Contemporary Mathematics
Volume **168**, 1994

On the Gross-Koblitz Formula

PAUL THOMAS YOUNG

We use the methods of J. Stienstra to construct logarithms for the formal Picard groups of the Fermat curves. These are formal groups of dimension equal to the arithmetic genus g of the curve and the expansion coefficients of the logarithm are a sequence of g by g matrices. One may choose a subsequence consisting of diagonal matrices which yield rapidly converging p-adic limit formulae for Jacobi sums. These limit formulae imply the Gross-Koblitz formula for Gauss sums.

1. Introduction

In the study of algebraic varieties and character sums over finite fields, a natural problem is that of finding p-adic formulae, for roots of the associated zeta or L-functions or for the sums themselves. A celebrated result in this area is the elegant formula of Gross and Koblitz [**3**] expressing Gauss sums in terms of the p-adic gamma function at rational arguments, for which several proofs have been given, including those in [**1**], [**2**], [**4**], and [**8**]. In this article we give a proof of this theorem by using the methods of Stienstra ([**5**], [**6**]) to analyze the formal Picard groups attached to the Fermat curves.

By [**7**, Theorem 3.5; 2.10] one knows how to obtain limit formulae for the p-adic unit roots of L-functions from the congruences given in [**6**] in the case where $\det \beta_p$ is a p-adic unit. We show in §3 that this approach may also be used to determine the roots of q-ordinal less than 1 for the Fermat curves over $\mathbf{F}_q$, although the condition on $\det \beta_p$ is not satisfied. Whereas in [**4**] a p-adic limit formula for Jacobi sums is obtained from the expansion coefficients of differential forms on these curves, our method essentially uses the expansion coefficients of the right-invariant differential on the formal Picard group of the curve. The result is a very natural expression of Jacobi sums as rapidly converging limits of ratios of multinomial coefficients (cf. (3.10)).

The author thanks David Hayes for suggesting this approach, and for several helpful conversations.

1991 *Mathematics Subject Classification.* Primary 11L05; Secondary 14L05.
This paper is in final form and no version of it will be submitted for publication elsewhere.

2. Gauss Sums and Jacobi Sums

Throughout this paper p will denote an odd prime, $\mathbf{F}_q$ the finite field of $q = p^f$ elements, $\mathbf{Z}_p$ the ring of p-adic integers, $\mathbf{Q}_p$ the field of p-adic numbers, K the unramified extension of $\mathbf{Q}_p$ of degree f, and $\mathcal{O}_K$ the ring of integers of K. We fix a p-th root of unity $\zeta = \zeta_p$ and let π be the unique element of $K(\zeta_p)$ such that $\pi^{p-1} = -p$ and $\zeta \equiv 1 + \pi \pmod{\pi^2}$.

Let $\psi : \mathbf{F}_q \to \mathbf{Q}_p(\zeta)$ be the additive character on $\mathbf{F}_q$ defined by $\psi(t) = \zeta^{\mathrm{Tr}(t)}$, where $\mathrm{Tr} : \mathbf{F}_q \to \mathbf{F}_p$ is the trace map. The Teichmüller character $\omega_f : \mathbf{F}_q \to K$ is the unique multiplicative character on $\mathbf{F}_q$ such that, for all $t \in \mathbf{F}_q$, the reduction of $\omega_f(t)$ mod p is t. (We extend all multiplicative characters χ using the convention $\chi(0) = 0$). For $x \in \mathcal{O}_K$ the Teichmüller representative $\hat{x}$ of x is the unique element of $\mathcal{O}_K$ satisfying $\hat{x}^q = \hat{x}$ and $\hat{x} \equiv x \pmod{p\mathcal{O}_K}$.

