

*Pacific
Journal of
Mathematics*

**THE FORMAL GROUP OF THE JACOBIAN OF AN
ALGEBRAIC CURVE**

MARGARET N. FREIJE

Volume 157 No. 2

February 1993

THE FORMAL GROUP OF THE JACOBIAN OF AN ALGEBRAIC CURVE

MARGARET N. FREIJE

In this paper we give an explicit construction of the formal group of the Jacobian of an algebraic curve using a basis for the holomorphic differentials on the curve at a rational non-Weierstrass point. We construct the formal group of the Jacobian of the modular curve $X_0(l)$ and using a result of T. Honda, we prove that this formal group is p -integral for all but finitely many p .

Introduction. Formal group laws have proven to be very useful tools in many areas of mathematics and computer science. In particular, the formal group of an elliptic curve has been used to great effect in elliptic curve theory (for details see for example Silverman [13]) and the use of the formal group of an abelian variety is pervasive in arithmetic and algebraic geometry (see Shatz [11] or Milne [8]). Despite the fact that explicit formulae have been useful in the elliptic curve case, explicit examples of the formal group of other abelian varieties are few.

Recently, Grant [4] and Flynn [3] have independently given explicit constructions of the formal group of the Jacobian of curves of genus two. Grant uses classical formulae for genus two theta functions to give explicit defining equations for the Jacobian and a set of parameters for its group law in a specific \mathbb{P}^8 embedding. His embedding requires that the curve have a Weierstrass point defined over the base field. Flynn's result does not assume the existence of a rational Weierstrass point and thus he must use a \mathbb{P}^{15} embedding of the Jacobian. This paper gives an explicit construction of the formal group of the Jacobian using a basis for the holomorphic differentials on the curve. The construction generalizes that of the formal group of an elliptic curve.

In §I, we review some of the basic facts about higher dimensional formal groups. Hazewinkel [5] is a good reference for the theory of formal groups in general. Section II details the construction of the formal group of the Jacobian. Since this construction depends only on a basis for the holomorphic differentials on the curve at a non-Weierstrass point, it is especially useful in cases where much is known

about these differentials. In §III, we give an example of just such a case and construct the formal group of the Jacobian of the modular curve $X_0(l)$, l a prime. Using a result of T. Honda, and the connection between the differentials on this curve and the Fourier expansions of cusp forms of weight 2 on $\Gamma_0(l)$ we prove that this formal group is p -integral for all but finitely many primes p .

The author wishes to thank the referee for many helpful suggestions on the styles and organization of this paper.

I. Higher dimensional formal groups. Let R be a commutative ring with identity and let $R[[X]]$, $X = (x_1, \dots, x_n)$, be the power series ring in n variables over R . If $f(X)$ and $g(X) \in R[[X]]$ and n is a positive integer, we say $f(X) \equiv g(X) \pmod{\deg n}$ if $f(X) - g(X)$ has no terms of total degree less than n .

DEFINITION 1. A formal group law $F(X, Y)$ of dimension n over R is an n -tuple of power series $(F_1(X, Y), \dots, F_n(X, Y))$, $F_i(X, Y) \in R[[X, Y]]$, satisfying:

- (i) $F(X, 0) = X$, $F(0, Y) = Y$,
- (ii) $F(X, F(Y, Z)) = F(F(X, Y), Z)$.

It is an easy exercise to show that one has formal inverses, that is there is an n -tuple of power series $\iota(X) = (\iota_1(X), \dots, \iota_n(X))$, $\iota_j(X) \in R[[X]]$, satisfying $\iota(X) \equiv -X \pmod{\deg 2}$ and $F(X, \iota(X)) = 0$.

If $F(X, Y) = F(Y, X)$ we say F is a commutative formal group.

DEFINITION 2. (a) If $F(X, Y)$ is a formal group of dimension n and $G(X, Y)$ is a formal group of dimension m then $\alpha: F \rightarrow G$ is a formal group homomorphism over R if $\alpha(X) = (\alpha_1(X), \dots, \alpha_m(X))$ is an m -tuple of power series, $\alpha_i(X) \in XR[[X]]$, satisfying $\alpha(F(X, Y)) = G(\alpha(X), \alpha(Y))$.

(b) If $\alpha: F \rightarrow G$ is a formal group homomorphism over R , then α is a formal group isomorphism over R if and only if there is a formal group homomorphism $\beta: G \rightarrow F$ over R such that $\alpha(\beta(Y)) = Y$ and $\beta(\alpha(X)) = X$.

It can be shown that $\alpha: F \rightarrow G$ is a formal group isomorphism over R if and only if $\dim F = \dim G$ and the Jacobian matrix of α , $J(\alpha) = ((\partial\alpha_i/\partial x_j)(0))$ is invertible over R .

EXAMPLES. 1. The additive group of dimension n , $\mathbb{G}_a(X, Y)$:

$$\mathbb{G}_a(X, Y) = (x_1 + y_1, \dots, x_n + y_n).$$

2. The multiplicative group of dimension n , $\mathbb{G}_m(X, Y)$:

$$\mathbb{G}_m(X, Y) = (x_1 + y_1 + x_1 y_1, \dots, x_n + y_n + x_n y_n).$$

3. Let $\alpha(X) = (\ln(1 + x_1), \ln(1 + x_2), \dots, \ln(1 + x_n))$. Then α is a formal group isomorphism over \mathbb{Q} between \mathbb{G}_m and \mathbb{G}_a , i.e.,

$$\alpha(\mathbb{G}_m(X, Y)) = \mathbb{G}_a(\alpha(X), \alpha(Y)) = \alpha(X) + \alpha(Y) \quad \text{and} \\ J(\alpha) = n \times n \text{ identity matrix.}$$

The isomorphism α is an example of a more general fact. If R is a \mathbb{Q} -algebra and $F(X, Y)$ is a commutative formal group over R of dimension n then there is a formal group isomorphism between F and the additive group of dimension n . We now show briefly how to construct this isomorphism.

