that Lemma 3.3 implies Proposition 3.2. However, $f(x) \geqq -p-2$ is immediate because there are at most $2(p-1)$ solutions b (with repetition) to $b^2 + (1-xc)b + c^3 = 0$, and $\varphi(b) + \varphi(c^3/b) = -1$ for pairs of non-cube solutions.

Finally we come to the proof of Lemma 3.3. In fact, we show that $f(x)$ is a constant mod p. If we choose $b, c \in \{1, \ldots, p-1\}$, then $\varphi(b) \equiv b^{(p-1)/3} (\text{mod } p)$ and the quadratic character $\chi(b) = b^{(p-1)/2}$. In Lemma 3.3 we put $h(x,c) = (1-xc)^2 - 4c^3$. If $h(x,c)$ is a non-zero square, then

$$\varphi(b_1) + \varphi(b_2) \equiv \left(\frac{cx - 1 + \sqrt{h(x,c)}}{2}\right)^{(p-1)/3} + \left(\frac{cx - 1 - \sqrt{h(x,c)}}{2}\right)^{(p-1)/3}$$

$$\equiv \sum_{n \geqq 0} \binom{(p-1)/3}{2n} \left(\frac{cx-1}{2}\right)^{(p-1)/3 - 2n} \left(\frac{h(x,c)}{4}\right)^n. \tag{3.4}$$

Also (3.4) holds if $h(x,c) = 0$ so that there is a simple repeated root b_1. Because mod p we have

$$1 + [h(x,c)]^{(p-1)/2} \equiv \begin{cases} 0 & h(x,c) \text{ a non-square} \\ 2 & h(x,c) \text{ a square,} \end{cases}$$

we see that

$$f(x) \equiv 2^{(-2-p)/3} \sum_{n \geqq 0} \binom{(p-1)/3}{2n} \sum_{\substack{c \in GF(p) \\ c \neq 0}} \{1 + [h(x,c)]^{(p-1)/2}\}$$

$$(cx-1)^{(p-1)/3 - 2n} [h(x,c)]^n. \tag{3.5}$$

Note that $h(x,c)$ is a polynomial in c of degree three so that the individual terms in (3.5) are polynomials in c of degree at most $2(p-1)$. However

$$\sum_{c \in GF(p)} c^l = 0 \text{ unless } (p-1) | l.$$

So the only possible contributions to (3.5) are the c^0, c^{p-1}, and $c^{2(p-1)}$ terms.

For the c^0 term, we put $c = 0$, $h(x,0) = 1$. We see that there is no x dependence in (3.5) for $c = 0$.

For the $c^{2(p-1)}$ term, we need to choose $[h(x,c)]^{(p-1)/2+n}(cx-1)^{(p-1)/3-2n}$ for $n = (p-1)/6$. Again this is clearly independent of x.

By the binomial theorem we find that the c^{p-1} term is a multiple of

$$A(x) = \sum_{n \geqq 0} \binom{(p-1)/3}{2n} \sum_{k \geqq 0} \binom{(p-1)/2+n}{k} \binom{4(p-1)/3-2k}{p-1-3k} (-4)^k \times x^{p-1-3k}(-1)^{(p-1)/3+k}. \quad (3.6)$$

Clearly

$$\binom{4(p-1)/3-2k}{p-1-3k} \equiv 0 \text{ for } 0 \leqq 2k \leqq (p-1)/3. \quad (3.7)$$

So it is sufficient to prove

$$\sum_{n \geqq 0} \binom{(p-1)/3}{2n} \binom{(p-1)/2+n}{k} \equiv 0 \text{ for } (p-1)/6 < k < (p-1)/3. \quad (3.8)$$

In terms of generalized hypergeometric series (3.8) is [5, Chap. IV]

$${}_3F_2\left(\begin{matrix}(1-p)/6, (4-p)/6, (p+1)/2 \\ 1/2, (p+1)/2-k\end{matrix}\middle| 1\right) \equiv 0 \pmod{p} \quad (3.9)$$

for $(p-1)/6 < k < (p-1)/3$. In order to show (3.9) we use a terminating ${}_3F_2$ transformation (put $p = 1$ in [13, Eq. (4.4)])

$$(-1)^n (c)_n \, {}_3F_2\left(\begin{matrix}-n, a, b \\ c, d\end{matrix}\middle| 1\right) = \sum_{l=0}^{n} \frac{(-n)_l (a)_l (d-b)_l (1+a-n-c+l)_{n-l}}{l!(d)_l}. \quad (3.10)$$

For $n = (p-1)/6$, $a = (p+1)/2$, $b = (4-p)/6$, $c = 1/2$, and $d = (p+1)/2 - k$ we need

$$\sum_{l=0}^{(p-1)/6} \frac{((1-p)/6)_l ((p+1)/2)_l ((p+1)/2+(p-1)/6-k-\frac{1}{2})_l ((p+2)/3+l+\frac{1}{2})_{(p\mp 1)/6-l}}{l!((p+1)/2-k)_l} \equiv 0 \pmod{p} \quad (3.11)$$

for $(p-1)/6 < k < (p-1)/3$.

