JOURNAL OF NUMBER THEORY 43, 31–42 (1993)

Kummer Congruences and Formal Groups

MARGARET N. FREIJE

Department of Mathematics, College of the Holy Cross, Worcester, Massachusetts 01610

Communicated by W. Sinnott

Received March 12, 1991; revised July 25, 1991

Let R be an integral domain and let $f(X) = (f_1(X), ..., f_n(X))$ be an n-tuple of power series in n variables $X = (x_1, ..., x_n)$ such that $df_i \in \bigoplus R[[X]]\, dx_i$, $f(X) \equiv 0 \pmod{\deg 1}$, and $J(f) = ((\partial f_i/\partial x_j)(0))$ is invertible over R. We can form the formal group $F_f(X, Y) = f^{-1}(f(X) + f(Y))$. A priori, the coefficients of F_f are in K, the quotient ring of R. T. Honda (*J. Math. Soc. Japan* **22**, 1970, 213–246) and M. Hazewinkel ("Formal Groups and Applications," Academic Press, Orlando, FL, 1978) give some sufficient conditions for $F_f(X, Y)$ to be defined over R in the form of functional equations for the coefficients of the f_i. This paper considers the converse question: Given a commutative formal group $F(X, Y)$ defined over a ring R, what necessary conditions must be satisfied by the coefficients of the logarithm of $F(X, Y)$? These results generalize the results of C. Snyder (*Rocky Mountain J. Math.* **15**, No. 1, 1985, 1–11) in the one dimensional case.

Notation. Let $I = (i_1, ..., i_n)$ be an index set. We let $I!$ denote $i_1! \cdots i_n!$, X^I denote the monomial $x_1^{i_1} \cdots x_n^{i_n}$, and $g(I)$ denote the g.c.d. of $i_1, ..., i_n$. (We say that the g.c.d. of n and 0 is n for all $n \geqslant 0$.)

INTRODUCTION

Kummer congruences for Hurwitz series were first studied in depth by L. Carlitz around 1940. Carlitz was able to give some sufficient conditions for a Hurwitz series to have Kummer congruences at a rational prime $\mathbf{p}$ by looking at the action of the differential operator $\Omega_{\mathbf{p}} = D^{\mathbf{p}} - a_{\mathbf{p}} D$, $D = d/dt$, on the series $f(t)$ [1]. Snyder was able to strengthen these results through a closer analysis of the action of $\Omega_{\mathbf{p}}$ [7].

Snyder also observed that the standard examples of Hurwitz series with Kummer congruences at all primes, satisfied algebraic laws of addition. In [8], Snyder generalized this and showed in particular that if $F(x, y)$ is a one dimensional formal group defined over $R_{(\mathbf{p})}$ (where R is an integral domain in a number field K and $R_{(\mathbf{p})}$ is R localized at $\mathbf{Z} - (\mathbf{p})$), then the

0022-314X/93 $5.00

641 43 1-3

inverse of the logarithm of F is a Hurwitz series with strong Kummer congruences at $\mathbf{p}$ [8, Theorem 2]. This result gives some interesting congruences for the coefficients of the logarithm and the invariant differential of the formal group. In particular he is able to recover the Atkin and Swinnerton-Dyer congruences for the coefficients in the expansion of the holomorphic differential on an elliptic curve.

In this paper we generalize some of Snyder's results to formal groups of higher dimension. In Section 1, we give the basic definitions for higher dimensional Hurwitz series, Kummer congruences, and the analog of the operator $\Omega_{(\mathbf{p})}$. In Theorem 1 we prove the equivalence of strong Kummer congruences for an n-dimensional series $f(T)$ and a set of congruences for the coefficients of the inverse series of f. In Section 2 we give the connections between higher dimensional formal groups and Hurwitz series. Theorem 2 gives the relationship between integral formal groups and strong Kummer congruences. A corollary of these results is a set of congruences that the coefficients of the logarithm of any integral formal group must satisfy. These congruences are similar to those given in Honda [4] and Hazewinkel [3] as necessary conditions for the integrality of a formal group. In Section 3 we apply these results to the formal group of the Jacobian of an algebraic curve. Using a construction for the formal group of the Jacobian given in Freije [2], we prove that the integrality of the formal group of the Jacobian gives a set of congruences which must be satisfied by the coefficients of the expansions at a non-Weierstrass point of a basis for the holomorphic differentials on the curve.