Let $\Omega = \sum R[[X]] dx_i$ be the space of differential 1-forms where d is the total derivative map from $R[[X]]$ to Ω . If $\omega = \sum_{i=1}^n \varphi_i(X) dx_i$, $\varphi_i(X) \in R[[X]]$ is in Ω , then you can get a new differential by evaluating $\omega(a) = \sum_{i=1}^n \varphi_i(a) dx_i$ for any $a \in R^n$.

We define $\omega = \sum_{i=1}^n \varphi_i(X) dx_i$, $\varphi_i(X) \in R[[X]]$, to be translation invariant if $\omega(F(X, T)) = \sum_{i=1}^n \varphi_i(F(X, T)) dF(X, T) = \omega$. Thus we have ω is invariant if and only if

$$(1) \quad (\varphi_1(F(X, T)), \dots, \varphi_n(F(X, T))) \left(\frac{\partial F_i}{\partial x_j}(X, T) \right) \\ = (\varphi_1(X), \dots, \varphi_n(X)).$$

Evaluating at $X = 0$ clearly implies

$$(2) \quad (\varphi_1(T), \dots, \varphi_n(T)) = (\varphi_1(0), \dots, \varphi_n(0)) \left(\frac{\partial F_i}{\partial x_j}(0, T) \right)^{-1}.$$

On the other hand if we use the associative law for F , differentiate $F_i(Y, F(X, T)) = F_i((F(Y, X), T))$ with respect to y_j and then set $Y = 0$, we have:

$$(3) \quad \left(\frac{\partial F_i}{\partial x_j}(0, F(X, T)) \right) = \left(\frac{\partial F_i}{\partial x_j}(X, T) \right) \left(\frac{\partial F_i}{\partial x_j}(0, X) \right).$$

Substituting $F(X, T)$ for T in (2) and using (3) we have (2) is equivalent to (1).

We have therefore that ω is invariant if and only if

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

Thus the space of invariant differentials of F is an R module of rank n .

There is also a map d from Ω to the space of differential 2-forms Ω^2 . If R is a \mathbb{Q} -algebra, $d\omega = 0$ implies $\omega = df$ for some $f \in R[[X]]$. If F is a commutative formal group over R and ω is an invariant differential of F then $d\omega = 0$ (Proposition 1.3, Honda [6]) and thus if R is a \mathbb{Q} -algebra $\omega = df$, $f \in R[[X]]$.

Let F be a commutative formal group defined over a \mathbb{Q} -algebra R and let $\omega_1, \dots, \omega_n$ be a basis for the invariant differentials of F over R . Let $\mathcal{L}_i(X) \in R[[X]]$ be the unique power series such that

$$d\mathcal{L}_i = \sum_{j=1}^n \frac{\partial \mathcal{L}_i}{\partial x_j}(X) dx_j = \omega_i \quad \text{and} \quad \mathcal{L}_i(0) = 0.$$

We then have the following well-known theorem:

THEOREM 1. *Let F be a commutative formal group of dimension n defined over a \mathbb{Q} -algebra R . Let $\mathcal{L}(X) = (\mathcal{L}_1(X), \dots, \mathcal{L}_n(X))$ with $\mathcal{L}_i(X)$ defined as above. Then $\mathcal{L}(X)$ is a formal group isomorphism $\mathcal{L}: F \rightarrow \mathbb{G}_a^n$ from F to the additive group of dimension n .*

Proof. ω_i is an invariant differential of F ; thus $\omega_i(F(X, T)) = \omega_i(X)$ over $R[[T]]$. This implies that $\mathcal{L}_i(F(X, T)) = \mathcal{L}_i(X) + c(T)$ where $c(T) \in R[[T]]$. Evaluating at $X = 0$ we get $c(T) = \mathcal{L}_i(F(0, T)) = \mathcal{L}_i(T)$. Thus \mathcal{L} is a formal group homomorphism from F to \mathbb{G}_a^n over R . The Jacobian matrix of \mathcal{L} , $J(\mathcal{L}) = (a_{ij})$ where $\omega_i(0) = \sum a_{ij} dx_j$. This is invertible over F since $\omega_1, \dots, \omega_n$ is an R -basis. Thus \mathcal{L} is a formal group isomorphism over R and $F(X, Y) = \mathcal{L}^{-1}(\mathcal{L}(X) + \mathcal{L}(Y))$.

The isomorphism \mathcal{L} is called a logarithm of F . If $J(\mathcal{L}) =$ the identity matrix, then \mathcal{L} is called the strict logarithm of F .

II. The formal group of the Jacobian of an algebraic curve.

NOTATION. If $I = (i_1, \dots, i_g)$ is an index set of nonnegative integers, let $I!$ denote $i_1!i_2! \cdots i_g!$, $N_I = i_1 + 2i_2 + \cdots + gi_g$ and

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

For any $k = 1, \dots, g$, $i_k B(I)$ is a multinomial coefficient and thus is an integer. If $X = (x_1, \dots, x_g)$ is a g -tuple of variables, let X^I denote $x_1^{i_1} x_2^{i_2} \cdots x_g^{i_g}$ and $S(X) = (s_1(X), \dots, s_g(X))$ where $s_i(X)$ is the i th symmetric function on g letters. Finally, let e_k be the standard k th basis vector in \mathbb{R}^g and let e be the g -tuple $(1, 1, \dots, 1)$.

