

On the differentials associated to congruence relations and the Schwarzian equations defining uniformizations¹⁾

By Yasutaka IHARA

We shall show first, under an abstract setting, that whenever there is a congruence relation, there is a special differential ω of degree $q-1$ in characteristic p associated to it, where q is a certain power of p . We shall then study some basic properties of this differential ω .

Let F_q be the finite field with q elements, and F_{q^2} be its unique quadratic extension. Let X_s and cX_s be proper smooth geometrically irreducible algebraic curves over F_{q^2} that are mutually conjugate over F_q . Roughly speaking, the congruence relation (in our formulation) is a certain nice lifting (to some geometric object in characteristic 0) of the sum of two q -th power morphisms $X_s \rightarrow {}^cX_s$ and ${}^cX_s \rightarrow X_s$. It defines in a natural way a special differential ω of degree $q-1$ on X_s , and ω has its $(q-1)$ -th "root" ω_1 on a $(q-1)$ -fold cyclic covering of X_s . We shall study the divisor of ω , the behavior of ω_1 under the Cartier operator, and the differential equation satisfied by ω_1 which is essentially (the reduction of) the Schwarzian equation defining the uniformization of the lifting of X_s . Our study may also be regarded as (a part of) the general study of "supersingular crossings". It was motivated by our previous work [10]. For further comments and connection with other works, cf. §1.2.

1. Definitions and summary of main results.

1.1 The congruence relation. Our abstract definition of the congruence relation is as follows.

The base ring. As above, let F_q be a finite field with $q=p^f$ elements (p : a prime number), F_{q^2} be its unique quadratic extension, and ι_s be the involutive automorphism of F_{q^2} over F_q given by $\iota_s(a)=a^q$ ($a \in F_{q^2}$). Our base ring is a discrete valuation ring \mathfrak{o} given together with an involutive automorphism ι of \mathfrak{o} , such that

¹⁾ The main content of this paper except §3 had been exposed in a series of informal notes [7].

(a) \mathfrak{o} is of characteristic 0, (b) $\mathfrak{o}/\pi = F_{q^2}$ (π : a prime element of \mathfrak{o}), and (c) ι induces the involution ι_s of the residue field F_{q^2} . For the sake of brevity of notations, we shall write ι also for ι_s . The quotient field of \mathfrak{o} will be denoted by k , and the corresponding additive normalized discrete valuation will be denoted by ord_s . Put $S = \text{Spec } \mathfrak{o} = \{\eta, s\}$, with the generic point η and the closed point s . If Z is any S -scheme²⁾, Z_η will denote its general fiber over S (which is a k -scheme), and Z_s its special fiber (which is an F_{q^2} -scheme). The ι -conjugate ${}^{\iota}Z$ of Z is defined in a natural way³⁾, and then ${}^{\iota}Z_s$ is the conjugate of Z_s over F_q .

The system in characteristic p . It is defined by two mutually ι -conjugate proper smooth geometrically irreducible algebraic curves X_s and ${}^{\iota}X_s$ over F_{q^2} . Let Π (resp. Π') be the graph on $X_s \otimes_{F_{q^2}} {}^{\iota}X_s$ of the q -th power morphism $X_s \rightarrow {}^{\iota}X_s$ (resp. ${}^{\iota}X_s \rightarrow X_s$), both considered as closed reduced subschemes of $X_s \otimes_{F_{q^2}} {}^{\iota}X_s$. Then Π and Π' intersect transversally at each F_{q^2} -rational closed point of the form (x, x^q) , $x^{q^2} = x$. The union $\Pi \cup \Pi'$, which will henceforth be considered as a reduced closed subscheme of $X_s \otimes_{F_{q^2}} {}^{\iota}X_s$, is regular outside these intersecting points.

In the following, an S -surface will mean a two dimensional integral scheme having a structure of a proper and flat S -scheme.

The congruence relation. It is defined whenever there is a lifting $\{X \leftarrow T \rightarrow {}^{\iota}X\}$ of the system $\{X_s \leftarrow \Pi \cup \Pi' \rightarrow {}^{\iota}X_s\}$ in the following sense. X is to be an S -surface which is smooth over S , having X_s as its special fiber, and having a geometrically irreducible algebraic curve X_η as its general fiber. The two curves X_η, X_s then must have the equal genus, which we denote by g . ${}^{\iota}X$ is the ι -conjugate of X . T is an S -surface imbedded in $X \times_S {}^{\iota}X$ as a closed subscheme (by an S -morphism) such that (A) T is invariant by the involution $(x, x') \rightarrow ({}^{\iota}x', {}^{\iota}x)$ of $X \times_S {}^{\iota}X$, (B) T_η is a geometrically irreducible algebraic curve, and (C) $T_s = \Pi \cup \Pi'$ (as F_{q^2} -schemes). By the condition (C), T_η cannot be of the form $(x) \times {}^{\iota}X_\eta$ ($x \in X_\eta$) or $X_\eta \times ({}^{\iota}x')$ ($x' \in {}^{\iota}X_\eta$); therefore, T is finite and surjective over X and ${}^{\iota}X$. Now let $\mu: Y \rightarrow T$ be the normalization of T . Then Y is a normal S -surface, Y_η is a geometrically irreducible normal (hence regular) algebraic curve, and Y_s has two irreducible components of multiplicity one which are isomorphically mapped onto Π and Π' by μ . We

²⁾ "Scheme" in the sense of the Springer edition of [4] I (i.e., "prescheme" in the older sense). But the schemes that we actually consider in this paper are either affine, or proper over S ; hence they are necessarily separated.

³⁾ ${}^{\iota}Z = Z$ as abstract schemes, and the structure morphisms ${}^{\iota}Z \rightarrow S, Z \rightarrow S$ are mutually ι -conjugate. The identification morphisms between ${}^{\iota}Z$ and Z will also be denoted by ι .

shall denote these components of Y_s also by Π, Π' . Then, on Y , Π and Π' intersect transversally at above those points $P \in \Pi \cap \Pi'$ of T with which the local ring $\mathcal{O}_{T,P}$ is normal. These intersecting points of Π and Π' on Y_s will be denoted by P_1, \dots, P_H , and their projections on X_s , by S_1, \dots, S_H . These are F_q -rational closed points of X_s . By the Zariski connection theorem, we have $H \geq 1$. If g_Y denotes the genus of Y_s , then the invariance of Euler-Poincaré characteristic [4] III §7.9, [15] [16], applied to the two fibers of Y over S , gives

$$g_Y - 1 = 2(g - 1) + H.$$

It is clear that the involution of T defined by (A) can be uniquely extended to an involution of Y (which we denote by ι_Y).

Let $\varphi_1: Y \rightarrow X$ (resp. $\varphi_2: Y \rightarrow {}^cX$) be the composite of $\mu: Y \rightarrow T$ with the projection $T \rightarrow X$ (resp. $T \rightarrow {}^cX$). Then φ_1, φ_2 are finite surjective morphisms of degree $q+1$ (by (C)). We shall call such system $\{X \xleftarrow{\varphi_1} Y \xrightarrow{\varphi_2} {}^cX\}$ a *congruence relation*. It is called *unramified* if φ_1, φ_2 are both unramified on the general fiber Y_s of Y . In this case, we have $g_Y - 1 = (q+1)(g-1)$; hence

$$H = (q-1)(g-1).$$

The works of Shimura [20] [21] provide many (and in fact, all known) examples of the unramified congruence relations. They are obtained by the reduction mod p of the arithmetic quotients of complex upper half plane. (There are some differences in formulations. One can transform Shimura's relations into our form only after a careful choice of the model curve and the base ring. Cf. [8] to get its idea.)