1. Hurwitz Series and Kummer Congruences

Let K be a field of characteristic 0, $R \subset K$ an integral domain containing Z, p a prime ideal in R, and $\mathbf{p}$ a prime number with $p \mid \mathbf{p}$.

Definition 1. An n-dimensional Hurwitz series over R is an n-tuple of power series

$$f(T) = (f_1(T), \ldots, f_n(T))$$

each of the form

$$f_i(T) = \sum_{I \geq 0} \frac{a_i(I)}{I!} T^I, \qquad a_i(I) \in R.$$

If $f(0) = 0$ and $J(f)$ is invertible over R, then it is easily shown that the inverse of $f(T)$, $\lambda(T)$ is also an n-dimensional Hurwitz series over R by repeatedly differentiating the equation $f(\lambda(T)) = T$.

We wish to consider only those invertible Hurwitz series f which satisfy the following hypothesis.

HYPOTHESIS K. *Let $f(T)$ be an invertible Hurwitz series over R and let $\lambda(T) = (\lambda_1(T), ..., \lambda_n(T))$ be the inverse of f where*

$$\lambda_j(T) = \sum_{I>0} \frac{c_j(I)}{I!} T^I, \qquad c_j(I) \in R.$$

We assume that

$$\frac{c_j(I)}{I!} = \frac{1}{g(I)} \varepsilon_j(I) \qquad \text{with} \quad \varepsilon_j(I) \in R.$$

Thus

$$\lambda_j(T) = \sum_{I>0} \frac{1}{g(I)} \varepsilon_j(I)\, T^I.$$

This hypothesis implies that

$$\frac{\partial \lambda_j}{\partial t_k}(T) \in R[[T]]$$

for all $j, k = 1, ..., n$.

PROPOSITION 1. *If f is an n-dimensional Hurwitz series satisfying Hypothesis K, then*

$$\frac{\partial f_i}{\partial t_j}(T) = \sum_{I \geq 0} d_{ij}(I)(f(T))^I,$$

where $d_{ij}(I) \in R$ for all $i, j = 1, ..., n$ and all I.

Proof. $\lambda(f(T)) = T$ implies

$$\left(\frac{\partial \lambda_i}{\partial t_j}(f(T))\right)\left(\frac{\partial f_i}{\partial t_j}(T)\right) = I_n$$

$$\left(\frac{\partial f_i}{\partial t_j}(T)\right) = \left(\frac{\partial \lambda_i}{\partial t_j}(f(T))\right)^{-1} \in GL_n(R[[f(T)]])$$

since $(\partial \lambda_i / \partial t_j)(T) \in R[[T]]$ and the Jacobian matrix of λ $J(\lambda)$ is invertible over R.

If $f(t)=\sum_{n=1}^{\infty} a_n(t^n/n!)$, $a_n \in R$, $a_1=1$, is an invertible one-dimensional Hurwitz series satisfying Hypothesis K, $f(t)$ is said to have Kummer congruences at $\mathbf{p}$, a rational prime, if and only if

$$\sum_{i=0}^{r} (-1)^{r-i} \binom{r}{i} a_{\mathbf{p}}^{r-i} a_{m+i(\mathbf{p}-1)} \equiv 0 \pmod{\mathbf{p}^r}$$

for all positive integers r and all $m \geqslant r$. Carlitz defined an operator $\Omega_{\mathbf{p}} = (D^{\mathbf{p}} - a_{\mathbf{p}} D)$, where Df is the derivative of f with respect to t and showed that if

$$\Omega_{\mathbf{p}}(f) = \sum \eta_j t^j \qquad \text{with} \quad \eta_j \in R \text{ and } \eta_j \equiv 0 \pmod{\mathbf{p}}$$

then f has Kummer congruences at $\mathbf{p}$ [1].

Snyder showed that f has Kummer congruences at $\mathbf{p}$ if and only if $\eta_j \equiv 0 \pmod{\mathbf{p}}$ for all $j < \mathbf{p}^2$ and gave the following definition [7].

DEFINITION 2. A series is said to have a strong Kummer congruence at $\mathbf{p}$ if $\eta_j \equiv 0 \pmod{\mathbf{p}}$, for all j.

