

## BIBLIOGRAPHY

- [1] M. ATIYAH and I. SINGER, *The Index of Elliptic Operators: III*, Ann. of Math., 87 (1968), 546-604.
- [2] W.-C. HSIANG and R. H. SZCZARBA, *On embedding surfaces in four-manifolds*, A.M.S. Proc. Symposia in Pure Math., XXII (1971), 97-104.
- [3] M. A. Kervaire and J. W. Milnor, *On 2-spheres in 4-manifolds*, Proc. Nat. Acad. Sci., 47 (1961), 1651-1657.
- [4] W. S. MASSEY, *Proof of a conjecture of Whitney*, Pac. J. Math., 31 (1969), 143-156.
- [5] V. ROHLIN, *Classification of the mappings of the  $(n+3)$ -sphere into the  $n$ -sphere*, Doklady Akad. Nauk SSSR, 81 (1951), 19-22.
- [6] V. ROHLIN, *New results in the theory of 4-dimensional manifolds*, Doklady Akad. Nauk. SSSR, 84 (1952), 221-224.
- [7] V. ROHLIN, *Two-dimensional submanifolds of four-dimensional manifolds*, Jour. Funct. Anal. and Applications, 5 (1971), 48-60.
- [8] W. WHITNEY, *On the topology of differentiable manifolds*, Lectures in Topology, Michigan University Press, 1940.

ON THE FORMAL STRUCTURE OF THE JACOBIAN VARIETY OF THE FERMAT CURVE OVER A  $P$ -ADIC INTEGER RING (\*)

TAIRA HONDA

Let  $\Gamma_N$  be the algebraic curve  $x^N + y^N = 1$  ( $N \geq 3$ ) and  $J_N$  its Jacobian variety, defined over a field  $K$ . When  $K$  is a finite field  $F_q$  with  $q$  elements such that  $N \nmid q-1$ , the zeta function of  $\Gamma_N$ , which is essentially the same thing as that of  $J_N$ , was calculated by Davenport-Hasse [1] and written in terms of so-called Jacobi sums. Later Manin [9] showed how the formal structure of an abelian variety over  $F_q$  is determined by the prime ideal decomposition of the eigenvalues of its  $q$ -th power endomorphism. According to his result the formal structure of  $J_N$  (up to isogeny over the algebraic closure of  $F_q$ ) is also described by using the classical formula on the prime ideal decomposition of a Jacobi sum.

When  $K$  is the rational numbers  $\mathbb{Q}$ , a formal group  $F_N$ , obtained by formalization of group law of  $J_N$ , has  $p$ -integral coefficients for almost all primes  $p$ . The purpose of this article is to study this group as a formal group over  $\mathbb{Z}_p$ , the ring of  $p$ -adic integers, and to show how its structure is determined by the coefficients of the differentials of the first kind on  $\Gamma_N$ .

In 1, we yield a general theorem on the formal structure of a Jacobian variety over a finite algebraic number field  $K$ . Let  $\Gamma$  be a complete non-singular curve,  $J$  its Jacobian,  $A: \Gamma \rightarrow J$  a canonical map, all defined over  $K$ . Let  $F$  be the formal group obtained by expansion into power series of the group law of  $J$  relative to some system of local parameters at the origin. For a prime  $\mathfrak{p}$  of  $K$ , let  $\mathfrak{o}_{\mathfrak{p}}$  denote the completion of integers of  $K$  at  $\mathfrak{p}$ . In [6] we showed how a formal group over  $\mathfrak{o}_{\mathfrak{p}}$  is determined by some type of matrix (called *special*) with entries in the ring of non-commutative power series over  $\mathfrak{o}_{\mathfrak{p}}$ , when  $\mathfrak{p}$  is unramified in  $K/\mathbb{Q}$ . Now we claim that for almost all  $\mathfrak{p}$ , a special

(\*) I risultati conseguiti in questo lavoro sono stati esposti nella conferenza tenuta il 22 maggio 1972.

matrix, which kills mod  $\mathfrak{p}$  a (fixed) base of integrals of the first kind on  $\Gamma$ , determines the structure of  $F$  as a formal group over  $\mathfrak{o}_{\mathfrak{p}}$ . Thus our problem is transferred from  $J$  to  $\Gamma$ .

In 3 we determine a special matrix which kills mod  $\mathfrak{p}$  the well known base of integrals of the first kind on  $\Gamma_N$  for every  $p \nmid N$ . It turns out that it is of special and fairly simple form. For it we must study congruence properties of binomial type numbers on the base of Dwork's congruence ([4]). This study is done in 2.

Considering the reduction mod  $\mathfrak{p}$  of our principal result we get a refinement of Manin's theorem for the Jacobian  $J_N$ . Further it results that the  $p$ -adic limit of the ratio of certain binomial coefficients coincides with some Jacobi sum. About this N. Katz recently proved a more precise theorem which had been conjectured by the author in [7].

### 1. Formalization of the Jacobian variety over a number field.

Let  $K$  be a finite algebraic number field and  $\mathfrak{o}$  the ring of integers in  $K$ . For a prime ideal  $\mathfrak{p}$  of  $\mathfrak{o}$  we denote by  $K_{\mathfrak{p}}$  and  $\mathfrak{o}_{\mathfrak{p}}$  the completions of  $K$  and  $\mathfrak{o}$  at  $\mathfrak{p}$ . We often write  $\mathfrak{p}$  instead of  $\mathfrak{p}\mathfrak{o}_{\mathfrak{p}}$  if there is no fear of confusion. Let  $\Gamma$  be a complete non-singular algebraic curve,  $J$  its Jacobian, and  $A: \Gamma \rightarrow J$  a canonical map, all defined over  $K$ . The formalization of  $J$  with respect to some system of local parameters at the origin is a formal group over  $\mathfrak{o}_{\mathfrak{p}}$  for all but a finite number of primes  $\mathfrak{p}$  of  $K$ . In this section we show that for these primes  $\mathfrak{p}$  the study of this formal group over  $\mathfrak{o}_{\mathfrak{p}}$  is reduced to that of «integrals of the first kind» on  $\Gamma$ .