For any multiplicative character χ of $\mathbf{F}_q$, the Gauss sum $g_\psi(\chi)$ over $\mathbf{F}_q$ associated to the characters ψ and χ is defined by

$$g_\psi(\chi) = -\sum_{t \in \mathbf{F}_q} \psi(t)\chi(t). \tag{2.1}$$

Let a be an integer, $0 \le a < q-1$, and put $\alpha = a/(q-1)$. The Gross-Koblitz formula [**3**] states that

$$g_\psi(\omega_f^{-a}) = \pi^{S(a)} \cdot \prod_{i=0}^{f-1} \Gamma_p(\alpha^{(i)}), \tag{2.2}$$

where $S(a)$ denotes the sum of the digits in the base p expansion of a, Γ_p denotes Morita's p-adic gamma function, and for elements $\alpha \in \mathbf{Q} \cap \mathbf{Z}_p$, $\alpha^{(i)}$ denotes the i-th iterate of Dwork's shift map, which defines α' to be the unique element of $\mathbf{Q} \cap \mathbf{Z}_p$ satisfying $p\alpha' - \alpha = \mu_\alpha \in \{0, 1, 2, ..., p-1\}$, with $\alpha^{(0)} = \alpha$, and $\alpha^{(i)} = (\alpha^{(i-1)})'$ for $i > 0$. Recall that Γ_p is defined for positive integers n by

$$\Gamma_p(n) = (-1)^n \prod_{\substack{0<i<n \\ p \nmid i}} i, \tag{2.3}$$

extends to a continuous, unit-valued function on $\mathbf{Z}_p$ which is Lipschitz with constant 1, and satisfies the functional equations

$$\Gamma_p(x+1) = \begin{cases} -x\Gamma_p(x), & x \in \mathbf{Z}_p^\times, \\ -\Gamma_p(x), & x \in p\mathbf{Z}_p; \end{cases} \tag{2.4}$$

$$\Gamma_p(x)\Gamma_p(1-x) = -(-1)^{\mu_x}, \quad x \in \mathbf{Z}_p. \tag{2.5}$$

If $s > 0$ and $\chi_0, ..., \chi_s : \mathbf{F}_q \to K$ are multiplicative characters, the Jacobi sum $J(\chi_0, ..., \chi_s)$ is defined by

$$J(\chi_0, ..., \chi_s) = -\sum_{t_0 + \cdots + t_s = 1} \chi_0(t_0) \cdots \chi_s(t_s). \tag{2.6}$$

One has the well-known relation

$$J(\chi_0, ..., \chi_s) = \frac{(-1)^{s+1}}{G} \cdot \frac{g_\psi(\chi_0)\cdots g_\psi(\chi_s)}{g_\psi(\chi_0\cdots\chi_s)}, \tag{2.7}$$

between the Gauss and Jacobi sums (cf. [**10**]), where

$$G = \begin{cases} 1, & \text{if } \chi_0\cdots\chi_s \text{ is nontrivial,} \\ q, & \text{if } \chi_0\cdots\chi_s \text{ is trivial but each } \chi_i \text{ is nontrivial.} \end{cases} \tag{2.8}$$

3. The Fermat Curves

We will analyze the Fermat curves of degree d with projective equation $a_0T_0^d + a_1T_1^d + a_2T_2^d = 0$ and their reductions to characteristic p, where $(d,p) = 1$. Specifically, we choose $q = p^f$ so that $q - 1 = cd$ for some integer c, and then take our parameters a_i to lie in the ring $R = \mathbf{Z}[\zeta_{q-1}]$, where ζ_{q-1} is a primitive $(q-1)$-st root of unity.

Following [**10**] and [**5**], we define the sets

$$\mathcal{J} = \{(i_0, i_1, i_2) \in \mathbf{Z}^3 : 0 < i_0, i_1, i_2 < d \text{ and } i_0 + i_1 + i_2 \equiv 0 \pmod d\}, \tag{3.1}$$

$$\mathcal{J}_1 = \{(i_0, i_1, i_2) \in \mathbf{Z}^3 : 0 < i_0, i_1, i_2 < d \text{ and } i_0 + i_1 + i_2 = d\}. \tag{3.2}$$

