Annals of Mathematics, **109** (1979), 569-581

Gauss sums and the p-adic Γ-function

By BENEDICT H. GROSS and NEAL KOBLITZ

Introduction

Let p be an odd prime. Many authors have considered p-adic analogs of the classical gamma function [7], [15], [16]. The simplest construction, due to Morita, is to define for $z \in \mathbf{Z}_p$,

$$\Gamma_p(z) = \lim_{m \to z} (-1)^m \prod_{\substack{0<j<m \\ (p,j)=1}} j ,$$

where m approaches z through positive integers. This gives a continuous function $\Gamma_p: \mathbf{Z}_p \to \mathbf{Z}_p^*$ which satisfies the functional equation:

$$\Gamma_p(z+1) = \begin{cases} -\Gamma_p(z) & \text{if} \quad z \in p\mathbf{Z}_p \\ -z\Gamma_p(z) & \text{if} \quad z \in \mathbf{Z}_p^* . \end{cases}$$

Morita [15] shows that $\Gamma_p(z)$ is analytic on $p\mathbf{Z}_p$ and gives a uniform analytic function on the set $\{z \in C_p : |z| \leqq |p|\}$, where C_p is the completion of the algebraic closure of $\mathbf{Q}_p$. It is *not* analytic on the closed unit disc, or else the functional equation $\Gamma_p(z+1) = -\Gamma_p(z)$ would hold on all of $\mathbf{Z}_p$.

In this paper, we investigate the values of $\Gamma_p(z)$ at rational arguments. Let N be a positive integer prime to p, and let r be an integer between 0 and N. In Section 1 we show how the value $\Gamma_p(r/N)$ is related to a Gauss sum whose multiplicative character is the r^{th}-power of the standard power residue symbol on $\mathbf{Q}(\mu_N)$. The proof, which uses Stickleberger's theorem and a result of Katz [11] on the p-adic cohomology of the Fermat curve $x^N + y^N = 1$, is given in Section 2. As corollaries, we prove that $\Gamma_p(r/N)$ is algebraic when $p \equiv 1 \pmod{N}$, and derive a multiplication formula for the function $\Gamma_p(z)$. In Section 4, we give a new proof of some of Deligne's recent results [5], [6] on Kummer extensions of $\mathbf{Q}(\mu_N)$ whose Galois character may be identified with a Hecke character defined by Jacobi sums. These extensions are generated by products of values of the *classical* Γ-function at rational arguments, and our method yields a striking formula relating $\Gamma(z)$ to its p-adic analog. We also show how the classical and p-adic Γ-functions are

0003-486X/79/0109-3/0013/000 $ 00.65/1

related via the Chowla-Selberg formula, which gives the periods of elliptic curves with complex multiplication.

Acknowledgments. We wish to express our appreciation to P. Deligne, B. Dwork, and N. Katz for many helpful comments.

1. Gauss sums and the p-adic Γ-function

Let N be a positive integer, and let $K = \mathbf{Q}(\mu_N)$ be the cyclotomic field of N^{th} roots of unity. Let $\mathcal{P}$ be a prime of K which does not divide $2N$, with $\mathbf{N}\mathcal{P} = q = p^f$, and let t be the map from N^{th} roots of unity in the residue field $k_{\mathcal{P}}$ to the N^{th} roots of unity in K which is the inverse to reduction mod $\mathcal{P}$.

Fix a non-trivial additive character

$$\Psi: \mathbf{F}_p \longrightarrow \mu_p \,. \tag{1.1}$$

For any $a \in (1/N)\mathbf{Z}/\mathbf{Z} - \{0\}$, define the Gauss sum (note the minus signs) [17]:

$$g(a, \mathcal{P}, \Psi \circ \mathrm{Tr}) = -\sum t(x^{-a(q-1)})\Psi(\mathrm{Tr}\, x) \tag{1.2}$$

where the sum is taken over $x \in k_{\mathcal{P}}^*$ and the trace is from $k_{\mathcal{P}}$ to $\mathbf{F}_p$. Then $g(a, \mathcal{P}, \Psi \circ \mathrm{Tr})$ is a non-zero element of the field $L = K(\mu_p)$; it depends on the choice of Ψ, but, as this character will be fixed throughout, we shall write it simply as $g(a, \mathcal{P})$.

If $\boldsymbol{a} = \sum m(a)\delta_a$ is an element of the free abelian group with basis $(1/N)\mathbf{Z}/\mathbf{Z} - \{0\}$, we may define the generalized Gauss sum:

$$g(\boldsymbol{a}, \mathcal{P}) = \prod g(a, \mathcal{P})^{m(a)} \,. \tag{1.3}$$

For $u \in (\mathbf{Z}/N\mathbf{Z})^*$ let $\boldsymbol{a}^{(u)} = \sum m(a)\delta_{ua}$. Then one has

$$g(\boldsymbol{a}^{(p)}, \mathcal{P}) = g(\boldsymbol{a}, \mathcal{P}) \,, \tag{1.4}$$

as the additive character defining $g(a, \mathcal{P})$ comes from a character of the prime field.

Let $\mathcal{B}$ be the unique prime over $\mathcal{P}$ in L, and let $L_{\mathcal{B}}$ be the completion of L at $\mathcal{B}$. Our aim in this section is to express $g(a, \mathcal{P})$ in $L_{\mathcal{B}}$ in terms of Morita's p-adic gamma function. The field $L_{\mathcal{B}}$ contains the $(p-1)$-st roots of $-p$; if $\zeta = \Psi(1)$ let π be the unique $(p-1)$-st root satisfying

$$\pi \equiv (\zeta - 1) \mod (\zeta - 1)^2 \,. \tag{1.5}$$

Then π gives a uniformizing element in $L_{\mathcal{B}}$ which is completely determined by the choice of additive character Ψ. Furthermore, by (1.4) we see that $g(a, \mathcal{P})$ lies in the subfield $\mathbf{Q}_p(\pi) = \mathbf{Q}_p(\mu_p)$ of $L_{\mathcal{B}}$.