Let C be a complete nonsingular algebraic curve of genus g defined over a field K , of characteristic zero. Let A be the Jacobian of C . A is an abelian variety of dimension g defined over K . If O is the local ring of functions defined at the origin, \mathcal{M} its maximal ideal and \widehat{O} the completion of O in the \mathcal{M} -adic topology, then \widehat{O} is isomorphic to $K[[X]]$ where $X = (x_1, \dots, x_g)$ is a system of parameters at the origin. The group morphism $m: A \times A \rightarrow A$ induces a map $m^*: \widehat{O} \rightarrow \widehat{O} \times \widehat{O}$. Thus there are power series $\widehat{A}_i(X, Y) \in K[[X, Y]]$ such that $m_i^* = \widehat{A}_i(X, Y)$. Since A is an abelian variety, it is easy to check that $\widehat{A}(X, Y) = (\widehat{A}_1(X, Y), \dots, \widehat{A}_g(X, Y))$ defines a commutative formal group, the formal group of the Jacobian of C . Changing the choice of parameters gives rise to an isomorphic though not strictly isomorphic formal group so we will make a definite choice of parameters.

Let P_0 be a K -rational point on C which is not a Weierstrass point and let t be a local parameter at P_0 . Choose a basis $\{\eta_1, \dots, \eta_g\}$ for the holomorphic differentials of C such that the K -expansion of η_i with respect to the parameter t satisfies

$$\eta_i \equiv (-t)^{i-1} dt \pmod{t^g dt}.$$

(See for example [1] to see that this can be done.) Let $l_i(t) = \int \eta_i$ be the integral of the formal power series η_i satisfying $l_i(0) = 0$ for $i = 1, \dots, g$ and let

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

L_i is symmetric in t_1, \dots, t_g and thus $L_i(t_1, \dots, t_g) = \mathcal{L}_i(S(T))$ where \mathcal{L}_i is a power series in g variables.

Let $\Lambda: C \rightarrow A$ be the canonical map defined over K with $\Lambda(P_0) =$ origin of A . Λ extends to a map $\Lambda^{(g)}: \text{Sym}^{(g)} C \rightarrow A$ which is birational over K and biregular in a neighborhood of $Q = (P_0, \dots, P_0)$. This map induces isomorphisms between the completed local ring of A and the completed local ring of $\text{Sym}^{(g)} C$ and between the space of holomorphic differentials on A and those on $\text{Sym}^{(g)} C$. Thus we regard $(s_1(T), \dots, s_g(T))$ as a set of local parameters at the origin of A and $d\mathcal{L}_i$ as the local expansion at the origin of a differential on A . Using this identification we have the following theorem:

THEOREM 2. $\mathcal{L}(X) = (\mathcal{L}_1(X), \dots, \mathcal{L}_g(X))$ is the strict logarithm of the formal group of the Jacobian of C , i.e.,

$$\widehat{A}(X, Y) = \mathcal{L}^{-1}(\mathcal{L}(X) + \mathcal{L}(Y))$$

is the formal group of the Jacobian of C and $\mathcal{L}(X) \equiv X \pmod{\deg 2}$.

Before proving the theorem, we need the following lemma expressing the sum of the n th powers of the variables x_i as a polynomial in the symmetric functions.

LEMMA 1. Let $P_n(X) = x_1^n + \dots + x_g^n$.
Then

$$P_n(X) = n \sum_{\substack{I \\ N_i=n}} B(I)(S(X))^I.$$

Proof. $P_n(X)$ satisfies Newton's identities. That is,

$$P_n(X) = \sum_{j=1}^{n-1} (-1)^{j+1} s_j(X) P_{n-j}(X) + (-1)^{n+1} n s_n(X)$$

where $s_j(X)$ is defined to be 0 if $j > g$.

The lemma follows from these identities by induction. It is clearly true for $n = 1$. Assume it is true for all integers less than n , then we have:

$$\begin{aligned} P_n(X) &= \sum_{j=1}^{n-1} (-1)^{j+1} s_j(X) \left((n-j) \sum_{\substack{I' \\ N_{i'}=n-j}} B(I')(S(X))^{I'} \right) \\ &\quad + (-1)^{n+1} n s_n(X) \\ &= \sum_{j=1}^{\min(n-1, g)} (-1)^{j+1} \left((n-j) \sum_{j=1}^{n-1} B(I')(S(X))^{I'+e_j} \right) \\ &\quad + (-1)^{n+1} n s_n(X). \end{aligned}$$

Let $I = I' + e_j$ then $B(I') = ((-1)^{j+1} i_j / (i_1 + \dots + i_g - 1)) B(I)$.

As j runs from 1 to $\min(n - 1, g)$ and I' runs through all index sets with $N_{I'} = n - j$, I runs through index sets with $N_I = n$ except possibly $I = e_n$ where $n \leq g$.

If $n \geq g$ we get:

$$\begin{aligned} P_n(X) &= \sum_{\substack{I \neq e_n \\ N_I = n}} B(I)(S(X))^I \frac{1}{i_1 + \dots + i_g - 1} \sum_{j=1}^{n-1} (n-j)i_j + B(e_n)ns_n(X) \\ &= \sum_{\substack{I \neq e_n \\ N_I = n}} B(I)(S(X))^I \frac{1}{i_1 + \dots + i_g - 1} \sum_{j=1}^g (n-j)i_j + B(e_n)ns_n(X) \end{aligned}$$

since if $N_I = n \leq g$, $I \neq e_n$, $i_j = 0$ for $j = n, \dots, g$, we can replace $n - 1$ by g in the summation. Therefore

$$\begin{aligned} &= \sum_{\substack{I \neq e_n \\ N_I = n}} B(I)(S(X))^I \frac{1}{i_1 + \dots + i_g - 1} \left(\sum_{j=1}^g (ni_j) - N_I \right) + B(e_n)ns_n(X) \\ &= \sum_{\substack{I \neq e_n \\ N_I = n}} nB(I)(S(X))^I \frac{1}{i_1 + \dots + i_g - 1} \left(\sum_{j=1}^g (i_j) - 1 \right) + B(e_n)ns_n(X) \\ &= n \sum_{\substack{I \\ N_I = n}} B(I)(S(X))^I. \end{aligned}$$