For $j = (j_0, j_1, j_2) \in \mathcal{J}$ set $\bar{\jmath} = (\bar{\jmath}_0, \bar{\jmath}_1, \bar{\jmath}_2) = (d - j_0, d - j_1, d - j_2)$. It is easily seen that $\mathcal{J}$ may be written as a disjoint union $\mathcal{J}_1 \cup \mathcal{J}_2$ where $\mathcal{J}_2 = \{\bar{\jmath} : j \in \mathcal{J}_1\}$. For $j \in \mathcal{J}$ we define the integer $e_j = ((S(cj_0) + S(cj_1) + S(cj_2))/(p-1)) - f$, which is the number of carries in the base p addition $cj_0 + cj_1 + cj_2$. Then for $j \in \mathcal{J}$ we define

$$B(j) = (-p)^{e_j} \prod_{i=0}^{f-1} \frac{\Gamma_p((j_0/d)^{(i)})\Gamma_p((j_1/d)^{(i)})\Gamma_p((j_2/d)^{(i)})}{\Gamma_p(1^{(i)})}. \tag{3.3}$$

Proposition. *For $j \in \mathcal{J}$ we have $B(j)B(\bar{\jmath}) = q$.*

Proof. We first compute

$$e_j + e_{\bar{\jmath}} = \frac{\sum_{k=0}^{2} S(cj_k) + S(c\bar{\jmath}_k)}{p-1} - 2f = 3f - 2f = f, \tag{3.4}$$

since $S(cj_k) + S(c\bar{\jmath}_k) = S(q-1) = f(p-1)$ for each k. Therefore $(-p)^{e_j}(-p)^{e_{\bar{\jmath}}} = (-1)^f q$, so

$$\begin{aligned} B(j)B(\bar{\jmath}) &= (-1)^f q \prod_{i=0}^{f-1}\prod_{k=0}^{2} \Gamma_p((j_k/d)^{(i)})\Gamma_p((\bar{\jmath}_k/d)^{(i)}) \\ &= (-1)^{4f} q \cdot (-1)^{\sum_{i=0}^{f-1}\sum_{k=0}^{2} \mu_{j_k/d}^{(i)}} \\ &= q \cdot (-1)^{\sum_{k=0}^{2}\sum_{i=0}^{f-1} \mu_{j_k/d}^{(i)} p^i} = q \cdot (-1)^{\sum_{k=0}^{2} cj_k} = q, \end{aligned} \tag{3.5}$$

since $\sum_{k=0}^{2} cj_k = q - 1$ or $2(q-1)$ according to whether $j \in \mathcal{J}_1$ or $j \in \mathcal{J}_2$.

For a projective curve X in $\mathbf{P}^2$ defined by a single equation $F = 0$, where $F \in R[T_0, T_1, T_2]$ is a homogeneous form of degree $d > 2$, the method of Stienstra [**5**] produces a logarithm

$$\ell(\tau) = \sum_{m=1}^{\infty} m^{-1} \beta_m \tau^m \tag{3.6}$$

for the formal Picard group $H^1(X, \hat{\mathbf{G}}_{m,X})$ associated to X. This is a formal group of dimension equal to the arithmetic genus $g = (d-1)(d-2)/2$ of X, and so the logarithm $\ell = (\ell_1, ..., \ell_g)$ is a g-tuple of formal power series $\ell_i \in R[[\tau]]$ in the g-tuple $\tau = (\tau_1, ..., \tau_g)$ of variables, τ^m denotes $(\tau_1^m, ..., \tau_g^m)$, and each β_m is a $g \times g$ matrix, whose rows and columns are indexed by the set $\mathcal{J}_1$ described above. For $i, j \in \mathcal{J}_1$ the entry $\beta_{m,i,j}$ of the matrix β_m is given by

$$\beta_{m,i,j} = \text{the coefficient of } T_0^{mj_0 - i_0} T_1^{mj_1 - i_1} T_2^{mj_2 - i_2} \text{ in } F^{m-1}. \tag{3.7}$$