Recall that the function $\Gamma_p: \mathbf{Z}_p \to \mathbf{Z}_p$ is defined by

$$\Gamma_p(z) = \lim_{m \to z} (-1)^m \prod_{\substack{0 < j < m \\ (p,j)=1}} j \,, \tag{1.6}$$

where m approaches z through positive integers. If a is any element of $(1/N)\mathbf{Z}/\mathbf{Z}$, let $\langle a\rangle$ be the unique rational number with $0 < \langle a\rangle \leqq 1$ and $a \equiv \langle a\rangle \bmod \mathbf{Z}$. We shall prove:

THEOREM 1.7.

$$g(a, \mathcal{P}) = \pi^{(p-1)\sum_{j=0}^{f-1}\langle p^j a\rangle} \prod_{j=0}^{f-1} \Gamma_p(\langle p^j a\rangle) \quad in \quad L_{\mathfrak{B}} .$$

Note that the exponent of π is an integer.

This theorem yields the algebraicity of certain Γ_p-values:

COROLLARY 1.8. *If* $p \equiv 1 \pmod N$ *then* $\Gamma_p(r/N) \in \mathbf{Q}(\mu_{Np}, \sqrt[N]{-p})$.

Indeed, for $0 < r/N < 1$ this follows directly from Theorem 1.7. Since $\Gamma_p(z+1)/\Gamma_p(z)$ is always rational when z is rational, the corollary holds in general.

Theorem 1.7 is easily generalized to the Gauss sums $g(\boldsymbol{a}, \mathcal{P})$. For $\boldsymbol{a} = \sum m(a)\delta_a$, define

$$n(\boldsymbol{a}) = \sum m(a)\langle a\rangle , \tag{1.9}$$

$$\Gamma_p(\boldsymbol{a}) = \prod \Gamma_p(\langle a\rangle)^{m(a)} . \tag{1.10}$$

Then we obtain:

COROLLARY 1.11.

$$g(\boldsymbol{a}, \mathcal{P}) = \pi^{(p-1)\sum_{j=0}^{f-1} n(\boldsymbol{a}^{(p^j)})} \prod_{j=0}^{f-1} \Gamma_p(\boldsymbol{a}^{(p^j)}) \quad in \quad L_{\mathfrak{B}} .$$

In the special case when $n(\boldsymbol{a}) \in \mathbf{Z}$, the Gauss sum $g(\boldsymbol{a}, \mathcal{P})$ is independent of the choice of additive character Ψ and lies in $K = \mathbf{Q}(\mu_N)$. These Jacobi sums were studied by Weil in connection with the zeta-functions of Fermat hypersurfaces; as a function of $\mathcal{P}$, $g(\boldsymbol{a}, \cdot)$ gives a Hecke character of type A_0 for K with values in K [14], [2]. This character has algebraic part

$$\Theta = \sum\nolimits_{u \in (\mathbf{Z}/N\mathbf{Z})^*} n(\boldsymbol{a}^{(u)})\sigma_u^{-1} .$$

If we consider $g(\boldsymbol{a}, \mathcal{P})$ in the completion $K_{\mathcal{P}}$, then by (1.4) $g(\boldsymbol{a}, \mathcal{P})$ lies in the subfield $\mathbf{Q}_p$. As a special case of Corollary 1.11 we have:

THEOREM 1.12. *If* $n(\boldsymbol{a}) \in \mathbf{Z}$ *then*

$$g(\boldsymbol{a}, \mathcal{P}) = (-p)^{\sum_{j=0}^{f-1} n(\boldsymbol{a}^{(p^j)})} \prod_{j=0}^{f-1} \Gamma_p(\boldsymbol{a}^{(p^j)}) \quad in \quad K_{\mathcal{P}} .$$

Note that both sides are now independent of Ψ.

Finally, suppose $\boldsymbol{a}$ satisfies the condition:

$$n(\boldsymbol{a}^{(u)}) \text{ is an integer which is independent of } u \in (\mathbf{Z}/N\mathbf{Z})^* . \tag{1.13}$$

The Hecke character

$$\chi_{\boldsymbol{a}}(\mathcal{P}) = g(\boldsymbol{a}, \mathcal{P})\mathbf{N}(\mathcal{P})^{-n(\boldsymbol{a})} \tag{1.14}$$

is then of finite order.

COROLLARY 1.15. *If* $\boldsymbol{a}$ *satisfies* (1.13) *then*

$$\chi_{\boldsymbol{a}}(\mathcal{P}) = (-1)^{n(\boldsymbol{a})f} \prod_{j=0}^{f-1} \Gamma_p(\boldsymbol{a}^{(p^j)}) .$$

This implies, in particular, that the product of gamma values on the right is a root of unity in K^*.

2. The proof of Theorem 1.7

We begin with a proof of Theorem 1.12: the corresponding result for Jacobi sums. Here are two important examples:

(2.1) $$\boldsymbol{a} = \delta_{r/N} + \delta_{(N-r)/N} \quad \text{with} \quad 0 < r < N .$$

Then

$$g(\boldsymbol{a}, \mathcal{P}) = q(-1)^{r(p-1)/N} .$$

(2.2) $$\boldsymbol{a} = \delta_{r/N} + \delta_{s/N} - \delta_{(r+s)/N} \quad \text{with} \quad 0 < r, s < N,\ r + s \neq N .$$

Then

$$g(\boldsymbol{a}, \mathcal{P}) = -\sum_{k_p - \{0,1\}} t(x^{-r(q-1)/N}) t\big((1-x)^{-s(q-1)/N}\big) .$$

The latter Jacobi sum arises as an eigenvalue of Frobenius on the Fermat curve $x^N + y^N = 1$ over $\mathbf{Q}(\mu_N)$. As any $\boldsymbol{a}$ with $n(\boldsymbol{a}) \in \mathbf{Z}$ is a $\mathbf{Z}$-linear combination of the elements in examples (2.1) and (2.2), it is sufficient to prove Theorem 1.12 in these special cases (Lemmas 2.5 and 2.6).

