TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 278, Number 1, July 1983

UNIQUENESS OF Γ_p IN THE GROSS-KOBLITZ FORMULA FOR GAUSS SUMS

BY

ALAN ADOLPHSON[1]

ABSTRACT. It is determined what continuous functions besides the p-adic gamma function make the Gross-Koblitz formula valid.

Introduction. Let p be an odd prime, $\mathbf{Q}_p$ the p-adic numbers, and $\overline{\mathbf{Q}}_p$ its algebraic closure. For $q = p^f$, $0 \leq j < q - 1$, define a Gauss sum

$$g(j, q) = - \sum_{x^{q-1}=1} x^{-j}\zeta_p^{\operatorname{Tr} x}, \tag{1}$$

where the sum is over the $(q-1)$st roots of unity in $\overline{\mathbf{Q}}_p$, ζ_p is a primitive pth root of unity in $\overline{\mathbf{Q}}_p$, and

$$\operatorname{Tr} x = x + x^p + x^{p^2} + \cdots + x^{p^{f-1}}.$$

Let π denote that $(p-1)$st root of $-p$ satisfying $\zeta_p - 1 \equiv \pi \pmod{\pi^2}$. Let $\Gamma_p(x)$ be Morita's p-adic Γ-function [4]. It is the unique continuous $\mathbf{Z}_p$-valued function on $\mathbf{Z}_p$ whose value at a positive integer n is

$$\Gamma_p(n) = (-1)^n \prod_{\substack{1 \leq i \leq n-1 \\ (p,i)=1}} i.$$

The Gross-Koblitz formula [3, Theorem 1.7] states

$$\frac{g(j,q)}{\pi^k} = \prod_{i=0}^{f-1} \Gamma_p\left(\left\langle \frac{p^i j}{q-1} \right\rangle\right), \tag{2}$$

where $\langle x \rangle = x - [x]$ is the fractional part of the real number x and k is the sum of the digits in the p-adic expansion of j: $j = c_0 + c_1 p + \cdots + c_{f-1}p^{f-1}$, $k = c_0 + c_1 + \cdots + c_{f-1}$.

Recently, R. Greenberg asked us whether this formula determines Γ_p uniquely; i.e., is there another continuous, p-adic valued function $F(x)$ on $\mathbf{Z}_p$ such that (2) remains true when Γ_p is replaced by F? The answer is that there are many continuous functions F with this property, however, they are all obtained from Γ_p by a simple procedure. This result (Theorem 2) is similar in form to a theorem of Katz [2, Theorem 5], but we do not know if they are related. The proofs are quite different.

Received by the editors July 31, 1981.

1980 *Mathematics Subject Classification*. Primary 12B40; Secondary 10G05.

Key words and phrases. Gross-Koblitz formula, p-adic gamma function.

[1]Supported in part by NSF grant MCS-7903315.

0002-9947/82/0000-1307/$02.75

Greenberg also points out that it would be interesting to determine what quantities can appear on the left-hand side of a formula such as (2): Given for each $q = p^f$ and each j, $0 \leqslant j < q - 1$, a p-adic number $h(j, q)$, when does there exist a continuous p-adic valued function F on $\mathbf{Z}_p$ such that for all j and q,

$$h(j,q) = \prod_{i=0}^{f-1} F\left(\left\langle \frac{p^i j}{q-1} \right\rangle\right)?$$

We do not discuss this question here.

I would like to thank N. Koblitz for constructing nontrivial functions F satisfying (8) below. Studying these examples led me to a proof in the general case. Some motivation is given in the remark following the proof of Theorem 2. The two concluding remarks are due to the referee.

Main result. We begin with a slight reformulation of (2). The map $j/(q-1) \mapsto \langle pj/(q-1)\rangle$ does not extend to a p-adic continuous function, so we replace it by its inverse, which is continuous. For $x \in \mathbf{Z}_p$, write

$$x = \sum_{i=0}^{\infty} x_i p^i, \tag{3}$$

where each x_i is a rational integer, $0 \leqslant x_i \leqslant p - 1$. Define φ: $\mathbf{Z}_p \to \mathbf{Z}_p$ by

$$\varphi(x) = \sum_{i=1}^{\infty} x_i p^{i-1}.$$

Note that

$$x \equiv y \pmod{p^n} \quad \text{implies} \quad \varphi(x) \equiv \varphi(y) \pmod{p^{n-1}}, \tag{4}$$