It is clear that

$$2^l ((p+1)/2 + (p-1)/6 - k - 1/2)_l \equiv 0 \text{ for } (p-1)/6 \leqq k \leqq (p-1)/6 + l - 1 \quad (3.12)$$

and

$$2^{(p-1)/6-l} ((p+2)/3 + l + \tfrac{1}{2})_{(p-1)/6-l} \equiv 0 \text{ for } 0 \leqq l < (p-1)/6. \quad (3.13)$$

Because all of the other factors in (3.11) are integers, and p never divides the denominator of (3.11), (3.12) and (3.13) imply that (3.11) holds for $(p-1)/6 < k < (p-1)/3$. This completes the proof of (3.11), which implies (3.8) and thus finally Lemma 3.3.

We remark that the constant -3 can be obtained by carefully computing the constants in this section.

4. Remarks

There is an analogue of Proposition 3.2 for $n \neq 3$ but the techniques here do not apply. Alan Adolphson has shown us a geometric proof of Proposition 3.2 from Bezout's theorem. It also works for $q = p^{\alpha}$. Our proof is motivated by the analogy with gamma functions and is formal in nature.

The ${}_3F_2$ transformation can be found in the work of Thomae in the late 1800's.

It is interesting to note that Jacobi [9] had discovered the Hasse-Davenport formula. In fact, he was motivated by the analogy with gamma functions. Yet he could not give a proof that was analogous.

Our ultimate aim is to find a field theoretic foundation for the q-gamma and q-beta functions [1]. They have nice analogues of (1.2), (1.4), and (1.5) in [1, Th. 5.1], [1, Eq. 5.20], and [1, Eq. (3.18)]. Unfortunately we do not have a field theoretic interpretation of the q-gamma function.

There is a relation between Gauss sums and the p-adic Γ-function due to Gross and Koblitz [7, Th. 1.12]. The p-adic Γ-function has a multiplication formula which implies the Hasse-Davenport formula for Gauss sums [7, Eq. (3.3)]. However, the proof is not character related. Boyarsky [2] gave a proof based upon the functional equation for the p-adic gamma function. He commented that such a theorem could be expected in view of Dirichlet's proof of the multiplication formula. Dirichlet used an integral representation of the logarithmic derivative of the gamma function. Jacobi [9] found this proof remarkable. Yet Dirichlet's proof does not work for Gauss sums because there is no analogue of a first derivative for characters of $GF(p)$.

Koblitz has given many properties of the q-analogue of the p-adic gamma function in [10], [11].

Acknowledgement

Research of the second author has been partially supported by a NSF grant MCS-8102237.

REFERENCES

[1] ASKEY, R., *The q-gamma and q-beta functions.* Applicable Anal. *8* (1978/79), 125–141.

[2] BOYARSKY, M., *p-adic gamma functions and Dwork cohomology*. Trans. Amer. Math. Soc. *257* (1980), 359–568.

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

[4] EDWARDS, J., *Integral calculus, vol. 2*. Macmillan, London, 1922.

[5] ERDÉLYI, A., *Higher transcendental functions, vol. I*. McGraw Hill, New York–Toronto–London, 1953.

[6] GEL'FAND, I., GRAEV, M., and PYATECKIĬ-SAPIRO, I., *Representation theory and automorphic functions*. Saunders, 1969.

[7] GROSS, B. and KOBLITZ, N., *Gauss sums and the p-adic Γ-function*. Ann. of Math. (2) *109* (1979), 569–581.

[8] IRELAND, K. and ROSEN, M., *Elements of number theory*. Bogden and Quigley, Tarrytown-on-Hudson, 1972.

[9] JACOBI, C., *Über die Kreistheilung und ihre Anwendung auf die Zahlentheorie*. J. Reine Angew. Math. *30* (1846), 166–182.

[10] KOBLITZ, N., *q-extensions of the p-adic gamma function*. Trans. Amer. Math. Soc. *260* (1980), 449–457.

[11] KOBLITZ, N., *q-extensions of the q-adic gamma function, II*. Trans. Amer. Math. Soc. *273* (1982), 111–130.

[12] LIOUVILLE, J., *Détermination des valeurs d'une class remarquable d'intégrales definies multiples, et demonstration nouvelle d'une célèbre formule de Gauss concernant les fonctions gamma de Legendre*. J. Math. (2nd series) *1* (1856), 82–88.

[13] SEARS, D., *On the transformation theory of basic hypergeometric functions*. Proc. London Math. Soc. (2) *53* (1951), 158–180.

[14] YAMAMOTO, K., *On a conjecture of Hasse concerning multiplicative relations of Gaussian sums*. J. Combin. Theory Ser. *A 1* (1966), 476–489.

School of Mathematics,
University of Minnesota,
Minneapolis, MN 55455
U.S.A.