We use the notations, definitions and results of Honda [6]. Let  $K'$  be a valuation field satisfying the assumption (F) of [6, § 2],  $\mathfrak{o}'$  the ring of integers in  $K'$ , and  $\mathfrak{p}'$  the maximal ideal of  $\mathfrak{o}'$ . Let  $\sigma$  and  $q$  be as in (F). Denote by  $\mathfrak{U}_n(\mathfrak{p}')$  the full matrix ring  $M_n(\mathfrak{o}'[[T]])$ .

LEMMA 1: Let  $x$  be an indeterminate and  $f = (f_1, \dots, f_n)$  an  $n$ -tuple of power series over  $K'$ ;

$$f_i(x) = \sum_{\alpha=\alpha_1}^{\infty} a_{\alpha}^{(i)} x^{\alpha} \quad (1 \leq i \leq n).$$

Assume that the following assumptions are satisfied:

- (a) The  $a_{\alpha_i}^{(i)}$  are units of  $\mathfrak{o}'$  ( $1 \leq i \leq n$ ).
- (b)  $1 \leq \alpha_1 < \dots < \alpha_n < q\alpha_1$ .
- (c)  $a_{\alpha}^{(i)} \in \mathfrak{o}'$  for  $1 \leq i \leq n$ ,  $\alpha \leq \alpha_n$ .

Then, if  $u$  and  $v$  are special elements of  $\mathfrak{U}_n(\mathfrak{p}')$  such that

$$u * f \equiv v * f \equiv 0 \pmod{\mathfrak{p}'},$$

$v$  is left associate with  $u$ , namely there is a unit  $t$  of  $\mathfrak{U}_n(\mathfrak{p}')$  such that  $v = tu$ .

PROOF: Write

$$(1.1) \quad u = \pi I_n + \sum_{\nu=1}^{\infty} C_{\nu} T^{\nu}, \quad v = \pi I_n + \sum_{\nu=1}^{\infty} D_{\nu} T^{\nu},$$

where  $\pi$  is a (fixed) prime of  $\mathfrak{o}'$  and  $C_{\nu}, D_{\nu} \in M_n(\mathfrak{o}')$ . We will show that if  $C_{\nu} = D_{\nu}$  for  $0 \leq \nu \leq \mu - 1$  with some  $\mu \geq 1$ , then

$$(1.2) \quad C_{\mu} \equiv D_{\mu} \pmod{\mathfrak{p}'}.$$

By (b) it follows from our assumption

$$\sum_{\nu=\mu}^{\infty} (C_{\nu} - D_{\nu}) f^{\sigma^{\nu}}(x^{\alpha^{\nu}}) \equiv 0 \pmod{\mathfrak{p}'}$$

that

$$(1.3) \quad (C_{\mu} - D_{\mu}) f^{\sigma^{\mu}}(x^{\alpha^{\mu}}) \equiv 0 \pmod{\mathfrak{p}', \text{ mod deg } (\alpha_n + 1)}.$$

Let  $c_{i,j}$  be the  $(i, j)$ -entry of  $C_{\mu} - D_{\mu}$ . Then it follows from (1.3)

$$(1.4) \quad \begin{cases} c_{i,1} a_{\alpha_1}^{(1)\sigma^{\mu}} \equiv 0 \\ c_{i,1} a_{\alpha_2}^{(1)\sigma^{\mu}} + c_{i,2} a_{\alpha_2}^{(2)\sigma^{\mu}} \equiv 0 \\ \dots \dots \dots \\ c_{i,1} a_{\alpha_n}^{(1)\sigma^{\mu}} + c_{i,2} a_{\alpha_n}^{(2)\sigma^{\mu}} + \dots + c_{i,n} a_{\alpha_n}^{(n)\sigma^{\mu}} \equiv 0. \end{cases} \pmod{\mathfrak{p}'}$$

From (a), (c) and (1.4) we get easily

$$c_{i,j} \in \mathfrak{p}' \quad \text{for } 1 \leq i, j \leq n.$$

This proves (1.2).

Now put

$$(1.5) \quad t_{\mu} = I_n - (C_{\mu} - D_{\mu}) T_{\mu} \cdot \pi^{-1}.$$

Then  $t_\mu$  is a unit of  $\mathfrak{A}_n(\mathfrak{p}')$  and

$$(1.6) \quad t_\mu u \equiv v \pmod{\deg \mu + 1}.$$

In this way we can find units  $t_1, \dots, t_\lambda$  successively for each  $\lambda > 0$  so that

$$t_\lambda \dots t_1 u \equiv v \pmod{\deg(\lambda + 1)}$$

and  $t_\lambda \dots t_1$  converges as  $\lambda \rightarrow \infty$ . The limit  $t$  of  $t_\lambda \dots t_1$  clearly satisfies the requirement of our lemma.