1.2. The main results (special case). We shall summarize our main results in the following special case where $\{X \xleftarrow{\varphi_1} Y \xrightarrow{\varphi_2} {}^cX\}$ is an *unramified* congruence relation. Note first that the surface Y is regular outside P_1, \dots, P_H . And at P_i , Y is formally isomorphic over S to the affine plane defined by the equation $xy = \pi^{\nu_i}$ for some positive integer ν_i . We shall show that ν_i is independent of i and is equal to the exponent of the different defined with respect to φ_2 and Π . In particular, we obtain

THEOREM (cf. §3.1) *If $\text{ord}_\pi q = 1$, then $\nu_1 = \nu_2 = \dots = \nu_H = 1$; hence Y is regular.*

A result of this type was first proved by Deligne for the modular curves (see §3.1 for this reference).

THEOREM (cf. §3.1) *There is a differential ω of degree $q-1$ on X_s such that*

$$(\omega) = (S_1 \cdots S_H)^2.$$

Actually, we define ω under a more fairly general setting (§2), and then prove that its divisor is given by $(S_1 \cdots S_H)^2$ in the case of the unramified congruence relations. These results of §3 are proved at the same time by using a sort of intersection theory on the S -surfaces defining stable reductions (Lemma 3).

Now the differential ω has its $(q-1)$ -th root ω_1 (which is a differential of degree one) on a $(q-1)$ -fold cyclic covering of X_s . In the case where $\text{ord}_s q = 1$, we can normalize the constant factor of ω uniquely, so that ω_1 is determined up to F_q^\times -multiples.

THEOREM (cf. §2.3) *Let γ be the Cartier operator. Then*

$$\gamma\omega_1 = c\omega_1$$

with some constant c . If $\text{ord}_s q = 1$, then $c = 1$.

Now the connection with the Schwarzian equations. Suppose given an imbedding of \mathfrak{o} into the complex number field \mathbf{C} , and put $X_{\mathbf{C}} = X_{\mathfrak{o}} \otimes_{\mathfrak{o}} \mathbf{C}$, which we consider as a compact Riemann surface. Since $H \geq 1$, we have $g \geq 2$. Let $\mathcal{H} \rightarrow X_{\mathbf{C}}$ be the uniformization of $X_{\mathbf{C}}$ by the complex upper half plane $\mathcal{H} = \{\tau \in \mathbf{C} \mid \Im \tau > 0\}$, and let

$$\begin{aligned} S_{\mathbf{C}}^X \langle \xi \rangle &= \langle \xi, d\tau \rangle \\ &= w_1^{-2} (2w_1 w_3 - 3w_2^2) (d\tau)^2 \end{aligned}$$

($w_1 = \xi/d\tau$, $w_{i+1} = dw_i/d\tau$ ($i \geq 1$)) be the canonical S -operator of $X_{\mathbf{C}}$ with respect to this uniformization. (It is a mapping of the space of differentials $\xi \neq 0$ of $X_{\mathbf{C}}$ into the space of quadratic differentials of $X_{\mathbf{C}}$, and is one way of formulating the Schwarzian differential equation defining uniformization. Cf. [9].) By our previous result [9], $S_{\mathbf{C}}^X$ is a lifting of an S -operator S^X of X_v , and S^X is independent of the choice of an imbedding $\mathfrak{o} \rightarrow \mathbf{C}$ (see §4.1).

THEOREM (cf. §4.2) (i) S^X is π -integral (§4.2) and its reduction S_*^X is an inner S -operator with respect to ω_1 ; i.e.,

$$S_*^X \langle \xi_* \rangle = \langle \xi_*, \omega_1 \rangle$$

holds for any differential $\xi_* \neq 0$ of X_s ; (ii) if $\text{ord}_s q = 1$, then ω is uniquely characterized by the two conditions, the above property (i) and the invariance by the Cartier operator, for its $(q-1)$ -th root ω_1 .

This suggests that ω_1 can be regarded as the “ $d\tau \pmod{p}$ ”. In some special cases, this characterization can be used to calculate the explicit formula for ω

(§ 4.3). (It includes the elliptic modular case, though it is not an unramified congruence relation.) The author believes that ω is a natural *non-abelian analogue* of the invariant differentials of elliptic curves over finite fields. (The differential ω associated to the weak congruence relation (§ 1.3), where X/S is an elliptic “surface” defining good reduction of elliptic curves having complex multiplications and Y is a lifting of H to an endomorphism of X , is nothing but the $(q-1)$ -th power of the invariant differential of X .) Some application of the π -integrality of S^X , as well as some formal p -adic study of ω and S^X , are given in [7] (b), (c).

In the elliptic modular case, $\omega_1^{(p-1)/2}$ appears *implicitly* in the works of various authors. It is essentially the Hasse invariant of elliptic curves with variable modulus, and is also known to be the reduction mod p of the Eisenstein series of weight $p-1$. (Cf. Serre [18] [19] for the works related to Eisenstein series mod p , of Deligne, Serre and Swinnerton-Dyer. See also Igusa [5], Tate [22], Ihara [6], Dwork [3], Koike [12] and Katz [11], for other related works on this subject.) Some of these works are p -adic, instead of just modulo p . On the other hand, each of them uses either elliptic curves fibered, or Fourier expansions at the cusp. We want to stress that ω is *directly associated to the congruence relation*, so that it can be immediately generalized to each case where there is a congruence relation.

Besides the elliptic modular case, all known “almost unramified congruence relations” (cf. § 1.3) belong to the works of Shimura [20] [21], where the abelian varieties are used for the proofs. During this past one year, I obtained some progress in cultivating a method for proving the congruence relations more directly and under more abstract assumptions, although it has not yet been sufficiently developed. We hope to be able to discuss this subject (together with more examples!) in a near future.

1.3 Weaker assumptions. We shall sometimes base our argument on the following weaker assumptions.

The weak congruence relation. This is a “one-sided” congruence relation having no symmetry at all. This weak setting is sufficient as long as the definition of ω and the results of § 2 and § 4 are concerned.

First, the conditions on (\mathfrak{o}, ι) will be weakened as follows. ι is any automorphism of a discrete valuation ring \mathfrak{o} of characteristic 0, such that $\mathfrak{o}/\pi = F_{q^r}$ for some positive integer r , and such that ι induces the q -th power automorphism $a \rightarrow a^q$ of F_{q^r} . It need not be assumed that the order of ι is strictly r . For such

(0, ι), if Z is any S -scheme ($S = \text{Spec } \mathfrak{o}$), ιZ will denote its ι -transform; i.e., $\iota Z = Z$ as abstract schemes and the structure morphism $\iota Z \rightarrow S$ is the composite of the structure morphism $Z \rightarrow S$ and the automorphism $S \rightarrow S$ that corresponds to ι^{-1} . If ξ is any scheme-theoretic object on Z , we denote by $\iota \xi$ the same object considered as an object on ιZ . (We shall sometimes call $\iota \xi$ the ι -conjugate of ξ .)

Secondly, the conditions (A) (B) (C) for T (§ 1.1) will be weakened as follows. Instead of (A) (B) (C), we only assume (B) and the following weakening (C') of (C):

(C') T_* contains Π (the graph of the q -th power morphism $X_* \rightarrow \iota X_*$) as a simple component.

Note that even under this weaker assumption, T (and hence also Y) is finite and surjective over X and ιX .

A system $\{X \xleftarrow{\varphi_1} T \xrightarrow{\varphi_2} \iota X\}$ with these weakened conditions will be called a *weak congruence relation*.