Furthermore, we know from Stienstra's work in [**6**] that if $P(T) = 1 + b_1 T + b_2 T^2 + \cdots + b_{2g} T^{2g}$ is the numerator of the zeta-function (over $\mathbf{F}_q$) of the reduction of X modulo p then there are congruences

$$\beta_{mq^r} + b_1 \beta_{mq^{r-1}} + \cdots + b_{2g} \beta_{mq^{r-2g}} \equiv 0 \pmod{pq^{r-g} M_{g \times g}(R)} \tag{3.8}$$

of Atkin-Swinnerton-Dyer type for all $m \in \mathbf{Z}_+$ and $r \geq g$. It follows that if $\lim_{r\to\infty} \beta_{q^r} \beta_{q^{r-1}}^{-1} = H$ exists in $M_{g\times g}(\mathcal{O}_K)$ and $\lim_{r\to\infty}(fr + \operatorname{ord}\beta_{q^r}^{-1}) = +\infty$ then $P(H^{-1}) = 0$ and therefore each eigenvalue of H is a reciprocal root of $P(T)$. In general this p-adic limit need not exist (cf. [**11**, §4]). We now show that it does exist in the case of the Fermat curves of degree d when d divides $q - 1$.

THEOREM. *For the Fermat curve $a_0 T_0^d + a_1 T_1^d + a_2 T_2^d = 0$ with $q - 1 = cd$, $c \in \mathbf{Z}$, the limit $\lim_{r\to\infty} \beta_{q^r} \beta_{q^{r-1}}^{-1} = H$ of matrices as constructed above exists and is a diagonal matrix in $M_{g\times g}(\mathcal{O}_K)$. Furthermore, for each $j \in \mathcal{J}_1$, the (j,j)-entry of H is given by $\hat{a}_0^{cj_0} \hat{a}_1^{cj_1} \hat{a}_2^{cj_2} B(j)$, and for all $j \in \mathcal{J}$ this expression gives a reciprocal root of the zeta function of this curve over $\mathbf{F}_q$.*

PROOF. If d divides $n - 1$ then $\beta_{n,i,j} = 0$ unless $i = j$, in which case we have

$$\beta_{n,j,j} = \binom{n-1}{(n-1)j_0/d, (n-1)j_1/d, (n-1)j_2/d} \cdot \prod_{k=0}^{2} a_k^{(n-1)j_k/d}. \tag{3.9}$$

We apply the calculation in Theorem 2.2 of [**11**] to the entries of the diagonal matrices $\beta_{q^r} \beta_{q^{r-1}}^{-1}$; for each $j \in \mathcal{J}_1$ we compute the (j,j)-entry by taking $\alpha_k = j_{k-1}/d$ for $k = 1, 2, 3$, $\alpha = 1$, and $t = 0$ in the notation of that theorem. From [**11**, eq. 2.14] and the congruence $x^{q^r} \equiv \hat{x} \pmod{pq^r \mathcal{O}_K}$ for $x \in \mathcal{O}_K$, we find that the (j,j)-entry of $\beta_{q^r} \beta_{q^{r-1}}^{-1}$ satisfies the congruence

$$(\beta_{q^r} \beta_{q^{r-1}}^{-1})_{(j,j)} \equiv \hat{a}_0^{cj_0} \hat{a}_1^{cj_1} \hat{a}_2^{cj_2} B(j) \pmod{p^{1+e_j} q^{r-1} \mathcal{O}_K}. \tag{3.10}$$