so φ is continuous. (Thus φ is the continuous extension to $\mathbf{Z}_p$ of the function on nonnegative integers $n \mapsto [n/p]$: See [**1**, §8].) Put $a = j/(q-1)$. Then $a = -\varphi(-\langle pa\rangle)$, so $-\varphi^{(f)}(-a) = a$ and the set $\{\langle p^i a\rangle\}_{i=0}^{f-1}$ is identical to the set $\{-\varphi^{(i)}(-a)\}_{i=0}^{f-1}$. This latter set is the orbit of a under the map $a \mapsto -\varphi(-a)$. Thus (2) may be expressed

$$\frac{g(j,q)}{\pi^k} = \prod_{i=0}^{f-1} \Gamma_p(-\varphi^{(i)}(-a)). \tag{5}$$

The nonuniqueness of Γ_p is now clear. In (5), one may replace $\Gamma_p(x)$ by $\Gamma_p(x)G(x)/G(-\varphi(-x))$, where G is any continuous, nonvanishing function on $\mathbf{Z}_p$, since

$$\prod_{i=0}^{f-1} G(-\varphi^{(i)}(-a))/G(-\varphi^{(i+1)}(-a)) = 1.$$

The point is that any substitute for Γ_p must be of this form.

THEOREM 1. *Let F: $\mathbf{Z}_p \to \mathbf{Q}_p$ be a continuous, nonvanishing function satisfying, for all positive integers n*:

$$\textit{If } \varphi^{(n)}(-x) = -x, \textit{ then } \prod_{i=0}^{n-1} F(-\varphi^{(i)}(-x)) = 1. \tag{6}$$

Then there exists a continuous, nonvanishing function $G: \mathbf{Z}_p \to \mathbf{Q}_p$ *such that*

$$F(x) = G(x)/G(-\varphi(-x)) \tag{7}$$

for all $x \in \mathbf{Z}_p$.

Changing the variable to eliminate the minus signs, Theorem 1 is equivalent to

THEOREM 2. *Let* $F: \mathbf{Z}_p \to \mathbf{Q}_p$ *be a continuous, nonvanishing function satisfying, for all positive integers* n:

$$\text{If } \varphi^{(n)}(x) = x, \text{ then } \prod_{i=0}^{n-1} F(\varphi^{(i)}(x)) = 1. \tag{8}$$

Then there exists a continuous, nonvanishing function $G: \mathbf{Z}_p \to \mathbf{Q}_p$ *such that*

$$F(x) = G(x)/G(\varphi(x)) \tag{9}$$

for all $x \in \mathbf{Z}_p$.

REMARK. We conjecture, but cannot prove, that any continuous function F: $\mathbf{Z}_p \to \mathbf{Q}_p$ which satisfies (8) is nonvanishing. However, if there were such a function F with, say, $F(x_0) = 0$, then it could not be written in the form (9). For every positive integer k, there exists in every residue class mod p^k an element y such that $\varphi^{(k)}(y) = x_0$. (9) would imply that $G(y) = 0$, hence by continuity G would be identically zero, an impossibility.

If one assumes $F: \mathbf{Z}_p \to \mathbf{Z}_p$, then (8) implies that F takes on only unit values, since the fixed points of iterates of φ are dense in $\mathbf{Z}_p$. In particular, F is nonvanishing in this case.

PROOF OF THEOREM 2. Write $x \in \mathbf{Z}_p$ as in (3). Fix a rational integer b, $0 \leqslant b \leqslant p - 1$. For each positive integer n, define locally constant (hence continuous) functions of x:

$$\alpha_n(x) = \frac{1}{1 - p^{2n-1}}\left[b + bp + \cdots + bp^{n-2} + p^{n-1}\left(\sum_{i=0}^{n-1} x_i p^i\right)\right], \tag{10}$$

$$\beta_n(x) = \frac{1}{1 - p^{2n-2}}\left[b + bp + \cdots + bp^{n-2} + p^{n-1}\left(\sum_{i=0}^{n-2} x_i p^i\right)\right]. \tag{11}$$

Note that

$$\varphi^{(2n-1)}(\alpha_n(x)) = \alpha_n(x), \qquad \varphi^{(2n-2)}(\beta_n(\varphi(x))) = \beta_n(\varphi(x)). \tag{12}$$

