Advanced Studies in Pure Mathematics 12, 1987
Galois Representations and Arithmetic Algebraic Geometry
pp. 21–52

The Gross-Koblitz Formula

Robert F. Coleman

§ 0. Introduction

Our intent in this note is to give a relatively self-contained and not completely ad hoc proof of the beautiful formula discovered by Gross and Koblitz [G-K] expressing Gauss sums in terms of Morita's p-adic gamma function. In fact we give two proofs.

The first is nothing more than a reorganization of that given by Boyarski in [B], who observed that the Gross-Koblitz formula could be recovered easily from results in a series of papers by Dwork. In this proof one makes use of Dwork cohomology spaces of the most elementary sort. These spaces are ultimately connected to the geometry of the Fermat curves but this connection is neither made explicit nor used in this note (see the appendix however). Unfortunately, this proof fails to work when $p=2$.

Our second proof was motivated by the first. It is more elementary in that it avoids the Dwork cohomology. Also, it does work when $p=2$.

A key ingredient in both proofs is formula (9) of Section II below, which is a formal version of Euler's integral representation of the classical gamma function. Other proofs of the Gross-Koblitz formula may be found in [K] and [L].

We will now state the Gross-Koblitz formula. Let $\boldsymbol{N}$ donote the natural numbers and $\boldsymbol{N}^*$ the positive integers. Let p be a prime. Let $\boldsymbol{C}_p$ denote the completion of an algebraic closure of $\boldsymbol{Q}_p$, the field of p-adic numbers. Let $q=p^f$ where $f \in \boldsymbol{N}^*$. Let $\boldsymbol{F}_q$ denote the field of order q contained in the residue field of $\boldsymbol{C}_p$. Let $t\colon \boldsymbol{F}_q \to \boldsymbol{C}_p$ denote the Teichmüller character on $\boldsymbol{F}_q$. That is, $t(x)$ is the unique element of $\boldsymbol{C}_p$ which reduces to x and satisfies $t(x)^q=t(x)$. It is a multiplicative character on $\boldsymbol{F}_q^*$. Fix a solution of $\pi^{p-1}=-p$ in $\boldsymbol{C}_p$, and let ζ_π denote the unique p^{th} root of unity in $\boldsymbol{C}_p$ satisfying

$$|\zeta_\pi-(1+\pi)|<|\pi|.$$

Set for $x \in \boldsymbol{F}_q$

$$\omega_q(x)=\zeta^{\mathrm{Trace}_{F_q/F_p}(x)}.$$

Received October 14, 1985.

Then $\omega_q(x)$ is a non-trivial additive character on $\boldsymbol{F}_q$. For $b \in \boldsymbol{Q}/\boldsymbol{Z}$, we let $\langle b\rangle$ denote its representative in [0, 1). If $(q-1)b=0$ we set

$$g_q(b)=-\sum_{x\in\boldsymbol{F}_q} t(x)^{(1-q)\langle b\rangle}\omega_q(x).$$

Then $g_q(b)$ is a Gauss sum. We also set

$$S_q(b)=(p-1)\sum_{i=0}^{f-1}\langle p^i b\rangle.$$

Note that this is the sum of the p-adic digits of $(q-1)\langle b\rangle$, and so lies in $\boldsymbol{N}$.

Next for $n \in \boldsymbol{N}^*$, set

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

Morita [Mo] has shown and we shall show below that Γ_p extends uniquely to a continuous function on $\boldsymbol{Z}_p$. The Gross-Koblitz formula is now

$$g_q(b)=\pi^{S_q(b)}\prod_{i=0}^{f-1}\Gamma_p(\langle p^i b\rangle).$$

In the last section, we use this formula together with the Gauss multiplication formula to deduce generalizations of the Hasse-Davenport relation for Gauss sums. In the appendix we compute the Frobenious matrix of the Fermat curves in two ways.

I. Standard Results

§ 1. Mahler series

Let M denote the $\boldsymbol{C}_p$-vector space of series of the form

$$F(z)=\sum_{n=0}^{\infty} a_n\binom{z}{n}, \qquad a_n \in \boldsymbol{C}_p.$$

For $m \in \boldsymbol{N}$, the series $F(m)$ has only a finite number of nonzero terms and hence converges. In fact the map $F(z)\mapsto(m\mapsto F(m))$ gives a bijection between M and the space of functions from $\boldsymbol{N}$ into $\boldsymbol{C}_p$. Henceforth we shall identify these two spaces. Since the latter space has a natural ring structure, so does M. We define for F as above

$$F^*(T)=\sum_{n=0}^{\infty} a_n\frac{T^n}{n!},$$

$$\hat{F}(T)=\sum_{n=0}^{\infty} F(n)\frac{T^n}{n!}$$

as a power series over C_p. Both "*" and "^" give bijections from M onto $C_p[[T]]$, the ring of power series over C_p.

Lemma 1. *Let $F \in M$. Then*

i) $T\frac{d}{dT}\hat{F}=\widehat{TF(z+1)}=\widehat{zF(z)}$;

ii) $F^*+\frac{d}{dT}F^*=(F(z+1))^*$;

iii) $\exp(T)F^*(T)=\hat{F}(T)$.

Proof.

$$\frac{Td}{dT}\hat{F}(T)=\sum_{n=0}^{\infty} F(n)\frac{T^n}{(n-1)!}=\sum_{n=0}^{\infty}(nF(n))\frac{T^n}{n!}=T\sum_{n=0}^{\infty} F(n+1)\frac{T^n}{n!}$$

which proves (i). Next if $F(T)=\sum_{n=0}^{\infty} b_n\binom{T}{n}$,

$$\begin{aligned}F^*(T)+\frac{d}{dT}F^*(T)&=\sum b_n\left(\frac{T^n}{n!}+\frac{T^{n-1}}{(n-1)!}\right)\\&=\left(\sum b_n\left(\binom{T}{n}^*+\binom{T}{n-1}^*\right)\right)\\&=\left(\sum b_n\binom{T+1}{n}\right)^*=F(T+1)^*.\end{aligned}$$

Here we used the continuity and linearity of "*". This gives (ii). Finally, using (i), (ii) and induction, we have

$$\begin{aligned}\left(\frac{d}{dT}\right)^n(\exp(T)F^*(T))|_{T=0}&=\exp(T)F(T+n)^*|_{T=0}\\&=F(n)\\&=\widehat{F(T+n)}|_{T=0}\\&=\left(\frac{d}{dT}\right)^n\hat{F}(T)|_{T=0}.\end{aligned}$$

This gives (iii).

If $r \in \boldsymbol{R}$, we say $F \in M$ has radius of convergence r if the series $F(z)$ converges for all $z \in C_p$, $|z-N|<r$. By the open disk of radius r we

mean the set $\{z \in C_p\colon |z|<r\}$.

Proposition 2. *Let $r \in R$ and $H \in M$. Then H has radius of convergence r iff H^* has radius of convergence* $\mathrm{Max}\{r^{1/p}, r\}$.

Proof. Suppose $z \in C_p$ and $|z-N|\le r$. Then

$$\left|\binom{z}{n}\right|=\left|\frac{1}{n!}\right||z(z-1)\cdots(z-(n-1))| \tag{1}$$
$$\le\left|\frac{1}{n!}\right|\begin{cases} r^{[n/p]}, & \text{if } r<1\\ r^{n}\quad, & \text{if } r\ge 1.\end{cases}$$

Now suppose

$$H^*(T)=\sum_{n=0}^{\infty} b_n\frac{T^n}{n!}.$$

Then $H^*(T)$ has radius of convergence s iff

$$\frac{|b_n|}{n!}t^n\longrightarrow 0, \qquad 0\le t<s. \tag{2}$$

As $H(z)$ must equal $\sum_{n=0}^{\infty} b_n\binom{z}{n}$ the proposition follows from (1) and (2).

§ 2. The Dwork exponential

Now fix a solution π of $\pi^{p-1}=-p$ in C_p. Let exp (T) denote the exponential power series. It is well known that exp (T) converges on the open disk of radius $|\pi|$. Set, for $q \in N^*$,

$$\theta_q(T)=\exp(\pi T-\pi T^q).$$

Then, a priori, this series converges only on the open disk of radius one. However,

Lemma 3 (Dwork). *Let $q=p^f$ for some $f \in N^*$. The series $\theta_q(T)$ converges on the open disk of radius*

$$|p|^{(1-p)/pq}$$

and is bounded by one on this disk. Moreover,

$$\theta_q(T)\equiv 1+\pi(T+T^p+\cdots+T^{p^{f-1}}) \mod \pi^2R[[T]] \tag{3}$$

where $R=\boldsymbol{Z}_p[\pi]\subseteq\boldsymbol{C}_p$.

Proof. As $\theta_q(T)=\theta_p(T)\theta_p(T^p)\cdots\theta_p(T^{p^{f-1}})$, it suffices to prove the lemma for $q=p$. First it is well known that $\exp(T)$ is bounded by one on the disk of radius $|\pi|$. Second it is well known that the Artin-Hasse exponential

$$\exp\left(\sum_{n=0}^{\infty}\frac{T^{p^n}}{p^n}\right)=A(T)$$

has coefficients in $\boldsymbol{Z}_p$ and hence converges on the disk of radius one where it is bounded by one. Now,

$$\theta_p(T)=A(\pi T)\prod_{n=2}^{\infty}\exp\left(\frac{-(\pi T)^{p^n}}{p^n}\right)^{-1} \tag{4}$$

so $\theta_p(T)$ converges on the intersection of the disks of convergence of all the terms on the right-hand side and is bounded by one on this disk. An easy calculation shows that this disk has radius at least

$$\min_{n\geq 2}\{|p|^{-1/(p-1)},|p|^{(n(p-1)+1-p^n)/n^n(p-1)}\}=|p|^{(1-p)/p^2}.$$

The congruence (3) follows immediately from (4) and the fact that $\exp(\pi T)\in R[[T]]$, since it is bounded by one on the unit disk.