Almost unramified congruence relation. The following condition of almost unramifiedness, which is somewhat weaker than the unramifiedness, singles out the class of those congruence relations that are related to automorphic functions. Let $\{X \xleftarrow{\varphi_1} Y \xrightarrow{\varphi_2} \iota X\}$ be a weak congruence relation. For $Z = X, \iota X$ or Y , let $R(Z)$ denote the function field of Z . Then each $R(Z)$ is an algebraic function field of one variable over k , $R(Y)$ contains $R(X)$ and $R(\iota X)$ (by φ_1, φ_2), and $R(Y) = R(X)R(\iota X)$. Consider the smallest normally algebraic extension M of $R(Y)$ which is normal over both $R(X)$ and $R(\iota X)$. In general, M is an infinite normal extension of $R(Y)$. Again, for $Z = X, \iota X$ or Y , let g_Z denote the genus of Z_η . For each closed point P of Z_η (considered also as a discrete valuation of $R(Z)$ over k), let $\deg P$ denote its relative degree over k , and $e(P)$ denote its ramification index in $M/R(Z)$. We shall say that $M/R(Z)$ is almost unramified if $e(P) = 1$ for almost all closed points P of Z_η . It is obvious that $M/R(Y)$ is almost unramified if and only if $M/R(X)$ (resp. $M/R(\iota X)$) is so. In this case, put

$$\mu(Z) = 2g_Z - 2 + \sum_P \left(1 - \frac{1}{e(P)}\right) \deg P,$$

where P runs over all closed points of Z_η . The Hurwitz formula gives $\mu(Y) = (R(Y) : R(X))\mu(X) = (R(Y) : R(\iota X))\mu(\iota X)$. Now, we shall say that $\{X \xleftarrow{\varphi_1} Y \xrightarrow{\varphi_2} \iota X\}$ is *almost unramified* if the following condition (AU) is satisfied:

(AU) $M/R(Y)$ is almost unramified, and the ι -conjugate closed points $P, \iota P$ of $X_\eta, \iota X_\eta$ have the same ramification indices in M .

It is easy to see that if $R(Y)/R(X)$ and $R(Y)/R(\iota X)$ are both unramified then

$M/R(Y)$ is unramified. Therefore, an unramified congruence relation (resp. an unramified weak congruence relation) is almost unramified.

We shall say that a weak congruence relation $\{X \xleftarrow{c_1} Y \xrightarrow{c_2} {}^cX\}$ belongs to the *general type* if $\mu(Y) > 0$ and $R(X) \cap R({}^cX) = k$. Every unramified congruence relation belongs to the general type. In fact, since $g \geq 2$ in this case, we have $\mu(X) = 2g - 2 > 0$. To check that $R(X) \cap R({}^cX) = k$, look at the algebraic correspondence ${}^cT \circ T$ (the composite of T with its transpose cT) which induces a "multi-valued action" on the geometric points of each fiber of X over S . By (C), its action on the special fiber contains the q^2 -th power morphism of X_s . But X_s has closed geometric points of arbitrary large degree over F_{q^2} , and on the other hand, if $R(X)$ (and hence also $R({}^cX)$) were finite over $R(X) \cap R({}^cX)$, the cardinality of each orbit of the iterates of $({}^cT \circ T)_s$ acting on the closed geometric points of X_s must be bounded, a contradiction.

2. The differential ω .

In §2, $\{X \xleftarrow{c_1} Y \xrightarrow{c_2} {}^cX\}$ is any weak congruence relation (cf. §1.3).

2.1. The integer ν . Let Z be either one of $X, {}^cX$ and Y , with function field $R(Z)$. The space $D(Z/S)$ of differentials on Z/S is the one-dimensional $R(Z)$ -module $\mathcal{S}/\mathcal{S}^2$, where \mathcal{S} is the kernel of the homomorphism $R(Z) \otimes_k R(Z) \rightarrow R(Z)$ defined by $f_1 \otimes f_2 \rightarrow f_1 f_2$, $\mathcal{S}/\mathcal{S}^2$ being considered as an $R(Z)$ -module through the homomorphism $R(Z) \rightarrow R(Z) \otimes_k R(Z)$ defined by $f \rightarrow f \otimes 1$. If $\Omega_{Z/S}$ is the sheaf of relative differentials on Z/S , then $D(Z/S)$ is nothing but the stalk of $\Omega_{Z/S}$ at the generic point of Z . Thus, $D(Z/S)$ can be identified with the union of $\Gamma(U, \Omega_{Z/S})$ for all non-empty open subsets U of Z . The space $D^h(Z/S)$ of differentials of degree h on Z/S ($h \geq 1$) is the tensor product of h copies of $D(Z/S)$ over $R(Z)$. It is the stalk of $\Omega_{Z/S}^h$ at the generic point of Z , where $\Omega_{Z/S}^h$ is the tensor product of h copies of $\Omega_{Z/S}$ over the structure sheaf of Z . The direct sum $R(Z) \oplus (\bigoplus_{h \geq 1} D^h(Z/S))$ is a graded $R(Z)$ -algebra. Instead of writing $\xi \otimes \cdots \otimes \xi$ (r copies) for its element ξ , we shall write ξ^r . Restriction to the general fiber gives an $R(Z)$ -isomorphism $\xi \rightarrow \xi_\eta$ of $D^h(Z/S)$ onto the space $D^h(Z_\eta/k)$ of differentials of degree h on the curve Z_η/k .

When an element ξ of $D^h(X/S)$ (resp. $D^h(Y/S)$) is finite at the generic point of X_s (resp. Π), its restriction to X_s (resp. Π) will be denoted by ξ_{X_s} (resp. ξ_Π). Otherwise, we shall write $\xi_{X_s} = \infty$ (resp. $\xi_\Pi = \infty$). Let f be an element of the local ring \mathcal{O}_{X, X_s} such that $R(X_s)/F_{q^r}(f_{X_s})$ is finite separable. Then $(df)_{X_s} = d(f_{X_s}) \neq 0, \infty$.

Therefore, $\xi = F(df)^h$ with $F \in R(X)$ (resp. $\eta = G \cdot \varphi_1^*(df)^h$ with $G \in R(Y)$) is finite at the generic point of X_* (resp. Π) if and only if $F_{X_*} \neq \infty$ (resp. $G_\Pi \neq \infty$). If $F \in R(X)$ is such that $F_{X_*} \neq \infty$, then $(dF)_{X_*} = d(F_{X_*}) \neq \infty$; if $G \in R(Y)$ is such that $G_\Pi \neq \infty$, then $(dG)_\Pi = d(G_\Pi) \neq \infty$.

Let ord_{X_*} (resp. $\text{ord}_{X_*}, \text{ord}_\Pi$) denote the normalized additive discrete valuation of $R(X)$ (resp. $R({}^tX), R(Y)$) defined at X_* (resp. ${}^tX_*, \Pi$). Since Π is of multiplicity one in Y_* , we have $\text{ord}_\Pi \pi = 1$. On the other hand, since Π and X_* are canonically isomorphic, the two valuations ord_{X_*} and ord_Π have the common residue field $R(X_*)$. Therefore, $R(X)$ is Π -adically dense in $R(Y)$.

Let ξ be any element of $D(X/S)$ with $\xi \neq 0$, and ${}^t\xi$ be the ι -conjugate of ξ on tX . Consider the integer

$$\nu = \text{ord}_\Pi (\varphi_2^*({}^t\xi) / \varphi_1^*(\xi)).$$

Then ν is independent of the choice of ξ . In fact, if $F \in R(X)$, $F \neq 0$, then

$$\text{ord}_\Pi (\varphi_2^*({}^tF)) = \text{ord}_{X_*} ({}^tF) = \text{ord}_{X_*} (F) = \text{ord}_\Pi (\varphi_1^*(F)).$$

PROPOSITION 1. $1 \leq \nu \leq \text{ord}_\pi q$; in particular, $\nu = 1$ if $q = p$ and p is a prime element of \mathfrak{o} .