Returning to the curve  $\Gamma$  over  $K$ , let  $n$  be the genus of  $\Gamma$  and assume  $n > 0$ . Let  $P$  be the  $K$ -rational point of  $\Gamma$  such that  $A(P)$  is the origin of  $J$ . Furthermore let  $\eta_1, \dots, \eta_n$  be a base of differentials of the first kind on  $\Gamma$ , each defined over  $K$ . Then  $x \in K(\Gamma)$  being a local parameter at  $P$ , there are  $\Psi_i(x) \in K[[x]]$  ( $1 \leq i \leq n$ ) such that  $\Psi_i(0) = 0$  and  $\eta_i = d\Psi_i(x)$ . Let  $y = (y_1, \dots, y_n) (\subset K(J))$  be a system of local parameters at the origin of  $J$  and let  $\omega_1, \dots, \omega_n$  be the invariant differentials on  $J$  such that

$$\omega_i \circ A = \eta_i \quad (1 \leq i \leq n).$$

Then we can write

$$\omega_i = \sum_{j=1}^n \varphi_{ij}(y_1, \dots, y_n) dy_j$$

with  $\varphi_{ij} \in K[[y_1, \dots, y_n]]$ . Since the  $\omega_i$  are closed as invariant differentials, they are also exact in  $K[[y]]$ . Hence there are  $\Phi_i(y) \in K[[y]]$  ( $1 \leq i \leq n$ ) such that

$$\Phi_i(0) = 0 \quad \text{and} \quad \omega_i = d\Phi_i(y).$$

Now let  $S_1$  be the (finite) set of primes of  $K$  at which at least one of the above algebro-geometric objects has bad reduction. Let  $F$  be the formalization of  $J$  at the origin relative to the parameters  $y$ .  $F$  is also obtained from the invariant differentials  $d\Phi_i(y)$ ,  $1 \leq i \leq n$  (cf. [6, § 1]). If  $\mathfrak{p} \notin S_1$ , then  $F$  is a formal group over  $\mathfrak{o}_{\mathfrak{p}}$ . Let  $S_0$  be the set of ramified primes of  $K$ . If  $\mathfrak{p} \notin S_0$ , we can apply the result of [6, § 3] to the group  $F$  over  $\mathfrak{o}_{\mathfrak{p}}$  with  $q = p$  and  $\sigma =$  the Frobenius substitution of  $K_{\mathfrak{p}}$ . Thus [6, Theorem 4] shows that the transformer of  $F$  is killed mod  $\mathfrak{p}$  by some special element of  $\mathfrak{A}_n(\mathfrak{p}) = M_n((\mathfrak{o}_{\mathfrak{p}})_e[[T]])$  if  $\mathfrak{p} \notin S_0 \cup S_1$ .

**THEOREM 1:** *There is a finite set  $S$  of primes of  $K$  satisfying the following conditions:*

(a)  $S$  contains  $S_0 \cup S_1$ .

(b) *If  $\mathfrak{p} \notin S$  and  $u$  is a special element of  $\mathfrak{A}_n(\mathfrak{p})$  which kills  $\Psi(x) \bmod \mathfrak{p}$ , then  $u$  also kills the transformer of  $F \bmod \mathfrak{p}$ , so that  $F$  is of type  $u$  as a formal group over  $\mathfrak{o}_{\mathfrak{p}}$ .*

**PROOF:** Since the  $y_i \circ A$  are functions in  $K(\Gamma)$ , there is an  $n$ -tuple  $\xi = {}^t(\xi_1, \dots, \xi_n)$  of algebraic functions in  $K[[x]]$  such that  $y \circ A = \xi \circ x$ . Then  $\omega = d\Phi(y)$  implies  $\eta = d(\Phi(\xi(x)))$ , namely

$$(1.7) \quad \Phi \circ \xi = \Psi.$$

Let  $A$  be the invertible matrix in  $M_n(K)$  such that

$$\Phi(y) = Ay \pmod{\deg 2}.$$

By replacing the local parameters  $y$  by  $Ay$  if necessary, we may assume  $A = I_n$ , namely that  $\Phi(y)$  is the transformer of  $F$ . By (1.7),  $\xi_i(x) \in \mathfrak{o}_{\mathfrak{p}}[[x]]$  for  $\mathfrak{p} \notin S_1$ . Take  $\mathfrak{p} \notin S_0 \cup S_1$  and let  $v$  be a special element of  $\mathfrak{A}_n(\mathfrak{p})$  which kills  $\Phi \bmod \mathfrak{p}$ . Then it follows from [6, Lemma 2.3] that

$$v * \Psi = v * (\Phi \circ \xi) \equiv (v * \Phi) \circ \xi \equiv 0 \pmod{\mathfrak{p}}.$$

So we have only to prove the following assertion: « For almost all  $\mathfrak{p}$  two special elements of  $\mathfrak{A}_n(\mathfrak{p})$ , which kill  $\Psi \bmod \mathfrak{p}$ , are left associate with each other ».

Let  $C$  be an invertible matrix in  $M_n(\mathfrak{o}_{\mathfrak{p}})$ . If  $CuC^{-1}$  is left associate with  $CvC^{-1}$ , namely there is a unit  $t \in \mathfrak{A}_n(\mathfrak{p})$  with  $CuC^{-1} = t \cdot CvC^{-1}$ , then  $u = C^{-1}tCv$  and  $C^{-1}tC$  is also a unit, which implies that  $u$  is left associate with  $v$ . Hence we may replace  $\eta = {}^t(\eta_1, \dots, \eta_n)$  by  $C\eta$  with  $C \in GL_n(K)$ , since such  $C$  is a unimodular matrix in  $M_n(\mathfrak{o}_{\mathfrak{p}})$  for almost all  $\mathfrak{p}$ . Thus we may assume

$$(1.8) \quad \Psi_i(x) = \sum_{\alpha=\alpha_i}^{\infty} a_{\alpha}^{(i)} x^{\alpha} \quad (1 \leq i \leq n),$$

$$1 \leq \alpha_1 < \dots < \alpha_n, \quad a_{\alpha_i}^{(i)} \neq 0.$$

Now we can apply Lemma 1 to  $f = \Psi$  with  $\mathfrak{o}' = \mathfrak{o}_{\mathfrak{p}}$  and  $q = p$ . It is trivial that (a), (b), (c) of Lemma 1 are satisfied for almost all  $\mathfrak{p}$ . This proves the above assertion and completes the proof of our theorem.