For $x\neq 0$ in the residue field of $\boldsymbol{C}_p$ let $t(x)$ denote the unique root of unity of order prime to p whose reduction is x. We also set $t(0)=0$. This coincides on $\boldsymbol{F}_q$ with the "t" defined in the Introduction.

Lemma 4 (Dwork). *Let* $q=p^f$ *for some* $f\in\boldsymbol{N}^*$. *Then for* $x\in\boldsymbol{F}_q$,

$$\theta_q(t(x))=\omega_q(x)$$

where ω_q *is as defined in the Introduction.*

Proof. First we observe that

$$\theta_q(T)^p=\exp(\pi p(T-T^q)).$$

Since $\exp(\pi pT)$ converges on a disk of radius greater than one, the function $\theta_q(T)^p$ is the composition of the functions $\exp(\pi pT)$ and $T-T^q$. It follows that if $x\in\boldsymbol{F}_q$,

$$\theta_q(t(x))^p=1.$$

Hence $\theta_q(t(x))$ is a p^{th} root of unity. Since different p^{th} roots of unity are not congruent modulo π^2 the rest of the lemma follows immediately from (3).

Now for $b \in \boldsymbol{Q}/\boldsymbol{Z}$, we let $\langle b \rangle$ denote its unique representative in the interval $[0, 1)$. Suppose $q=p^f$ is such that $(q-1)b=0$. Then it follows from the previous lemma that

$$g_q(b) = -\sum_{\varepsilon^q=\varepsilon} \varepsilon^{(1-q)\langle b \rangle}\theta_q(\varepsilon). \tag{5}$$

In fact, if

$$\theta_q(T) = \sum_{n=0}^{\infty} A_n T^n$$

we have from (5),

Corollary 4.1. $(1/(1-q))g_q(b) = \sum_{r=0}^{\infty} A_{(q-1)(r+\langle b \rangle)}$.

II. The p-Adic Gamma Function

We first define an element $G \in M$ by setting

$$G(pn+a) = (-1)^{n+a} \frac{p^n(n!)}{(pn+a)!} \in \boldsymbol{Z}_p^* \tag{6}$$

for $a, n \in \boldsymbol{N}$, $0 \leq a < p$. For $F \in M$, a $\in \boldsymbol{N}$, $0 \leq a < p$, we set

$$\gamma_a(F)(z) = F(pz+a)(-\pi)^a$$

so that $\gamma_a F \in M$. For a Laurent series

$$H(T) = \sum_{n=-\infty}^{\infty} a_n T^n, \qquad a_n \in \boldsymbol{C}_p$$

and a natural number $q > 0$, we set

$$\psi_q(H)(T) = \sum_{r=-\infty}^{\infty} a_{qr} T^r.$$

Note that:

$$\psi_{q/p}(F(T)\psi_p(G(T))) = \psi_q(F(T^p)G(T))$$

and

$$\psi_q(F(T^q)G(T)) = F(T)\psi_q(G(T)).$$

Proposition 5. *For $a \in N$, $0 \leq a < p$ and $F \in M$ we have*

$$\psi_p(\hat{F}(\pi T)T^{-a}) = \widehat{\gamma_a(GF)}(\pi T).$$

Proof. Clearly

$$\begin{aligned}\psi_p(\hat{F}(\pi T)T^{-a}) &= \sum_{n=0}^{\infty} \frac{\pi^{pn+a}}{(pn+a)!} F(pn+a)T^n \\ &= (-\pi)^a \sum_{n=0}^{\infty} \frac{(-1)^a(\pi^{p-1})^n n!\,F(pn+a)}{(pn+a)!} \frac{(\pi T)^n}{n!} \\ &= (-\pi)^a \sum_{n=0}^{\infty} \frac{(-1)^{n+a} p^n n!\,F(pn+a)}{(pn+a)!} \frac{(\pi T)^n}{n!}.\end{aligned}$$

The result follows.

Corollary 5.1. $\psi_p(\theta_p(T)T^{-a}) = (\gamma_a G)^*(\pi T)$.

Proof. If we take $F = 1$ in the previous lemma then $\hat{F}(\pi T) = \exp(\pi T)$ and so

$$\psi_p(\exp(\pi T)T^{-a}) = \widehat{\gamma_a G}(\pi T). \tag{7}$$

Now multiply on both sides by $\exp(-\pi T)$ and apply Lemma 1.

Corollary 5.2. *The Mahler series $\gamma_a G$ has radius of convergence*

$$|p|^{(1-p)/p+1/(p-1)} > 1$$

if $p > 2$ and $|2|$ if $p = 2$. The Mahler series G has radius of convergence

$$|p|^{1/p+1/(p-1)}$$

if $p > 2$ and $|4|$ if $p = 2$. Moreover, for z in the domain of convergence of G, $|G(z)| = 1$.

Proof. We use Proposition 2 and Lemma 3 together with the fact that ψ_p raises radii of convergence to the p^{th} power. The last statement follows from the corresponding fact for $\theta_p(T)$.

Now, set, as Mahler series

$$\Gamma_p(z) = -G(z-1)^{-1} \qquad p > 2$$

and

$$\Gamma_p(z) = (-1)^{\{(z+1)/2\}} G(z-1)^{-1} \qquad p = 2$$

where {*} denotes the 2-adic integral part.*) It is easy to see that $\Gamma_p(z)$ has the same radius of convergence as G and that

$$\Gamma_p(n)=(-1)^n \prod_{\substack{k=1 \\ (k,p)=1}}^{n-1} k \tag{8}$$

for $n \in N^*$. Formula (7) now becomes

$$\frac{1}{p}\sum_{\zeta^p=1} (\exp(-\zeta T)(\zeta T)^{-a})=\widehat{-\Gamma_p(pz+a)^{-1}}(-T^p) \tag{9}$$

which can be thought of as a formal version of Euler's integral representation of the classical Γ-function.

Suppose $a \in N$ and

$$a=a_f+a_{f-1}p+\cdots+a_1p^{f-1}$$

where $0 \leq a_i < p$. Then we set $S(a)=a_1+a_2+\cdots+a_f$.

Corollary 5.3. *Let a be as above and $q=p^f$. Then*

$$\psi_q(\theta_q(T)T^{-a})=G_a^*(\pi T) \tag{10}$$

where

$$\begin{aligned} G_a(z)&=(-\pi)^{S(a)} \prod_{i=1}^{f} G\left(p^i z+\sum_{j=1}^{i} p^{i-j} a_j\right) \\ &=\gamma_{a_1}(G\gamma_{a_2}(G\gamma_{a_3}(\cdots G\gamma_{a_f}(G)\cdots)))(z). \end{aligned}$$

Proof. As $\psi_q(\theta_q(T)T^{-b})=\psi_{q/p}(\theta_{q/p}(T)(\psi_p(\theta_p(T)T^{-b})))$ and

$$\psi_p(T^{np}F(T))=T^n\psi_p(F(T)),$$

the result follows from Proposition 5, Corollary 5.1 and Lemma 1 by induction.

Corollary 5.4. $G_a(z)=\sum_{n=0}^{\infty}(A_{qn+a}n!/\pi^n)\binom{z}{n}$.

Proof. This follows immediately from Lemma 1 and (10).

Proposition 6. *The function $\Gamma_p(z)$ satisfies, on its region of convergence, the following functional equations*

*) This proof of the existence of the Γ-function is essentially the same as that of Barski, [L] p. 82.

$$(11) \qquad \Gamma_p(z+1)=\begin{cases} -z\Gamma_p(z) & |z|=1 \\ -\Gamma_p(z) & |z|<1 \end{cases}$$

and

$$(12) \qquad \Gamma_p(z)\Gamma_p(1-z)=(-1)^{l(z)}$$

where $l(z)$ is the unique element in $\{1, 2, \cdots, p\}$ such that $|z-l(z)|<1$ if $p>2$ and $l(z)=\{(z+2)/2\}$ if $p=2$. (Here $\{*\}$ denotes the 2-adic integral part.)

Proof. The functional equation (11), for $z \in N^*$ follows immediately from (8). Since $\Gamma_p(z)$ is analytic on a finite union of disks, each of which contains infinitely many elements of N, these equations hold for all z in this region.

Next let $H(z)=\Gamma_p(z)\Gamma_p(1-z)$. Then

$$H(z+1)=\Gamma_p(z+1)\Gamma_p(-z)=\begin{cases} -H(z) & \text{if } |z|=1 \\ H(z) & \text{if } |z|<1 \end{cases}$$

using (11). It follows that for $z \in N^*$,

$$H(z)=(-1)^{k(z)-1}H(1)=(-1)^{k(z)}$$

where $k(z)=(z-[(z-1)/p])\equiv l(z) \bmod 2$. The result now follows for all z by an analytic density argument as above.