We see that $0 \le e_j < f$ for all $j \in \mathcal{J}_1$ since $t = 0$, and we find by induction that $\mathrm{ord}_p \beta_{q^r,j,j} = re_j$. We conclude that the matrix limit $\lim_{r\to\infty} \beta_{q^r}\beta_{q^{r-1}}^{-1} = H$ exists and is a diagonal matrix, and in fact for each $j \in \mathcal{J}_1$ the scalar limit $\lim_{r\to\infty}(\beta_{q^r}\beta_{q^{r-1}}^{-1})_{(j,j)} = \hat{a}_0^{cj_0}\hat{a}_1^{cj_1}\hat{a}_2^{cj_2}B(j)$ is the corresponding diagonal entry of H. Since $\lim_{r\to\infty}(fr + \mathrm{ord}\beta_{q^r}^{-1}) = +\infty$, each such limit is an eigenvalue of H and a reciprocal root of $P(T)$. Knowing further that $\gamma \mapsto q/\gamma$ permutes the reciprocal roots and using the above proposition, we see that in fact $\hat{a}_0^{cj_0}\hat{a}_1^{cj_1}\hat{a}_2^{cj_2}B(j)$ is a reciprocal root of $P(T)$ for each $j \in \mathcal{J}$, completing the proof.

Remark. This construction of the matrix H actually describes the action of Frobenius F_q on the subspace of crystalline cohomology where it acts with slopes less than 1. The calculation in [**5**] is done via the isomorphism $H^1(X, \hat{\mathbf{G}}_{m,X}) \cong H^2(\mathbf{P}^2(R), \hat{\mathbf{G}}_{m,\tilde{F}})$, relative to the choice $\{FT^{-j}\}_{j\in\mathcal{J}_1}$ of Čech cocycles to represent a basis of $H^2(\mathbf{P}^2(R), \hat{\mathbf{G}}_{m,\tilde{F}})$ (cf. [**5**, eq. (4.6.1)]). Here X is the projective variety defined by $F = a_0T_0^d + a_1T_1^d + a_2T_2^d$, $\tilde{F}$ denotes the corresponding ideal sheaf on $\mathbf{P}^2(R)$, and T^{-j} denotes $T_0^{-j_0}T_1^{-j_1}T_2^{-j_2}$. Via this isomorphism this basis gives a coordinatization for the formal Picard group $H^1(X, \hat{\mathbf{G}}_{m,X})$ and in turn a basis for the Witt-vector cohomology $H^1(X, \mathcal{WO}_X)$ relative to which the diagonal matrix H^t is the matrix of Frobenius F_q (cf. [**7**, §§2.10,2.6,3.5]). After tensoring with $\mathbf{Q}$ this cohomology is isomorphic to the slope < 1 part of $H^1_{cris}(X)$ (cf. [**6**, §0.3], [**7**, §1]) and the image of the basis $\{FT^{-j}\}$ under this isomorphism is the set of eigenvectors of Frobenius corresponding to the eigenvalues $\hat{a}_0^{cj_0}\hat{a}_1^{cj_1}\hat{a}_2^{cj_2}B(j)$ for $j \in \mathcal{J}_1$.

As a corollary we have the following p-adic formula for Jacobi sums.

Corollary. *Let $s > 0$ and let $\alpha_0, ..., \alpha_s \in \mathbf{Z}_p \bigcap \mathbf{Q} \bigcap [0,1)$ satisfy $\alpha_k = j_k/(q-1)$ with each $j_k \in \mathbf{Z}$, and set $\alpha = \alpha_0 + \cdots + \alpha_s$. Write $\alpha = t + \gamma$ with $t \in \mathbf{Z}$ and $\gamma = c/(q-1) \in (0,1]$. Suppose that $\alpha > 0$, and if $\alpha \in \mathbf{Z}$ suppose that each $\alpha_k > 0$. Then*

$$(3.11) \qquad (-1)^{s+1}J(\omega_f^{-j_0}, ..., \omega_f^{-j_s}) = (-p)^e \prod_{i=0}^{f-1} \frac{\Gamma_p(\alpha_0^{(i)})\cdots\Gamma_p(\alpha_s^{(i)})}{\Gamma_p(\gamma^{(i)})},$$

where $e = (S(j_0) + \cdots + S(j_s) - S(c))/(p-1)$.