PROOF. One may take $\xi = df$, where f is an element of $\Theta_{X,X}$, such that $R(X_*)/F_{\mathfrak{o}}(f_{X_*})$ is finite separable. Put $f_1 = \varphi_1^*(f)$, $f_2 = \varphi_2^*(f)$. Then, since Π is the graph of the q -th power morphism $X_* \rightarrow {}^tX_*$, we have $f_2 \equiv f_1^q \pmod{\Pi}$. Let

$$f_2 = f_1^q + \sum_{i \in I} F_i^{p^{r_i}} \pi^i + \sum_{j \in J} c_j \pi^j$$

be a Π -adic expansion of f_2 , chosen in such a way that I, J are disjoint sets of positive integers, F_i ($i \in I$) are elements of $\Theta_{X,X}$, such that $(F_i)_{X_*}$ are not p -th powers in $R(X_*)$, and c_j ($j \in J$) are units of \mathfrak{o} . Differentiating this,⁴⁾ we obtain

$$(1) \quad \frac{df_2}{df_1} = q f_1^{q-1} + \sum_{i \in I} p^{r_i} F_i^{p^{r_i}-1} \frac{dF_i}{df_1} \pi^i.$$

Now, in general, if t_λ ($1 \leq \lambda \leq n$) are elements of an algebraic function field of one variable with finite constant field of characteristic p that are not p -th power elements, and if $m_1 > m_2 > \dots > m_n \geq 0$, then the differentials $t_\lambda^{m_\lambda-1} dt_\lambda$ ($1 \leq \lambda \leq n$) are

⁴⁾ Here, note that $\frac{d}{df_1}: R(Y) \rightarrow R(Y)$ is Π -adically continuous, because $\frac{d}{df}: R(X) \rightarrow R(X)$ is continuous and $\Theta_{Y,\Pi}$ is a localization of the integral closure of Θ_{X,X_*} in $R(Y)$ which is a finite Θ_{X,X_*} -module.

linearly independent over the constants. (This follows immediately by use of the Cartier operator γ . Indeed, $\gamma(t^{p^m-1}dt) = t^{p^m-1-1}dt$ ($m \geq 1$) and $\gamma(dt) = 0$.) Now put $q = p^{r_0}$, and

$$\nu' = \text{Min}(\text{ord}_\pi q, r_i, \text{ord}_\pi p + i \ (i \in I)) = \text{Min}(r_i, \text{ord}_\pi p + i \ (i \in I \cup (0))).$$

Let I_0 be the set of all $i \in I \cup (0)$ such that $r_i, \text{ord}_\pi p + i = \nu'$. Then $r_i > r_j$ for $i, j \in I_0$ with $i < j$. Therefore, by the above remark, the differentials $F_i^{p^{r_i-1}}dF_i$ ($i \in I_0$), where $F_0 = f_1$, are linearly independent over k , when reduced modulo π . Therefore, $\nu = \nu'$; in particular, $1 \leq \nu \leq \text{ord}_\pi q$. Q.E.D.

REMARKS. (i) The notation being as above, take $c \in \mathfrak{o}$ with $\text{ord}_\pi c = \nu$, and let ζ be the restriction of $c^{-1}df_2$ to Π , considered as a differential on X , through the canonical isomorphism $\Pi \xrightarrow{\sim} X_s$, and let γ be the Cartier operator on X_s . Then the above proof shows that $\gamma^m(\zeta) = 0$ for some finite iterate γ^m of γ . This implies that the residue of ζ at each pole must be zero. In particular, ζ cannot have simple poles. This fact will be used later. (ii) ν is equal to the exponent of the different of $R(Y)/R(X)$ at Π , but the above definition is more convenient for our purpose.

2.2 The definition of ω . Fix any element $c \in \mathfrak{o}$ with $\text{ord}_\pi c = \nu$. When $\text{ord}_\pi q = 1$, we shall always choose $c = p$. Take any $\xi \in D(X/S)$ with $\xi_{X_s} \neq 0, \infty$, let ${}^t\xi \in D({}^tX/S)$ be its t -conjugate, and put

$$\theta = \varphi_1^*(\xi)^q / (c^{-1}\varphi_2^*({}^t\xi)) \in D^{q-1}(Y/S).$$

Then, since $\text{ord}_\pi c = \nu$, we have $\theta_\Pi \neq 0, \infty$ for the restriction θ_Π of θ to Π ; and since $\varphi_2^*(f) \equiv \varphi_1^*(f)^q \pmod{\Pi}$ holds for any $f \in R(X)$ with $f_{X_s} \neq 0, \infty$, the differential θ_Π is independent of the choice of ξ . By the canonical isomorphism $\Pi \xrightarrow{\sim} X_s$, we shall identify X_s with Π , and consider θ_Π as a differential of degree $q-1$ on X_s/F_q^r , which we call ω .

The differential ω depends on the choice of the constant c , but only up to $F_{q^r}^\times$ -multiples, and in the case of $\text{ord}_\pi q = 1$, ω is uniquely determined according to our convention to choose $c = p$.

2.3 The differential ω_1 and the Cartier operator. As above, let $\xi \in D(X/S)$ be such that $\xi_{X_s} \neq 0, \infty$, put $G = \varphi_1^*(\xi) / (c^{-1}\varphi_2^*({}^t\xi))$, and consider G_Π as a function on X_s . Then $\omega = G_\Pi \cdot \xi_{X_s}^{q-1}$. Let $Z_s \rightarrow X_s$ be any finite separable covering of X_s on which the $(q-1)$ -th roots of G_Π are rational. Then we may write $\omega = (\omega_1)^{q-1}$, with a differential ω_1 which is of degree one and rational on Z_s . Let γ be the Cartier operator on Z_s .

THEOREM 1. *We have*

$$\gamma^f(\omega_1) = a \cdot \omega_1,$$

where f is defined by $q = p^f$, and $a^q \in F_q$ is the residue class of $qc^{-1} \bmod \pi$. In particular,

$$\gamma(\omega_1) = \omega_1,$$

if $q = p$ and p is a prime element of \mathfrak{o} ; hence in this case, $\omega_1 = t^{-1}dt$ with some rational function t on Z_s .

PROOF. Notation being as in the proof of Proposition 1, let ζ be the differential of X_s that corresponds to the restriction of $c^{-1}df_2$ on Π . Then it follows immediately from the proof of Proposition 1 that $\gamma^f(\zeta) = a \cdot (df_1)_{X_s}$. But $\omega_1 = ((df_1)_{X_s}/\zeta)^{q/(q-1)} \cdot \zeta = ((df_1)_{X_s}/\zeta)^{1/(q-1)} \cdot (df_1)_{X_s}$. Therefore,

$$\gamma^f(\omega_1) = ((df_1)_{X_s}/\zeta)^{1/(q-1)} \cdot a \cdot (df_1)_{X_s} = a \cdot \omega_1.$$

Q.E.D.

PROPOSITION 2. *The differential ω has no simple zeros on X_s .*

PROOF. Let P be any closed point of X_s and $f_{X_s} \in R(X_s)$ be a prime element at P . Extend f_{X_s} to $f \in R(X)$, and let ζ be as above, for this f . Then $\omega = (df_{X_s})^q/\zeta$, and $df_{X_s} \neq 0, \infty$ at P , while ζ cannot have simple poles (Remark at the end of §2.1).

Q.E.D.

3. The divisor of ω .

In §3 (except §3.4), we shall assume the unramified congruence relation (§1.1) for the system $\{X \xleftarrow{\varphi_1} Y \xrightarrow{\varphi_2} X\}$.