Hence by (8),

$$\prod_{i=0}^{2n-2} F(\varphi^{(i)}(\alpha_n(x))) = 1, \qquad \prod_{i=0}^{2n-3} F(\varphi^{(i)}(\beta_n(\varphi(x)))) = 1.$$

Equating these two products and solving for $F(\varphi^{(n-1)}(\alpha_n(x)))$,

$$F(\varphi^{(n-1)}(\alpha_n(x))) = \frac{\prod_{i=0}^{2n-3} F(\varphi^{(i)}(\beta_n(\varphi(x))))}{\prod_{i=0}^{n-2} F(\varphi^{(i)}(\alpha_n(x)))\prod_{i=n}^{2n-2} F(\varphi^{(i)}(\alpha_n(x)))}. \tag{13}$$

If we multiply and divide the right-hand side of (13) by $\prod_{i=0}^{n-2} F(\varphi^{(i)}(\beta_n(x)))$, it becomes

$$F(\varphi^{(n-1)}(\alpha_n(x))) = A_n(x)\cdot B_n(x)\cdot G_n(x)/G_n(\varphi(x)), \tag{14}$$

where

$$A_n(x) = \frac{\prod_{i=0}^{n-2} F(\varphi^{(i)}(\beta_n(x)))}{\prod_{i=0}^{n-2} F(\varphi^{(i)}(\alpha_n(x)))}, \qquad B_n(x) = \frac{\prod_{i=n-1}^{2n-3} F(\varphi^{(i)}(\beta_n(\varphi(x))))}{\prod_{i=n}^{2n-2} F(\varphi^{(i)}(\alpha_n(x)))},$$

$$G_n(x) = \left[\prod_{i=0}^{n-2} F(\varphi^{(i)}(\beta_n(x)))\right]^{-1}.$$

The idea now is to compute $\lim_{n\to\infty}$ of each term in (14).

LEMMA 1. $\lim_{n\to\infty} F(\varphi^{(n-1)}(\alpha_n(x))) = F(x)$.

PROOF. F is continuous and a calculation shows $\varphi^{(n-1)}(\alpha_n(x)) \equiv x \pmod{p^n}$. Q.E.D.

Since F is continuous and nonvanishing on the compact set $\mathbf{Z}_p$, there exist integers δ, ε such that

$$\delta \leqslant \operatorname{ord} F(x) \leqslant \varepsilon \tag{15}$$

for all $x \in \mathbf{Z}_p$. Furthermore, the compactness of $\mathbf{Z}_p$ implies that F is uniformly continuous. For every positive integer k there exists a positive integer N_k such that

$$x \equiv y \pmod{p^{N_k}} \quad \text{implies} \quad F(x) \equiv F(y) \pmod{p^{k+\varepsilon}}. \tag{16}$$

LEMMA 2. $\lim_{n\to\infty} A_n(x) = 1$.

PROOF. Note that $\alpha_n(x) \equiv \beta_n(x) \pmod{p^{2n-2}}$. So by (4),

$$\varphi^{(i)}(\alpha_n(x)) \equiv \varphi^{(i)}(\beta_n(x)) \pmod{p^n}$$

for $i = 0, 1, \ldots, n-2$. Thus for $n \geqslant N_k$,

$$F(\varphi^{(i)}(\alpha_n(x))) \equiv F(\varphi^{(i)}(\beta_n(x))) \pmod{p^{k+\varepsilon}},$$

which implies, since $\operatorname{ord} F(x) \leqslant \varepsilon$ for all $x \in \mathbf{Z}_p$,

$$F(\varphi^{(i)}(\beta_n(x)))/F(\varphi^{(i)}(\alpha_n(x))) \equiv 1 \pmod{p^k}.$$

Hence for $n \geqslant N_k$, one has $A_n(x) \equiv 1 \pmod{p^k}$. Q.E.D.

LEMMA 3. $\lim_{n\to\infty} B_n(x) = 1$.

PROOF. Note that

$$\varphi^{(n-1)}(\beta_n(\varphi(x))) \equiv \varphi^{(n)}(\alpha_n(x)) \pmod{p^{2n-2}}.$$

So by (4),

$$\varphi^{(n-1+i)}(\beta_n(\varphi(x))) \equiv \varphi^{(n+i)}(\alpha_n(x)) \pmod{p^n}$$

for $i = 0, 1, \ldots, n-2$. The argument now proceeds as in Lemma 2. Q.E.D.