Corollary 6.1. *Suppose $b \in Q/Z$ such that $(q-1)b=0$. If $a=(q-1)\langle b\rangle$, then*

$$G_a(-\langle b\rangle)=\pi^{S_q(b)}\prod_{i=0}^{f-1}\Gamma_p(\langle p^i b\rangle).$$

Proof. As

$$p^i\langle b\rangle-\langle pib\rangle=\sum_{j=1}^{i}p^{i-j}a_j$$

we have

$$\begin{aligned} G_a(-\langle b\rangle)&=(-\pi)^{S_q(b)}\prod_{i=1}^{f}((-1)^{r_i}\Gamma_p(1-\langle p^i b\rangle)^{-1}) \\ &=(-1)^r\pi^{S_q(b)}\prod_{i=1}^{f}\Gamma_p(\langle p^i b\rangle) \end{aligned}$$

where $r_i=1$ if p is odd and $r_i=\{(2-\langle p^i b\rangle)/2\}$ when $p=2$. Using the functional equation (12) where

$$r=S_q(b)+\sum_{i=1}^{f}(l(\langle p^ib\rangle)+r_i).$$

Now $S_q(b)=a_1+a_2+\cdots+a_f$, where $a_i=p\langle p^{i-1}b\rangle-\langle p^ib\rangle$. Hence $\langle p^ib\rangle\equiv \mathrm{a}_i \bmod p$. As $-p<-a_i\leq 0$, $l(\langle p^ib\rangle)=p-a_i$ when $p>2$ and so in this case $r_i=1$ and $((\langle p^ib\rangle)+r_i\equiv -a_i \bmod p$. When $p=2$,

$$\left\{\frac{\langle 2^ib\rangle+2}{2}\right\}+\left\{\frac{2-\langle 2^ib\rangle}{2}\right\}=2+\left\{\frac{a_i}{2}\right\}+\left\{\frac{-a_i}{2}\right\}\equiv -a_i \bmod 2.$$

The result follows in both cases.

III. Dwork Spaces and Operators; First Proof, $p>2$

For $b\in \boldsymbol{Q}/\boldsymbol{Z}$, let $\langle b\rangle$ denote its unique representative in $[0,1)$. Suppose $\langle b\rangle=j/m$ in lowest terms. (In the future when we write an equation of the form $\langle b\rangle\doteq j/m$ we will mean that j, $m\in \boldsymbol{N}$ and are relatively prime.) We define the map $l_b\colon M\to \boldsymbol{C}_p[[T]]$ by setting

$$l_b(H)(T)=H^*(\pi T^m)T^j.$$

Fix $m\in \boldsymbol{N}^*$, $(m,p)=1$ and set for $F\in \boldsymbol{C}_p[[T]]$

$$D=\frac{Td}{dT}+m\pi T^m$$

$$\phi_q(F)=\psi_q(\theta_q(T^m)F)$$

as

$$\psi_q\circ\frac{Td}{dT}=q\frac{Td}{dT}\circ\psi_q$$

and

$$D=\exp(-\pi T^m)\frac{Td}{dT}\exp(\pi T^m)$$

$$\phi_q=\exp(-\pi T^m)\psi_q\exp(\pi T^m)$$

we have

$$\phi_q\circ D=qD\circ\phi_q. \tag{14}$$

Lemma 7. *Let $b\in \boldsymbol{Q}/\boldsymbol{Z}$. Suppose $\langle b\rangle\doteq j/m$. Then*

$$Dl_bF=l_b((mT+j)F)\qquad \textit{for } F\in M.$$

Proof. By Lemma 1,

$$\begin{aligned} Dl_bF &= \exp(-\pi T^m)\frac{Td}{dT}\exp(\pi T^m)F^*(\pi T^m)T^j \\ &= \exp(-\pi T^m)\frac{Td}{dT}\hat{F}(\pi T^m)T^j \\ &= \exp(-\pi T^m)(m\widehat{(TF)}(\pi T^m)+j\hat{F}(\pi T^m))T^j \\ &= \exp(-\pi T^m)\widehat{(mT+j)F}(\pi T^m)T^j \\ &= ((mT+j)F)^*(\pi T^m)T^j. \end{aligned}$$

We define the subspace L_b of $C_p[[T]]$ to be the subspace consisting of all power series F of radius of convergence strictly greater than $|\pi|^{-1/m}$ which satisfy

$$H(\varepsilon T)=\varepsilon^j H(T) \tag{13}$$

for any m^{th} root of unity ε.

Also let M^1 denote the subspace of M consisting of all Mahler series of radius of convergence strictly greater than one. It follows from Proposition 2 that $l_b: M^1 \stackrel{\sim}{\to} L_b$. We now have immediately from the previous lemma,

Corollary 7.1. *$DL_b \subseteq L_b$ and L_b/DL_b is one-dimensional.*

For the rest of this section we suppose $p>2$.

Proposition 8. *For $F \in M$, $b \in \underline{Q}/Z$, $\langle b\rangle \doteq j/m$, $a=p\langle b\rangle-\langle pb\rangle$ and Γ_a as in Section* II *we have*

$$\phi_p l_{pb}F=l_b((\Gamma_a(GF)). \tag{15}$$

Proof. This is just a direct translation of Proposition 5 into our current language.

Thus on the Mahler space, the Dwork operator looks like a twisted multiplication by $-\Gamma_p(1+z)^{-1}$.

Corollary 8.1. *If $\langle b \doteq j/m\rangle$, $(m,p)=1$, then $\phi_p L_{pb} \subseteq L_b$.*

Proof. Let $F \in M$. It follows immediately from Corollary 5.2 that $\Gamma_a(GF)$ has radius of convergence strictly greater than one, as $p>2$. The corollary is thus an immediate consequence of (15) and the fact that $l_b\colon M^1 \to L_b$ is an isomorphism.

At this point we have the commutative diagram

$$\begin{tikzcd}
M^1/(mz+j')M^1 \arrow[r, "F\mapsto\gamma_a(GF)"] \arrow[d, "l_{pb}"', "\wr"] & M^1/(mz+j)M^1 \arrow[d, "l_b"', "\wr"] \\
L_{pb}/DL_{pb} \arrow[r, "\phi_p"] & L_b/DL_b
\end{tikzcd}$$

where $a=p\langle b\rangle-\langle pb\rangle$ and $\langle pb\rangle \doteq j'/m$. Now for $H \in M^1$ we have

$$H(z) \equiv H\left(-\frac{j}{m}\right) \quad \text{mod } (mz+j)M^1.$$

Hence

$$\begin{aligned}
\phi_p(T^{j'}) = \phi_p l_{pb}(1)) &= (l_b(\gamma_a(G)) \\
&\equiv l_b(\gamma_a G(-\langle b\rangle)) \quad \text{mod } DL_b \\
&\equiv l_b(G(-\langle pb\rangle)(-\pi)^q) \quad \text{mod } DL_b \\
&\equiv (-\pi)^q G(-\langle pb\rangle)T^j \quad \text{mod } DL_b.
\end{aligned}$$

In fact we have

Corollary 8.2. *Suppose $q=p^f$, $f \in N^*$, and $(q-1)b=0 \in Z$. Then the eigenvalue of ϕ_q acting on L_b/DL_b is $G_{(q-1)\langle b\rangle}(-\langle b\rangle)$.*

Proof. This follows by induction from the previous result using the fact that $(q-1)\langle b\rangle = a_f + a_{f-1}p + \cdots + a_1 p^{f-1}$ where $a_i = p\langle p^{i-1}b\rangle - \langle p^i b\rangle$.

Theorem 9 (Gross-Koblitz). *Let $b \in \underline{Q}/Z$, $q=p^f$, $(q-1)b=0$. Then*

$$g_q(b) = \pi^{S_q(b)} \prod_{i=0}^{f-1} \Gamma_p(\langle p^i b\rangle).$$

(*Recall*

$$g_q(b) = -\sum_{\varepsilon^q=\varepsilon} \varepsilon^{(1-q)\langle b\rangle}\theta_q(\varepsilon).)$$

Proof. We will compute the "trace" of ϕ_q acting on L_b in two different ways. Set $a=(q-1)\langle b\rangle$.

First we deduce that

$$\begin{aligned}\phi_q D^n T^j &= q^n D^n \phi_q T^j \\ &\equiv q^n G_a(-\langle b\rangle)T^j \mod D^{n+1}L_b.\end{aligned}$$

Hence the trace of ϕ_q on L_b, with respect to the "basis" $\{D^n T^j\}$, is

$$\sum_{n=0}^{\infty} q^n G_a(-\langle b\rangle) = \frac{1}{1-q} G_a(-\langle b\rangle). \tag{16}$$

On the other hand, if we write

$$\theta_q(T) = \sum_{n=0}^{\infty} A_n T^n$$

then

$$\begin{aligned}\phi_q(T^{mk+j}) &= \psi_q\left(\sum_{n=0}^{\infty} A_n T^{m(n+k)+j}\right) \\ &= \sum_{r=0}^{\infty} A(r, k) T^{mr+j}\end{aligned}$$

where $A(r, k) = A_{qr+a-k}$. Hence the trace of ϕ_q with respect to the "basis" $\{T^{mr+j}\}$ is

$$\sum_{k=0}^{\infty} A(k, k) = \sum_{k=0}^{\infty} A_{(q-1)k+a} = \frac{1}{1-q} g_q(b)$$

by Corollary 4.1. We shall show that, at least for these two "bases", the trace is independent of the choice of basis. The theorem will follow from this and Corollary 6.1.

