Vol. 45, No. 1 DUKE MATHEMATICAL JOURNAL© March 1978

GAMMA FUNCTION IDENTITIES AND ELLIPTIC DIFFERENTIALS ON FERMAT CURVES

NEAL KOBLITZ

§1. Introduction

If C is a nonsingular algebraic curve with linearly independent differentials of the first kind $\omega_1, \cdots, \omega_g$, $g \leq$ genus C, all defined over a field $K \subset \mathbf{C}$, we say $\{\omega_i\}$ is a "genus g set of differentials over K" if

$$\mathscr{L}_{\{\omega_i\}} = \left\{ \int_\gamma \omega_1, \cdots, \int_\gamma \omega_g \right\}_{\gamma \in H_1(C,\mathbf{Z})} \subset \mathbf{C}^g$$

is a lattice, i.e., discrete of $\mathbf{Z}$-rank $2g$. Such a set of differentials gives a map of the jacobian J_C of C onto the g-dimensional abelian variety $A = \mathbf{C}^g/\mathscr{L}_{\{\omega_i\}}$. A is actually defined over K, because its cotangent space and hence its Lie algebra is defined over K ([8]). If $g = 1$, we call $\omega = \omega_1$ an elliptic differential. In that case $E_\omega = \mathbf{C}/\mathscr{L}_\omega$ is an elliptic curve.

For $N > 2$, let $F(N) = \{(X, Y, Z) \in \mathbf{P}^2(\mathbf{C}) | X^N + Y^N = Z^N\}$. A convenient basis of holomorphic differentials on $F(N)$ is

$$\omega_{r,s,t} = X^{Nr-1}Y^{Ns-1}\frac{dX}{Y^{N-1}} \quad (Nr, Ns, Nt \in \mathbf{Z}^+, r + s + t = 1).$$

Let $\zeta_N = e^{2\pi i/N}$, $\mathbf{Q}_N = \mathbf{Q}(\zeta_N)$. Let $\langle\ \rangle$ denote least nonnegative residue mod 1. Let

$$H_{r,s,t} = \{u \in (\mathbf{Z}/N\mathbf{Z})^* | \langle ur\rangle + \langle us\rangle + \langle ut\rangle = 1\}.$$

Then $H_{r,s,t}$ is a set of coset representatives for $\{\pm 1\}$ in $(\mathbf{Z}/N\mathbf{Z})^*$. Let $[r, s, t]$ be the equivalence class of triples where $(r, s, t) \sim (\langle ur\rangle, \langle us\rangle, \langle ut\rangle)$ $(u \in H_{r,s,t})$. Then $J_{F(N)}$ is isogenous over $\mathbf{Q}$ to a product of abelian varieties $J_{[r,s,t]}$ (see [7]); in fact, this decomposition of $J_{F(N)}$ is the eigen-space decomposition for the action of $(\mu_N)^3/\mu_N$ on the differentials, corresponding to $X \mapsto \zeta_1 X$, $Y \mapsto \zeta_2 Y$, $Z \mapsto \zeta_3 Z$ on the curve, where $\zeta_i \in \mu_N$ are N-th roots of unity and the diagonal (ζ, ζ, ζ) acts trivially. We also know [9] that, over $\overline{\mathbf{Q}}$, $J_{[r,s,t]}$ is isogenous to a product of w copies of a simple factor of dimension $\varphi(M)/2w$, where

$$M = N/g.c.d.(Nr, Ns, Nt), \qquad w = \#\{u \in (\mathbf{Z}/M\mathbf{Z})^* | uH_{r,s,t} = H_{r,s,t}\}.$$

In particular, $J_{[r,s,t]}$ is isogenous over $\overline{\mathbf{Q}}$ to a product of elliptic curves if and only if $H_{r,s,t} \subset (\mathbf{Z}/N\mathbf{Z})^*$ is a subgroup (necessarily of index 2).

In what follows we always assume that (r, s, t) is *primitive*, i.e., $g.c.d.(Nr, Ns, Nt) = 1$. If (r, s, t) were imprimitive, the $J_{[r,s,t]}$ piece of the jaco-

Received August 26, 1977. Revision received October 28, 1977