## 2. Congruences on binomial type numbers.

In order to apply Theorem 1 to the Fermat curve, we must study congruence properties of the coefficients of differentials of the first kind on it. Our results in this section extend the results of [8, Section 1]

to all primes not dividing  $N$ . Katz also obtained congruences of the same nature by an alternative method. Our treatment of the case of primes  $p$  with  $p < N$ ,  $p \nmid N$  was suggested by his method.

Let  $\vartheta$  be a positive rational number integral at  $p$ . Put for each non-negative integer  $\mu$

$$C(\vartheta; \mu) = \begin{cases} 1 & \text{for } \mu = 0 \\ \sum_{v=0}^{\mu-1} (\vartheta + v) & \text{for } \mu > 0, \end{cases}$$

and  $A(\vartheta; \mu) = C(\vartheta; \mu)/\mu!$ . We define  $\vartheta'$  to be the unique rational number, integral at  $p$ , such that  $p\vartheta' - \vartheta$  is an integer in  $[0, p-1]$ . For each real  $x$  put

$$\varrho(x) = \begin{cases} 0 & \text{if } x \leq 0 \\ 1 & \text{if } x > 0. \end{cases}$$

LEMMA 2: If  $a, \mu, m, s$  are non-negative ordinary integers,  $0 \leq a < p$ , then

$$(2.1) \quad \frac{A(\vartheta; mp^{s+1} + \mu p + a)}{A(\vartheta'; mp^s + \mu)} \equiv \frac{A(\vartheta; \mu p + a)}{A(\vartheta'; \mu)} \left(1 + \frac{mp^s}{\vartheta' + \mu}\right)^{\varrho(a + \vartheta - p\vartheta')} \pmod{\times p^{s+1}}.$$

(« mod  $\times$  » denotes the multiplicative congruence.) Moreover

$$(2.2) \quad \text{ord}_p A(\vartheta; \mu p + a)/A(\vartheta'; \mu) = (1 + \text{ord}_p(\mu + \vartheta')) \varrho(a + \vartheta - p\vartheta').$$

PROOF: This is an immediate consequence of Dwork [4, Lemma 1].

Let  $N \geq 3$  be an ordinary integer and  $p$  a prime number not dividing  $N$ . For a rational number  $r$ , whose denominator is prime to  $N$ , we denote by  $(r)_N$  the least (strictly) positive integer such that  $r \equiv (r)_N \pmod{N}$ . Let  $i, j$  be integers such that  $1 \leq i \leq N$  and  $1 \leq j \leq N-1$ , and put  $(p^{-1}i)_N = i_1$ ,  $(p^{-1}j)_N = j_1$ . Then there are non-negative integers  $s, t$  such that  $pi_1 = i + Ns$ ,  $pj_1 = j + Nt$ . Put  $I = pj_1 - j + i - pi_1 = N(t-s)$ .

LEMMA 3: If  $m \geq 1$ ,  $v \geq 1$  are ordinary integers and  $i \neq j$ , then

$$(2.3) \quad [(mp^v + i - j)/(i - j)]^{\varrho(i-j)} \\ \equiv [(mp^{v-1} + i_1 - j_1)/(i_1 - j_1)]^{\varrho(i_1-j_1)-\varrho(I)} \pmod{\times p^v}.$$

Furthermore

$$(2.4) \quad \varrho(j-i) \text{ ord}(mp^v + i - j) \\ = \{\varrho(j_1 - i_1) - \varrho(I)\} (1 + \text{ord}(mp^{v-1} + i_1 - j_1)).$$

PROOF: We divide the proof into several cases.

(a)  $i > j$ ,  $i_1 > j_1$ .

We first note that  $i_1 > j_1$  implies  $s \geq t$  and hence  $I \leq 0$ , namely  $\varrho(I) = 0$ . Consequently

$$\varrho(I) = \varrho(j-i) = \varrho(j_1-i_1) = 0$$

and our assertions are trivial.

(b)  $i < j$ ,  $i_1 > j_1$ .

In this case  $\varrho(I) = \varrho(j_1-i_1) = 0$ , and we have only to prove  $\text{ord}(j-i) = 0$ . In fact  $(i-j)(i_1-j_1) < 0$  implies  $0 \neq I = N(t-s)$ . Consequently if  $p|j-i$ , then  $p|t-s$  and  $|I| \geq Np$ , which is a contradiction.

(c)  $i > j$ ,  $i_1 < j_1$ .

In this case  $\varrho(j-i) = 0$  and  $\varrho(I) = \varrho(j_1-i_1) = 1$ , from which follow our assertions trivially.

(d)  $i < j$ ,  $i_1 < j_1$  and  $\varrho(I) = 1$ .

Since  $\varrho(j-i) = \varrho(j_1-i_1) = 1$ , it suffices to show  $\text{ord}(i-j) = 0$ . If  $p|i-j$ , then  $p|I \neq 0$  and  $|I| \geq pN$ , a contradiction.

(e)  $i < j$ ,  $i_1 < j_1$  and  $\varrho(I) = 0$ .