The vector space $V_n = L_b/D^n L_b$ has dimension n and the image of $\{D^i x^j : 0 \leq i < n\}$ is a basis for V_n. It follows that the image B_n of $\{(\pi T^m)^i x^j : 0 \leq i < n\}$ is also a basis. By (14) and Corollary 8.1, ϕ_q acts on these vector spaces and, by what we showed above,

$$\lim_{n\to\infty} \text{Trace}\,(\phi_q;\, V_n) = \frac{1}{1-q} G_a(-\langle b\rangle).$$

To complete the proof it suffices to check that

$$\lim_{n\to\infty}\left(\text{Trace}\,(\phi_q;\, V_n) - \sum_{k=0}^{n-1} A(k, k)\right) = 0. \tag{17}$$

For this we will estimate this trace using the basis B_n. Set

$$\nu_r = \frac{(\pi T^m)^r T^i}{r!}.$$

We have

$$\phi_q(v_k)=\sum_{r=0}^{\infty}\frac{A(r,k)r!}{\pi^{rk}k!}v_r=\left(\sum_{r=0}^{\infty}\frac{A(r,k)r!}{\pi^{r-k}k!}\binom{T}{r}\right)^*.$$

Clearly

$$r!\binom{T}{r}\equiv\sum_{i=0}^{n-1}i!b_i\binom{T}{i} \quad \mod (mT+j)^n$$

for some $b_i \in \boldsymbol{Z}[1/m]\subseteq\boldsymbol{Z}_p$ since the polynomials $i!\binom{T}{i}$ are monic. Hence using Lemma 7 again

$$\phi_q(v_k)\equiv\sum_{i=0}^{n-1}B_k(r,k)v_r \quad \mod D^nL_b$$

where

$$\text{(18)} \qquad \operatorname{ord}_p(B_n(k,k)-A(k,k))\geq\min_{r\geq n}\left(\operatorname{ord}_p\left(\frac{A(r,k)}{\pi^{r-k}}\right)\right).$$

Meanwhile, the fact that $\theta_q(T)$ is bounded by one on the disk of radius $|p|^{(1-p)/pq}$ implies

$$\operatorname{ord} A_n\geq n\left(\frac{p-1}{qp}\right)$$

so

$$\begin{aligned}\operatorname{ord}_p\left(\frac{A(r,k)}{\pi^{r-k}}\right)&\geq(qr+a--k)\frac{p-1}{pq}+(r-k)\frac{-1}{p-1}\\ &\geq r\left(\frac{p-1}{1}-\frac{1}{p-1}\right)+a\frac{p-1}{pq}+k\left(\frac{1}{p-1}-\frac{p-1}{pq}\right)\\ &\geq n\left(\frac{p-1}{p}-\frac{1}{p-1}\right)\end{aligned}$$

for $r\geq n$. Since $p>2$, $(p-1)/p-1/(p-1)>0$, so the right-hand side of (18) tends to infinity with n which establishes (17) and proves the theorem.

IV. Second Proof

By Corollaries 4.1, 5.4, and 6.1, to prove the Gross-Koblitz formula it suffices to prove

$$\sum_{r=0}^{\infty}\frac{A_{qr+a}r!}{\pi^r}\binom{-\langle b\rangle}{r}=\sum_{k=0}^{\infty}A_{(q-1)k+a} \tag{19}$$

where $a=(p-1)\langle b\rangle$ and $\theta_q(T)=\sum_{n=0}^{\infty}A_nT^n$. For this set

$$G_a(z)=\sum_{r=0}^{\infty}\frac{A_{qr+a}r!}{\pi^r}\binom{z}{r}. \tag{20}$$

We have seen in Section II that this is a Mahler series with a positive radius of convergence if $0\leq a<q$. From the relation

$$\frac{A_{qr+a+q}r!}{\pi^r}\binom{z}{r}=\frac{A_{q(r+1)+a}(r+1)!}{\pi^{r+1}}\binom{z+1}{r+1}\cdot\frac{\pi}{z+1}.$$

We deduce that

$$G_{a+q}(z)=\frac{\pi}{z+1}(G_a(z+1)-A_a).$$

In particular for $a\in N$, the series $G_a(z)$ has a positive radius of convergence. Set $A(r, n)=A_{qr+(q-1)(\langle b\rangle+n)}$.

Lemma 9.1. *Set* $a_n=(q-1)(\langle b\rangle+n)$. *Then*

$$G_{a_n}(-(\langle b\rangle+n))=G_{a_{n+1}}(-(\langle b\rangle+n+1))+(1-q)A(0, n).$$

Proof. Let $\langle b\rangle\doteq j/m$. Set $k=ms+j$, $s\geq0$. Then we have the relation

$$\phi_qD(T^k)=q\phi_qD(T^k).$$

We shall expand this out. The left-hand side equals

$$\begin{aligned}\psi_q\sum_{n=0}^{\infty}(kA_n+m\pi A_{n-1})T^{nm+k}&=\sum_{r=0}^{\infty}(kA_{qr+a_s}+m\pi A_{qr+a_s-1})T^{rm+k}\\&=\sum_{r=0}^{\infty}((ms+j)A(r, s)+m\pi A(r+1, s+1))T^{rm+k}.\end{aligned}$$

The right-hand side equals

$$\begin{aligned}qD\left(\sum_{r=0}^{\infty}A_{qr+a_s}T^{mr+k}\right)&=\sum_{r=0}^{\infty}(q((mr+k)A_{qr+a_s}+m\pi A_{q(r-1+a_s)})T^{mr+k})\\&=\sum_{r=0}^{\infty}q((m(r+s)+j)A(r, s)+m\pi A(r-1, s))T^{mr+k}.\end{aligned}$$

Comparing coefficients yields

$$\frac{-(\langle b\rangle+s)}{\pi}A(r,s)=A(r-1,s+1)-q\left(\frac{\langle b\rangle+r+s}{\pi}A(r,s)+A(r-1,s)\right).$$

Hence

$$\begin{aligned}\frac{A(r,s)r!}{\pi^r}&\binom{-(\langle b\rangle+s)}{r}\\ &=\frac{-(\langle b\rangle+s)}{\pi}A(r,s)\left(\frac{r!}{-\pi^{r-1}(\langle b\rangle+s)}\binom{-(\langle b\rangle+s)}{r}\right)\\ &=\frac{A(r-1,s+1)(r-1)!}{\pi^{r-1}}\binom{-(\langle b\rangle+s+1)}{r-1}\\ &\quad+q\frac{A(r,s)r!}{\pi^r}\binom{-(\langle b\rangle+s+1)}{r}\\ &\quad-q\frac{A(r-1,s)}{\pi^{r-1}}(r-1)!\binom{-(\langle b\rangle+s+1)}{r-1}.\end{aligned}$$

Now summing both sides from $r=1$ to ∞ gives us the lemma.

Proof of (19). Let $a=(q-1)\langle b\rangle$. Then by induction we have

$$G_a(-\langle b\rangle)=(1-q)\sum_{r=0}^{n-1}A(0,r)+G_{a_n}(-(\langle b\rangle+n)).$$

As $A(0,r)=A_{qr+a}$, it suffices to prove

$$\lim_{n\to\infty}G_{a_n}(-(\langle b\rangle+n))=0. \tag{21}$$

From (20), clearly

$$\begin{aligned}\operatorname{ord}_p G_{a_n}(-(\langle b\rangle+n))&\geq\min_{r\geq 0}\left(\operatorname{ord}_p A(r,n)+\operatorname{ord}_p r!-\frac{r}{p-1}\right)\\ &\geq\min_{r\geq 0}\left((qr+a_n)\frac{p-1}{pq}+\operatorname{ord}_p r!-\frac{r}{p-1}\right)\\ &=\min_{r\geq 0}\left(r\left(\frac{p-1}{p}-\frac{1}{p-1}\right)+\operatorname{ord}_p r!\right.\\ &\quad\left.+n\frac{(p-1)(q-1)}{pq}+a\frac{p-1}{pq}\right)\\ &\geq\min_{r\geq 0}\left(r\left(\frac{p-1}{p}-\frac{1}{p-1}\right)\right.\\ &\quad\left.+\operatorname{ord}_p r!+n\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right)\right).\end{aligned}$$

As $r((p-1)/p-1/(p-1))+\mathrm{ord}_p r!>-1/2$ for all p, this last expression tends to infinity with n which proves (21) and so also the Koblitz-Gross formula.

