PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 139, Number 4, April 2011, Pages 1273–1276
S 0002-9939(2010)10662-7
Article electronically published on September 30, 2010

GAUSS SUMS OVER FINITE FIELDS AND ROOTS OF UNITY

ROBERT J. LEMKE OLIVER

(Communicated by Matthew A. Papanikolas)

Abstract. Let χ be a non-trivial character of $\mathbb{F}_q^\times$, and let $g(\chi)$ be its associated Gauss sum. It is well known that $g(\chi) = \varepsilon(\chi)\sqrt{q}$, where $|\varepsilon(\chi)| = 1$. Using the p-adic gamma function, we give a new proof of a result of Evans which gives necessary and sufficient conditions for $\varepsilon(\chi)$ to be a root of unity.

1. Introduction and statement of results

Let $p > 2$ be a prime, and let $q = p^f$ for some $f \geq 1$. Let $\psi : \mathbb{F}_p \to \mathbb{C}^\times$ be a non-trivial additive character, and let $\chi : \mathbb{F}_q^\times \to \mathbb{C}^\times$ be a non-trivial multiplicative character. The Gauss sum $g(\chi) = g(\chi, \psi)$ associated to χ is given by

$$g(\chi) := \sum_{x \in \mathbb{F}_q^\times} \chi(x)\psi(\mathrm{tr}(x)), \tag{1.1}$$

where $\mathrm{tr}(x) := x + x^p + \ldots + x^{p^{f-1}}$. The determination of $g(\chi)$ is of central importance in analytic number theory, as it reflects both the multiplicative and additive structure of $\mathbb{F}_q$. Classical arguments show that $|g(\chi)| = \sqrt{q}$. On the other hand, the quantity $\varepsilon(\chi) := g(\chi)/\sqrt{q}$ has only been determined for χ of certain orders (see [1] for a comprehensive treatment of recent results). Motivated by private communications with Zagier, we determine when $\varepsilon(\chi)$ is a root of unity.

Theorem 1.1. *Let $\chi : \mathbb{F}_q^\times \to \mathbb{C}^\times$ be a multiplicative character of order m and let r be the order of p modulo m. The quantity $\varepsilon(\chi)$ is a root of unity if and only if for every integer t coprime to m we have that*

$$\sum_{i=0}^{r-1} \overline{tp^i} = \frac{rm}{2}, \tag{1.2}$$

where $\overline{tp^i}$ denotes the canonical representative of tp^i modulo m in $[0, \ldots, m-1]$.

Remark. After this work was done, the author learned that Theorem 1.1 was first obtained by Evans [2]. Evans's proof used Stickelberger's relation on the decomposition of $g(\chi)$ into prime ideals (see [4]). An equivalent condition, essentially (2.5) below, was later obtained by Yang and Zheng [5], again using Stickelberger's relation. We give a different proof of Theorem 1.1, one based on a deep theorem of Gross and Koblitz [3] relating Gauss sums to the p-adic gamma function.

Received by the editors April 22, 2010.
2010 *Mathematics Subject Classification.* Primary 11T24.
Key words and phrases. Gauss sums, Gross-Koblitz.

2. Proof of Theorem 1.1

In Section 2.1 we begin by defining the p-adic gamma function $\Gamma_p(z)$. We then state the Gross-Koblitz formula, which relates Gauss sums over a finite field to a product of values of $\Gamma_p(z)$. In Section 2.2 we apply the Gross-Koblitz formula to prove Theorem 1.1.

2.1. **The Gross-Koblitz formula.** Let $p > 2$ be a prime and $q = p^f$ for some $f \geq 1$. The p-adic gamma function $\Gamma_p(z) : \mathbb{Z}_p \to \mathbb{Z}_p^\times$ is defined by

$$\Gamma_p(z) := \lim_{\substack{m \to z \\ m \in \mathbb{Z}}} (-1)^m \prod_{\substack{j < m \\ (j,p)=1}} j. \tag{2.1}$$

Let $\omega_f : \mathbb{F}_q^\times \to \mathbb{C}^\times$ be the Teichmüller character of $\mathbb{F}_q$, $\psi : \mathbb{F}_p \to \mathbb{C}^\times$ be a non-trivial additive character, and $\zeta_p = \psi(1)$. Let $\pi \in \mathbb{Q}_p(\zeta_p)$ be the unique element satisfying both $\pi^{p-1} = -p$ and $\zeta_p \equiv 1 + \pi \pmod{\pi^2}$. For integers $0 \leq a < q-1$, the Gauss sum $g(\omega_f^{-a})$ is defined by

$$g(\omega_f^{-a}) := -\sum_{x \in \mathbb{F}_q^\times} \omega_f^{-a}(x)\psi(\mathrm{tr}(x)), \tag{2.2}$$

where $\mathrm{tr}(x) := x + x^p + \ldots + x^{p^{f-1}}$. The Gross-Koblitz formula [3] states that

$$g(\omega_f^{-a}) = \pi^{S(a)} \prod_{j=0}^{f-1} \Gamma_p\left(\left\{\frac{ap^j}{q-1}\right\}\right), \tag{2.3}$$

where $S(a)$ denotes the sum of digits in the base p expansion of a and, for any $x \in \mathbb{R}$, $\{x\} := x - \lfloor x \rfloor$ denotes the fractional part of x.