Proof. We consider first the case where $s = 2$ and $\alpha \in \mathbf{Z}$, so that the ordered triple $j = (j_0, j_1, j_2)$ lies in the set $\mathcal{J}$ corresponding to the Fermat curve $a_0T_0^d + a_1T_1^d + a_2T_2^d = 0$ for $d = q - 1$. From the work of Weil ([**10**, eq. 8]) one knows that for all $j \in \mathcal{J}$, $-\hat{a}_0^{j_0}\hat{a}_1^{j_1}\hat{a}_2^{j_2}J(\omega_f^{-j_0}, \omega_f^{-j_1}, \omega_f^{-j_2})$ is a reciprocal root of the zeta function of this curve. Indeed the group $\mu_d \times \mu_d$ acts on this curve by $(\zeta_0, \zeta_1) : (T_0, T_1, T_2) \mapsto (\zeta_0T_0, \zeta_1T1, T_2)$, and $H^1_{cris}(X)$ decomposes into a direct sum of the $2g$ one-dimensional $(\omega_f^{-j_0}, \omega_f^{-j_1})$-isotypical subspaces corresponding to the pairs of characters $\{(\omega_f^{-j_0}, \omega_f^{-j_1})\}_{j\in\mathcal{J}}$ of μ_d. For $j \in \mathcal{J}$ the Jacobi sum $\sigma(j) = -J(\omega_f^{-j_0}, \omega_f^{-j_1}, \omega_f^{-j_2})$ is characterized by the property that $\hat{a}_0^{j_0}\hat{a}_1^{j_1}\hat{a}_2^{j_2}\sigma(j)$ is the eigenvalue of Frobenius on the $(\omega_f^{-j_0}, \omega_f^{-j_1})$-isotypical subspace for all $(a_0, a_1, a_2) \in \mathbf{P}^2(R)$ (cf. [**4**, Corollary 2.4; §6.3]). The above remark implies that the part of this decomposition corresponding to $\mathrm{ord}_q \sigma(j) < 1$ (i.e., to $j \in \mathcal{J}_1$) is identical to the decomposition into eigenspaces corresponding to the eigenvalues $\hat{a}_0^{cj_0}\hat{a}_1^{cj_1}\hat{a}_2^{cj_2}B(j)$. So for $j \in \mathcal{J}_1$, $B(j)$ is characterized by the property that $\hat{a}_0^{j_0}\hat{a}_1^{j_1}\hat{a}_2^{j_2}B(j)$ is the eigenvalue of Frobenius on an isotypical subspace of cohomology of the curve $a_0T_0^d + a_1T_1^d + a_2T_2^d = 0$ for all $(a_0, a_1, a_2) \in \mathbf{P}^2(R)$. Since this property also characterizes $\sigma(j)$, we have $B(j) = \sigma(j)$ for $j \in \mathcal{J}_1$. Since $B(j)B(\bar{j}) = q = \sigma(j)\sigma(\bar{j})$, this holds for all $j \in \mathcal{J}$. As the right member of the equality (3.11) is precisely $B(j)$, we have proved (3.11) for $s = 2$, $\alpha \in \mathbf{Z}$.

We generalize the definition of $B(j)$ by denoting the right member of equation (3.11) by $B((j_0, \ldots, j_s))$. Considering the case $s = 1$, if $\alpha_0\alpha_1 = 0$ the theorem reduces to $1 = 1$, and if $\alpha_0 + \alpha_1 = 1$ it reduces to $(-1)^{-j_0} = \prod_{i=0}^{f-1}(-1)^{\mu_{\alpha_0}}$ by the reflection formula (2.5); this equality holds because $j_0 = \sum_{i=0}^{f-1} \mu_{\alpha_0}^{(i)} p^i$. Thus we may assume none of α_0, α_1, α lie in $\mathbf{Z}$. In this case there is a unique j_2 such that $j = (j_0, j_1, j_2) \in \mathcal{J}$, and from (2.7) we know $J(w_f^{-j_0}, \omega_f^{-j_1}) = -\omega_f^{-j_2}(-1)J(\omega_f^{-j_0}, \omega_f^{-j_1}, \omega_f^{-j_2})$. Since in this case we also have $B((j_0, j_1)) = (-1)^{j_2}B((j_0, j_1, j_2))$, the result for $s = 1$ follows from the $s = 2$, $\alpha \in \mathbf{Z}$ case.