If $n > g$, as j runs from 1 to $n - 1$ and I' runs through all index sets with $N_{I'} = n - j$, I runs through all index sets with $N_I = n$. Thus we have

$$\begin{aligned} P_n(X) &= \sum_{\substack{I \\ N_I = n}} B(I)(S(X))^I \frac{1}{i_1 + \dots + i_g - 1} \left(\sum_{j=1}^g (n-j)i_j \right) \\ &= \sum_{\substack{I \\ N_I = n}} B(I)(S(X))^I \quad \text{as above.} \end{aligned}$$

Proof of Theorem 2. By the results of the last section, we must show that $\{d\mathcal{L}_1, \dots, d\mathcal{L}_g\}$, where $d\mathcal{L}_i = \sum_{j=1}^g (\partial \mathcal{L}_i(X)/\partial x_j) dx_j$, is the standard basis for the invariant differentials on \widehat{A} . The canonical map Λ from C to A induces a bijection $\Lambda_*: H^0(A, \Omega^1) \rightarrow H^0(C, \Omega^1)$ from the holomorphic differentials on A to the holomorphic differentials on C . (See [9].) Since all holomorphic differentials on an abelian variety are invariant, it suffices to show that $\Lambda_* d\mathcal{L}_i$ is a holomorphic differential of C for $i = 1, \dots, g$ and that $d\mathcal{L}_i(0) = dx_i$.

We write $\eta_j = \sum_{n=1}^\infty a_j(n)t^{n-1} dt$ where as above t is a parameter at a rational non-Weierstrass point P_0 and $a_j(i) = (-1)^{j-1} \delta_{ij}$ for $i, j = 1, \dots, g$. Then

$$l_j(t) = \sum_{n=1}^\infty a_j(n)/n t^n,$$

$$L_j(T) = \sum_{n=1}^\infty \frac{a_j(n)}{n} (t_1^n + \dots + t_g^n).$$

By Lemma 1,

$$L_j(T) = \mathcal{L}_j(S(T)) = \sum_{n=1}^\infty \sum_{\substack{I \\ N_I=n}} a_j(n) B(I)(S(T))^I$$

i.e.,

$$\mathcal{L}_j(X) = \sum_{I>0} a_j(N_I) B(I)(X)^I,$$

$$d\mathcal{L}_j(X) = \sum_{k=1}^g \left(\sum_I i_k B(I) a_j(N_I)(X)^{I-e_k} \right) dx_k,$$

$$d\mathcal{L}_j(0) = \sum_{k=1}^g B(e_k) a_j(k) dx_k = (-1)^{j+1} (-1)^{j-1} dx_j = dx_j.$$

There is a natural map $\varphi: C \rightarrow \text{Sym}^{(g)} C$ which is given by the composition of the diagonal map $C \rightarrow C^g$ with the natural projection $C^g \rightarrow \text{Sym}^{(g)} C$. The induced map on the completed local rings takes x_k to $x_k \circ \Lambda = s_k(t, \dots, t) = s_k(e)t^k$ and $(X \circ \Lambda)^I = (S(e))^I t^{N_I}$.

$$\begin{aligned}
 \Lambda_* d\mathcal{L}_j(X) &= \sum_{k=1}^g \sum_I i_k B(I) a_j(N_I) (X \circ \Lambda)^{I-e_k} d(x_k \circ \Lambda) \\
 &= \sum_{k=1}^g \sum_I i_k B(I) a_j(N_I) (S(e))^{I-e_k} (t^{N_I-e_k}) (k s_k(e) t^{k-1}) dt \\
 &= \sum_I B(I) \left(\sum_{k=1}^g k i_k \right) a_j(N_I) (S(e))^I (t^{N_I-1}) dt \\
 &= \sum_I B(I) N_I a_j(N_I) (S(e))^I (t^{N_I-1}) dt \\
 &= \sum_{n=1}^{\infty} \left(\sum_{\substack{I \\ N_I=n}} B(I) n (S(e))^I \right) a_j(n) t^{n-1} dt \\
 &= \sum_{n=1}^{\infty} P_n(e) a_j(n) t^{n-1} dt = g \eta_j.
 \end{aligned}$$

Note: if a different basis of differentials is used we still have $\mathcal{L}(X)$ is a logarithm of the formal group of the Jacobian but it is not the strict logarithm.

III. The formal group of the Jacobian of $X_0(l)$. Let l be an odd positive prime and

$$\Gamma_0(l) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z}) \mid c \equiv 0 \pmod{l} \right\}.$$

Let \mathcal{H} be the complex upper half-plane. Let $Y_0(l) = \mathcal{H} / \Gamma_0(l)$. Then $Y_0(l)$ can be compactified by the addition of finitely many cusps. The resulting complex curve has a complete non-singular model defined over \mathbb{Q} which we denote by $X_0(l)$ (Shimura [12]). The genus of $X_0(l)$ is

$$\begin{cases} \left\lfloor \frac{l+1}{12} \right\rfloor & \text{if } 12 \nmid l-1, \\ \left\lfloor \frac{l+1}{12} \right\rfloor - 1 & \text{if } 12 \mid l-1. \end{cases}$$

Atkin and Ogg have shown that the cusp at ∞ is not a Weierstrass point on $X_0(l)$, (Ogg [10]), so we will use this as base point to construct the formal group of the Jacobian of $X_0(l)$.

If $f(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i z n}$ is the Fourier expansion at $i\infty$ of a cusp form of weight 2 for $\Gamma_0(l)$ then a parameter q can be chosen on $X_0(l)$ at the cusp at $i\infty$ so that

$$\omega = 2\pi i f(z) dz = \sum_{n=1}^{\infty} a_n q^{n-1} dq$$

is the expansion at $i\infty$ of a holomorphic differential on $X_0(l)$.