V. Final Remarks

Corollary 5.2 implies that for $z, z' \in \boldsymbol{Z}_p$,

$$\Gamma_p(z) \equiv \Gamma_p(z') \quad \bmod (z-z')\boldsymbol{Z}_p$$

if $p>2$ and

$$\Gamma_2(z) \equiv \Gamma_2(z') \quad \bmod \left(\frac{z-z'}{2}\right)\boldsymbol{Z}_2.$$

From this we can deduce Stickleberger's theorem for the "leading term" of the Gauss sum,

$$g_q(b) \sim \prod_{i=1}^{f} a_i! \cdot \pi^{S_q(b)},$$

where $a_i = p\langle p^{i-1}b\rangle - \langle p^i b\rangle$. Another immediate corollary is

$$g_{q^n}(b) = (g_q(b))^n.$$

We shall now recall the Gauss multiplication formula for the p-adic gamma function and, as Boyarski recommends [B], derive some of its consequences for the Gauss sums. For $a=(a_0, a_1) \in \boldsymbol{Z}_p \times \boldsymbol{Z}$ and $x \in \boldsymbol{Z}_p^*$ we set

$$x^a = (x^{p-1})^{a_0} x^{a_1} \in \boldsymbol{Z}_p^*$$

so that $(x, a) \mapsto x^a$ is a bilinear, bicontinuous pairing from $\boldsymbol{Z}_p^* \times (\boldsymbol{Z}_p \times \boldsymbol{Z})$ into $\boldsymbol{Z}_p^*$,with $\boldsymbol{Z}$ given the discrete topology. Clearly $x^a \equiv x^{a_1} \bmod p$. We consider $\boldsymbol{Z}$ as a subgroup of $\boldsymbol{Z}_p \times \boldsymbol{Z}$ embedded diagonally. Also set

$$a' = (p-1)a_0 + a_1 \in \boldsymbol{Z}_p.$$

If $n \in \boldsymbol{Z}$ such that $na_0 \in \boldsymbol{Z}$, then

$$(x^a)^n = x^{na'}.$$

Next for $b \in \boldsymbol{Q}_p$, let $\langle b\rangle_p$ denote its unique representative mod $\boldsymbol{Z}_p$ in $[0, 1) \cap \boldsymbol{Q}$. Finally, for $x \in \boldsymbol{Q}_p$ we set

$$A(x) = (A_0(x), A_1(x)) = \left(\frac{x-1}{p} - \left\langle\frac{x-1}{p}\right\rangle_p, p\left\langle\frac{x-1}{p}\right\rangle\right)$$

so that $A'(x)=((p-1)/p)(x-1)+\langle(x-1)/p\rangle$. Clearly, $A(x)$ is continuous in$x$.

Theorem 10. *Let $n\in N$, $(n,p)=1$. For $x\in Z_p$ we have*

$$\prod_{i=0}^{n-1}\Gamma_p\left(\frac{x+i}{n}\right)=\Gamma_p(x)\prod_{i=0}^{n-1}\Gamma_p\left(\frac{i}{n}\right)n^{-A(x)}.$$

Moreover,

$$\prod_{i=0}^{n-1}\Gamma_p\left(\frac{i}{n}\right)=\Gamma_p(1/2)^{2\langle(n-1)/2\rangle}(-1)^{r_n} \tag{22}$$

where $r_n=\sum_{1\leq j<n/2}l(j/n)$, with l as in Proposition 6.

Remarks. First if $p=2$, equation (22) still makes sense since, in this case, $\langle(n-1)/2\rangle=0$. Second, as Boyarski points out, it is not difficult to deduce these equations from the others already proven. Indeed, if one sets

$$\phi_n(x)=\frac{\prod\Gamma_p\left(\frac{x+i}{n}\right)}{\Gamma_p(x)},$$

for $x\in Z_p$ one obtains

$$\phi_n(x)=\phi_n(0)n^{-A'(x)}=\phi_n(0)n^{-A(x)}$$

for $x\in N$, easily from (11). This equation remains valid for all $x\in Z_p$ by continuity. The evaluation of $\phi_n(0)$ is accomplished using (12). Finally, using (12) again we see that

$$\Gamma_n(1/2)^2=(-1)^{(p+1)/2}.$$

As $\Gamma_p(1/2)\equiv((p-1)/2)!\bmod p$, this determines it. In fact it follows from the analytic class number formula [M], [C] that

$$\Gamma_p(1/2)\equiv(-1)^{(h(-p)+1)/2}$$

when $p\equiv 3(4)$ and $p>3$ and if $p\equiv 1(4)$,

$$\Gamma_p(1/2)=(-1)^{(h(p)+1)/2}t(\varepsilon)$$

where $h(d)$ is the class number of $Q(\sqrt{d})$ and if $p\equiv 1(4)$, ε is a fundamental unit of $Q(\sqrt{p})\subseteq C_p$ which is greater than one in some real embedding. Also here and below, for an integer $k \in \boldsymbol{C}_p$, we set $t(k)=t(\tilde{k})$.

The following identities include those of Hasse-Davenport [H-D], Dwork, Langlands [B], and Kubert [Ku].

Theorem 11. *Let $f \in \boldsymbol{N}^*$, $q=p^f$, $b \in \boldsymbol{Q}/\boldsymbol{Z}$, $d \in \boldsymbol{N}^*$, $(d,p)=1$ such that $(q-1)db=0$. Let $S \subseteq \boldsymbol{Q}/\boldsymbol{Z}$ be a set of representatives for the orbits of the subgroup of $(\boldsymbol{Z}/(q-1)d\boldsymbol{Z})^*$ generated by q acting on $b+(1/d)\boldsymbol{Z}/\boldsymbol{Z} \subseteq \boldsymbol{Q}/\boldsymbol{Z}$. For $s \in S$ let $o(s)$ denote the order of the orbit containing s. Then*

$$\prod_{s \in S} g_{q0(s)}(s)=g_q(db)\,t(d)^{(q-1)d\langle b\rangle}((\sqrt{-p}\,)^{d-1}\phi_d(0))^f \tag{23}$$

where $\sqrt{-p}=\pi^{(p-1)/2}$.

Note that Theorems 9 and 10 imply

$$(\sqrt{-p}\,)^{d-1}\phi_d(0)=(-1)^{r_d}(-p)^{[(d-1)/2]}g_p(1/2)^{2\langle(d-1)/2\rangle},$$

with r_d as above.

Taking $b=0$ in the above Theorem we get

Corollary 11a.

$$\prod_{\substack{s \in S \\ s \neq 0}} g_{q0(s)}(s)=(\sqrt{-p}\,)^{d-1}\phi_d(0))^f$$

and when $q \equiv 1(\operatorname{mod} d)$ this equals

$$(-1)^{(q-1)/d}(([(d-1)/2]^2-[(d-1)/2])/2)q^{[(d-1)/2]}g_q\left(\frac{1}{2}\right)^{2\langle(d-1/2)\rangle}.$$

Proof. The second part of the corollary follows from the identity:

$$g_q(s)g_q(-s)=(-1)^{(q-1)\langle s\rangle}q$$

if $s \in \boldsymbol{Q}/\boldsymbol{Z}$, $s \neq 0$, $(q-1)s=0$.

Before we begin the proof we need several lemmas.

Lemma 12. *Let $a \in \boldsymbol{Q}/\boldsymbol{Z}$, $d \in \boldsymbol{N}^*$. Then*

$$\frac{\prod_{i=0}^{d-1} \Gamma_p\left(\left\langle a+\frac{i}{d}\right\rangle\right)}{\Gamma_p(\langle da\rangle)}=\phi_d(d\langle a\rangle)d^{B(d\langle a\rangle)}$$

where $B(x)=[(r(x)-x)/p]+[-r(x)/p]-[-x]$ for $x \in \boldsymbol{Q}^+ \cap \boldsymbol{Z}_p$ where $r(x)$ is *any element of* $\boldsymbol{Z}$ *such that* $|x-r(x)|<1$.

Proof. This is an easy consequence of (11), noting that, for $x\in \boldsymbol{Q}^+\cap \boldsymbol{Z}_p$, $B(x)=\#\{i\colon 1\le i<x,\ i\not\equiv x \bmod p\}$.

Lemma 13. *If* $x\in \boldsymbol{R}$, $\sum_{i=0}^{d-1}\langle x+(i/d)\rangle=\langle dx\rangle+(d-1)/2$.

Proof. The proof is straightforward.

Lemma 14. *With* $b\in \boldsymbol{Q}/\boldsymbol{Z}$, $q=p^f$, $(q-1)b=0$, *we have*

$$\langle pb\rangle=p\langle qb\rangle-p\left\langle\frac{(q-1)\langle pb\rangle}{p}\right\rangle.$$

Proof. Write $\langle pb\rangle=n/(q-1)$ with $0\le n<q-1$. Then the right-hand side equals

$$p\left\langle\frac{qn}{p(q-1)}\right\rangle-p\left\langle\frac{n}{p}\right\rangle=p\left\langle\frac{n}{p}+\frac{n}{p(q-1)}\right\rangle-p\left\langle\frac{n}{p}\right\rangle=\frac{n}{q-1}$$

since $n/p+n/p(q-1)<1$.