2.2. **Proof of Theorem 1.1.** Let χ be a multiplicative character of $\mathbb{F}_q^\times$ of order m. There is a unique a such that $0 \leq a < q-1$ and $\chi = \omega_f^{-a}$. Since $g(\chi) \in \mathbb{Q}(\zeta_p, \zeta_{q-1})$, $\varepsilon(\chi)$ is a root of unity if and only if $g(\chi)^{2p(q-1)} = q^{p(q-1)}$. The Gross-Koblitz formula (2.3) yields that

$$g(\chi)^{2p(q-1)} = p^{2p(q-1)S(a)/(p-1)} \left(\prod_{j=0}^{f-1} \Gamma_p\left(\left\{\frac{ap^j}{q-1}\right\}\right)\right)^{2p(q-1)}, \tag{2.4}$$

and by comparing the p-adic valuation of both sides, we see that a necessary condition for $\varepsilon(\chi)$ to be a root of unity is $S(a) = \frac{f(p-1)}{2}$. In fact, if χ' is another character of $\mathbb{F}_q^\times$ of order m, then there is an element of $\mathrm{Gal}(\mathbb{Q}(\zeta_p, \zeta_m))$ taking $g(\chi)$ to $g(\chi')$. Hence, $\varepsilon(\chi)$ is a root of unity if and only if $\varepsilon(\chi')$ is as well. Thus, if $\varepsilon(\chi)$ is a root of unity, for all t coprime to m we have that

$$S(\overline{ta}^{(q-1)}) = \frac{f(p-1)}{2}, \tag{2.5}$$

where $\overline{ta}^{(q-1)}$ is the canonical reduction of ta modulo $q-1$. This condition will prove to be sufficient to guarantee that $\varepsilon(\chi)$ is a root of unity. To see this, we begin by reinterpreting the sum of digits function $S(a)$.

Lemma 2.1. *For any $0 \le b < q-1$, we have that*

$$\sum_{j=0}^{f-1} \left\{ \frac{bp^j}{q-1} \right\} = \frac{S(b)}{p-1}.$$

Proof. Write $b = \sum_{i=0}^{f-1} b_i p^i$. For any $0 \le j \le f-1$, we observe that $bp^j \equiv b^{(j)} \pmod{q-1}$, where $0 \le b^{(j)} < q-1$ is the j-th iterate of the cyclic permutation on the base p digits of b. Hence, we have that

$$\begin{aligned}\sum_{j=0}^{f-1} \left\{ \frac{bp^j}{q-1} \right\} &= \frac{1}{q-1} \sum_{j=0}^{f-1} b^{(j)} \\ &= \frac{S(b)}{p-1}.\end{aligned}$$

□

Write $a = t_0 \cdot (a, q-1)$ for some t_0 coprime to m. Since $m = \frac{q-1}{(a,q-1)}$, we have that

$$\left\{ \frac{ap^j}{q-1} \right\} = \left\{ \frac{t_0 p^j}{m} \right\} = \frac{\overline{t_0 p^j}}{m},$$

whence

$$\sum_{j=0}^{f-1} \left\{ \frac{ap^j}{q-1} \right\} = \frac{f}{r} \sum_{j=0}^{r-1} \frac{\overline{t_0 p^j}}{m}, \tag{2.6}$$

where $\overline{tp^j}$ is the reduction of tp^j modulo m and r is the multiplicative order of p modulo m. Hence, by Lemma 2.1, (2.5) holds for t coprime to m if and only if we have that

$$\sum_{j=0}^{r-1} \overline{tp^j} = \frac{rm}{2}. \tag{2.7}$$

This establishes the necessity of (1.2) in the statement of Theorem 1.1. Sufficiency follows immediately from a result of Gross and Koblitz [3]: If $\{a_1, \ldots, a_k, n_1, \ldots, n_k\}$ is a set of integers such that, for all u coprime to m, $\sum_{i=1}^{k} n_i \cdot \overline{ua_i}$ is an integer independent of u, then the product $\prod_{i=1}^{k} \prod_{j=0}^{f-1} \Gamma_p \left(\frac{\overline{a_i p^j}}{m} \right)^{n_i}$ is a root of unity. We apply this result with $k = r$, $a_i = p^i$, and $n_i = 2$, showing that if (1.2) is satisfied, then $\varepsilon(\chi)$ is a root of unity.

References

[1] B. C. Berndt, R. J. Evans, and K. S. Williams. *Gauss and Jacobi sums.* Canadian Mathematical Society Series of Monographs and Advanced Texts. John Wiley & Sons Inc., New York, 1998. A Wiley-Interscience Publication. MR1625181 (99d:11092)

[2] R. J. Evans. Generalizations of a theorem of Chowla on Gaussian sums. *Houston J. Math.*, 3(3):343–349, 1977. MR0498491 (58:16600)

[3] B. H. Gross and N. Koblitz. Gauss sums and the p-adic Γ-function. *Ann. of Math. (2)*, 109(3):569–581, 1979. MR534763 (80g:12015)

[4] K. Ireland and M. Rosen. *A classical introduction to modern number theory*, volume 84 of Graduate Texts in Mathematics. Springer-Verlag, New York, second edition, 1990. MR1070716 (92e:11001)

[5] J. Yang and W. Zheng. On a theorem of Chowla. *J. Number Theory*, 106(1):50–55, 2004. MR2049591 (2005b:11197)

Department of Mathematics, University of Wisconsin, Madison, Wisconsin 53706

Current address: Department of Mathematics and Computer Science, Emory University, Atlanta, Georgia 30322

E-mail address: `lemkeoliver@gmail.com`