Let $\{f_1, \dots, f_g\}$ be a \mathbb{Q} -basis for the cusp forms of weight 2 on $\Gamma_0(l)$ with Fourier expansions $\sum c_i(n) e^{2\pi i z n}$ at $i\infty$ and $[c_i(j)] = \text{Id}_g$, the $g \times g$ identity matrix. Let $\{\omega_1, \dots, \omega_g\}$ be the corresponding basis for the holomorphic differentials on $X_0(l)$. Let

$$\mathcal{L}(X) = (\mathcal{L}_1(X), \dots, \mathcal{L}_g(X))$$

be the logarithm map as given in the construction above. In this case the Jacobian matrix of \mathcal{L} , $J(\mathcal{L}) = [(-1)^{i+1} \delta_{ij}]$.

Since the cusp forms of weight 2 on $\Gamma_0(l)$ have a \mathbb{Z} basis also, (Shimura [12]), there are only finitely many primes which divide the denominators of $\{c_i(n)\}$ for $i = 1, \dots, g$ and $n \in \mathbb{Z}^+$. Let S be this finite set of primes.

THEOREM 3. *Let $l \in \mathbb{Z}$ be a prime. If the formal group of the Jacobian of the modular curve $X_0(l)$ is given by $\mathfrak{J}(X, Y) = \mathcal{L}^{-1}(\mathcal{L}(X) + \mathcal{L}(Y)) = (J_1(X, Y), \dots, J_g(X, Y))$, then $J_i(X, Y) \in \mathbb{Z}_p[[X, Y]]$ for all primes $p \notin S$.*

Before proving this we will need the following lemmas. Let $M_p = [c_i(jp) + p c_i(j/p)]$ for $p \neq l$, and $M_l = [c_i(jl)]$ where $c_i(j/p) = 0$ if $p \nmid j$.

LEMMA 2.

$$\begin{bmatrix} c_1(np) \\ \vdots \\ c_g(np) \end{bmatrix} - M_p \begin{bmatrix} c_1(n) \\ \vdots \\ c_g(n) \end{bmatrix} + p \begin{bmatrix} c_1(n/p) \\ \vdots \\ c_g(n/p) \end{bmatrix} = 0$$

for all $n \in \mathbb{Z}^+$ and for all primes p .

Proof. Let T_p and U_p be the standard Hecke and Atkin operators. Since f_i is a cusp form of weight two on $\Gamma_0(l)$, $T_p(f_i)$ for all primes $p \neq l$ and $U_l(f_i)$ are also cusp forms of weight two on $\Gamma_0(l)$ (Atkin

[2]). Since $\{f_1, \dots, f_g\}$ is a basis we have

$$\begin{aligned} \begin{bmatrix} T_p(f_1) \\ \vdots \\ T_p(f_g) \end{bmatrix} &= C_p \begin{bmatrix} f_1 \\ \vdots \\ f_g \end{bmatrix} && \text{for some } C_p \in M_n(\mathbb{Q}) \quad \text{and} \\ \begin{bmatrix} U_l(f_1) \\ \vdots \\ U_l(f_g) \end{bmatrix} &= C_l \begin{bmatrix} f_1 \\ \vdots \\ f_g \end{bmatrix} && \text{for some } C_l \in M_n(\mathbb{Q}). \end{aligned}$$

Thus the Fourier coefficients of the f_i satisfy the following:

$$\begin{bmatrix} c_1(np) + pc_1(n/p) \\ \vdots \\ c_g(n/p) + pc_g(n/p) \end{bmatrix} = C_p \begin{bmatrix} c_1(n) \\ \vdots \\ c_g(n) \end{bmatrix} \quad \begin{array}{l} \text{for all } p \neq l \text{ and} \\ \text{for all } n \in \mathbb{Z}^+ \end{array}$$

and

$$\begin{bmatrix} c_1(nl) \\ \vdots \\ c_g(nl) \end{bmatrix} = C_l \begin{bmatrix} c_1(n) \\ \vdots \\ c_g(n) \end{bmatrix} \quad \text{for all } n \in \mathbb{Z}^+.$$

Evaluating at $n = 1, \dots, g$ gives $C_p = M_p$ and $C_l = M_l$.

The following is a special case of a theorem of T. Honda. (Honda [6].) Hazewinkel ([5] page 59) gives a similar result in a functional equation lemma. Let $U_n = \{n \times n \text{ matrices over } \mathbb{Z}_p[[t]]\}$. We say $u \in U_n$ is a special element if $u \equiv pI_n \pmod{\text{degree } 1}$. For $f(X) = (f_1(X), \dots, f_n(X))$, $f_i(X) \in \mathbb{Q}_p[[X]]$, $f_i(0) = 0$ and $u = \sum C_j t^j \in U_n$, we define $(u * f)(X) = \sum C_j f(X^{p^j})$.

LEMMA 3 (Honda [6]). *Let $f(X) = (f_1(X), \dots, f_n(X))$, $f_i(X) \in \mathbb{Q}_p[[x]]$ with $f_i(0) = 0$. Assume $J(f)$ is an invertible matrix in $M_n(\mathbb{Z}_p)$. If there exists a special element $u \in U_n$ such that $u * f \equiv 0 \pmod{p}$ then $F(X, Y) = f^{-1}(f(X) + f(Y))$ is a commutative formal group of dimension n defined over \mathbb{Z}_p . Moreover, if $g(X) = (g_1(X), \dots, g_n(X))$, with $g_i(X) \in \mathbb{Q}_p[[X]]$ and $g_i(0) = 0$ also has $J(g)$ invertible in $M_n(\mathbb{Z}_p)$ and $u * g \equiv 0 \pmod{p}$ for the same element u , then $G(X, Y) = g^{-1}(g(X) + g(Y))$ is isomorphic to $F(X, Y)$ over \mathbb{Z}_p .*

LEMMA 4. $pB(I/p^r) - B(I/p^{r+1}) \equiv 0 \pmod{p\mathbb{Z}_p}$ for any r and for any index set $I = (i_1, \dots, i_g)$ where $B(I/p^r) = 0$ if $p^r \nmid I$ (i.e., if $p^r \nmid i_k$ for some k).