Fix a rational prime $\mathbf{p}$ and a prime $p \in R$ with $p \mid \mathbf{p}$. We define $\Omega_{\mathbf{p}}$ as

$$\begin{aligned}\Omega_{\mathbf{p}}(f) &= \left(\frac{\partial^{\mathbf{p}} f_i}{\partial t_j^{\mathbf{p}}}(T)\right) - \left(\frac{\partial f_i}{\partial t_j}(T)\right)\left(\frac{\partial f_i}{\partial t_j}(0)\right)^{-1}\left(\frac{\partial^{\mathbf{p}} f_i}{\partial t_j^{\mathbf{p}}}(0)\right) \\ &= \left(\sum \eta_{ij}(I)(f(T))^I\right).\end{aligned}$$

If $f(T)$ satisfies Hypothesis K, then $\eta_{ij}(I) \in R$ by Proposition 1.

DEFINITION 3. We say $f(T)$ has strong Kummer congruences at $p \subset R$ if $\eta_{ij}(I) \equiv 0 \pmod{p}$ for all $i, j = 1, \ldots, n$ and all I.

THEOREM 1. *Let $f(T)$ be an invertible n-dimensional Hurwitz series satisfying Hypothesis* K. *Let $\lambda(T) = (\lambda_1(T), \ldots, \lambda_n(T))$ with*

$$\lambda_j(T) = \sum_{I>0} \frac{\varepsilon_j(I)}{g(I)} T^I$$

be its composition inverse, then f has strong Kummer congruences at p if and only if for every index set $I = (i_1, \ldots, i_n)$ we have

$$(\varepsilon_i(\mathbf{p}e_j))(\varepsilon_i^{\mathbf{p}}(e_j))^{-1}\begin{pmatrix} \varepsilon_1^{\mathbf{p}}(I) \\ \vdots \\ \varepsilon_n^{\mathbf{p}}(I) \end{pmatrix} \equiv \begin{pmatrix} \varepsilon_1(\mathbf{p}I) \\ \vdots \\ \varepsilon_n(\mathbf{p}I) \end{pmatrix} \pmod{p},$$

where e_j = jth standard basis vector.

(Note: If we assume $f(T) \equiv T \pmod{\deg 2}$, $(\varepsilon_i^{\mathbf{p}}(e_j)) = I_n$.)

Proof. Repeated differentiation of $f((\lambda(T))) = T$ implies

$$\left(\frac{\partial^{\mathbf{p}} f_i}{\partial t_j^{\mathbf{p}}}(\lambda(T))\right)\left(\left(\frac{\partial \lambda_j}{\partial t_j}(T)\right)^{\mathbf{p}}\right) + \left(\frac{\partial f_i}{\partial t_j}(\lambda(T))\right)\left(\frac{\partial^{\mathbf{p}} \lambda_j}{\partial t_j^{\mathbf{p}}}(T)\right) \equiv 0 \pmod{\mathbf{p}R[[T]]}. \tag{1}$$

Now, substitute $f(T)$ for T and consider this congruence over $R[[f]]$ to get

$$\left(\frac{\partial^{\mathbf{p}} f_i}{\partial t_j^{\mathbf{p}}}(T)\right)\left(\left(\frac{\partial \lambda_j}{\partial t_j}(f(T))\right)^{\mathbf{p}}\right) + \left(\frac{\partial f_i}{\partial t_j}(T)\right)\left(\frac{\partial^{\mathbf{p}} \lambda_j}{\partial t_j^{\mathbf{p}}}(f(T))\right) \equiv 0 \pmod{\mathbf{p}R[[f]]}. \tag{2}$$

f has strong Kummer congruences at p if and only if

$$\left(\frac{\partial^{\mathbf{p}} f_i}{\partial t_j^{\mathbf{p}}}(T)\right) \equiv \left(\frac{\partial f_i}{\partial t_j}(T)\right)\left(\frac{\partial f_i}{\partial t_j}(0)\right)^{-1}\left(\frac{\partial^{\mathbf{p}} f_i}{\partial t_j^{\mathbf{p}}}(0)\right) \pmod{pR[[f]]}.$$