LEMMA 2.3. *If* $z \in \mathbf{Z}_p$ *then* $\Gamma_p(z)\Gamma_p(1-z) = (-1)^{\hat{z}}$, *where* $\hat{z}$ *is the unique integer with* $0 < \hat{z} \leqq p$ *and* $\hat{z} \equiv z \pmod{p}$.

Proof. Write $z = \sum_{n=0}^{\infty} a_n p^n$ with $0 \leqq a_n < p$ and let $m_\nu = \sum_{n=0}^{\nu-1} a_n p^n$. Then

$$\begin{aligned}
\Gamma_p(z)\Gamma_p(1-z) &= \lim_{\nu\to\infty} \Big((-1)^{m_\nu} \prod_{\substack{j<m_\nu \\ (p,j)=1}} j\Big)\Big((-1)^{p^\nu+1-m_\nu} \prod_{\substack{j<p^\nu+1-m_\nu \\ (p,j)=1}} j\Big) \\
&= \lim_{\nu\to\infty} (-1)^{\operatorname{Card}\{j<m_\nu:\, p\nmid j\}} \prod_{\substack{j<p^\nu \\ p\nmid j}} j \\
&= (-1)^{\hat{z}-1} \Big(\lim_{\nu\to\infty} \prod_{\substack{j<p^\nu \\ p\nmid j}} j\Big) = (-1)^{\hat{z}}
\end{aligned}$$

by Wilson's Theorem.

LEMMA 2.4. *Assume* $0 < r/N < 1$ *and write*

$$(p^f - 1)(r/N) = z_f + z_1 p + z_2 p^2 + \cdots + z_{f-1} p^{f-1} \qquad \textit{with } 0 \leqq z_j < p .$$

Then

$$\langle \widehat{p^j r/N} \rangle = p - z_{f-j} .$$

Proof. This is clear for $j = 0$. For $j > 0$ write

$$p^j r/N = b_j + \langle p^j r/N \rangle \qquad \text{with } b_j \in \mathbf{Z} .$$

Then one has the formula

$$b_j = z_{f-j} + pz_{f-j+1} + \cdots + p^{j-1}z_{f-1}\,.$$

Consequently

$$\langle p^j r/N\rangle \equiv -b_j \equiv -z_{f-j} \pmod p$$

which gives the lemma.

LEMMA 2.5. *If* $\boldsymbol{a} = \delta_{r/N} + \delta_{(N-r)/N}$, *the formula for* $g(\boldsymbol{a}, \mathcal{P})$ *in* (1.12) *is true.*

Proof. We know $g(\boldsymbol{a}, \mathcal{P}) = q(-1)^{r(q-1)/N}$. As $n(\boldsymbol{a}^{(u)}) = 1$ for $u \in (\mathbf{Z}/N\mathbf{Z})^*$:

$$\begin{aligned}(-p)^{\Sigma n(\boldsymbol{a}^{(p^j)})}\textstyle\prod_{j=0}^{f-1}\Gamma_p(\boldsymbol{a}^{(p^j)}) &= q(-1)^f \textstyle\prod_{j=0}^{f-1}\Gamma_p\langle p^j r/N\rangle\Gamma_p\big(1-\langle p^j r/N\rangle\big)\\ &= q(-1)^{f+\Sigma_{j=0}^{f-1}\widehat{\langle p^j r\rangle N\rangle}} \quad \text{by (2.3).}\\ &= q(-1)^{f+\Sigma_{j=0}^{f-1}(p-z_{f-j})} \quad \text{by (2.4).}\\ &= q(-1)^{\Sigma_{j=1}^{f} z_j}\,.\end{aligned}$$

As $\sum_{j=1}^{f} z_j \equiv (q-1)r/N \pmod{p-1}$, this gives the required identity.

LEMMA 2.6. *If* $\boldsymbol{a} = \delta_{r/N} + \delta_{s/N} - \delta_{(r+s)/N}$, *the formula for* $g(\boldsymbol{a}, \mathcal{P})$ *in* (1.12) *is true.*

Proof. We must show

$$g(\boldsymbol{a}, \mathcal{P}) = \textstyle\prod_{j=0}^{f-1}(-p)^{\varepsilon_j}\dfrac{\Gamma_p\big(\langle p^j r/N\rangle\big)\Gamma_p\big(\langle p^j s/N\rangle\big)}{\Gamma_p\big(\langle p^j(r+s)/N\rangle\big)}\,,$$

where $\varepsilon_j = \langle p^j r/N\rangle + \langle p^j s/N\rangle - \langle p^j(r+s)/N\rangle$ is either 0 or 1. Set $t = (1+\varepsilon_0)N - r - s$.

By a comparison of the action of Frobenius on the crystalline cohomology of the Fermat curve $x^N + y^N = 1$ over $k_{\mathcal{P}}$ with its action on the eigendifferential

$$\omega_{r,s} = x^{r-1}y^{s-1}\frac{dx}{y^{N-1}} = x^{r-1}(1-x^N)^{(s-N)/N}\,dx$$

in the de Rham cohomology of the curve over the Witt vectors $W(k_{\mathcal{P}})$, Katz ([11], [12]) obtained the formula

$$g(\boldsymbol{a}, \mathcal{P}) = \textstyle\prod_{j=0}^{f-1}\lim_{k\to -\langle p^j r/N\rangle}\dfrac{\binom{\langle p^{j+1}t/N\rangle - 1}{pk + \big(p\langle p^j r/N\rangle - \langle p^{j+1}r/N\rangle\big)}}{\binom{\langle p^j t/N\rangle - 1}{k}}\,. \tag{2.7}$$

We want to interpret the limits on the right side of (2.7) as products of p-adic Γ-values.