The corollary may then be obtained by induction on s. Specifically, assuming the above conditions on $\{\alpha_0, \ldots, \alpha_s\}$ and on $\{\alpha_0, \ldots, \alpha_{s+1}\}$, one uses (2.5), (2.7) to check that

$$\frac{(-1)^{s+2}J(\omega_f^{-j_0}, \ldots, \omega_f^{-j_{s+1}})}{(-1)^{s+1}J(\omega_f^{-j_0}, \ldots, \omega_f^{-j_s})} = C \cdot J(\omega_f^{-(j_0+\cdots+j_s)}, \omega_f^{-j_{s+1}}) \tag{3.12}$$

and

$$\frac{B((j_0, \ldots, j_{s+1}))}{B((j_0, \ldots, j_s))} = C \cdot B((j', j_{s+1})), \tag{3.13}$$

where $j' \in \{0, 1, \ldots, q-2\}$ satisfies $j' \equiv j_0 + \cdots + j_s \pmod{q-1}$, and

$$C = \begin{cases} q, & \text{if } j_0 + \cdots + j_s \in (q-1)\mathbf{Z}, \\ 1, & \text{otherwise.} \end{cases} \tag{3.14}$$

Remark. In view of this corollary, we may view the $a_i = 1$ case of congruence (3.10) as a special case of the more general result

$$\frac{\binom{n_r + t}{n_{0,r}, \ldots, n_{s,r}, t}}{\binom{n_{r-1} + t}{n_{0,r-1}, \ldots, n_{s,r-1}, t}} \equiv (-1)^{s+1}J(\omega_f^{-j_0}, \ldots, \omega_f^{-j_s}) \pmod{p^{1+e}q^{r-1}\mathbf{Z}_p} \tag{3.15}$$

[**11**, Theorem 2.2], where for $r \geq 0$ we set $n_{i,r} = (q^r - 1)\alpha_i$, $n_r = (q^r - 1)\alpha$, and all other notation as in the corollary. If one applies Stienstra's construction to the diagonal hypersurface $T_0^d + \cdots + T_s^d = 0$, one essentially recovers these congruences in the cases where $t = 0$ and $\alpha \in \mathbf{Z}$.

4. The Gross-Koblitz Formula

THEOREM. (Gross-Koblitz). *Let a be an integer, $0 \leq a < q-1$, and put $\alpha = a/(q-1)$. Then*

$$g_\psi(\omega_f^{-a}) = \pi^{S(a)} \cdot \prod_{i=0}^{f-1} \Gamma_p(\alpha^{(i)}),$$

where $\pi^{p-1} = -p$ and $\zeta \equiv 1 + \pi \pmod{\pi^2 \mathcal{O}_K}$.

PROOF. Write $p\alpha = t + \gamma$ with $t \in \mathbf{Z}$ and $\gamma = c/(q-1) \in (0,1]$. Then using the above Corollary and the well-known fact that $g_\psi(\chi) = g_\psi(\chi^p)$ for any multiplicative character χ [**9**, Lemma 6.5], we compute

$$\begin{aligned} g_\psi(\omega_f^{-a})^{p-1} &= \frac{g_\psi(\omega_f^{-a})^p}{g_\psi(\omega_f^{-pa})} = -J(\underbrace{\omega_f^{-a}, \ldots, \omega_f^{-a}}_{p \text{ copies}}) \\ &= (-p)^e \prod_{i=0}^{f-1} \Gamma_p(\alpha^{(i)})^p / \Gamma_p(\gamma^{(i)}), \end{aligned} \tag{4.1}$$

where $e = (pS(a) - S(c))/(p-1)$. Since $p\alpha - \gamma = t \in \{0, 1, \ldots, p-1\}$, we have $\gamma' = \alpha$ and thus $\gamma^{(i)} = \alpha^{(i-1)}$ for $i > 0$, so $\gamma = \gamma^{(f)} = \alpha^{(f-1)}$. Therefore $S(c) = S(a)$, so $e = S(a)$, whence

$$g_\psi(\omega_f^{-a})^{p-1} = (-p)^{S(a)} \prod_{i=0}^{f-1} \Gamma_p(\alpha^{(i)})^{p-1}. \tag{4.2}$$