Lemma 15. *With notation as in the theorem.*

$$\sum_{i=0}^{f-1}A'(d\langle p^ib\rangle)=\sum_{i=0}^{f-1}B(d\langle p^ib\rangle).$$

Proof. Taking $r(d\langle p^ib\rangle)=(1-q^d)d\langle p^ib\rangle$, we have

$$B(d\langle p^ib\rangle)=\left[\frac{(q^d-1)d\langle p^ib\rangle}{p}\right]+\left[\frac{q^dd\langle p^ib\rangle}{p}\right]-[-d\langle p^ib\rangle].$$

Suppose

$$\langle p^ib\rangle=\frac{a_0+a_1p+\cdots+a_{df-1}p^{df-1}}{q^d-1}$$

with $0\le a_i<p$. Define a_i, $\forall i\in \boldsymbol{Z}$, so that $a_{i+df}=a_i$. Then we easily deduce that

$$\begin{aligned}B(d\langle p^ib\rangle)&=\left[\frac{da_{-i}}{p}\right]+[-d\langle q^dp^{i-1}b\rangle]-[-d\langle p^ib\rangle]\\&=\left[\frac{da_{-i}}{p}\right]+[-d\langle(p^{i-1})^*b\rangle]-[-d\langle p^ib\rangle]\\&\quad+d\langle(p^{i-1})^*b\rangle-d\langle q^dp^{i-1}b\rangle\end{aligned}$$

where $(p^{i-1})^*=p^{i-1}$ if $i>0$ and p^{f-1}, $i=0$, using the fact that

$$(d\langle cb\rangle - d\langle q^d cb\rangle) \in \boldsymbol{Z}.$$

Thus

$$\sum_{i=0}^{f-1} B(d\langle p^i b\rangle) = \sum_{i=0}^{f-1}\left[\frac{da_{-i}}{p}\right] + d\left(\sum_{i=0}^{f-1}\langle p^j b\rangle - \sum_{i=0}^{f-1}\langle q^d p^{i-1} b\rangle\right) \tag{24}$$

$$= \sum_{i=0}^{f-1}\left[\frac{da_{-i}}{p}\right] + d(\langle p^{f-1}b) - \langle q^d p^{-1}b\rangle).$$

On the other hand,

$$A'(d\langle p^i b\rangle) = \frac{p-1}{p}\, d\langle p^i b\rangle + \left(\left\langle\frac{d\langle p^i b\rangle - 1}{p}\right\rangle_p - \frac{p-1}{p}\right)$$

$$= \frac{p-1}{p}\, d\langle p^i b\rangle - \left\langle\frac{(q^d-1)d\langle p^i b\rangle}{p}\right\rangle$$

$$= \left[\frac{da_{-i}}{p}\right] + d\left(\frac{p-1}{p}\langle p^i b\rangle - \left\langle\frac{(q^d-1)\langle p^i b\rangle}{p}\right\rangle\right).$$

The lemma now follows from Lemma 14 and (24).

Lemma 16. *With notation as in Lemma* 15,

$$\prod_{i=0}^{f-1} d^{B(d\langle p^i b\rangle)} = f(d)^{(q-1)d\langle b\rangle} \prod_{i=0}^{f-1} d^{A(d\langle p^i b\rangle)}.$$

Proof. Since $(q-1)A_0(d\langle p^i b\rangle) \in \boldsymbol{Z}$, it follows from the previous lemma that the ratio of the two sides is a $(q-1)^{\text{st}}$ root of unity. We only have to evaluate it mod p. First,

$$d^{A(x)} \equiv d^{A_1(x)} \bmod p$$

and

$$A_1(d\langle p^i b\rangle) = p\left\langle\frac{d\langle p^i b\rangle - 1}{p}\right\rangle_p \equiv -p\left\langle\frac{da_{-i}}{p}\right\rangle \quad \bmod p-1.$$

Second, from this and (24), we see easily that

$$\sum_{i=0}^{f-1} B(d\langle p^i b\rangle) - \sum_{i=0}^{f-1} A_1(d\langle p^i b\rangle)$$

$$\equiv \sum_{i=0}^{f-1}\left[\frac{da_{-i}}{p}\right] + p\left\langle\frac{da_{-i}}{p}\right\rangle + d(\langle p^{f-1}b\rangle - \langle q^d p^{-1}b\rangle)$$

$$\equiv d\left(\sum_{i=0}^{f-1} a_{-i}+\langle p^{f-1}b\rangle-\langle q^d p^{-1}b\rangle\right) \bmod \quad (p-1)$$

$$=d\left(\sum_{i=0}^{f-1} a_{-i}+\frac{\sum_{i=0}^{f-1} a_{-i}(q-q^d)p^{-(i+1)}+(q-1)\sum_{k=1}^{(d-1)f} a_k p^{k-1}}{q^d-1}\right)$$

$$=d(q-1)\langle qp^{-1}b\rangle\equiv(q-1)d\langle b\rangle \quad \bmod p-1.$$

This completes the proof.

Proof of Theorem 11. The left-hand side of (23) equals

$$\pi^M \prod_{s\in S}\left(\prod_{i=0}^{o(s)f-1} \Gamma_p(\langle p^i s\rangle)\right)=\pi^M \prod_{s\in S}\left(\prod_{j=0}^{f-1}\prod_{k=0}^{o(s)-1} (\Gamma_p(\langle q^k p^j s\rangle)\right)$$

$$=\pi^M \prod_{j=0}^{f-1}\prod_{i=0}^{d-1} \Gamma_p\left(\left\langle p^j b+\frac{i}{d}\right\rangle\right)$$

$$=\pi^M \prod_{j=0}^{f-1} (\Gamma_p(\langle p^j db\rangle)d^{B(d\langle p^j b\rangle)}\phi_d(d\langle p^j b\rangle))$$

$$=\pi^{M-N} g_q(db)\phi_d(0)^f \prod_{j=0}^{f-1} d^{B(d\langle p^j b\rangle)-A(d\langle p^j b\rangle)},$$

using Theorems 9 and 10, where

$$M=\sum_{s\in S} S_{q^{o(s)}}(s)=(p-1)\sum_{i=0}^{f-1}\sum_{j=0}^{d-1}\left\langle p^i b+\frac{j}{d}\right\rangle$$

$$N=S_q(db)=(p-1)\sum_{i=0}^{f-1}\langle p^i dp\rangle$$

using the definition of S_q. Lemma 13 implies

$$M-N=f\frac{(d-1)(p-1)}{2}.$$

The theorem follows from Lemma 16.

Remarks. It seems natural to ask whether or not there are more multiplicative identities among the Gauss sums, $g_q(b)$.

VI. The Frobenius Matrix of Fermat Curves

Because of its importance and because there is no adequate treatment elsewhere in the literature we would like to demonstrate how the methods of [K] and [G-K] lead to the determination of the matrix of Frobenius acting on the standard basis of the first de Rham cohomology group of a Fermat curve. We will also indicate, briefly, how the intriguing argument sketched in [B] can also be turned into a determination of this matrix.

Suppose K is a finite unramified extension of $\boldsymbol{Q}_p$. Let σ denote the absolute Frobenius automorphism of K. Suppose X is a proper smooth connected curve over K with good reduction. Let $H(X)$ denote the first de Rham cohomology group of X. Then there exists a canonical σ-linear endomorphism Φ of $H(X)$ called the Frobenius endomorphism. Let Q be a point in $X(K)$ and U the residue class of X containing Q. Let T be a uniformizing parameter on U centered at Q. Suppose now ω and ν are differentials of the second kind on X regular on U such that in $H(X)$, $\Phi\omega = \alpha\nu$ for some $\alpha \in K$. Suppose

$$\omega = \sum b(n) T^n dT/T$$

and

$$\nu = \sum c(n) T^n dT/T$$

on U. The coefficients of these two series are bounded and we have,

Theorem 17. *Suppose the class of* ν *is not in the unit root subspace of* $H(X)$. *Then there exists a sequence* $\{n_i\}$ *of integers such that* $n_i \to 0$ *and*

$$\alpha = \lim pb(n_i)^\sigma / c(pn_i).$$

Proof. By Corollary 5.9.6 of [K], the coefficients of the series

$$\sum c(n) T^n / n$$

are unbounded, while those of

$$\sum b(n)^\sigma T^{pn}/n - \alpha \sum c(n) T^n / n$$

are bounded. Hence there exists a sequence $\{n_i\}$ such that

$$c(n_i)/n_i \to \infty$$

and there exists a constant A such that

$$|b(n)^\sigma/n - \alpha c(pn)/pn| \leq A.$$

It follows that $n_i \to 0$ and

$$|pb(n_i)^\sigma / c(pn_i) - \alpha| \to 0.$$

This concludes the proof.

Remark. This generalizes and slightly weakens Theorem 6.2 of [K].

Now, we will apply this result to Fermat curves. Let F_m denote the smooth plane curve with affine model

$$u^m + v^m = 1,$$

over $\boldsymbol{Q}_p$ where m is an integer prime to p. Let

$$\omega_{a,b} = u^a v^b (v/u) d(u/v).$$

Then, $\{\omega_{a,b}: 0 < a, b, a+b < m\}$ forms a basis of the holomorphic differentials on F_m (even over $\boldsymbol{Z}_p$) and $\{\omega_{a,b}: 0 < a, b < m, a+b \neq m\}$ forms a basis of $H(F_m)$ (but not over $\boldsymbol{Z}_p$ for $p < m$). For a real number t, $\langle t \rangle$ will denote the fractional part of t and $[t]$ the greatest integer less than or equal to t. Let $I = \{(r, s) \in 1/m\boldsymbol{Z} \times 1/m\boldsymbol{Z}: r+s \neq 0\}$. For $t \in \boldsymbol{Q}/\boldsymbol{Z}$, $\langle t \rangle$ will denote the fractional part of any representative of t in $\boldsymbol{Q}$. For $(r, s) \in I$ we set

$$\varepsilon(r, s) = \langle r \rangle + \langle s \rangle - \langle r+s \rangle$$
$$K(r, s) = (1 - (\langle r \rangle + \langle s \rangle))^{\varepsilon(r,s)}$$
$$\nu_{r,s} = K(r, s)\omega_{m\langle r \rangle, m\langle s \rangle}.$$

Now $\{\nu_{r,s}: (r, s) \in I\}$ forms a basis for $H(F_m)$ over $\boldsymbol{Z}_p$. (Recall, this means that $\nu_{r,s}$ is locally holomorphic plus exact over $\boldsymbol{Z}_p$). Moreover for $(r, s) \in I$

$$\nu_{r,s} \cdot \nu_{t,u} = 0$$

with respect to the cup product, unless $(t, u) = (-r, -s)$ in which case

$$\nu_{r,s} \cdot \nu_{-r,-s} = (-1)^{\varepsilon(r,s)}.$$

We wish to compute the matrix of Φ with respect to this basis.