Let h and k be positive even integers with

$$\begin{aligned} h &\equiv -t/N \pmod{p^a}\,,\\ k &\equiv -r/N \pmod{p^b}\,,\end{aligned}$$

with a and b large. Let $[x]$ be the greatest integer less than or equal to x. Since

$$ph + [pt/N] \equiv -\langle pt/N\rangle \pmod{p^{a+1}},$$
$$pk + [pr/N] \equiv -\langle pr/N\rangle \pmod{p^{b+1}},$$

we see the $j = 0$ term in (2.7) is approximated by

$$(2.8)\qquad (-1)^{[pr/N]}\frac{(p(h+k) + [pt/N] + [pr/N])!}{(ph + [pt/N])!\,(pk + [pr/N])!}\Big/\frac{(h+k)!\,p^{h+k}}{h!\,p^h k!\,p^k}.$$

If $\varepsilon_0 = 0$, then $[pt/N] + [pr/N] < p$, and this ratio approaches

$$(-1)^{[pr/N]+\varepsilon_1}\frac{\Gamma_p(1 - \langle pr/N\rangle - \langle pt/N\rangle)}{\Gamma_p(1 - \langle pr/N\rangle)\Gamma_p(1 - \langle pt/N\rangle)}.$$

Using Lemma 2.3 and the functional equation for $\Gamma_p(z)$, we see this is equal to

(2.9)

$$(\varepsilon_0 = 0)\begin{cases}\Gamma_p(\langle pr/N\rangle)\Gamma_p(\langle ps/N\rangle)/\Gamma_p(\langle p(r+s)/N\rangle) & \text{if } \varepsilon_1 = 0\\ \dfrac{1}{(1 - \langle pr/N\rangle - \langle pt/N\rangle)}\Gamma_p(\langle pr/N\rangle)\Gamma_p(\langle ps/N\rangle)/\Gamma_p(\langle p(r+s)/N\rangle) & \text{if } \varepsilon_1 = 1.\end{cases}$$

If $\varepsilon_0 = 1$, then we find that the $j = 0$ term in (2.7) is equal to

(2.10)

$$(\varepsilon_0 = 1)\begin{cases}-p(1 - r/N - t/N)\Gamma_p(\langle pr/N\rangle)\Gamma_p(\langle ps/N\rangle)/\Gamma_p(\langle p(r+s)N\rangle) & \text{if } \varepsilon_1 = 0\\ \dfrac{-p(1 - r/N - t/N)}{(1 - \langle pr/N\rangle - \langle pt/N\rangle)}\Gamma_p\Big(\Big\langle\frac{pr}{N}\Big\rangle\Big)\Gamma_p(\langle ps/N\rangle)/\Gamma_p(\langle p(r+s)/N\rangle) & \text{if } \varepsilon_1 = 1.\end{cases}$$

Now repeat the argument for each term in the product of (2.7), replacing r/N by $\langle p^j r/N\rangle$, etc. Multiplying these results for $j = 0, 1, \cdots, f-1$ and noting the telescoping of the $1 - r/N - s/N$ terms, we obtain the lemma, and hence Theorem 1.12.

We can obtain Theorem 1.7 from Theorem 1.12 as follows. For any $a \in (1/N)\mathbf{Z}/\mathbf{Z} - \{0\}$ let $\boldsymbol{a} = (p^f - 1)\delta_a$. Theorem 1.12 then gives

$$g(\boldsymbol{a}, \mathcal{P}) = g(a, \mathcal{P})^{p^f-1} = (-p)^{\sum_{j=0}^{f-1} n\langle a^{(p^j)}\rangle}\prod_{j=0}^{f-1}\Gamma_p(\boldsymbol{a}^{(p^j)})$$
$$= \big(\pi^{(p-1)\sum\langle p^j a\rangle}\prod\Gamma_p\langle p^j a\rangle\big)^{p^f-1}.$$

Therefore the quantities $g(a, \mathcal{P})$ and $\pi^{(p-1)\sum\langle p^j a\rangle}\prod\Gamma_p\langle p^j a\rangle$ differ by a (p^f-1)-st root of unity. As they both lie in $\mathbf{Q}_p(\pi) = \mathbf{Q}_p(\mu_p)$, they must differ by a $(p-1)$-st root of unity. To show they are equal, we shall prove that they are congruent $(\mathrm{mod}\,\pi)$.

Write $(p^f - 1)\langle a\rangle = z_f + z_1 p + \cdots + z_{f-1}p^{f-1}$ with $0 \leqq z_i < p$ as in

(2.4).

LEMMA 2.11. 1) $(p-1)\sum_{j=0}^{f-1}\langle p^j a\rangle = \sum_{j=1}^{f} z_j$.

2) $g(a, \mathcal{P})\pi^{-\Sigma z_j} = u \in \mathbf{Z}_p^*$.

3) $u \equiv \prod_{j=0}^{f-1}\Gamma_p(\langle p^j a\rangle) \pmod{p}$.

Proof. 1) is immediate from the formula ($j \geqq 1$):

$$\langle p^j a\rangle = \frac{z_f p^j + \cdots + z_{f-j-1}p^{f-1} + z_{f-j} + \cdots + z_{f-1}p^{j-1}}{(p^f - 1)} .$$

Thus $u = g(a, \mathcal{P})\pi^{-\Sigma z_j}$ is a product of Γ_p-values times a $(p-1)$-st root of unity, by our preceding remarks. Hence u is a p-adic unit.