LEMMA 4. *There exist integers M_1 and M_2 such that for all positive integers n and all $x \in \mathbf{Z}_p$,*

$$M_1 \leqslant \operatorname{ord} G_n(x) \leqslant M_2.$$

PROOF. By (8), $F(b/(1-p)) = 1$. By continuity of F, there exists a positive integer N' such that $\operatorname{ord}(y - b/(1-p)) \geqslant N'$ implies $F(y) \equiv 1 \pmod p$. For such y, one has $\operatorname{ord} F(y) = 0$. Now $\beta_n(x) \equiv (b/(1-p)) \pmod{p^{n-1}}$; hence by (4),

$$\varphi^{(i)}(\beta_n(x)) \equiv (b/(1-p)) \pmod{p^{N'}}$$

for $i \leqslant n - N' - 1$. Therefore, for $i \leqslant n - N' - 1$, $\operatorname{ord} F(\varphi^{(i)}(\beta_n(x))) = 0$, and by the definition of $G_n(x)$,

$$\operatorname{ord} G_n(x) = \operatorname{ord}\left[\prod_{i=n-N'}^{n-2} F(\varphi^{(i)}(\beta_n(x)))\right]^{-1}.$$

Thus by (15),

$$-(N'-1)\varepsilon \leqslant \operatorname{ord} G_n(x) \leqslant -(N'-1)\delta. \quad \text{Q.E.D.}$$

LEMMA 5. *The sequence* $\{G_n\}_{n=1}^{\infty}$ *is uniformly Cauchy on* $\mathbf{Z}_p$.

PROOF. By the ultrametric property of the p-adic norm, it suffices to show that the sequence $\{G_n - G_{n+1}\}_{n=1}^{\infty}$ converges uniformly on $\mathbf{Z}_p$ to the zero function. But

$$G_n - G_{n+1} = G_{n+1}(G_n/G_{n+1} - 1)$$

(where the second factor on the right-hand side is well defined because Lemma 4 implies G_{n+1} is nonvanishing on $\mathbf{Z}_p$ for all n), and by Lemma 4, $\{G_{n+1}\}_{n=1}^{\infty}$ is uniformly bounded on $\mathbf{Z}_p$. So it suffices to show that given $k > 0$ there exists a positive integer N such that $n \geqslant N$ implies that for all $x \in \mathbf{Z}_p$,

$$G_n(x)/G_{n+1}(x) - 1 \equiv 0 \pmod{p^k}. \tag{17}$$

By definition of G_n,

$$\frac{G_n(x)}{G_{n+1}(x)} - 1 = \left[F(\beta_{n+1}(x))\frac{\prod_{i=0}^{n-2} F(\varphi^{(i+1)}(\beta_{n+1}(x)))}{\prod_{i=0}^{n-2} F(\varphi^{(i)}(\beta_n(x)))}\right] - 1.$$

By (8), $F(b/(1-p)) = 1$, and by definition of $\beta_{n+1}(x)$,

$$\beta_{n+1}(x) \equiv (b/(1-p)) \pmod{p^n}.$$

Hence by continuity of F, for sufficiently large n,

$$F(\beta_{n+1}(x)) \equiv 1 \pmod{p^k}.$$

Note that

$$\varphi(\beta_{n+1}(x)) \equiv \beta_n(x) \pmod{p^{2n-2}},$$

so by (4),

$$\varphi^{(i+1)}(\beta_{n+1}(x)) \equiv \varphi^{(i)}(\beta_n(x)) \pmod{p^n}$$

for $i = 0, 1, \ldots, n-2$. Thus for $n \geqslant N_k$ (see (16))

$$F(\varphi^{(i+1)}(\beta_{n+1}(x))) \equiv F(\varphi^{(i)}(\beta_n(x))) \pmod{p^{k+\varepsilon}}$$

for $i = 0, 1, \ldots, n-2$ and all $x \in \mathbf{Z}_p$. This implies

$$F(\varphi^{(i+1)}(\beta_{n+1}(x)))/F(\varphi^{(i)}(\beta_n(x))) \equiv 1 \pmod{p^k},$$

from which (17) follows. Q.E.D.

CONCLUSION OF PROOF OF THEOREM 2. Lemma 5 implies that $\{G_n\}_{n=1}^{\infty}$ converges uniformly on $\mathbf{Z}_p$ to a function G, hence G is continuous. By Lemma 4, $\{G_n\}_{n=1}^{\infty}$ is uniformly bounded away from zero, hence G is nonvanishing. Therefore

$$\lim_{n\to\infty} G_n(x)/G_n(\varphi(x)) = G(x)/G(\varphi(x)).$$

The theorem now follows from (14) and Lemmas 1–3. Q.E.D.