We follow [K]. We expand $\omega_{a,b}$ at the point $x=0, y=1$ on F_m with respect to the parameter x. We find,

$$\omega_{a,b} = \sum b_{a,b}(n) u^n du/u$$

where

$$b_{a,b}(n) = (-1)^{(n-a)/m} \binom{\dfrac{b}{m} - 1}{(n-a)/m}$$

with the understanding, that this expression is zero as whenever $(n-a)/m$ is not an integer. Now $\{\omega_{a,b}\colon 0<a,\ b<m,\ a+b\neq m\}$ is an eigenbasis for the obvious action of $\mu_m\times\mu_m$. It follows from this that there exists a constant $\alpha_{a,b}\in \boldsymbol{Q}_p$ such that in $H(F_m)$

$$\Phi\omega_{a,b}=\alpha_{a,b}\omega_{a',b'}$$

where $0<a',\ b'<m$ are such that $a'\equiv pa \bmod m$ and $b'\equiv pb \bmod m$. Suppose $\omega_{a,b}$ is not in the unit root subspace (this is automatic if $\omega_{a,b}$ is holomorphic). It follows from the previous theorem that there exists a sequence of positive integers $\{n_i\}$ tending toward zero such that

$$\alpha_{a,b}=\lim pb_{a,b}(n_i)/b_{a',b'}(pn_i).$$

If we set $k_i=(n_i-a)/m$, then k_i must be an integer and $k_i\to-\langle a/m\rangle$. Hence

$$\alpha_{a,b}=\lim(-1)^{(p-1)k_i+[p\langle a/m\rangle]}p\binom{\langle b/m\rangle-1}{k_i}\Big/\binom{\langle pb/m\rangle-1}{pk_i+[p\langle a/m\rangle]}.$$

Now this limit was evaluated in [G-K]. More precisely;

Lemma 18. *We have*

$$\lim\binom{\langle b/m\rangle-1}{k}\Big/\binom{\langle pb/m\rangle-1}{pk+[p\langle am\rangle]}$$

as k runs through positive integers approaching $-\langle a/m\rangle$, *equals*

$$\varepsilon A\Gamma_p(1-\langle pa/m\rangle)\Gamma_p(1-\langle pb/m\rangle)/\Gamma_p(1-\langle pa/m\rangle-\langle pb/m\rangle).$$

Where Γ_p *denotes the p-adic gamma function,*

$$\varepsilon=(-1)^{1+(p-1)\langle pa/m\rangle+[p\langle a/m\rangle]}$$

(*note the middle term is considered even when p is odd*) *and*

$$A=p^{-\varepsilon(\langle a/m\rangle,\langle b/m\rangle)}K(a/m,\ b/m)^{-1}$$

unless $K(pa/m,pb/m)\equiv 0 \bmod p$, *in which case* $A=1$.

Because the conclusion of the above lemma differs from the corresponding statements in [G-K] we will give the proof.

Proof. Since the binomial coefficient $\binom{x}{n}$ is a polynomial in x and

$\langle pb/m\rangle = p\langle b/m\rangle - [p\langle b/m\rangle]$, the above limit equals:

$$\lim\lim \binom{-h-1}{k} \Big/ \binom{-ph-[p\langle b/m\rangle]-1}{pk+[p\langle a/m\rangle]}$$

as h approaches $-\langle b/m\rangle$ and k approaches $-\langle a/m\rangle$. Now,

$$\binom{-h-1}{k} = (-1)^h \frac{(h+k)!}{h!\,k!}$$

while

$$\binom{-ph-[p\langle b/m\rangle]-1}{pk+[p\langle a/m\rangle]}$$
$$= (-1)^{ph+[p\langle a/m\rangle]} \frac{(p(h+k)+[p\langle a/m\rangle]+[p\langle b/m\rangle])!}{(ph+[p\langle a/m\rangle])!\,(pk+[p\langle b/m\rangle])!}.$$

By definition, for positive integers n,

$$\Gamma_p(1+n) = (-1)^{n+1} n!/[n/p]!\,p^{[n/p]}.$$

Claim: $[p\langle a/m\rangle]+[p\langle b/m\rangle] < p$ iff $\langle a/m\rangle + \langle b/m\ \rangle < 1$ or

$$1-(\langle pa/m\rangle + \langle pb/m\rangle) \equiv 0 \mod p.$$

It is clear that $[p\langle a/m\rangle]+[p\langle b/m\rangle] < p$ if $\langle a/m\rangle + \langle b/m\rangle < 1$. Therefore suppose $\langle a/m\rangle + \langle b/m\rangle > 1$. We may assume $0 < a, b < m$. Write $b = m-a+c$ with $0 < c < a$ and

$$pa = nm + r$$

with $0 \leq r < m$. Then

$$pb = (p-n)m + pc - r.$$

Now $pm > pa > nm + r \geq nm$, so $p > n$. Also

$$-m < pc - r \leq p(a-1) - r = nm - p < (p-1)m.$$

Hence $[p\langle a/m\rangle]+[p\langle b/m\rangle] < p$ iff $pc < r$, $\langle pa/m\rangle = r/m$ and $\langle pb/m\rangle = 1 + (pc-r)/m$ iff $1-(\langle pa/m\rangle + \langle pb/m\rangle) \equiv 0 \mod p$. This establishes the claim.

We now see that the h, k term in the above limit is equal to the product of

$$(-1)^{(p-1)h+[p\langle a/m\rangle]}$$

$$A(-1)^{1+p(k+k)+[p\langle a/m\rangle]+[p\langle b/m\rangle]}p^{-(h+k)}$$
$$\times\Gamma_p(1+p(h+k)+[p\langle a/m\rangle]+[p\langle b/m\rangle])^{-1}$$

$$(-1)^{1+ph+[p\langle a/m\rangle]}p^h\Gamma_p(1+ph+[p\langle a/m\rangle])$$

and

$$(-1)^{1+pk+[p\langle b/m\rangle]}p^k\Gamma_p(1+pk+[p\langle b/m\rangle])$$

where $A=1$ if $\langle a/m\rangle+\langle b/m\rangle<1$ or $1-(\langle pa/m\rangle+\langle pb/m\rangle)\equiv 0 \bmod p$ and

$$p^{-1}(1+h+k)^{-1}$$

otherwise. Hence finally the h, k term equals

$$A(-1)^{1+(p-1)h+[p\langle a/m\rangle]}$$

times

$$\frac{\Gamma_p(1+ph+[p\langle a/m\rangle])\Gamma_p(1+pk+[p\langle b/m\rangle])}{\Gamma_p(1+p(h+k)+[p\langle a/m\rangle]+[p\langle b/m\rangle])}.$$

Since Γ_p is continuous, this converges to the limit given in the statement of the lemma.

Corollary. *We have,*

$$\alpha_{a,b}=\iota Ap\Gamma_p(1-\langle pa/m\rangle)\Gamma_p(1-\langle pb/m\rangle)/\Gamma_p(1-(\langle pa/m\rangle+\langle pb/m\rangle))$$

with A as in the lemma and

$$\iota=(-1)^{1+(p-1)(\langle pa/m\rangle+\langle pb/m\rangle)}.$$

Note that this is just -1 if p is odd.

We have;

Theorem 19. *In $H(F_m)$*

$$\Phi\nu_{r,s}=\beta_{r,s}\nu_{pr,ps}$$

where

$$\beta_{r,s}=\iota_{r,s}p^{\varepsilon(-r,-s)}\frac{\Gamma_p(\langle p(r+s)\rangle)}{\Gamma_p(\langle pr\rangle)\Gamma_p(\langle ps\rangle)}$$

where

$$\iota_{r,s}=(-1)^{\varepsilon(r,s)} \qquad \textit{when } p \textit{ is odd and}$$
$$\iota_{r,s}=(-1)^{\varepsilon(r,s)+\langle 2r\rangle+\langle 2s\rangle} \qquad \textit{when } p=2.$$

Lemma 20. *Suppose* $(r, s) \in I$ *such that* $K(pr, ps)\equiv 0 \bmod p$, *then*

$$K(pr, ps)=pK(r, s)$$

and

$$\varepsilon(pr, ps)=\varepsilon(r, s).$$

Proof. The last statement follows immediately from the previous one. Now write

$$\begin{aligned} p\langle r\rangle+p\langle s\rangle &= [pr]+[ps]+\langle ps\rangle+\langle pr\rangle \\ &= [pr]+[ps]+1+K(ps, pr). \end{aligned}$$

Hence our hypothesis implies

$$[pr]+[ps]+1\equiv 0 \quad \bmod p.$$

But $0<[pr]$, $[ps]<p$, $[pr]+[ps]=p-1$ which gives the lemma.