3) is essentially the content of Stickleberger's famous theorem on Gauss sums [17], [14]. This states that

$$g(a, \mathcal{P}) \equiv \left(\frac{\pi^{\Sigma z_j}}{\prod_{j=1}^{f} z_j!}\right) \pmod{\pi^{\Sigma z_j + 1}} ,$$

which gives

$$u \equiv \left(\prod_{j=1}^{f} z_j!\right)^{-1} \pmod{p} .$$

On the other hand, since $\widehat{\langle p^j a\rangle} = p - z_{f-j}$ by (2.4), we have

$$\begin{aligned}\Gamma_p(\langle p^j a\rangle) &\equiv (p - z_{f-j} - 1)!\,(-1)^{p-z_{f-j}} \\ &\equiv (z_{f-j}!)^{-1} \pmod{p} .\end{aligned}$$

Therefore

$$u \equiv \prod_{j=0}^{f-1}\Gamma_p(\langle p^j a\rangle) \pmod{p}$$

as claimed.

This completes the proof of Theorem 1.7.

3. A multiplication formula for $\Gamma_p(z)$

Let p be an odd prime, and $q = p^f$. Let ω be the Teichmüller character on $\mathbf{Z}_p^*$, and let m be a positive integer prime to p.

THEOREM 3.1. *Assume* $0 < x < 1$ *and* $(q-1)x \in \mathbf{Z}$.

1) *If* $\boldsymbol{a} = \delta_x + \delta_{1-x} - 2\delta_{1/2}$ *then* $\prod_{j=0}^{f-1}\Gamma_p(\boldsymbol{a}^{(p^j)}) = (-1)^{(q-1)(x-1/2)}$.

2) *If* $\boldsymbol{a} = \delta_{x/m} + \delta_{(x+1)/m} + \cdots + \delta_{(x+m-1)/m} - \delta_x - \delta_{1/m} - \delta_{2/m} - \cdots - \delta_{m-1/m}$ *then*

$$\prod_{j=0}^{f-1}\Gamma_p(\boldsymbol{a}^{(p^j)}) = \omega(m^{(q-1)x}) .$$

Proof. Part 1) is a restatement of Lemma 2.5 for $x = r/(q-1)$, as $\Gamma_p(1/2)^2 = (-1)^{(p+1)/2}$.

To prove 2), let N be the common denominator of the terms $(x+h)/m$ for $h = 0, 1, \cdots, m-1$. Let g be the order of $p \pmod{N}$. Since $n(\boldsymbol{a}^{(u)}) = 0$ for all $u \in (\mathbf{Z}/N\mathbf{Z})^*$, Corollary 1.16 implies that $\prod_{j=0}^{g-1}\Gamma_p(\boldsymbol{a}^{(p^j)})$ is a root of

unity. But

$$\prod_{j=0}^{g-1}\Gamma_p(a^{(p^j)}) = \left(\prod_{j=0}^{f-1}\Gamma_p(a^{(p^j)})\right)^{g/f}$$

as $a^{(p^f)} = a$. Hence $\prod_{j=0}^{f-1}\Gamma_p(a^{(p^j)})$ must also be a root of unity; as it lies in $\mathbf{Z}_p^*$ we are reduced to a proof of the congruence:

$$\prod_{j=0}^{f-1}\Gamma_p(a^{(p^j)}) \stackrel{?}{\equiv} m^{(q-1)x} \pmod{p}\,. \tag{3.2}$$

Writing $(q-1)x = z_f + z_1 p + \cdots + z_{f-1}p^{f-1}$ as in (2.4), we have $\sum_{k=1}^{f} z_k \equiv (q-1)x \pmod{p-1}$, so

$$m^{(q-1)x} \equiv \prod_{k=1}^{f} m^{z_k} \equiv \prod_{j=0}^{f-1} m^{z_{f-j}} \pmod{p}\,.$$

Therefore (3.2) follows from the congruence

$$\Gamma_p(a) \equiv m^{z_f} \pmod{p}\,.$$

The proof of this congruence is elementary, and we omit it.

Notes: 1) A more general multiplication formula has been obtained by Dwork [1], [11]. His proof uses the functional equation of $\Gamma_p(z)$.

2) If we translate Theorem 3.1 into the language of Gauss sums, using Theorem 1.12, we obtain a result due to Hasse and Davenport [3]:

$$\frac{\prod_{h=0}^{m-1} g\left(\frac{a+h}{m}, \mathcal{P}\right)}{\prod_{h=1}^{m-1} g\left(\frac{h}{m}, \mathcal{P}\right)} = g(a, \mathcal{P}) \cdot t(m^{(q-1)a})\,. \tag{3.3}$$

Where a is an element in $(1/N)\mathbf{Z}/\mathbf{Z} - \{0\}$ with $\langle a\rangle =$ the x of Theorem 3.1, t is the Teichmüller map (see beginning of § 1), and $\mathcal{P}$ is a prime dividing p in $\mathbf{Q}(\mu_N)$.

3) Lang [14] has suggested interpreting the Hasse-Davenport theorem as a distribution relation for Gauss sums; one can also state this relation using $\Gamma_p(z)$.

Let $(\mathbf{Q}/\mathbf{Z})_{p'} = \perp\!\!\!\perp_{l\neq p} \mathbf{Q}_l/\mathbf{Z}_l$ and define the function

$$\varphi\colon (\mathbf{Q}/\mathbf{Z})_{p'} \longrightarrow p\mathbf{Z}_p$$

by setting

$$\varphi(a) = \log_p \prod_{j=0}^{f-1}\Gamma_p(\langle p^j a\rangle)\,,$$

where f is the least integer such that $(p^f - 1)a \equiv 0 \pmod{\mathbf{Z}}$. Then by (3.1) the function φ satisfies the relations

$$\varphi(-a) = -\varphi(a)\,, \tag{3.4}$$

$$\prod_{h=0}^{m-1}\varphi\left(\frac{a+h}{m}\right) = \varphi(a) \qquad \text{for all } m \text{ prime to } p\,; \tag{3.5}$$

$$\varphi(pa) = \varphi(a)\,. \tag{3.6}$$

Thus φ is an odd distribution on $(\mathbf{Q}/\mathbf{Z})_{p'}$ with values in the group $p\mathbf{Z}_p$; in fact, it is the *universal* odd distribution satisfying (3.6) with values in this (torsion-free) group [13]. Note that the values of φ are all p-adic logarithms of algebraic numbers.