Substituting this into (2) and using the fact that $((\partial f_i/\partial t_j)(T))$ is invertible over R we have that f has strong Kummer congruences at p if and only if

$$\left(\frac{\partial f_i}{\partial t_j}(0)\right)^{-1}\left(\frac{\partial^{\mathbf{p}} f_i}{\partial t_j^{\mathbf{p}}}(0)\right)\left(\left(\frac{\partial \lambda_j}{\partial t_j}(f(T))\right)^{\mathbf{p}}\right) + \left(\frac{\partial^{\mathbf{p}} \lambda_j}{\partial t_j^{\mathbf{p}}}(f(T))\right) \equiv 0 \pmod{pR[[f]]}.$$

Evaluating (1) at $T = 0$ gives

$$\left(\frac{\partial f_i}{\partial t_j}(0)\right)^{-1}\left(\frac{\partial^{\mathbf{p}} f_i}{\partial t_j^{\mathbf{p}}}(0)\right) \equiv -\left(\frac{\partial^{\mathbf{p}} \lambda_j}{\partial t_j^{\mathbf{p}}}(0)\right)\left(\left(\frac{\partial \lambda_j}{\partial t_j}(0)\right)^{\mathbf{p}}\right)^{-1} \pmod{\mathbf{p}R}.$$

Thus f has strong Kummer congruences at p if and only if

$$-\left(\frac{\partial^{\mathbf{p}} \lambda_j}{\partial t_j^{\mathbf{p}}}(0)\right)\left(\left(\frac{\partial \lambda_j}{\partial t_j}(0)\right)^{\mathbf{p}}\right)^{-1}\left(\left(\frac{\partial f_i}{\partial t_j}(f(T))\right)^{\mathbf{p}}\right) + \left(\frac{\partial^{\mathbf{p}} \lambda_j}{\partial t_j^{\mathbf{p}}}(f(T))\right) \equiv 0 \pmod{pR[[f]]}. \tag{3}$$

$$\left(\frac{\partial^{\mathbf{p}}\lambda_i}{\partial t_j^{\mathbf{p}}}(T)\right) = \sum \frac{i_j(i_j-1)\cdots(i_j-\mathbf{p}+1)}{g(I)}\varepsilon_i(I)\,T^{I-\mathbf{p}e_j}$$

$$\equiv -\sum \frac{i_j}{g(I)}\varepsilon_i(\mathbf{p}I)\,T^{\mathbf{p}I-\mathbf{p}e_j} \qquad (\mathrm{mod}\ \mathbf{p}).$$

$$\left(\frac{\partial\lambda_i}{\partial t_j}(T)\right)^{\mathbf{p}} \equiv \sum \frac{i_j}{g(I)}\varepsilon_i^{\mathbf{p}}(I)\,T^{\mathbf{p}I-\mathbf{p}e_j} \qquad (\mathrm{mod}\ \mathbf{p}R).$$

Substituting into (3) and comparing coefficients we have

$$\frac{i_k}{g(I)}\begin{pmatrix}\varepsilon_1(\mathbf{p}I)\\ \vdots\\ \varepsilon_n(\mathbf{p}I)\end{pmatrix} \equiv \frac{i_k}{g(I)}(\varepsilon_i(\mathbf{p}e_j))(\varepsilon_i^{\mathbf{p}}(e_j))^{-1}\begin{pmatrix}\varepsilon_1^{\mathbf{p}}(I)\\ \vdots\\ \varepsilon_n^{\mathbf{p}}(I)\end{pmatrix} \qquad (\mathrm{mod}\ p)$$

for all $k = 1, \ldots, n$ and all I.

The result follows since $i_k/g(I) \not\equiv 0 \pmod{\mathbf{p}}$ for at least one k.

2. Formal Groups and Kummer Congruences

Let K be a number field, $R \subset K$ an integral domain, p a prime ideal in R, and $\mathbf{p}$ a rational prime with $p \mid \mathbf{p}$.

Let $F(X, Y)$ be a commutative formal group of dimension n defined over K, i.e.,

$$F(X, Y) = (F_1(X, Y), \ldots, F_n(X, Y)), \qquad F_i(X, Y) \in K[[X, Y]]$$

satisfying

$$F(X, 0) = X \qquad F(0, Y) = Y$$

$$F(F(X, Y), Z) = F(X, F(Y, Z))$$

$$F(X, Y) = F(Y, X).$$

A differential $\omega \in \sum_{i=1}^{n} K[[X]]\,dx_i$ is an invariant differential of F if

$$\omega(F(X, Y)) = \omega(X) + \omega(Y).$$

It can be shown that ω is an invariant differential of F if and only if

$$\omega = (a_1, \ldots, a_n)\left(\frac{\partial F_i}{\partial x_j}(0, X)\right)^{-1}\begin{pmatrix}dx_1\\ \vdots\\ dx_n\end{pmatrix},$$

where $\omega|_0 = a_1\,dx_1 + \cdots + a_n\,dx_n$. Thus the space of invariant differentials has dimension n over K.