Since  $j_1 > i_1$  implies  $t \geq s$  and  $\varrho(I) = 0$  implies  $t \leq s$ , we get  $s = t$ . Consequently  $p(i_1-j_1) = i-j$  and  $mp^v + i-j = p(mp^{v-1} + i_1-j_1)$ . This completes the proof of our lemma.

Now put  $\vartheta = i/N$ . Then  $\vartheta' = i_1/N$ . For a natural number  $\mu$  not divisible by  $N$  define

$$(2.5) \quad b(\vartheta; \mu) = A(\vartheta; (\mu-j)/N) ((\mu-j)/N + \vartheta)^{\varrho(j-i)}$$

where  $j = (\mu)_N$ .

LEMMA 4: Let  $m, l$  be natural numbers such that  $m \equiv l \pmod{N}$  and  $N \nmid m$ . Then, for  $v \geq 1$

$$(2.6) \quad b(\vartheta; mp^v)/b(\vartheta; lp^v) \equiv b(\vartheta'; mp^{v-1})/b(\vartheta'; lp^{v-1}) \pmod{p^v}.$$

PROOF: Put  $(mp^v)_N = j$ ,  $(mp^{v-1})_N = j_1$ . Clearly we may assume  $l = (m)_N$ . Since

$$(2.7) \quad \frac{mp^v - j}{N} = \frac{m-l}{N} p^v + \frac{lp^{v-1} - j_1}{N} p + \frac{j_1 p - j}{N}$$

and  $0 \leq (j_1 p - j)/N < p$ , it follows from Lemma 2

$$(2.8) \quad \begin{aligned} & A(\vartheta; (mp^v - j)/N) / A(\vartheta'; (mp^{v-1} - j_1)/N) \\ & \equiv A(\vartheta; (lp^v - j)/N) / A(\vartheta'; (lp^{v-1} - j_1)/N) \\ & \times [(mp^{v-1} + i_1 - j_1)/(lp^{v-1} + i_1 - j_1)]^{e(I)} \pmod{p^v}. \end{aligned}$$

On the other hand we get by Lemma 3

$$(2.9) \quad \begin{aligned} & \left( \frac{mp^v + i - j}{lp^v + i - j} \right)^{e(j-i)} \equiv \left( \frac{mp^{v-1} + i_1 - j_1}{lp^{v-1} + i_1 - j_1} \right)^{e(j_1-i_1)} \\ & \times \left( \frac{lp^{v-1} + i_1 - j_1}{mp^{v-1} + i_1 - j_1} \right)^{e(I)} \pmod{p}. \end{aligned}$$

Now (2.6) is an immediate consequence of (2.8), (2.9) and the definition of  $b(\vartheta; \mu)$ .

LEMMA 5: With the same notations as in Lemma 4

$$(2.10) \quad \text{ord} [b(\vartheta; mp^v)/b(\vartheta'; mp^{v-1})] = e(j_1 - i_1).$$

PROOF: Since

$$\frac{mp^v - j}{N} = \frac{mp^{v-1} - j_1}{N} p + \frac{j_1 p - j}{N},$$

we get by (2.2)

$$(2.11) \quad \begin{aligned} & \text{ord} [A(\vartheta; mp^v - j)/N] / A(\vartheta'; (mp^{v-1} - j_1)/N) \\ & = (1 + \text{ord} (mp^{v-1} - j_1 + i_1)) e(I). \end{aligned}$$

Regarding

$$b(\vartheta; mp^v) = A(\vartheta; (mp^v - j)/N) ((mp^v - j + i)/N)^{e(j-i)},$$

our lemma follows from (2.11) and (2.4).

### 3. Formalization of the Jacobian of the Fermat curve.

Let  $N \geq 3$  be a natural number and let  $\Gamma_N$  be the Fermat curve  $x^N + y^N = 1$ ,  $J_N$  its Jacobian variety and  $A_N: \Gamma_N \rightarrow J_N$  a canonical map, all defined over  $\mathbb{Q}$ . It is well known that the genus  $n$  of  $\Gamma_N$  is given by

$$n = (N-1)(N-2)/2$$

and the space of differentials of the first kind on  $\Gamma_N$  is spanned by

$$(3.1) \quad \omega(i, j) = x^{j-1} y^{-i} dx = x^{j-1} (1 - x^N)^{-i/N} dx$$

$$(2 \leq i \leq N-1, 1 \leq j \leq i-1).$$

Using the notation of the previous section we can write

$$(3.2) \quad \omega(i, j) = \sum_{v=0}^{\infty} A(\vartheta; v) x^{Nv+j-1} dx$$

with  $\vartheta = i/N$ . Put

$$(3.3) \quad f(i, j; x) = \int_0^x \omega(i, j) = \sum_{v=0}^{\infty} A(\vartheta; v) x^{Nv+j} / (Nv + j).$$

These are integrals of the first kind on  $\Gamma_N$ . Let  $F_N$  be the formalization of  $J_N$  relative to some local parameters at the origin. By Theorem 1 there is a finite set  $S$  of prime numbers such that for  $p \notin S$  the special element of  $\mathfrak{A}_n(p)$ , killing  $\{f(i, j; x) | 2 \leq i \leq N-1, 1 \leq j \leq i-1\} \pmod{p}$ , determines the structure of  $F_N$  regarded as a formal group over  $\mathbb{Z}_p$ . In this section we study such a special element for every  $p \nmid N$ .