Proof. Let $n \in \mathbb{Z}$ with $p \nmid n$. Then by induction we see

$$(x_1 + \cdots + x_g)^{p^a n} \equiv (x_1^p + \cdots + x_g^p)^{p^{a-1} n} \pmod{p^a}.$$

Therefore by the multinomial theorem,

$$\sum_{r_1 + \cdots + r_g = p^a n} \frac{(p^a n)!}{R!} X^R \equiv \sum_{t_1 + \cdots + t_g = p^{a-1} n} \frac{(p^{a-1} n)!}{T!} X^{pT} \pmod{p^a}.$$

Let $J = (j_1, \dots, j_g)$ be an index set such that $p \nmid j_k$ for some k and $p^b(j_1 + \cdots + j_g) = p^a n$ for some b , $1 \leq b \leq a$. By comparing the coefficients of $X^{p^b J}$ above we have:

$$\frac{(p^a n)!}{(p^b J)!} \equiv \frac{(p^{a-1} n)!}{(p^{b-1} J)!} \pmod{p^a},$$

$$\begin{aligned} & \frac{p^a n}{p^b j_k} \left(\frac{(p^a n - 1)!}{(p^b j_1! \cdots (p^b j_k - 1)! \cdots (p^{b-1} j_g)!)} \right) \\ & \equiv \frac{p^{a-1} n}{p^{b-1} j_k} \left(\frac{(p^{a-1} n - 1)!}{(p^{b-1} j_1! \cdots (p^{b-1} j_k - 1)! \cdots (p^{b-1} j_g)!)} \right) \pmod{p^a} \end{aligned}$$

Since $p \nmid n$ and $p \nmid j_k$ we have:

$$(4) \quad \frac{(p^a n - 1)!}{(p^b j_1)! \cdots (p^b j_k - 1)! \cdots (p^b j_g)!} \equiv \frac{(p^{a-1} n - 1)!}{(p^{b-1} j_1)! \cdots (p^{b-1} j_k - 1)! \cdots (p^{b-1} j_g)!} \pmod{p^b \mathbb{Z}_p}.$$

Now let $I = (i_1, \dots, i_g)$ be any index set and fix $r \in \mathbb{Z}$. If $p^r \nmid I$ then $pB(I/p^r) - B(I/p^{r+1}) = 0$. Thus assume $I = p^b J$ where $p \nmid J$ and $b \geq r$.

If $b = r$,

$$pB(I/p^r) - B(I/p^{r+1}) = pB(I/p^r) = pB(J) = \pm(p/j_k)j_k B(J)$$

where $p \nmid j_k$ and $j_k B(J)$ is a multinomial coefficient. Thus $pB(I/p^r) - B(I/p^{r+1}) \equiv 0 \pmod{p\mathbb{Z}_p}$.

Assume $b > r$.

$$\begin{aligned} pB(I/p^r) - B(I/p^{r+1}) &= pB(p^{b-r} J) - B(p^{b-r-1} J) \\ &= \frac{\pm 1}{p^{b-r-1} j_k} \left(\frac{(p^a n - 1)!}{(p^{b-r} j_1)! \cdots (p^{b-r} j_k - 1)! \cdots (p^{b-r} j_g)!} \right. \\ & \quad \left. - \frac{(p^{a-1} n - 1)!}{(p^{b-r-1} j_1)! \cdots (p^{b-r-1} j_k - 1)! \cdots (p^{b-r-1} j_g)!} \right) \end{aligned}$$

where $p^a n = p^{b-r}(j_1 + \cdots + j_g)$ and $p \nmid n$.

Hence $pB(I/p^r) - B(I/p^{r+1}) \equiv 0 \pmod{p\mathbb{Z}_p}$ by (4) above.

THEOREM 4. For any prime $p \notin S$, let $u_p = pI_g - M_p t + t^2$. Then u_p is a special element in the sense of Honda and $u_p * \mathcal{L} \equiv 0 \pmod{p}$.

Theorem 3 follows immediately from this result and Lemma 3.

Proof. Recall that $\mathcal{L}_j(X) = \sum_{I>0} B(I)c_j(N_I)X^I$. Thus

$$\begin{aligned} u_p * \mathcal{L} &= p \begin{pmatrix} \mathcal{L}_1(X) \\ \vdots \\ \mathcal{L}_g(X) \end{pmatrix} - M_p \begin{pmatrix} \mathcal{L}_1(X^p) \\ \vdots \\ \mathcal{L}_g(X^p) \end{pmatrix} + \begin{pmatrix} \mathcal{L}_1(X^{p^2}) \\ \vdots \\ \mathcal{L}_g(X^{p^2}) \end{pmatrix} \\ &= p \begin{pmatrix} \sum_{I>0} B(I)c_1(N_I)X^I \\ \vdots \\ \sum_{I>0} B(I)c_g(N_I)X^I \end{pmatrix} - M_p \begin{pmatrix} \sum_{I>0} B(I)c_1(N_I)X^{pI} \\ \vdots \\ \sum_{I>0} B(I)c_g(N_I)X^{pI} \end{pmatrix} \\ &\quad + \begin{pmatrix} \sum_{I>0} B(I)c_1(N_I)X^{p^2I} \\ \vdots \\ \sum_{I>0} B(I)c_g(N_I)X^{p^2I} \end{pmatrix}. \end{aligned}$$

Using Lemma 2,

$$\begin{aligned} M_p \begin{pmatrix} \sum_{I>0} B(I)c_1(N_I)X^{pI} \\ \vdots \\ \sum_{I>0} B(I)c_g(N_I)X^{pI} \end{pmatrix} &= \begin{pmatrix} \sum_{I>0} B(I)c_1(pN_I)X^{pI} \\ \vdots \\ \sum_{I>0} B(I)c_g(pN_I)X^{pI} \end{pmatrix} \\ &\quad + p \begin{pmatrix} \sum_{I>0} B(I)c_1\left(\frac{1}{p}N_I\right)X^{pI} \\ \vdots \\ \sum_{I>0} B(I)c_g\left(\frac{1}{p}N_I\right)X^{pI} \end{pmatrix}. \end{aligned}$$

Let $J = pI$. Then $N_J = pN_I$.