Let $\omega_1, \ldots, \omega_n$ be a basis of invariant differentials of $F(X, Y)$. If $F(X, Y)$ is commutative there exist power series $\lambda_1(X), \ldots, \lambda_n(X)$ with $\lambda_i(X) \in K[[X]]$, $d\lambda_i(X) = \omega_i$, and $\lambda_i(0) = 0$.

Let $\lambda = (\lambda_1(X), \ldots, \lambda_n(X))$ then λ is invertible and $\lambda(F(X, Y)) = \lambda(X) + \lambda(Y)$. λ is called the logarithm of F associated to the basis $\omega_1, \ldots, \omega_n$. (See [4] for details.)

Let $F(X, Y)$ be a commutative formal group of dimension n defined over K and assume F has a basis of invariant differentials defined over R_p. Let λ be the logarithm associated to this basis. Then we can write

$$\lambda_j = \sum_{I>0} \frac{1}{g(I)}\,\varepsilon_j(I)\,X^I \qquad \text{with} \quad \varepsilon_j(I) \in R_p.$$

Let $f(X)$ be the composition inverse of λ. Then f is an n-dimensional Hurwitz series satisfying Hypothesis K of Section 1.

Conversely, if f is a Hurwitz series over R_p satisfying Hypothesis K, we can form the commutative formal group $F_f(X, Y)$ defined by

$$F_f(X, Y) = f(f^{-1}(X) + f^{-1}(Y)).$$

If $\lambda = f^{-1}$, λ is a logarithm of F_f and the basis of invariant differentials of F associated to λ, $\{d\lambda_1, \ldots, d\lambda_n\}$, is defined over R_p.

The following theorem gives the relationship between the integrality of a formal group and strong Kummer congruences.

THEOREM 2. *Let $F(X, Y)$ be a commutative formal group defined over R_p. Let $\omega_1, \ldots, \omega_n$ be a basis for the formal invariant differentials of F defined over R_p and let λ be the corresponding logarithm. Then $f(X) = \lambda^{-1}(X)$ has strong Kummer congruences at p.*

COROLLARY. *Let $F(X, Y)$ and $\lambda(X)$ satisfy the hypotheses of Theorem 2. We can write*

$$\lambda_j = \sum_{I>0} \frac{1}{g(I)}\,\varepsilon_j(I)\,X^I \qquad \text{with} \quad \varepsilon_j(I) \in R_p.$$

Then the coefficients satisfy

$$\begin{pmatrix} \varepsilon_1(\mathbf{p}I) \\ \vdots \\ \varepsilon_n(\mathbf{p}I) \end{pmatrix} \equiv (\varepsilon_i(\mathbf{p}e_j))(\varepsilon_i^{\mathbf{p}}(e_j))^{-1} \begin{pmatrix} \varepsilon_1^{\mathbf{p}}(I) \\ \vdots \\ \varepsilon_n^{\mathbf{p}}(I) \end{pmatrix} \pmod{pR_p}.$$

Proof of the Theorem. $f(X)$ is a Hurwitz series over R_p satisfying Hypothesis K so we must show

$$\Omega_{\mathbf{p}} f \equiv 0 \qquad (\text{mod } pR_p[[f]]).$$

$$f(X+Y) = F(f(X), f(Y))$$

$$\left(\frac{\partial f_i}{\partial x_j}(X+Y)\right) = \left(\frac{\partial F_i}{\partial x_j}(f(X), f(Y))\right)\left(\frac{\partial f_i}{\partial x_j}(X)\right).$$

Evaluating at $X=0$ and rearranging terms we have

$$\left(\frac{\partial F_i}{\partial x_j}(0, f(Y))\right) = \left(\frac{\partial f_i}{\partial x_j}(Y)\right)\left(\frac{\partial f_i}{\partial x_j}(0)\right)^{-1}.$$