For  $v \geq 0$  put

$$(3.4) \quad \begin{cases} a(i, Nv+1) = A(\vartheta; v) \\ a(i, v) = 0 \end{cases} \quad \text{if } v \not\equiv 1 \pmod{N}.$$

Then we have

$$(3.5) \quad f(i, j; x) = \sum_{v=j}^{\infty} a(i, v-j+1)x^v/v.$$

Fix a prime number  $p$  not dividing  $N$ . Put  $M = \{(i, j) | 1 \leq i \leq N-1, 1 \leq j \leq N-1, i \neq j\}$  and  $M_0 = \{(i, j) | 2 \leq i \leq N-1, 1 \leq j \leq i-1\}$ . For a while fix  $(i, j) \in M_0$ ; define  $(i(\alpha), j(\alpha))$  to be the element of  $M$  congruent to  $(ip^{-\alpha}, jp^{-\alpha}) \pmod{N}$  and put

$$\beta = \inf \{\alpha \geq 1 | (i(\alpha), j(\alpha)) \in M_0\}.$$

Then  $1 \leq \beta \leq d$  where  $d$  denotes the order of  $p \pmod{N}$ .

Now we have

$$(3.6) \quad a(i, mp^{dv} - j + 1) = A(i/N; (mp^{dv} - j)/N) = b(i/N; mp^{dv})$$

for  $m \equiv j \pmod{N}$ , since  $\varrho(j-i) = 0$ . By Lemma 4

$$a(i, jp^{dv} - j + 1)/a(i(\beta), jp^{dv-\beta} - j(\beta) + 1)$$

has a limit  $\xi(i, j)$  in  $\mathbb{Z}_p$  as  $v \rightarrow \infty$ .

LEMMA 6:  $\text{ord } \xi(i, j) = \beta - 1$

and

$$(3.7) \quad pf(i, j; x) \equiv \xi(i, j)p^{-(\beta-1)}f(i(\beta), j(\beta); x^{p\beta}) \pmod{p}.$$

PROOF: It follows from Lemma 5 that

$$\begin{aligned} \text{ord } \xi(i, j) &= \text{ord } a(i, jp^{dv} - j + 1)/a(i(\beta), jp^{dv-\beta} - j(\beta) + 1) \\ &= \text{ord } b(i/N; jp^{dv})/b(i(\beta)/N; jp^{dv-\beta}) \\ &= \sum_{\alpha=1}^{\beta} \varrho(j(\alpha) - i(\alpha)) \\ &= \beta - 1. \end{aligned}$$

Now (3.7) is equivalent with the following (3.8) and (3.9):

$$(3.8) \quad p \frac{a(i, mp^{\alpha} - j + 1)}{mp^{\alpha}} \equiv 0 \pmod{p}$$

for  $p \nmid m$ ,  $\alpha < \beta$ .

$$(3.9) \quad p \frac{a(i, mp^{\alpha} - j + 1)}{mp^{\alpha}} \equiv \xi(i, j)p^{-(\beta-1)} \frac{a(i(\beta), mp^{\alpha-\beta} - j(\beta) + 1)}{mp^{\alpha-\beta}} \pmod{p}$$

for  $p \nmid m$ ,  $\alpha \geq \beta$ . By Lemma 5 we have for  $\alpha < \beta$

$$\begin{aligned} \text{ord } a(i, mp^{\alpha} - j + 1) &= \text{ord } b(i/N; mp^{\alpha}) \\ &\geq \sum_{\gamma=1}^{\alpha} \text{ord } b(i(\gamma-1)/N; mp^{\alpha-\gamma+1})/b(i(\gamma)/N; mp^{\alpha-\gamma}) \\ &= \sum_{\gamma=1}^{\alpha} \varrho(j(\gamma) - i(\gamma)) \\ &= \alpha, \end{aligned}$$

which proves (3.8). Further it follows from Lemma 4 that for  $1 \leq \gamma \leq \alpha \leq dv$

$$\frac{b(i(\gamma-1)/N; mp^{\alpha-\gamma+1})}{b(i(\gamma)/N; mp^{\alpha-\gamma})} \equiv \frac{b(i(\gamma-1)/N; jp^{dv-\gamma+1})}{b(i(\gamma)/N; jp^{dv-\gamma})} \pmod{\times p^{\alpha-\gamma+1}}.$$

Consequently we get for  $\alpha \geq \beta$

$$\frac{b(i/N; mp^{\alpha})}{b(i(\beta)/N; mp^{\alpha-\beta})} \equiv \frac{b(i/N; jp^{dv})}{b(i(\beta)/N; jp^{dv-\beta})} \pmod{\times p^{\alpha-\beta+1}},$$

namely

$$(3.10) \quad \frac{a(i, mp^{\alpha} - j + 1)}{a(i(\beta), mp^{\alpha} - j(\beta) + 1)} \equiv \frac{a(i, jp^{dv} - j + 1)}{a(i(\beta), jp^{dv-\beta} - j(\beta) + 1)} \pmod{\times p^{\alpha-\beta+1}} \\ \equiv \xi(i, j).$$

Since  $\text{ord } \xi(i, j) = \beta - 1$ , (3.10) implies

$$a(i, mp^{\alpha} - j + 1) \equiv \xi(i, j)a(i(\beta), mp^{\alpha-\beta} - j(\beta) + 1) \pmod{p^{\alpha}},$$

which is equivalent with (3.9). This completes our proof.