4. Relation to the classical Γ-function

In this section we shall fix N and consider those $\boldsymbol{a}$ in the free abelian group on $(1/N)\mathbf{Z}/\mathbf{Z} - \{0\}$ which satisfy condition (1.13): $n(\boldsymbol{a}^{(u)})$ is an integer which is independent of $u \in (\mathbf{Z}/N\mathbf{Z})^*$. These elements form a subgroup A; for any $\boldsymbol{a} \in A$ we define

$$\Omega_{\boldsymbol{a}} = \frac{\Gamma(\boldsymbol{a})}{(2\pi i)^{n(\boldsymbol{a})}} . \tag{4.1}$$

When $\boldsymbol{a} \in A$, the Hecke character $\chi_{\boldsymbol{a}}$ defined in (1.14) is trivial on the connected component of the group of idele classes of K, so may be viewed as a character of $\mathrm{Gal}(\bar{\mathbf{Q}}/K)$. (We normalize the isomorphism of class field theory to take a uniformizing parameter to a geometric Frobenius.)

THEOREM 4.2 (Deligne [5]). *If $\boldsymbol{a} \in A$ then $\Omega_{\boldsymbol{a}}$ is algebraic and*

$$\sigma\Omega_{\boldsymbol{a}} = \chi_{\boldsymbol{a}}(\sigma) \cdot \Omega_{\boldsymbol{a}} \quad \textit{for any} \quad \sigma \in \mathrm{Gal}(\bar{\mathbf{Q}}/K) .$$

Deligne's proof involves the Hodge theory of Fermat hypersurfaces. Our methods give this result on a large subgroup of A. Namely, if m is a positive integer dividing N, write $N = mk$ and let $x = r/k$. Then

$$\boldsymbol{a} = \delta_{x/m} + \delta_{x+1/m} + \cdots + \delta_{x+(m-1)/m} - \delta_x - \delta_{1/m} - \delta_{2/m} - \cdots - \delta_{m-1/m} \tag{4.3}$$

is an element of A with $n(\boldsymbol{a}) = 0$. Let B be the subgroup generated by all these "basic relations", along with those of the form

$$\boldsymbol{a} = \delta_x + \delta_{1-x} \tag{4.4}$$

with $x = r/N$ and $n(\boldsymbol{a}) = 1$.

THEOREM 4.5. *If $\boldsymbol{a} \in B$ then $\sigma\Omega_{\boldsymbol{a}} = \chi_{\boldsymbol{a}}(\sigma)\Omega_{\boldsymbol{a}}$ for all $\sigma \in \mathrm{Gal}(\bar{\mathbf{Q}}/K)$.*

Note. Kubert [13] has shown that the quotient group A/B is killed by 2. Therefore Theorem 4.5 gives Deligne's full result "up to sign".

Proof. Let $w = |\mu(K^*)|$, so $w = \text{l.c.m.}(2, N)$. First we show that $\Omega_{\boldsymbol{a}}^w \in K^*$. It is enough to check this on basic relations. For $\boldsymbol{a}$ of type (4.3) we have

$$\Omega_{\boldsymbol{a}} = m^{1-x} .$$

For $\boldsymbol{a}$ of type (4·4) we have

$$\Omega_{\boldsymbol{a}} = \frac{e^{\pi i x}}{e^{2\pi i x} - 1} .$$

In both cases $\Omega_{\boldsymbol{a}}^w \in K^*$.

Now let $\boldsymbol{a}$ be an element of B and $\mathcal{P}$ a prime not dividing N in K. If $F_{\mathcal{P}}$ is a geometric Frobenius at $\mathcal{P}$ we must prove

$$\frac{F_{\mathcal{P}}\Omega_{\boldsymbol{a}}}{\Omega_{\boldsymbol{a}}} = \chi_{\boldsymbol{a}}(\mathcal{P}) \,. \tag{4.6}$$

Since both sides are roots of unity in K^* it is enough to check this (mod $\mathcal{P}$). Furthermore we may restrict to primes $\mathcal{P}$ of degree 1 in K, as such $F_{\mathcal{P}}$ are dense in the Galois group. But then

$$\frac{F_{\mathcal{P}}\Omega_{\boldsymbol{a}}}{\Omega_{\boldsymbol{a}}} \equiv \Omega_{\boldsymbol{a}}^{1-p} \qquad (\mathrm{mod}\, \mathcal{P})$$

and, by Corollary 1.15,

$$\chi_{\boldsymbol{a}}(\mathcal{P}) = (-1)^{n(\boldsymbol{a})}\Gamma_p(\boldsymbol{a}) \,.$$

It is now an easy matter to check (4.6) for basic relations $\boldsymbol{a}$ of type (4.3) and (4.4) using Theorem 3.1. Since both sides of (4.6) are multiplicative in $\boldsymbol{a}$, we obtain the theorem for all $\boldsymbol{a}$ in B.

In the proof of Theorem 4.5 we used only (mod p) information. The following result however employs the full p-adic theory.