3.1. Recall that the S -scheme Y is smooth on Y_τ , and that Y_s is the union of two smooth curves Π, Π' of genus $g \geq 2$ (isomorphic over F_q^2 to X_s, X_s , respectively) intersecting transversally at $H = (q-1)(g-1)$ distinct closed F_q^2 -rational points (the corresponding points of X_s being denoted by S_1, \dots, S_H). Thus, Y defines a stable reduction of Y_τ in the sense of Deligne-Mumford [1]. In particular, at each point of $\Pi \cap \Pi'$, Y is formally isomorphic over S to the affine plane defined by the equation $xy = \pi^n$ for some positive integer n . We shall check that this integer n is equal to the integer ν defined in §2.1.

THEOREM 2. *Let ν be the positive integer defined in §2.1. Then at each point of $\Pi \cap \Pi'$, Y is formally isomorphic over S to the affine plane defined by the equation $xy = \pi^\nu$. In particular, Y is a regular scheme if and only if $\nu = 1$.*

COROLLARY. *Y is a regular scheme if $q = p$ and p is a prime element of \mathfrak{o} .*

A result of this type was first obtained by Deligne, who observed among others

the regularity of the modular scheme corresponding to the modular group " $\Gamma_0(p) \cap \Gamma'(M)$ " ($M \geq 3$)⁵⁾.

Note that each totally ramified constant ring extension yields a new unramified congruence relation for which Y is not regular. So, the regularity of Y cannot hold in general without any assumptions on the choice of the constant ring \mathfrak{o} .

We shall then prove:

THEOREM 3. $(\omega) = (S_1 \cdots S_H)^2$.

3.2 Some lemmata. To prove these theorems, let us first review the following lemma which is well-known in the theory of stable reductions.

LEMMA 1. *Let A be a complete discrete valuation ring with prime element π , and (B, \mathfrak{m}) be a complete noetherian two-dimensional local domain dominating $(A, (\pi))$. Assume that*

$$B = \mathfrak{m} + A, \quad \pi B = \mathfrak{p} \cap \mathfrak{p}', \quad \mathfrak{m} = \mathfrak{p} + \mathfrak{p}',$$

with two distinct prime ideals $\mathfrak{p}, \mathfrak{p}'$ of B with height one, and moreover that $B/\mathfrak{p}, B/\mathfrak{p}'$ are normal (hence discrete valuation rings). Then for some positive integer n , B is isomorphic over A to the ring

$$A[[x, y]]/(xy - \pi^n).$$

PROOF. We can find three sequences

$$(1) \quad \{x_m\}, \quad \{y_m\}, \quad \{a_m\} \quad (m=1, 2, \dots)$$

in $\mathfrak{p}, \mathfrak{p}', A$, respectively, satisfying $x_{m+1} \equiv x_m, y_{m+1} \equiv y_m, a_{m+1} \equiv a_m \pmod{\pi^m B}$, and

$$(2) \quad x_m y_m \equiv a_m \pmod{\pi^m B}.$$

In fact, by our assumptions on $\mathfrak{p}, \mathfrak{p}'$, we can find $x_1 \in \mathfrak{p}, y_1 \in \mathfrak{p}'$ such that $\mathfrak{p} = (\pi, x_1), \mathfrak{p}' = (\pi, y_1)$. Then $x_1 y_1 \in \pi B$, so that (2) is satisfied for $m=1$ with $a_1=0$. Suppose we have already found the sequences up to m (≥ 1), and put

$$x_m y_m = a_m + \pi^m b_m, \quad b_m \equiv c_m + \alpha_m x_1 + \beta_m y_1 \pmod{\pi B},$$

with $b_m, \alpha_m, \beta_m \in B, c_m \in A$. Put $x_{m+1} = x_m - \pi^m \beta_m, y_{m+1} = y_m - \pi^m \alpha_m$, and $a_{m+1} = a_m + \pi^m c_m$. Then $x_{m+1} y_{m+1} \equiv a_{m+1} \pmod{\pi^{m+1} B}$. Now, being a noetherian local ring, B is separated for the ideal-adic topologies. Since B is \mathfrak{m} -adically complete, the sequences of (1) converge; let $x_\infty \in \mathfrak{p}, y_\infty \in \mathfrak{p}', a_\infty \in A$ be their limits. Then $\mathfrak{p} = (\pi, x_\infty), \mathfrak{p}' = (\pi, y_\infty), x_\infty y_\infty = a_\infty$, and B is an integral domain, so that $a_\infty \neq 0$. Replacing x_∞ by some A^\times -multiple, we obtain x_∞, y_∞ satisfying $\mathfrak{p} = (\pi, x_\infty), \mathfrak{p}' = (\pi, y_\infty)$ and $x_\infty y_\infty = \pi^n$ for some

⁵⁾ Stated without proof in [2a], and details appeared in [2b].

integer n . Now it is clear that elements of B can be expressed in the form $z = a + x_\infty f(x_\infty) + y_\infty g(y_\infty)$ with $a \in A$, and $f(x) \in A[[x]]$, $g(y) \in A[[y]]$, and it is easy to see that $z \in \pi B$ if and only if a and all coefficients of $f(x)$, $g(y)$ are divisible by π ; (proceed as: $z \in \pi B \Rightarrow a \in \mathfrak{m} \Rightarrow f(x_\infty) \in \mathfrak{p}'$, $g(y_\infty) \in \mathfrak{p} \Rightarrow f(0), g(0) \in \mathfrak{m}$, and so on). Therefore, the above expression for z is unique. Therefore, the A -homomorphism $A[[x, y]] \rightarrow B$ defined by $F(x, y) \mapsto F(x_\infty, y_\infty)$ induces an isomorphism $A[[x, y]]/(xy - \pi^n) \simeq B$. Q.E.D.

In the following, if B is any noetherian normal ring and \mathfrak{c} is a prime ideal of B with height one, so that the localization $B_{\mathfrak{c}}$ is a discrete valuation ring, we shall denote by $\text{ord}_{\mathfrak{c}}$ the corresponding normalized additive discrete valuation of the quotient field of B .

LEMMA 2. *Let A, π be as in Lemma 1, and n be a positive integer. Put $B = A[[x, y]]/(xy - \pi^n)$. Then (i) B satisfies the assumptions of Lemma 1 for $\mathfrak{m} = (\pi, x, y)$, $\mathfrak{p} = (\pi, x)$, $\mathfrak{p}' = (\pi, y)$; (ii) B is a normal ring; (iii) let ξ be any element of B with $\mathfrak{p} = (\pi, \xi)$; then $\text{ord}_{\mathfrak{p}} \xi \leq n$, and the equality holds if and only if (ξ) is \mathfrak{p} -primary, and also if and only if $(\xi) = (x)$; in particular, the integer n is characterized by $n = \text{Max}_{\mathfrak{p}=(\pi, \xi)} \text{ord}_{\mathfrak{p}} \xi$.*

PROOF. (i) Obvious. (ii) B is the integral closure of $A[[t]]$, $t = x - y$, in the quadratic extension defined by $x^2 - tx - \pi^n = 0$. (iii) By the Weierstrass' Preparation Theorem applied to $A[[y]][[x]]$, every element ξ of B with $\xi \notin \mathfrak{p}'$ is a unit multiple of an element of the form

$$x^m + a_1 x^{m-1} + \cdots + a_m + a_{m+1} y + a_{m+2} y^2 + \cdots,$$

with $a_i \in A$, $a_1, \dots, a_m \in (\pi)$. Here, m is nothing but the \mathfrak{m} -adic order of the residue class of $\xi \bmod \mathfrak{p}'$. If $\mathfrak{p} = (\pi, \xi)$, so that $\mathfrak{m} = (\mathfrak{p}', \xi)$, we have $m = 1$. Therefore, $\text{ord}_{\mathfrak{p}} \xi = \text{ord}_{\mathfrak{p}}(\xi y) = \text{ord}_{\mathfrak{p}}(\pi^n + a_1 y + \cdots)$; from this follows easily (as at the last part of the proof of Lemma 1) that $\text{ord}_{\mathfrak{p}} \xi \leq n$.