Now write the elements of the set  $\{0 \leq \alpha \leq d | (i(\alpha), j(\alpha)) \in M_0\}$  in order of magnitude:  $\beta_0 < \beta_1 < \dots < \beta_r$ . Then  $\beta_0 = 0$ ,  $\beta_1 = \beta$ ,  $\beta_r = d$  and  $r \leq d$ . Put for  $1 \leq l \leq r$

$$\lim_{v \rightarrow \infty} \frac{a(i(\beta_{l-1}), j(\beta_{l-1})p^{dv} - j(\beta_{l-1}) + 1)}{a(i(\beta_l), j(\beta_l)p^{dv-\beta_l+\beta_{l-1}} - j(\beta_l) + 1)} = \xi(i, j, l).$$

Then  $\xi(i, j) = \xi(i, j, 1)$  and  $\xi(i, j, l) \in \mathbb{Z}_p$ . It follows from Lemma 6

$\text{ord } \xi(i, j, l) = \beta_l - \beta_{l-1} - 1$ , and

$$(3.11) \quad pf(i(\beta_{l-1}), j(\beta_{l-1}); x) \\ \equiv \xi(i, j, l)p^{-\beta_l + \beta_{l-1} + 1} f(i(\beta_l), j(\beta_l); x^{p^{\beta_l - \beta_{l-1}}}) \pmod{p}$$

for  $1 \leq l \leq r$ . Let  $I_{l,m}$  be the matrix of order  $r$  whose  $(l, m)$ -entry is equal to 1 and other entries are all zero. Define the special element  $u(i, j)$  of  $\mathfrak{A}_r(p)$  and the  $r$ -tuple  $\Phi(i, j; x)$  of power series by

$$(3.12) \quad \begin{cases} u(i, j) = pI_r - \sum_{l=1}^r \xi(i, j, l)p^{-\beta_l + \beta_{l-1} + 1} T^{\beta_l - \beta_{l-1}} I_{l, l+1} & (I_{r, r+1} = I_{r, 1}) \\ \Phi(i, j; x) = (f(i(\beta_0), j(\beta_0); x), \dots, f(i(\beta_{r-1}), j(\beta_{r-1}); x)). \end{cases}$$

Then, regarding  $(i(\beta_0), j(\beta_0)) = (i(\beta_r), j(\beta_r)) = (i, j)$ , (3.11) implies

$$\text{THEOREM 2: } u(i, j) * \Phi(i, j; x) \equiv 0 \pmod{p}.$$

Define the equivalence relation in the set  $M_0$  so that  $(i_1, j_1) \sim (i_2, j_2)$  if and only if there is  $\alpha \geq 0$  satisfying  $(i_1 p^\alpha, j_1 p^\alpha) \equiv (i_2, j_2) \pmod{N}$ , and write  $M_0$  as the union of the resulting equivalence classes:

$$M_0 = \bigcup_{s=1}^h M_0(s).$$

For  $1 \leq s \leq h$  take  $(i, j)$  from  $M_0(s)$ , and put

$$u_s = u(i, j), \Phi_s(x) = \Phi(i, j; x)$$

$$\xi_s = \prod_{l=1}^r \xi(i, j, l) = \lim_{v \rightarrow \infty} a(i, jp^{av} - j + 1) / a(i, jp^{d(v-1)} - j + 1).$$

Then  $\xi_s$  is independent of the choice of  $(i, j)$ . Further  $u_s$  and  $\Phi_s(x)$  are uniquely determined by  $M_0(s)$  up to cyclic permutation of  $(\beta_0, \beta_1, \dots, \beta_{r-1})$ . By Theorem 1 and Theorem 2 we get

**THEOREM 3:** *There is a finite set  $S$  of prime numbers containing all prime divisors of  $N$  and satisfying the followings: Let  $p \notin S$  and let  $F_N^{(s)}$  be the formal group over  $\mathbf{Z}_p$  obtained from the special element  $u_s$  ( $1 \leq s \leq h$ ). Then  $F_N$  is the direct product of  $h$  factors  $F_N^{(s)}$  ( $1 \leq s \leq h$ ) regarded as a formal group over  $\mathbf{Z}_p$ .*

It is plausible that we may take  $S = \{p; p \nmid N\}$ .

**THEOREM 4:** *Let notations be as in Theorem 3. If  $p \notin S$ , the reduction of  $F_N^{(s)}$  mod  $p$  is isogenous to the Dieudonné group  $G_{r, d-r}$  over the algebraic closure of  $\mathbf{F}_p$ . (For the group  $G_{r, d-r}$  see [2] or [9].)*

**PROOF:** For any  $p$ -integral object  $U$  we denote by  $U^*$  the reduction of  $U$  mod  $p$ . Regarded as a matrix over  $\mathbf{Z}_p((T))$ , which is a principal ideal domain,  $u_s$  has the elementary divisors  $(1, \dots, 1, \det u_s)$ , because the  $\xi(i, j, l)p^{-\beta_l + \beta_{l-1} + 1}$  are units of  $\mathbf{Z}_p$ . Now

$$(3.13) \quad \det u_s = p^r - \xi_s p^{-(d-r)} T^d$$

and  $\xi_s p^{-(d-r)}$  is a unit of  $\mathbf{Z}_p$ . Since  $F_N^{(s)*}$  corresponds to the Dieudonné module  $\mathfrak{A}_1(p)/(\det u_s)\mathfrak{A}_1(p)$  ([3]), it is isogenous to  $G_{r, d-r}$  over the algebraic closure of  $\mathbf{F}_p$  [3, Lemma 5]. This completes the proof.