Similarly,

$$\left(\frac{\partial^{\mathbf{p}} f_i}{\partial x_j^{\mathbf{p}}}(Y)\right) \equiv \left(\frac{\partial^{\mathbf{p}} F_i}{\partial x_j^{\mathbf{p}}}(0, f(Y))\right)\left(\left(\frac{\partial f_i}{\partial x_j}(0)\right)^{\mathbf{p}}\right)$$
$$+\left(\frac{\partial F_i}{\partial x_j}(0, f(Y))\right)\left(\frac{\partial^{\mathbf{p}} f_i}{\partial x_j^{\mathbf{p}}}(0)\right) \qquad (\text{mod } \mathbf{p}R_p[[f]]).$$

But

$$\frac{\partial^{\mathbf{p}} F_i}{\partial x_j^{\mathbf{p}}}(0, f(Y)) \equiv 0 \qquad (\text{mod } pR_p[[f]])$$

for all i, j since $F_i(X, Y) \in R_p[[X, Y]]$.

Thus

$$\left(\frac{\partial^{\mathbf{p}} f_i}{\partial x_j^{\mathbf{p}}}(Y)\right) \equiv \left(\frac{\partial f_i}{\partial x_j}(Y)\right)\left(\frac{\partial f_i}{\partial x_j}(0)\right)^{-1}\left(\frac{\partial^{\mathbf{p}} f_i}{\partial x_j^{\mathbf{p}}}(0)\right) \qquad (\text{mod } pR_p[[f]]),$$

i.e., $\Omega_p(f) \equiv 0 \pmod{pR_p[[f]]}$.

3. Kummer Congruences and Holomorphic Differentials on an Algebraic Curve

Let C be a complete non-singular curve of genus g defined over a number field K. The Jacobian of C is an abelian variety of dimension g defined over K. An explicit construction of the formal group of the Jacobian is given as follows. (For details see [2].)

Let P_0 be a K-rational point on C which is not a Weierstrass point and let t be a parameter at P_0. We can choose a basis for the holomorphic

differentials of C such that the K-expansions of $\omega_1, \ldots, \omega_g$ with respect to the parameter t satisfy

$$\omega_i = \sum_{n=1}^{\infty} a_i(n)\, t^{n-1}\, dt$$

with

$$\begin{pmatrix} a_1(1) \cdots a_1(g) \\ \vdots \quad \ddots \quad \vdots \\ a_g(1) \cdots a_g(g) \end{pmatrix}$$

invertible.

Let $l_i(t)$ be the integral of the formal power series ω_i satisfying $l_i(0) = 0$ for $i = 1, \ldots, g$ and let

$$L_i(T) = L_i(t_1, \ldots, t_g) = l_i(t_1) + \cdots + l_i(t_g).$$

The series $L_i(T)$ is symmetric in $t_1, \ldots, t_g$ and thus we can write

$$L_i(T) = \lambda_i(s_1(T), \ldots, s_g(T)),$$

where s_i is the i th symmetric function on g letters.

Let J be the Jacobian of C and let $\Lambda: C \to J$ be the canonical map defined over K with $\Lambda(P_0) =$ origin of J. Λ extends to a map Λ^g: $\mathrm{Sym}^{(g)}(C) \to J$ which is birational over K and biregular in a neighborhood of $\Lambda(P_0)$. In addition the induced map

$$(\Lambda^g)^*: \Gamma(J, \Omega^1) \to \Gamma(C^{(g)}, \Omega^1)$$

between the spaces of holomorphic differentials is an isomorphism (see, for example, [5]). Thus we regard $(s_i(T), \ldots, s_g(T))$ as a set of local parameters at the origin of J and $d\lambda_i$ as the local expansion at the origin of a differential on J.

The map $\Lambda: C \to J$ induces a bijection

$$\Lambda^*: \Gamma(J, \Omega^1) \to \Gamma(C, \Omega^1).$$

One can show that $\Lambda^*(d\lambda_i)$ is a holomorphic differential of C for $i = 1, \ldots, g$ and thus $d\lambda_i$ is the local expansion of a holomorphic differential on J. If $\omega_1, \ldots, \omega_g$ are chosen as above then $\{d\lambda_1, \ldots, d\lambda_g\}$ can be shown to be a basis for the invariant differentials of the formal group of J. Thus we have the following theorem.

THEOREM 3. *Let $\lambda(X) = (\lambda_1, \ldots, \lambda_g)$ where λ_i is the formal power series defined above. Then $\lambda(X)$ is the logarithm of the formal group of the Jacobian of C.*

Proof. See Freije [2].