As for the rest of (iii), first, it is clear that $\text{ord}_{\mathfrak{p}} x = n$; so that $(\xi) = (x)$ implies $\text{ord}_{\mathfrak{p}} \xi = n$. Secondly, suppose that $\text{ord}_{\mathfrak{p}} \xi = n$. Then since (x) is \mathfrak{p} -primary and $\text{ord}_{\mathfrak{p}} x = n$, ξx^{-1} belongs to $B_{\mathfrak{c}}$ for all prime ideals \mathfrak{c} of B with height one, and since B is normal, this implies $\xi x^{-1} \in B$, so that $\xi = xb$ ($b \in B$). But since $\mathfrak{m} = (\mathfrak{p}', \xi)$, b must be a unit of B ; hence $(\xi) = (x)$, and this implies (ξ) is \mathfrak{p} -primary. Finally, suppose that (ξ) is \mathfrak{p} -primary (and $\mathfrak{p} = (\pi, \xi)$). We may assume that ξ is of the form $\xi = x + a_1 + a_2 y + \cdots$, with $a_i \in A$, so that $\xi y = \pi^n + a_1 y + \cdots$. If not all coefficients a_i are divisible by π^n , we have $\text{ord}_{\mathfrak{c}} \xi y \neq 0$ for some $\mathfrak{c} \neq \mathfrak{p}, \mathfrak{p}'$, which is absurd. Therefore, ξy is a unit multiple of π^n , i.e., ξ is a unit multiple of x , i.e., $(\xi) = (x)$.

Q.E.D.

Let A, B, \dots , be as in Lemmas 1, 2. Consider the corresponding local schemes: $\text{Spec } B \rightarrow \text{Spec } A$, and let s_B resp. s_A be their closed points. A prime divisor of $\text{Spec } B$ is by definition a closed irreducible subset of $\text{Spec } B$ with codimension one, considered as a reduced scheme. It corresponds to a prime ideal of B with height one. The prime divisors corresponding to $\mathfrak{p}, \mathfrak{p}'$ will be denoted by Π, Π' , respectively. Then the special fiber $(\text{Spec } B)_{s_A}$ is reduced, and is the union of Π, Π' , crossing at s_B . For each prime divisor Γ of $\text{Spec } B$, ord_Γ will denote the normalized additive discrete valuation of the function field of $\text{Spec } B$ (the quotient field of B) defined by Γ . If $\Gamma \neq \Pi, \Pi'$, then Γ is finite and flat over $\text{Spec } A$, and its normalization $\tilde{\Gamma}$ is a Spec of a discrete valuation ring which is finite (and flat) over A . It is clear that $\Gamma \rightarrow \xi = x|_\Gamma$ gives a one-to-one correspondence between the prime divisors $\Gamma \neq \Pi, \Pi'$ of $\text{Spec } B$ and the elements ξ of the algebraic closure of the quotient field $R(A)$ of A , counted up to conjugacy over $R(A)$, satisfying $0 < \text{ord}_\pi \xi < n$. Here, ord_π is the unique extension of the normalized additive valuation of $R(A)$ to its algebraic closure. It is also clear that Γ (resp. $\tilde{\Gamma}$) is the Spec of $A[\xi, \eta]$ (resp. its integral closure in $R(A)(\xi)$), where η is defined by $\xi\eta = \pi^n$. So, $R(\Gamma) = R(A)(\xi)$. For each Γ , put $\deg(\Gamma/A) = [R(\Gamma) : R(A)]$ and

$$(3) \quad \epsilon_{\Gamma, \Pi} = \deg(\Gamma/A) \cdot \text{ord}_\pi(\xi).$$

This has an intrinsic meaning for the pair of two prime divisors Γ and Π , as (x) is the unique principal \mathfrak{p} -primary ideal of B , which, together with π , generate \mathfrak{p} (Lemma 2(iii)), and the value of (3) remains unaltered if one replaces x by its unit multiple. If s_Γ is the closed point of $\tilde{\Gamma}$ and $\deg(s_\Gamma/s_A)$ is the degree of the residue field extension at s_Γ/s_A , then $\epsilon_{\Gamma, \Pi}$ can also be expressed as

$$(4) \quad \epsilon_{\Gamma, \Pi} = \deg(s_\Gamma/s_A) \text{ord}_{s_\Gamma}(\tilde{\xi}),$$

where $\tilde{\xi}$ is the lift back of ξ on $\tilde{\Gamma}$, and $\text{ord}_{s_\Gamma}(\tilde{\xi})$ is its order at s_Γ .

Now let f be any element of the function field of $\text{Spec } B$ (the quotient field of B) such that $\text{ord}_\Pi(f) = 0$. Then the order of $f|_\Pi$ at s_B is given by the following

LEMMA 3⁶⁾. *We have*

$$\text{ord}_{s_B}(f|_\Pi) = \frac{1}{n} \left\{ \text{ord}_{\Pi'}(f) + \sum_{\Gamma \neq \Pi, \Pi'} \epsilon_{\Gamma, \Pi} \cdot \text{ord}_\Gamma(f) \right\}.$$

PROOF. We may assume that $f \in B$, and by the Weierstrass' Preparation Theorem applied to $A[[x]][[y]]$, we may further assume that f is of the form

⁶⁾ When $n=1$ so that B is regular, this type of result is well-known: cf. Šafarevich [17].

$$(5) \quad f = y^m + a_1 y^{m-1} + \cdots + a_m + a_{m+1} x + \cdots,$$

with $a_i \in A$, $a_1, \dots, a_m \in \pi A$, where $m = \text{ord}_{*B}(f|_H)$. Put $x^m f = \pi^k g$, with

$$g = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \cdots, \quad (\alpha_i \in A),$$

where k is determined by $\min_{i \geq 0} \text{ord}_{\pi} \alpha_i = 0$. Then $0 \leq k \leq mn$, and $k = \text{ord}_{H'}(x^m f) = \text{ord}_{H'}(f)$. Moreover, we have $\text{ord}_{\pi} \alpha_i + ni > mn - k$ ($i \geq 1$). Let l (≥ 0) be the minimum suffix such that $\text{ord}_{\pi} \alpha_l = 0$. Then g is a unit multiple of a polynomial

$$g_0 = \alpha'_0 + \alpha'_1 x + \cdots + \alpha'_{l-1} x^{l-1} + x^l,$$

where $\text{ord}_{\pi} \alpha'_0 = mn - k$, $\text{ord}_{\pi} \alpha'_i > 0$ ($i < l$), and $\text{ord}_{\pi} \alpha'_i + ni > mn - k$ ($i = 1, \dots, l$; $\alpha'_l = 1$). Therefore, each root ξ of g_0 satisfies $0 < \text{ord}_{\pi} \xi < n$. Let Γ_{ξ} be the corresponding prime divisor of $\text{Spec } B$. Then the irreducible polynomial (in x) for ξ over $R(A)$ is a prime element of $\text{ord}_{\Gamma_{\xi}}$. (In fact, let \mathfrak{c} be the prime ideal of B corresponding to Γ_{ξ} , and put $\mathfrak{c}_2 = \{z \in \mathfrak{c} \mid \text{ord}_{\mathfrak{c}}(z) \geq 2\}$. Then $\mathfrak{c}_2 \not\subseteq \mathfrak{p}$, as \mathfrak{c}_2 is \mathfrak{c} -primary and $\mathfrak{c} \not\subseteq \mathfrak{p}$. The prime elements of $\text{ord}_{\Gamma_{\xi}}$ which are contained in B are elements of $\mathfrak{c} - \mathfrak{c}_2$, so we may choose a prime element not belonging to \mathfrak{p} . By the Weierstrass' Preparation Theorem applied to $A[[x]][[y]]$, we may choose a prime element of the form (5), and as x is a \mathfrak{c} -unit, the multiplication of x^m yields a prime element which is a power series in x ; hence the multiplication of a suitable unit of B yields a prime element which is a polynomial in x .) Therefore, if ξ runs over the roots of g_0 counted up to conjugacy over $R(A)$, it holds that