Proof of Theorem. From Proposition 6 , we have

$$\Gamma_p(1-\langle pr\rangle)=(-1)^{l(\langle pr\rangle)}\Gamma_p(\langle pr\rangle)$$
$$\Gamma_p(1-\langle ps\rangle)=(-1)^{l(\langle ps\rangle)}\Gamma_p(\langle ps\rangle)$$

and

$$\begin{aligned} \Gamma_p(1-\langle pr\rangle-\langle ps\rangle) &= (-1)^{l(\langle pr\rangle+\langle ps\rangle)}\Gamma_p(\langle pr\rangle+\langle ps\rangle) \\ &= (-1)^{l(\langle pr\rangle+\langle ps\rangle)+1}\Gamma(\langle p(r+s)\rangle) \qquad \text{when } K(pr, ps)\equiv 0 \bmod p \end{aligned}$$

and

$$=(-1)^{l(\langle pr\rangle+\langle ps\rangle)}K(pr, ps)\Gamma_p(\langle p(r+s)\rangle) \qquad \text{otherwise.}$$

From this, the corollary, the previous lemma and the definition of $\nu_{r,s}$, we deduce the theorem for $\nu_{r,s}$ not in the unit root subspace except for the sign, which at this point equals:

$$(-1)^{1+(p-1)(\langle pr\rangle+\langle ps\rangle)+l(\langle pr\rangle+\langle ps\rangle)+l(\langle pr\rangle)+l(\langle ps\rangle)+j(pr,ps)},$$

where $j(r, s)=1$ when $K(r, s)\equiv 0 \bmod p$ and 0 otherwise. To get the sign in the above simple form we need

Lemma 21. *Let* $(r, s) \in I$. *Then,*
(i) $l(1-r) \equiv p - l(r) \bmod 2$
(ii) $l(x) \equiv l(x-1) + (x-1) \quad \bmod 2 \qquad$ *if* $p=2$
(iii) $l(\langle pr \rangle + \langle ps \rangle) \equiv l(\langle p(r+s) \rangle) + \varepsilon(pr, ps) + j(pr, ps) \quad \bmod 2$
(iv) $l(\langle p(r+s) \rangle) + l(\langle pr \rangle) + l(\langle ps \rangle) \equiv 1 + \varepsilon(r, s) + \varepsilon(pr, ps) \quad \bmod 2.$

We leave the proof, as well as the deduction of sign, to the reader.

Now by duality we have

$$\beta_{r,s}\beta_{-r,-s} = (-1)^{\varepsilon(r,s)+\varepsilon(pr,ps)}p.$$

The theorem in general follows from this and the previous lemma, since as we mentioned earlier the holomorphic differentials are not in the unit root subspace.

We will now indicate, briefly, how the argument sketched in [B] may be turned into another calculation of this Frobenius matrix. This calculation is analogous to the classical proof that the Beta function is a product of Gamma functions. Unfortunately, while the proof uses results which should be standard in p-adic analysis, like the Kunneth formula, it is very difficult to extract them from the literature. We will only explain the heart of this computation.

Let A_m denote the affine Artin-Schreier curve given by the equation;

$$x^p - x = a^m$$

The key to the following computation is the following correspondence between $A_m \times A_m$ and $F_m \times A_m$. We represent $A_m \times A_m$ by the equations:

$$x^p - x = a^m, \; y^p - y = b^m$$

and $F_m \times A_m$ by the equations:

$$u^m + v^m = 1, \; z^p - z = c^m.$$

Finally, we let W denote the fiber product of $A_m \times A_m$ and $F_m \times A_m$ over the $a \times b$ plane via the equations

$$a = cu, \; b = cv.$$

Now we don't want to consider all of any of the above surfaces, but rather, certain rigid subspaces of them.

First, we let A_m^0 denote the affinoid subdomain of A_m, where $|a| \leq 1$ (in the co ordinates $x^p - x = a^m$). We also let F_m^0 denote the affinoid subdomain of W where $|u| \leq 1$. Let W^0 denote the affinoid subdomain of W where $|u| \leq 1$ and $|c| \leq 1$. Let f: $W^0 \to A_m^0 \times A_m^0$ and g: $W^0 \to F_m^0 \times A_m^0$

denote the natural maps. Let $\theta(T)=\theta_p(T)$ be the Dwork exponential defined in Section II. Now set

$$\eta_r(a)=\theta(x)a^r da/a$$

and as above

$$\omega_{r,s}=u^r v^s(v/u)\,d(u/v).$$

Then, $\eta_r(a)$ is an overconvergent differential on A_m^0 and of course $\omega_{r,s}$ is an overconvergent differential on F_m^0. (We use the corresponding notation for our other presentations of A_m.) The following is the analogue of the change of variables argument in the classical theory of the Beta function.

Lemma 22. *As overconvergent differentials on* W^0,

$$f^*(\eta_r(a)\wedge\eta_s(b))=g^*(\omega_{r,s}\wedge\eta_{r+s}(c)).$$

Proof. On W^0,

$$\begin{aligned}f^*(\eta_r(a)\wedge\eta_s(b))&=\theta(x)a^r da/a\wedge\theta(y)b^s db/b\\&=\theta(x)(cu)^r d(cu)/(cu)\wedge\theta(y)(cv)^s d(cv)/(cv)\\&=u^r v^s(v/u)d(u/v)\wedge\theta(x)\theta(y)c^{r+s}dc/c.\end{aligned}$$

To complete the proof, it suffices to show that $\theta(x)\theta(y)=\theta(z)$, and since these are overconvergent rigid analytic functions on W^0 it suffices to check this on an open subset of W^0. The open subset we will consider is the set U where $|z|<1$. On U we also have $|x|<1$ and $|y|<1$. Hence on U,

$$\theta(x)\theta(y)=\exp(\pi(x-x^p))\exp(\pi(y-y^p))$$

since $\exp(\pi T)$ converges on the open unit disk, and this equals

$$\begin{aligned}&\exp(-\pi a^m)\exp(-\pi b^m)=\exp(-\pi(a^m+b^m))\\&\quad=\exp(-\pi((cu)^m+(cv)^m))=\exp(-\pi c^m)=\exp(\pi(z-z^p))=\theta(z),\end{aligned}$$

as required. This completes the proof.

To obtain the Frobenius matrix from this, one has to interpret the above differentials as dagger cohomology classes. Suppose $0<u<2m$, $u\neq m$, is an integer. By an elementary computation,

$$\eta_u=S(u)\eta_{m\langle u/m\rangle}$$

where

$$\begin{aligned} S(u)&=1 && \text{if } u<m,\\ &=\pi^{-1}(\langle u/m\rangle-1) && \text{if } u>m.\end{aligned}$$

For an integer u let u' denote the least positive residue of pu mod m. Suppose, in the following, that r, s, t are positive integers such that $r, s, t<m$, $r+s\neq m$. By comparing the dagger cohomology of A_m^0 with the spaces L_b of Section III and using the computation after Corollary 8.1 (see [L] Chapter 16) we see that as dagger cohomology classes on A_m^0,

$$\Phi\eta_r=\alpha_r\eta_{r'}$$

where

$$\alpha_r=-p\Gamma_p(1-r'/m)/\pi^{(pr-r')/m}.$$

It follows from this and Lemma 22 that as dagger cohomology classes on W^0 we have on the one hand

$$\begin{aligned}\Phi g^*(\omega_{r,s}\wedge\eta_t(c))&=g^*(\Phi(\omega_{r,s}\wedge\eta_t(c)))\\ &=g^*(\Phi\omega_{r,s}\wedge\Phi\eta_t(c))\\ &=g^*(\beta_{r,s}\omega_{r',s'}\wedge\alpha_t\eta_{t'}(c))\\ &=\beta_{r,s}\alpha_t g^*(\omega_{r',s'}\wedge\eta_{t'}(c))\end{aligned}$$

where $\beta_{r,s}$ is as above, while on the other hand,

$$\begin{aligned}\Phi g^*(\omega_{r,s}\wedge\eta_{r+s}(c))&=\Phi f^*(\eta_r(a)\wedge\eta_s(b))\\ &=\alpha_r\alpha_s f^*(\eta_{r'}(a)\wedge\eta_{s'}(b))\\ &=\alpha_r\alpha_s g^*(\omega_{r',s'}\wedge\eta_{r'+s'}(c)).\end{aligned}$$

Taking $t=m\langle(r+s)/m\rangle$ and putting these formulas together we see that, in cohomology,

$$(\beta_{r,s}-S\alpha_r\alpha_s/\alpha_t)\cdot g^*(\omega_{r',s'}\wedge\eta_{t'}(c))=0$$

where

$$S=S(r'+s')/S(r+s).$$

Theorem 19 follows immediately from this once we know that $g^*(\omega_{r',s'}\wedge\eta_{t'}(c))$ is not exact. But this follows from the Kunneth formula and the fact that g is a finite morphism.

References

[B] Boyarsky, M., p-adic gamma functions and Dwork cohomology, Trans. Amer. Math. Soc., **257**, no. 2 (1980), 359–369.

[C] Chowla, S., On the class number of real quadratic fields, Proc. Nat. Acad. Sci. USA, **47** (1961), 878.

[D-H] Davenport, H. and Hasse, H., Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen, J. Reine Angew. Math., **172** (1934), 151–182.

[G-K] Gross, B. and Koblitz, W., Gauss sums and the p-adic Γ-function, Ann. of Math., **109** (1979), 569–581.

[K] Katz, N., Crystalline cohomology, Dieudonné modules and Jacobi sums, in Automorphic Forms, Representation Theory and Arithmetic, (Tata Institute of Fundamental Research, Bombay, India, 1979), pp. 165–245.

[Ku] Kubert, D., Jacobi sums and Hecke characters, Amer. J. Math., **107**, No. 2 (1985), 253–280.

[L] Lang, S., Cyclotomic Fields, II, Springer-Verlag, 1978.

[M] Mordell, C. J., The congruence $((p-1)/2)! \equiv \pm 1$ (mod p), Amer. Math. Monthly, **68** (1961), 145–146.

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

Department of Mathematics
University of California
Berkeley, California 94720
U.S.A.