Thus we have:

$$\begin{aligned}
 u_p * \mathcal{L} &= p \begin{pmatrix} \sum_{I>0} B(I)c_1(N_I)X^I \\ \vdots \\ \sum_{I>0} B(I)c_g(N_I)X^I \end{pmatrix} - \begin{pmatrix} \sum_{I>0} B(I)c_1(pN_I)X^{pI} \\ \vdots \\ \sum_{I>0} B(I)c_g(pN_I)X^{pI} \end{pmatrix} \\
 &\quad - p \begin{pmatrix} \sum_{\substack{J=pI \\ I>0}} B\left(\frac{J}{p}\right) c_1\left(\frac{1}{p^2}N_j\right) X^J \\ \vdots \\ \sum_{\substack{J=pI \\ I>0}} B\left(\frac{J}{p}\right) c_g\left(\frac{1}{p^2}N_J\right) X^J \end{pmatrix} \\
 &\quad + \begin{pmatrix} \sum_{\substack{J=pI \\ I>0}} B\left(\frac{J}{p}\right) c_1\left(\frac{I}{p}N_J\right) X^{pJ} \\ \vdots \\ \sum_{\substack{J=pI \\ I>0}} B\left(\frac{J}{p}\right) c_1\left(\frac{I}{p}N_J\right) X^{pJ} \end{pmatrix} \\
 &\hspace{15em} \text{where } B(J/p^i) = 0 \text{ if } p^i \nmid J. \\
 &= \begin{pmatrix} \sum_{I>0} \left(pB(I) - B\left(\frac{I}{p}\right) \right) c_g(N_I)X^I \\ \vdots \\ \sum_{I>0} \left(pB(I) - B\left(\frac{I}{p}\right) \right) c_g(N_I)X^I \end{pmatrix} \\
 &\quad - \begin{pmatrix} \sum_{\substack{J=pI \\ I>0}} \left(pB\left(\frac{J}{p}\right) - B\left(\frac{J}{p^2}\right) \right) c_1\left(\frac{1}{p^2}N_J\right) X^J \\ \vdots \\ \sum_{\substack{J=pI \\ I>0}} \left(pB\left(\frac{J}{p}\right) - B\left(\frac{J}{p^2}\right) \right) c_g\left(\frac{1}{p^2}N_J\right) X^J \end{pmatrix} \\
 &\equiv 0 \pmod{p\mathbb{Z}_p}
 \end{aligned}$$

by Lemma 4.

REMARKS. (1) If $p > g$, M_p reduces to the matrix $[c_i(jp)]$, the Hasse-Witt matrix of the curve. The special element u_p is then a generalization of the special element found by Honda ([7]) in the elliptic

curve case, namely $u_p = p - a_p t + t^2$ where a_p is the Hasse invariant of the elliptic curve.

(2) The cusp forms of weight 2 on $\Gamma_0(l)$ also have a \mathbb{Z} -basis. (See Shimura [12]). If $\{f_1, \dots, f_g\}$ is this basis with $f_i(q) = \sum a_i(n)q^n$, then the primes in the set S are precisely those primes which divide the determinant of the matrix $[a_i(j)]$.

3. The author wishes to thank M. Rosen and J. Lubin for many helpful discussions about this material. In particular, it was J. Lubin who suggested the construction given in §II.

REFERENCES

- [1] E. Arbarello, M. Cornalba, P. A. Griffiths and J. Harris, *Geometry of Algebraic Curves*, Volume I, Springer-Verlag, 1985.
- [2] A. Atkin and J. Lehner, *Hecke operators on $\Gamma_0(m)$* , Math. Ann., **185** (1970), 134–160.
- [3] E. V. Flynn, *The Jacobian and formal group of a curve of genus 2 over an arbitrary ground field*, Math. Proc. Camb. Phil. Soc., **107** (1990), 425–441.
- [4] D. Grant, *Formal groups in genus 2*, J. Reine Angew. Math., (1990), 96–121.
- [5] M. Hazewinkel, *Formal Groups and Applications*, Academic Press, 1978.
- [6] T. Honda, *On the theory of commutative formal groups*, J. Math. Soc. Japan, **22** (1970), 213–246.
- [7] ———, *Formal groups and zeta functions*, Osaka J. Math., **5** (1968), 199–213.
- [8] J. S. Milne, *Abelian Varieties*, In Arithmetic Geometry, G. Cornell and J. Silverman Eds., Springer-Verlag 1986.
- [9] ———, *Jacobian Varieties*, In Arithmetic Geometry, G. Cornell and J. Silverman Eds., Springer-Verlag 1986.
- [10] A. Ogg, *On the Weierstrass points of $X_0(N)$* , Illinois J. Math., **22** (1978), 31–35.
- [11] S. Shatz, *Group Schemes, Formal Groups and p -Divisible Groups*, in Arithmetic Geometry, G. Cornell and J. Silverman Eds., Springer-Verlag 1986.
- [12] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Princeton University Press, 1971.
- [13] J. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, 1986.

Received August 4, 1990.