$$\text{ord}_{\pi} \alpha'_0 = \sum_{\xi} [R(\Gamma_{\xi}) : R(A)] (\text{ord}_{\pi} \xi) (\text{ord}_{\Gamma_{\xi}} f);$$

therefore,

$$mn - k = \sum_{\Gamma \neq H, H'} \iota_{\Gamma, H} \cdot \text{ord}_{\Gamma}(f).$$

Q.E.D.

3.3 Proofs of Theorems 2, 3. As before, we shall identify H with X_s by the isomorphism $H \xrightarrow{\sim} X_s$ induced from φ_1 . Take any closed point $P \in H$, considered also as a point of X_s . Take any differential of the first kind ξ_x on X_s such that $\xi_x \neq 0$ at P , and extend it to a differential ξ of the first kind on X/S (i.e., a global section of $\Omega_{X/S}$). Then the closure of the zeros of ξ_{η} cannot meet P . Put $G = \varphi_1^*(\xi) / (c^{-1} \varphi_2^*(\xi)) \in R(Y)$. Then $\text{ord}_H(G) = 0$ and $\omega = G_H \cdot \xi_{X_s}^{-1}$, so that $\text{ord}_P \omega = \text{ord}_P(G_H)$. Now, since φ_1, φ_2 are unramified on Y_{η} , the zeros of G_{η} must lie on the zeros of ξ_{η} ; hence the closure of each zero of G_{η} cannot meet P . By the same reason, the poles of G_{η} must lie on the zeros of ξ_{η} . But since φ_2 maps P to its conjugate cP , and since the closure of the zeros of ξ_{η} cannot meet cP , the closure of each pole of

G_η cannot meet P . Therefore, if Γ is any prime divisor of Y passing through P and $\Gamma \neq \Pi, \Pi'$, then $\text{ord}_\Gamma(G) = 0$. On the other hand, by the condition of symmetry (A) (§1.1), we have $\text{ord}_{\Pi'}(G) = \nu + \text{ord}_{\Pi'}(\varphi_1^*(\xi)/\varphi_2^*(\xi)) = \nu + \text{ord}_\Pi(\varphi_2^*(\xi)/\varphi_1^*(\xi)) = 2\nu$.

First, let $P \in \Pi \cap \Pi'$. Then G and G^{-1} belong to the local ring $\Theta_{Y,\Gamma}$ for every prime divisor Γ of Y passing through P . Since Y is normal, this implies $G, G^{-1} \in \Theta_{Y,P}$; hence $\text{ord}_P(G_\Pi) = 0$.

Secondly, let $P \in \Pi \cap \Pi''$. Then P is an F_{q^2} -rational point, and the completion $\hat{\Theta}_{Y,P}$ of $\Theta_{Y,P}$ satisfies the assumptions of Lemma 1. (As Y is proper and hence in particular of finite type over S , $\Theta_{Y,P}$ is a locality over \mathfrak{o} in the sense of Nagata [14]. Since \mathfrak{o} is a discrete valuation ring in characteristic 0, a theorem of Nagata [14] Theorem (37.5) guarantees that the property of $\Theta_{Y,P}$ being normal is invariant under the completion. In particular, $\hat{\Theta}_{Y,P}$ is a domain.) So, by Lemma 1, $\hat{\Theta}_{Y,P}$ is isomorphic over $\hat{\mathfrak{o}}$ with $\hat{\mathfrak{o}}[[x, y]]/(xy - \pi^n)$ for some positive integer $n = n_P$, where $\hat{\mathfrak{o}}$ is the completion of \mathfrak{o} . Since $\text{ord}_{\Pi'}(G) = 2\nu$ and $\text{ord}_\Gamma(G) = 0$ for all $\Gamma \neq \Pi, \Pi'$, we obtain by Lemma 3 that $\text{ord}_P(G_\Pi) = 2\nu/n_P$. Write $n_P = n_i$ when P corresponds to S_i . Then, by what we have shown,

$$(6) \quad (\omega) = \prod_{i=1}^H (S_i)^{2\nu/n_i}.$$

But $\nu > 0$ (Proposition 1) and ω cannot have a simple zero (Proposition 2); therefore, $\nu \geq n_i$. On the other hand, since $\deg(\omega) = (q-1)(2g-2) = 2H$, we obtain immediately from (6) that $2H = \sum_{i=1}^H (2\nu/n_i)$. Therefore, $n_1 = n_2 = \dots = n_H = \nu$, and

$$(\omega) = \left(\prod_{i=1}^H S_i \right)^2.$$

This completes the proofs of Theorems 2, 3.

3.4 Remarks for the general case⁷⁾. Let $\{X \xleftarrow{\varphi_1} Y \xrightarrow{\varphi_2} X\}$ be a congruence relation, *not assumed to be unramified*. Let P_1, \dots, P_H be the intersections of Π and Π' on Y . Then at each P_i , Y is formally isomorphic over S to the affine plane defined by $xy = \pi^{n_i}$ for some unique positive integer n_i (Lemmas 1, 2). What we can say in general about n_i is the following:

PROPOSITION 3. $n_i \geq \nu \quad (i=1, \dots, H).$

PROOF. Put $P = P_i$, $n = n_i$, and let S (resp. $\mathfrak{o}(S)$) be the projection of P to X (resp. $\mathfrak{o}(X)$). Let $\mathfrak{m}_{X,S}$ be the maximal ideal of the local ring $\Theta_{X,S}$. Then $\mathfrak{m}_{X,S} = (\pi, t)$ for some $t \in \mathfrak{m}_{X,S}$. Put $t_1 = \varphi_1^*(t)$, $t_2 = \varphi_2^*(t)$, so that $t_1, t_2 \in \Theta_{Y,P}$ and the maximal

⁷⁾ §3.4 was added in September 24, 1974.

ideal $\mathfrak{m}_{Y,P}$ of $\Theta_{Y,P}$ is generated by π, t_1, t_2 . If $w \in \Theta_{Y,P}$, then dw is of the form $Adt_1 + Bdt_2$ ($A, B \in \Theta_{Y,P}$), since the corresponding fact holds on $X \times_S X$. Put

$$(7) \quad (t_2 - t_1^q)(t_1 - t_2^q) = \pi w \quad (w \in \Theta_{Y,P}),$$

$dw = Adt_1 + Bdt_2$ ($A, B \in \Theta_{Y,P}$), and $z = dt_2/dt_1$, so that $\nu = \text{ord}_H z$. Differentiating (7) we obtain

$$z = u^{-1}\{t_1^q - t_2 + \pi v\},$$

with

$$u = (t_1 - t_2^q) - \pi B - qt_2^{q-1}(t_2 - t_1^q),$$

$$v = A + q\pi^{-1}t_1^{q-1}(t_1 - t_2^q).$$

Since $\text{ord}_H u = 0$, $\nu = \text{ord}_H \{t_1^q - t_2 + \pi v\}$. But π and $t_1^q - t_2 + \pi v$ generate the prime ideal of $\Theta_{Y,P}$ corresponding to H . (Here, note that the restriction to H' of $t_1^q - t_2$ is the same as that of $t_2^{q^2} - t_2$; hence it is of order one at P .) Therefore, Lemma 2 (iii) gives $\nu \leq n$. Q.E.D.