THEOREM 4.6. *Let $\mathcal{P}$ be a prime of K with $\mathbf{N}\mathcal{P} = p$, let* Frob$(\mathcal{P})$ *be a geometric Frobenius at $\mathcal{P}$ in* Gal$(\bar{\mathbf{Q}}/K)$, *and let $i_{\mathcal{P}}$ be the inclusion of K into $K_{\mathcal{P}}$. If $\boldsymbol{a} \in A$ then*

$$\left(\frac{\Gamma(\boldsymbol{a})}{(2\pi i)^{n(\boldsymbol{a})}}\right)^{\mathrm{Frob}(\mathcal{P})-1} = \left(\frac{\Gamma_p(\boldsymbol{a})}{(-1)^{n(\boldsymbol{a})}}\right)^{i_{\mathcal{P}}^{-1}} .$$

Indeed, this is merely a combination of Theorem 4.2 and Corollary 1.15. Deligne interprets this theorem in terms of periods of Hodge classes of type $(n(\boldsymbol{a}), n(\boldsymbol{a}))$ on products of Fermat hypersurfaces. We can obtain a similar theorem for the periods of one-forms on certain abelian varieties with complex multiplication by an abelian field; here we give the result for elliptic curves.

Let k be an imaginary quadratic field of discriminant $-N$; let h be the class number of k, w the number of roots of unity, and ε the quadratic Dirichlet character (mod N) associated to this extension. Define the element

$$\boldsymbol{a} = \frac{w}{2}\sum\nolimits_{\varepsilon(a)=1}\delta_a \,. \tag{4.7}$$

Then $n(\boldsymbol{a}) + n(\boldsymbol{a}^{(-1)}) = w\varphi(N)/4$ and, by Dirichlet's class-number formula: $n(\boldsymbol{a}^{(-1)}) - n(\boldsymbol{a}) = h$. Therefore $n(\boldsymbol{a})$ is half-integral; by genera theory $n(\boldsymbol{a})$ is integral whenever N is not a power of 2.

Let E be an elliptic curve with complex multiplication by the integers

of k; suppose E is defined over H, the Hilbert classfield of k. If ω is a differential of the first kind on E and v is an infinite place of H, let

$$\int\omega_v \quad \text{in} \quad H_v^*/k^*$$

be the integral of ω around any 1-cycle in the rational homology of $E_v(H_v)$. If v_∞ is a complex place of k, put

$$\text{Per}_{v_\infty}(E) = \prod_{v|v_\infty}\int\omega_v \quad \text{in} \quad k_{v_\infty}^*/k^* \,. \tag{4.8}$$

Modulo k^* this period depends only on E, and not on the differential or cycles chosen. An application of the Chowla-Selberg formula, as stated in [10], gives

$$\text{Per}_{v_\infty}(E) \sim_{\bar{\mathbf{Q}}^*} \frac{\Gamma(\boldsymbol{a})}{(2\pi i)^{n(a)}} \tag{4.9}$$

where $\sim_{\bar{\mathbf{Q}}^*}$ means that the ratio is an algebraic number. To determine this algebraic number up to an element of k^* we shall use the p-adic gamma-function and the zeta-function of the curve.

In fact, the L-function of E can be expressed as the product of abelian L-series (see, e.g., [9]):

$$L(H^1(E), s) = L(\chi, s)L(\bar{\chi}, s) \,,$$

where χ is an algebraic Hecke character of H with values in k. If q is a prime of H where E has good reduction, we can normalize so that $(\chi(q)) = \overline{\mathbf{N}_{H/k}q}$ as ideals in k. If $v_{\mathcal{P}}$ is a finite place of k over which E has good reduction, we can imitate (4.8) by defining

$$\text{Per}_{v_{\mathcal{P}}}(E) = \chi(\mathcal{P}) = \prod_{q|\mathcal{P}}\chi(q) \,. \tag{4.10}$$

By so restricting χ to k, we obtain a Hecke character which was related to a Jacobi sum on $\mathbf{Q}(\mu_N)$ by Weil [17], [18]. If $\mathbf{N}\mathcal{P} = p$ we can use this expression and Theorem 1.7 to show

$$\text{Per}_{v_{\mathcal{P}}}(E) \sim_\mu \Gamma_p(\boldsymbol{a}) \quad \text{in} \quad K_{v_{\mathcal{P}}}^* \tag{4.11}$$

where $\sim_\mu$ means the ratio is a root of unity. Since $\text{Per}_{v_{\mathcal{P}}}(E) = \chi(\mathcal{P})$ generates the principal ideal $(\bar{\mathcal{P}})^h = (\bar{\alpha})$, we can take the p-adic logarithm of (4.11) to obtain the identity

$$\sum_{0<a<N}\varepsilon(a)\log_p\Gamma_p(a/N) = \frac{4}{w}\log_p\bar{\alpha} \quad \text{in} \quad K_{v_{\mathcal{P}}} \,. \tag{4.12}$$

This evaluates the derivative at zero of the p-adic L-series with character ε [8], much as the Chowla-Selberg formula interprets the derivative of the classical Dirichlet L-function [2].

But the relationship between (4.9) and (4.11) is more than formal: the

root of unity in (4.11) controls the algebraic number in (4.9) via Kummer theory. Here is the simplest case.

THEOREM 4.13. *Let E be an elliptic curve with complex multiplication by the integers of k which is defined over H, the Hilbert classfield of k. Assume the discriminant $-N$ of k is prime, and let $\mathcal{P}$ be a prime of k with $\mathbf{N}\mathcal{P} = p$, $p \nmid N$. Assume E has good reduction at all places q of H dividing $\mathcal{P}$. Then*

$$\left(\frac{\mathrm{Per}_{v_\infty}(E)}{\Gamma(\boldsymbol{a})/(2\pi i)^{n(a)}}\right)^{\mathrm{Frob}(\mathcal{P})-1} = \left(\frac{\mathrm{Per}_{v\mathcal{P}}(E)}{\Gamma_p(\boldsymbol{a})/(-1)^{n(a)}}\right)^{i_{\mathcal{P}}^{-1}} \qquad \textit{in} \quad \mu(k^*) .$$

Proof. Assume, for simplicity, that $N > 3$ so $w = 2$. Let j be the modular invariant of E. There is a canonical curve $E(N)$ over H with this j-invariant. In fact, $E(N)$ can be defined over the subfield $\mathbf{Q}(j)$ and is characterized by the properties [9]:

1) $E(N)$ is isogenous over H to its conjugates by $\mathrm{Gal}(H/\mathbf{Q})$.