Let C be a curve with good reduction at p, p a prime ideal in the ring of integers of K. We can find a basis $\omega_1, \ldots, \omega_g$ of holomorphic differentials such that the K-expansions at P_0 satisfy

$$\omega_i = \sum_{n=1}^{\infty} a_i(n)\, t^{n-1}\, dt$$

with $a_i(n) \in R_p$ and

$$\begin{pmatrix} a_1(1) \cdots a_1(g) \\ \vdots \quad \ddots \quad \vdots \\ a_g(1) \cdots a_g(g) \end{pmatrix}$$

invertible over R_p.

The series $\lambda_i(X)$ constructed above can be given explicitly by

$$\lambda_i(X) = \sum_{I>0} B(I)\, a_i(N_I)\, X^I,$$

where $I = (i_1, \ldots, i_g)$ runs through all index sets with $i_k \geqslant 0$ for all k, $i_k \neq 0$ for at least one k, $N_I = i_1 + 2i_2 + \cdots + gi_g$, and

$$B(I) = \frac{(-1)^{i_2+i_4+\cdots}(i_1+i_2+\cdots+i_g-1)!}{i_1!\, i_2!, \ldots, i_g!}.$$

If the formal group of the Jacobian constructed from this logarithm is defined over R_p, the results of Section 2 give the following congruences for the coefficients in the expansions of the holomorphic differentials $\omega_1, \ldots, \omega_g$ on C.

THEOREM 4. *If the formal group of the Jacobian of C, $\mathrm{Jac}(X, Y)$ constructed from the basis described above is defined over R_p, then the coefficients in the expansions of $\omega_1, \ldots, \omega_g$ satisfy*

$$\begin{pmatrix} a_1(\mathbf{p}n) \\ \vdots \\ a_g(\mathbf{p}n) \end{pmatrix} \equiv (a_i(j\mathbf{p}))(a_i^{\mathbf{p}}(j))^{-1} \begin{pmatrix} a_1^{\mathbf{p}}(n) \\ \vdots \\ a_g^{\mathbf{p}}(n) \end{pmatrix} \pmod{pR_p}$$

for all $n \in \mathbf{Z}^+$.

Proof. The logarithm of $\mathrm{Jac}(X, Y)$, $\lambda(X) = (\lambda_1(X), \ldots, \lambda_g(X))$ with

$$\lambda_i(X) = \sum_{I>0} B(I)\, a_i(N_I)\, X^I = \sum_{I>0} \frac{1}{g(I)} (g(I)\, B(I)\, a_i(N_I))\, X^I.$$

Since $i_k B(I)$ is a multinomial coefficient and thus an integer for all $k = 1, ..., g$, $g(I)\, B(I) \in \mathbf{Z}$. Thus

$$\varepsilon_i(I) = B(I)\, g(I)\, a_i(N_I) \in R_p.$$

We can therefore apply the Corollary to Theorem 2,

$$\varepsilon_i(e_j) = (-1)^{j+1}\,(1)(a_i(j))$$

$$\varepsilon_i(\mathbf{p}e_j) = \left(\frac{(-1)^{j+1}}{\mathbf{p}}\right)(\mathbf{p})(a_i(j\mathbf{p})),$$

$$\begin{pmatrix} \varepsilon_1(\mathbf{p}I) \\ \vdots \\ \varepsilon_g(\mathbf{p}I) \end{pmatrix} \equiv (a_i(j\mathbf{p})(a_i^{\mathbf{p}}(j))^{-1} \begin{pmatrix} \varepsilon_1^{\mathbf{p}}(I) \\ \vdots \\ \varepsilon_g^{\mathbf{p}}(I) \end{pmatrix} \pmod{pR_p}$$

for all I.

Let $I = (n, 0, ..., 0)$,

$$\varepsilon_i(\mathbf{p}I) = \left(\frac{1}{\mathbf{p}n}\right)(\mathbf{p}n)(a_i(\mathbf{p}n)).$$

$$\varepsilon_i(I) = \left(\frac{1}{n}\right)(n)(a_i(n)).$$

Thus

$$\begin{pmatrix} a_1(\mathbf{p}n) \\ \vdots \\ a_g(\mathbf{p}n) \end{pmatrix} \equiv (a_i(j\mathbf{p}))(a_i^{\mathbf{p}}(j))^{-1} \begin{pmatrix} a_1^{\mathbf{p}}(n) \\ \vdots \\ a_g^{\mathbf{p}}(n) \end{pmatrix} \pmod{pR_p}$$

for all n.