It is well known that the endomorphism ring of a formal group over a field of characteristic  $p$  has natural structure of  $\mathbf{Z}_p$ -algebra. For  $\xi \in \mathbf{Z}_p$  we denote by  $[\xi]$  the image of  $\xi$  under the natural injection of  $\mathbf{Z}_p$  into  $\text{End } F_N^{(s)*}$ . By [6, 5.5] it follows from (3.13) that the  $p$ -th power endomorphism of  $F_N^{(s)*}$  satisfies the equation

$$(3.14) \quad [p^r] - [\xi_s p^{-(d-r)}] X^d = 0.$$

Put  $p^d = q$  and denote by  $\Pi_s$  the  $q$ -th power endomorphism of  $F_N^{(s)*}$ . Then (3.14) implies

$$\Pi_s \cdot [\xi_s] = [q].$$

Hence there is  $\pi_s \in \mathbf{Z}_p$  such that  $[\pi_s] = \Pi_s$  and consequently

$$(3.15) \quad \pi_s \xi_s = q.$$

Let

$$(3.16) \quad \varphi(X) = 0$$

be the characteristic equation of the  $q$ -th power endomorphism of  $J_N^*$ . Then the  $q$ -th power endomorphism of  $F_N^*$  satisfies (3.16) too. Hence  $\Pi_s$  is a root of (3.16), so is  $\pi_s$ . Consequently  $\xi_s$  is also a root of (3.16) as is well known. In view of the well known result of Davenport-Hasse [1] we have proved: For all but a finite number of  $p$  the  $\xi_s$  ( $1 \leq s \leq h$ ) are Jacobi sums made from characters, of order  $N$ , of the multiplicative group of  $\mathbf{F}_q$ . In [7] the author conjectured more precisely that for every  $p \nmid N$ ,  $1 \leq s \leq h$  and  $(i, j) \in M_0(s)$  we have

$$(3.17) \quad \xi_s = \pi(\chi^{-j}, \chi^i),$$

where

$$\pi(\chi^{-j}, \chi^i) = - \sum_{a \in F_q} \chi^{-j}(a) \chi^i(1-a)$$

and  $\chi$  denotes the  $N$ -th power residue symbol. This conjecture was proved by Katz by the method of  $p$ -adic analysis.

Now it is not difficult to show that (3.17) is reduced to the case  $j=1$  and in this case (3.17) is equivalent with congruences

$$(3.18) \quad (1-q) \sum_{s=1 \bmod (q-1)} \binom{q^{r-1}i}{s} \equiv \binom{M_r i}{M_r} \bigg/ \binom{M_{r-1} i}{M_{r-1}} \pmod{p^r}$$

for all  $r \geq 1$  where we put  $M_r = (q^r - 1)/(q - 1)$ . It might be an interesting problem to prove (3.18) directly, namely to give an elementary proof of (3.17). The author checked (3.18) only for  $r \leq 2$ .

Testo pervenuto il 22 aprile 1972.

Bozze licenziate il 28 febbraio 1973.

## REFERENCES

- [1] H. DAVENPORT and H. HASSE, *Die Nullstellen den Kongruenz-zetafunktionen in gewissen zyklischen Fällen*, J. Reine Angew. Math., 172 (1934), 151-182.
- [2] J. DIEUDONNÉ, *Lie groups and Lie hyperalgebras over a field of characteristic  $p > 0$  (IV)*, Amer. J. Math., 77 (1955), 429-452.
- [3] J. DIEUDONNÉ, *Groupes de Lie et hyperalgèbres de Lie sur un corps caractéristique  $p > 0$  (VII)*, Math. Ann., 134 (1954), 113-133.
- [4] B. DWORK,  *$p$ -adic cycles*, Publ. I.H.E.S., 37 (1969).
- [5] H. HASSE, *Zetafunktionen und L-Funktionen zu einem arithmetischen Funktionenkörper vom Fermatschen Typus*, Abh. Deutsche Akad. d. Wiss. zu Berlin, Math.-Naturw. Kl., Jahrg. 1955.
- [6] T. HONDA, *On the theory of commutative formal groups*, J. Math. Soc. Japan, 22 (1970), 213-246.
- [7] T. HONDA, *Differential equations and formal groups*, U.S.-Japan Seminar on Modern Methods in Number Theory, Tokyo, 1971.
- [8] T. HONDA, *Formal groups obtained from generalized hypergeometric functions*, to appear in Osaka J. Math.
- [9] Y. MANIN, *The theory of commutative formal groups over fields of finite characteristic*, Russian Math. Surveys, 18 (1963), 1-81.

## A THEOREM ON THE DE RHAM COHOMOLOGY OF A HYPERSURFACE (\*)

NICHOLAS M. KATZ

### Introduction.

The main result of this paper is that, over any base scheme, the primitive part of the middle-dimensional relative De Rham cohomology of the universal family of smooth hypersurfaces of given degree and dimension is «generated» over the (algebra generated by the) derivations of the base (acting through the Gauss-Manin connection) by the submodule consisting of all the classes of highest possible Hodge filtration. Over  $\mathbb{C}$ , the result is entirely without interest, because in that case it is an immediate consequence of Lefschetz's theorem [8] that in any Lefschetz pencil of hypersurfaces of given degree and dimension, the monodromy representation on the primitive part of the middle dimensional complex cohomology of a fibre is irreducible. Indeed, by the regularity theorem [2], Lefschetz's theorem is equivalent to the fact, that over  $\mathbb{C}$ , there is no non-zero proper submodule of the primitive middle-dimensional cohomology of the universal family which is stable under the Gauss-Manin connection.

Over fields of characteristic  $p > 0$  however, the situation is quite different. In that case, the «conjugate filtration» of De Rham cohomology is a highly non-trivial filtration by submodules which are stable by Gauss-Manin. So the moral of the result is that, at least in the universal family, the Hodge filtration is quite transversal to the conjugate filtration, and is as unstable as possible under the Gauss-Manin connection.

In the first section, we recall some basic facts about the Hodge and De Rham cohomology of hypersurfaces, for which [1] is a most convenient reference. The second section is devoted to the statement and proof of the theorem. In a final section, we apply the result to

(\*) I risultati conseguiti in questo lavoro sono stati esposti nella conferenza tenuta il 22 maggio 1972.