Therefore

$$g_\psi(\omega_f^{-a}) = \pi_a^{S(a)} \prod_{i=0}^{f-1} \Gamma_p(\alpha^{(i)}), \tag{4.3}$$

where π_a is some $(p-1)$st root of $-p$. It remains to show that for each a, (4.3) holds with $\pi_a = \pi$.

We proceed by induction on a. For $a = 0$, (4.3) reduces to $1 = \pi_0^0$, which is satisfied by $\pi_0 = \pi$. For $a = 1$, we have $\alpha = 1/(q-1)$ and $\alpha^{(i)} = p^{f-i}/(q-1)$ for $1 < i < f$, so that $\prod_{i=0}^{f-1} \Gamma_p(\alpha^{(i)}) \equiv 1 \pmod{p\mathbf{Z}_p}$; therefore $g_\psi(\omega_f^{-1}) \equiv \pi_1 \pmod{(\pi^2)}$. But from the proof of [**9**, Lemma 6.12] we have $g_\psi(\omega_f^{-1}) \equiv \zeta - 1 \pmod{(\pi^2)}$, so $\zeta \equiv 1 + \pi_1 \pmod{(\pi^2)}$; thus $\pi_1 = \pi$.

Now suppose that (4.3) holds with $\pi_a = \pi$ for $0 \leq a \leq k < q-1$. Then since $g_\psi(\omega_f^{-(k+1)}) = g_\psi(\omega_f^{-1}) g_\psi(\omega_f^{-k}) / J(\omega_f^{-1}, \omega_f^{-k})$, equating the corresponding expressions from (3.11) and (4.3) for the members of this equality yields

$$\pi_{k+1}^{S(k+1)} = \pi_1 \pi_k^{S(k)} (-p)^{-e}, \tag{4.4}$$

where $e = (S(k) + 1 - S(k+1))/(p-1)$. Since the right side of (4.4) is $\pi^{S(k+1)}$, we may take $\pi_{k+1} = \pi$, completing the induction.

References

1. M. Boyarsky, *p-adic gamma functions and Dwork cohomology*, Trans. AMS **257** (1980), 359–369.
2. R. Coleman, *The Gross-Koblitz formula,*, Advanced Studies in Pure Math. **12** (1987), 21–52.
3. B. Gross and N. Koblitz, *Gauss sums and the p-adic Γ-function*, Ann. Math. **109** (1979), 569–581.
4. N. Katz, *Crystalline cohomology, Dieudonné modules, and Jacobi sums*, Automorphic Forms, Representation Theory, and Arithmetic: Proceedings, Tata Institute Studies in Mathematics, Bombay, India, 1979, pp. 165–245.
5. J. Stienstra, *Formal group laws arising from algebraic varieties*, Amer. J. Math. **109** (1987), 907–925.
6. J. Stienstra, *Formal groups and congruences for L-functions*, Amer. J. Math. **109** (1987), 1111–1127.
7. J. Stienstra, M. van der Put, and B. van der Marel, *On p-adic monodromy*, Math. Z. **208** (1991), 309–325.
8. N. Suwa, *A p-adic limit formula for Gauss sums*, J. Number Theory **34** (1990), 276–283.
9. L. Washington, *Introduction to Cyclotomic Fields*, Springer-Verlag, New York, 1982.
10. A. Weil, *Numbers of solutions of equations in finite fields*, Bull. Amer. Math. Soc. **55** (1949), 497–508.
11. P. T. Young, *On Jacobi sums, multinomial coefficients, and p-adic hypergeometric functions*, J. Number Theory (to appear).

E-mail address: youngp@citadel.edu