COROLLARY. *If* $a_i(j\mathbf{p}) \equiv a_i(\mathbf{p})\, a_i^{\mathbf{p}}(j) \pmod{pR_p}$ *for* $j \leqslant$ *genus* g *then* $a_i(n\mathbf{p}) \equiv a_i(\mathbf{p})\, a_i^{\mathbf{p}}(n) \pmod{pR_p}$ *for all* n.

Proof.

$$a_i(n\mathbf{p}) \equiv (a_i(\mathbf{p}), ..., a_i(g\mathbf{p}))(a_i^{\mathbf{p}}(j))^{-1} \begin{pmatrix} a_1^{\mathbf{p}}(n) \\ \vdots \\ a_g^{\mathbf{p}}(n) \end{pmatrix} \pmod{pR_p}$$

$$\equiv a_i(\mathbf{p})(a_i^{\mathbf{p}}(1), ..., a_i^{\mathbf{p}}(g))(a_i^{\mathbf{p}}(j))^{-1} \begin{pmatrix} a_1^{\mathbf{p}}(n) \\ \vdots \\ a_g^{\mathbf{p}}(n) \end{pmatrix} \pmod{pR_p}$$

$$= a_i(\mathbf{p})\, a_i^{\mathbf{p}}(n).$$

Remarks. (1) In the case where the base field is $\mathbf{Q}$, the congruences given in the Corollary to Theorem 2 for the coefficients of the logarithm of an integral formal group are very similar to the functional equations given in Honda [4] and Hazewinkel [3] as sufficient conditions for the integrality of the formal group. It is an open question whether a modification of these results would give a set of necessary and sufficient conditions for the coefficients of the logarithm to ensure the integrality of the corresponding formal group.

(2) For formal groups of dimension one, these results were proven by Snyder [8]. It is well known that the formal group of a curve of genus one, an elliptic curve, defined over $\mathbf{Q}$ has coefficients in $\mathbf{Z}$ (see [6]). When applied to these curves, the congruences of Theorem 4 (Theorem 2 in [8]) are the congruences of Atkin and Swinnerton-Dyer for the holomorphic differential on the elliptic curve.

(3) If the curve C is a modular curve $X_0(l)$, l a prime, the cusp at $i\infty$ is not a Weierstrass point. One can choose a basis for the holomorphic differentials at this point corresponding to the $\mathbf{Q}$-basis for the cusp forms of weight 2 for $\Gamma_0(l)$. Using the action of the Hecke and Atkin operators on the Fourier expansions of these cusp forms one can show that the formal group of the Jacobian of C is defined over $\mathbf{Z}_\mathbf{p}$ for all primes $\mathbf{p}$ not in an explicit finite set. (See [2]). On the other hand, if one knows a priori that the formal group constructed from a particular basis is defined over $\mathbf{Z}_\mathbf{p}$, Theorem 4 gives congruences of Atkin Lehner type for the coefficients in the Fourier expansions of the corresponding cusp forms.

REFERENCES

1. L. CARLITZ, The coefficients of the reciprocal of a series, *Duke Math. J.* **8** (1941), 689–700.
2. M. FREIJE, The formal group of the Jacobian of an algebraic curve, *Pacific J. Math.*, in press.
3. M. HAZEWINKEL, "Formal Groups and Applications," Academic Press, Orlando, FL, 1978.
4. T. HONDA, On the theory of commutative formal groups, *J. Math. Soc. Japan* **22** (1970), 213–246.
5. J. S. MILNE, Abelian varieties, *in* "Arithmetic Geometry" (G. Cornell and J. Silverman, Eds.), Springer-Verlag, New York/Berlin, 1986.
6. J. SILVERMAN, "The Arithmetic of Elliptic Curves," Springer-Verlag, New York/Berlin, 1986.
7. C. SNYDER, Kummer congruences for the coefficients of Hurwitz series, *Acta Arith.* **40** (1982), 175–191.
8. C. SNYDER, Kummer congruences in formal groups and algebraic groups of dimension one, *Rocky Mountain J. Math.* **15**, No. 1 (1985), 1–11.