2) $E(N)$ has good reduction at all primes q of H not dividing N.

If ω is a differential on $E(N)$ with associated discriminant ideal $\Delta = (-N^3)$, one can derive the formula,

$$\left|\prod_{v|v_\infty} \int_{E(H_v)} \omega \wedge \bar{\omega}\right| = \left(\frac{2\pi}{N}\right)^h \prod_{0<\alpha<N} \Gamma(\alpha/N)^{\varepsilon(\alpha)} , \tag{4.14}$$

directly from the identity of Chowla and Selberg [2]. From this identity and an analysis of $E(N)$ at the real infinite place of $\mathbf{Q}(j)$, one shows that [9]

$$\mathrm{Per}_{v_\infty}(E(N)) \sim_{k^*} \Gamma(\boldsymbol{a})/(2\pi i)^{n(a)} .$$

To establish the theorem for $E = E(N)$ we must show that

$$\mathrm{Per}_{v\mathcal{P}}(E(N)) = \Gamma_p(\boldsymbol{a})/(-1)^{n(a)} \quad \text{in} \quad k_{\mathcal{P}} \tag{4.15}$$

for all primes $\mathcal{P}$ of degree 1 not dividing N.

Choose a triple (r, s, t) with $0 < r, s, t < N$, $r + s + t = N$ and $\varepsilon(r) + \varepsilon(s) + \varepsilon(t) = 1$ (this is always possible). Then the character χ of $E(N)$, when restricted to ideals $\mathcal{P}$ of k, is given by the formula

$$g(\delta_{r/N} + \delta_{s/N} - \delta_{(r+s)/N}, \mathcal{P}) = \chi(\mathcal{P})\mathbf{N}\mathcal{P}^{n(a)} .$$

Indeed, the quotient character $g/\chi \cdot \mathbf{N}^{n(a)}$ would be a quadratic *Galois* character of k, as it has trivial infinite part. Furthermore, it is ramified only at $(\sqrt{-N})$, so must be trivial by classfield theory. Theorem (1.12) and (1.4) now give an expression for g in the completion $k_{\mathcal{P}}$, which in turn yields (4.15).

Since E and $E(N)$ have the same j-invariant, they become isomorphic over some quadratic extension $H(\sqrt{\alpha})$. One then finds

$$\mathrm{Per}_{v_\infty}(E) \sim_{k^*} \sqrt{\beta}\,\frac{\Gamma(a)}{(2\pi i)^{n(a)}}$$

with $\beta = \mathbf{N}_{H/k}(\alpha)$. On the other hand, restricting the Hecke characters to k, we find

$$\chi_E = \chi_{E(N)} \cdot \psi_\beta$$

where ψ_β is the quadratic Galois character associated to the extension $k(\sqrt{\beta})$. Theorem 4.13 thus reduces to the identity:

$$(\sqrt{\beta})^{\mathrm{Frob}(\mathfrak{f})-1} = \psi_\beta(\mathcal{P}) \quad \text{in} \quad \mu(k^*)\,.$$

The case $N = 3$ is similar, but ψ may have values in 6^{th} roots of unity.

PRINCETON UNIVERSITY, PRINCETON, N. J.
HARVARD UNIVERSITY, CAMBRIDGE, MASS.

BIBLIOGRAPHY

[1] M. BOYARSKY, p-adic gamma functions and Dwork cohomology, to appear.
[2] S. CHOWLA and A. SELBERG, On Epstein's zeta-function, Crelle J. **227** (1967), 86-110.
[3] H. DAVENPORT and H. HASSE, Die Nullstellen der Kongruenz-zetafunktionen in gewissen zyklischen Fällen, J. reine angew. Math. **172** (1935), 151-182.
[4] P. DELIGNE, Applications de la formule des traces aux sommes trigonométriques, in SGA 4½, Lecture Notes in Math. 569, Springer-Verlag, Heidelberg, 1977.
[5] ———, Cycles de Hodge sur les variétés abéliennes, preprint.
[6] ———, Valeurs de fonctions L et périodes d'intégrales, to appear in Proc. A.M.S. Summer School, 1977.
[7] J. DIAMOND, The p-adic log gamma function and p-adic Euler constants, Trans. A.M.S. **233** (1977), 321-337.
[8] B. FERRERO and R. GREENBERG, On the behavior of p-adic L-functions at $s=0$, Inv. Math. **50** (1978), 91-102.
[9] B. GROSS, Thesis, Harvard University, 1978, to appear in Springer Lecture Notes.
[10] ———, On the periods of abelian integrals and a formula of Chowla and Selberg, Invent. Math. **45** (1978), 193-211.
[11] N. KATZ, LETTERS to T. HONDA, 7 Nov. 1971 and to N. Koblitz, 22 Feb. 1978; the results of which will appear in a forthcoming article.
[12] N. KOBLITZ, A short course on some current research in p-adic analysis (talks given at the Hanoi Mathematical Institute in July, 1978), to appear.
[13] D. KUBERT, The universal ordinary distribution of $\mathbf{Q}^k/\mathbf{Z}^k$, to appear.
[14] S. LANG, *Cyclotomic Fields*, Springer-Verlag, 1978.
[15] Y. MORITA, A p-adic analogue of the Γ-function, J. Fac. Science Univ. Tokyo, **22** (1975), 255-266.
[16] G. OVERHOLTZER, Some functions in elementary p-adic analysis, Amer. J. Math. **74** (1952), 332-346.
[17] A. WEIL, La cyclotomie jadis et naguère, Sém. Bourbaki 452, June 1974, Lecture Notes in Math. 431, Springer-Verlag, 1975.
[18] ———, Jacobi sums as Grössencharaktere, Trans. A.M.S. **73** (1952), 487-495.

(Received April 26, 1978)