COLLEGE OF THE HOLY CROSS
WORCESTER, MA 01610

PACIFIC JOURNAL OF MATHEMATICS

Founded by

E. F. BECKENBACH (1906–1982) F. WOLF (1904–1989)

EDITORS

V. S. VARADARAJAN
(Managing Editor)
University of California
Los Angeles, CA 90024-1555
vsv@math.ucla.edu

HERBERT CLEMENS
University of Utah
Salt Lake City, UT 84112
clemens@math.utah.edu

F. MICHAEL CHRIST
University of California
Los Angeles, CA 90024-1555
christ@math.ucla.edu

THOMAS ENRIGHT
University of California, San Diego
La Jolla, CA 92093
tenright@ucsd.edu

NICHOLAS ERCOLANI
University of Arizona
Tucson, AZ 85721
ercolani@math.arizona.edu

R. FINN
Stanford University
Stanford, CA 94305
finn@gauss.stanford.edu

VAUGHAN F. R. JONES
University of California
Berkeley, CA 94720
vfr@math.berkeley.edu

STEVEN KERCKHOFF
Stanford University
Stanford, CA 94305
spk@gauss.stanford.edu

C. C. MOORE
University of California
Berkeley, CA 94720

MARTIN SCHARLEMANN
University of California
Santa Barbara, CA 93106
mgscharl@henri.ucsb.edu

HAROLD STARK
University of California, San Diego
La Jolla, CA 92093

SUPPORTING INSTITUTIONS

UNIVERSITY OF ARIZONA
UNIVERSITY OF BRITISH COLUMBIA
CALIFORNIA INSTITUTE OF TECHNOLOGY
UNIVERSITY OF CALIFORNIA
MONTANA STATE UNIVERSITY
UNIVERSITY OF NEVADA, RENO
NEW MEXICO STATE UNIVERSITY
OREGON STATE UNIVERSITY

UNIVERSITY OF OREGON
UNIVERSITY OF SOUTHERN CALIFORNIA
STANFORD UNIVERSITY
UNIVERSITY OF HAWAII
UNIVERSITY OF TOKYO
UNIVERSITY OF UTAH
WASHINGTON STATE UNIVERSITY
UNIVERSITY OF WASHINGTON

The Supporting Institutions listed above contribute to the cost of publication of this Journal, but they are not owners or publishers and have no responsibility for its content or policies.

Mathematical papers intended for publication in the *Pacific Journal of Mathematics* should be in typed form or offset-reproduced (not dittoed), double spaced with large margins. Please do not use built up fractions in the text of the manuscript. However, you may use them in the displayed equations. Underline Greek letters in red, German in green, and script in blue. The first paragraph must be capable of being used separately as a synopsis of the entire paper. In particular it should contain no bibliographic references. Please propose a heading for the odd numbered pages of less than 35 characters. Manuscripts, in triplicate, may be sent to any one of the editors. Please classify according to the 1991 *Mathematics Subject Classification* scheme which can be found in the December index volumes of *Mathematical Reviews*. Supply name and address of author to whom proofs should be sent. All other communications should be addressed to the managing editor, or Julie Speckart, University of California, Los Angeles, California 90024-1555.

There are page-charges associated with articles appearing in the Pacific Journal of Mathematics. These charges are expected to be paid by the author's University, Government Agency or Company. If the author or authors do not have access to such Institutional support these charges are waived. Single authors will receive 50 free reprints; joint authors will receive a total of 100 free reprints. Additional copies may be obtained at cost in multiples of 50.

The *Pacific Journal of Mathematics* (ISSN 0030-8730) is published monthly except for July and August. Regular subscription rate: \$190.00 a year (10 issues). Special rate: \$95.00 a year to individual members of supporting institutions.

Subscriptions, orders for numbers issued in the last three calendar years, and changes of address should be sent to Pacific Journal of Mathematics, P.O. Box 969, Carmel Valley, CA 93924, U.S.A. Old back numbers obtainable from Kraus Periodicals Co., Route 100, Millwood, NY 10546.

The Pacific Journal of Mathematics at P.O. Box 969, Carmel Valley, CA 93924 (ISSN 0030-8730) is published monthly except for July and August. Second-class postage paid at Carmel Valley, California 93924, and additional mailing offices. Postmaster: send address changes to Pacific Journal of Mathematics, P.O. Box 969, Carmel Valley, CA 93924.

PUBLISHED BY PACIFIC JOURNAL OF MATHEMATICS, A NON-PROFIT CORPORATION

Copyright © 1993 by Pacific Journal of Mathematics

PACIFIC JOURNAL OF MATHEMATICS

Volume 157 No. 2 February 1993

Strong integral summability and the Stone-Čech compactification of the half-line	201
JEFF CONNOR and MARY ANNE SWARDSON	
The endlich Baer splitting property	225
THEODORE GERARD FATICONI	
The formal group of the Jacobian of an algebraic curve	241
MARGARET N. FREIJE	
Concordances of metrics of positive scalar curvature	257
PAWEL GAJER	
Explicit construction of certain split extensions of number fields and constructing cyclic classfields	269
STANLEY JOSEPH GURAK	
Asymptotically free families of random unitaries in symmetric groups	295
ALEXANDRU MIHAI NICA	
On purifiable subgroups and the intersection problem	311
TAKASHI OKUYAMA	
On the incidence cycles of a curve: some geometric interpretations	325
LUCIANA RAMELLA	
On some explicit formulas in the theory of Weil representation	335
R. RANGA RAO	
An analytic family of uniformly bounded representations of a free product of discrete groups	373
JANUSZ WYSOCZAŃSKI	
Errata: "Dentability, trees, and Dunford-Pettis operators on L_1 "	389
MARIA GIRARDI and ZHIBAO HU	
Errata: "Poincaré cobordism exact sequences and characterisation"	395
HIMADRI KUMAR MUKERJEE	



0030-8730(1993)157:2;1-I