REMARK 1. In the examples of Koblitz, the functions F satisfying (8) were locally constant, say $F(x) = F(y)$ whenever $x \equiv y \pmod{p^N}$. In this case (13) simplifies when we take $n = N$:

$$F\big(\varphi^{(N-1)}(\alpha_N(x))\big) = F(x),$$
$$F\big(\varphi^{(i)}(\beta_N(\varphi(x)))\big) = F\big(\varphi^{(i+1)}(\alpha_N(x))\big) \quad \text{for } i = N-1, N, \ldots, 2N-3,$$
$$F\big(\varphi^{(i)}(\alpha_N(x))\big) = F\big(\varphi^{(i)}(\beta_N(x))\big) \quad \text{for } i = 0, 1, \ldots, N-2,$$

and (13) becomes

$$F(x) = \prod_{i=0}^{N-2} \frac{F\big(\varphi^{(i)}(\beta_N(\varphi(x)))\big)}{F\big(\varphi^{(i)}(\beta_N(x))\big)} = G_N(x)/G_N(\varphi(x)),$$

which proves Theorem 2 in this special case. In the general case (13) does not simplify and, in addition, it is necessary to introduce $\prod_{i=0}^{n-2} F(\varphi^{(i)}(\beta_n(x)))$ to create a factor of the form $G_n(x)/G_n(\varphi(x))$ on the right-hand side.

REMARK 2. Functions F having the property that (2) remains valid when Γ_p is replaced by F arise naturally. In [**5**, §4], Dwork constructs "splitting" functions θ_s, where s can be either a positive integer or $+\infty$, each of which can be used to define a p-adic analytic function which lifts the additive character to characteristic 0. Boyarsky [**1**] used the simplest one, namely, $\theta_1(x) = \exp \pi(x - x^p)$, which leads to Γ_p. However, one can replace θ_1 by any θ_s and repeat Boyarsky's arguments; this leads to a formula for Gauss sums with Γ_p replaced by some other locally analytic function F_s, i.e., (2) is valid with Γ_p replaced by F_s.

REMARK 3. Let K be a discretely valued field with ring of integers $\mathcal{O}$, uniformizer π, and a finite residue field $\bar{K}$. Let V denote the direct sum of n copies of $\mathcal{O}$, $\bar{V}$ the direct sum of n copies of $\bar{K}$, and $v \mapsto \bar{v}$ the natural map of V onto $\bar{V}$. Fix a set S of representatives in V of the elements of $\bar{V}$, and let rep: $\bar{V} \to S$ be the map rep(u) = the representative of u in S ($u \in \bar{V}$). Then the map φ: $V \to V$, defined by $\varphi(v) = (v - \text{rep}(\bar{v}))/\pi$, is a continuous map of V into itself. The proof of Theorem 2 can be generalized in a straightforward manner to show

THEOREM 3. *Let F: $V \to \mathbf{Q}_p$ be a continuous, nonvanishing function satisfying, for all positive integers n*:

$$\text{(18)} \qquad \textit{If } \varphi^{(n)}(v) = v, \textit{ then } \prod_{i=0}^{n-1} F\big(\varphi^{(i)}(v)\big) = 1.$$

Then there exists a continuous, nonvanishing function G: $V \to \mathbf{Q}_p$ such that $F(v) = G(v)/G(\varphi(v))$ for all $v \in V$.

REFERENCES

1. M. Boyarsky, *p-adic gamma functions and Dwork cohomology*, Trans. Amer. Math. Soc. **257** (1980), 359–369.

2. B. Dwork, *p-adic cycles*, Inst. Hautes Études Sci. Publ. Math. **37** (1969), 27–115.

3. B. Gross and N. Koblitz, *Gauss sums and the p-adic* Γ*-function*, Ann. of Math. (2) **109** (1979), 569–581.

4. Y. Morita, *A p-adic analogue of the* Γ*-function*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **22** (1975), 255–266.

5. B. Dwork, *On the zeta function of a hypersurface*, Inst. Hautes Études Sci. Publ. Math. **12** (1962), 5–68.

DEPARTMENT OF MATHEMATICS, THE INSTITUTE FOR ADVANCED STUDY, PRINCETON, NEW JERSEY 08540