REMARK. At the last stage in the proof of Theorems 2, 3, we used an unnecessary "global argument"; in fact, we made use of the equality $\deg(\omega) = 2H$, which can be substituted by the direct use of Proposition 3.

Also, it is clear by the proof of Theorems 2, 3 and by Proposition 3, that $n_i = \nu$ holds as long as φ_1 and φ_2 are unramified at every generisation of P on Y_τ . Under the same circumstance, for each $P \in H$ (considered also as a point of X_s), the order of ω at P is equal to 0 (resp. 2), if $P \notin H'$ (resp. $P \in H'$) and if φ_1, φ_2 are unramified at every generisation of P on Y_τ .

4. Connection with the Schwarzian differential equations.

This section is based on my previous paper [9]. The definitions and the basic properties of the Schwarzian derivative $\langle \eta, \xi \rangle$, the canonical S -operator $\xi \rightarrow \langle \xi, d\tau \rangle$, etc., are given in [9], and will not be repeated here.

For the system $\{X \xleftarrow{\varphi_1} Y \xrightarrow{\varphi_2} X\}$, we shall only assume the weak almost unramified congruence relation and that it belongs to the general type (cf. §1.3). But we shall impose the following (harmless) restriction on k that its transcendence degree over the prime field is at most \aleph -infinity⁸⁾, so that there is an embedding $k \subset \mathbb{C}$ of k into the complex number field \mathbb{C} . Such an embedding is fixed once and for all.

⁸⁾ This condition is not essentially necessary, as the study of [9] Theorem B shows.

By Z , we shall denote any one of the three S -schemes X , tX and Y .

4.1. For $Z=X$, tX or Y , put $Z_c = Z \otimes_{\mathcal{O}} \mathcal{C}$. Then Z_c can be regarded as a compact Riemann surface. The corresponding base-changes for φ_i ($i=1,2$) will be denoted by φ_{ic} . By our assumptions, we have $R(X)R({}^tX)=R(Y)$, $R(X) \cap R({}^tX)=k$, and $R(Y)$ and \mathcal{C} (as subfields of $R(Y_c)$) are linearly disjoint over k . Therefore, (a) $R(X_c)R({}^tX_c)=R(Y_c)$, and (b) $R(X_c) \cap R({}^tX_c)=\mathcal{C}$. A point P_c of Z_c is called a cusp of Z_c if $e(P)=\infty$ for the point $P \in Z$ lying below P_c , where $e(P)$ is the ramification index of P in $M/R(Z)$ (see § 1.3). Let \mathcal{H} be the complex upper half plane; $\mathcal{H}=\{\tau \in \mathcal{C} \mid \Im \tau > 0\}$. By the almost unramifiedness condition (AU) (§ 1.3), there is a normal covering $u_Y: \mathcal{H} \rightarrow Y_c$, unique up to automorphisms of \mathcal{H} , having the same ramifications as $M/R(Y)$. (The image of u_Y is the complement of the cusps of Y_c .) The composites $\varphi_{ic} \circ u_Y$ ($i=1,2$) are also the normal coverings of X_c , tX_c having the same ramifications as $M/R(X)$, $M/R({}^tX)$, respectively. Let Δ , ${}^t\Delta$ and Δ^0 be the covering groups of $\varphi_{1c} \circ u_Y$, $\varphi_{2c} \circ u_Y$ and u_Y , respectively. Then X_c , tX_c and Y_c can be considered as the compactified quotients of \mathcal{H} by Δ , ${}^t\Delta$ and Δ^0 , respectively. The above properties (a) (b) for the function fields of X_c , tX_c and Y_c imply that (a)' $\Delta \cap {}^t\Delta = \Delta^0$, and that (b)' Δ and ${}^t\Delta$ generate a dense subgroup of the full automorphism group of \mathcal{H} .

Let S_c^Z be the canonical S -operator of Z_c with respect to the above uniformization ($\varphi_{1c} \circ u_Y$, $\varphi_{2c} \circ u_Y$ or u_Y , according to $Z=X$, tX or Y , respectively). They are compatible, i.e., S_c^Y is the lifting of S_c^X , and of S_c^{tX} . Moreover, by Theorem A (§ 3.1) of [9], each S_c^Z is k -rational, i.e., there exists a (unique) S -operator S^Z of Z_η which lifts to S_c^Z . (The key point in this proof is the above property (b)' for the covering groups.) Obviously, S^Y is then the lifting of S^X and of S^{tX} , but we also know that S^Y is the unique S -operator of Y_η which is at the same time the lifting of an S -operator of X_η and that of ${}^tX_\eta$ ([9]; Cor. of Lemma A, § 4.1). In particular, S^Y , S^X , S^{tX} are independent of the choice of an embedding $k \subset \mathcal{C}$.

PROPOSITION 4. $(S^X \langle \xi \rangle) = S^{tX} \langle {}^t\xi \rangle$ ($\xi \in D(X/S)$, $\xi \neq 0$).

PROOF. The proof is based on the notions of [9] § 2.3. Let M^* be the maximum algebraic extension of M in which all discrete valuations of M/k are unramified. It contains the algebraic closure \bar{k} of k . For $Z=X$, tX or Y , $M^*/R(Z)$ can be characterized as the maximum algebraic extension of $R(Z)$ having the same ramifications as $M/R(Z)$. Therefore, $M^*/R(Z)$ (and hence also $M^*/R(\bar{Z})$, where $\bar{Z}=Z \otimes_{\mathcal{O}} \bar{k}$) are normal extensions. Moreover, since $e(P)=e({}^tP)$ holds for the corresponding closed points P , tP of X_η , ${}^tX_\eta$ (the condition (AU), § 1.3), the ι -conjugation

$R(X) \xrightarrow{\sim} R({}^tX)$ can be extended to an automorphism I of M^* . (Since I extends the ι -conjugation of k , I acts non-trivially on \bar{k} . But I commutes with the differentiation; i.e., ${}^t(dg/df) = d({}^t g)/d({}^t f)$ holds for any $f, g \in M^*$ with $f \notin \bar{k}$.) Let G be the automorphism group of M^* over \bar{k} , equipped with the usual topology (cf. e.g. [9] §2.3). Then since $M^*/R(\bar{X}), M^*/R({}^t\bar{X})$ are normal and $R(\bar{X}) \cap R({}^t\bar{X}) = \bar{k}$, the open subgroup Φ of G generated by the Galois groups of $M^*/R(\bar{X}), M^*/R({}^t\bar{X})$ is *non-compact*. Therefore, G is non-compact, and M^*/\bar{k} is an *ample* generalized algebraic function field of one variable in the sense of [9] §2.3. Therefore, by Theorem B [9] §3.2, there is a unique G -invariant S -operator of M^*/\bar{k} , and it is uniquely characterized by the Φ' -invariance, for any open non-compact subgroup Φ' of G . Now let S be the S -operator of M^*/\bar{k} that extends S^Y . Then since S^Y extends both S^X and $S^{X'}$, S is Φ -invariant. On the other hand, since I commutes with the differentiation, the equality ${}^t(S'\langle\xi\rangle) = S'\langle{}^t\xi\rangle$ defines another S -operator S' of M^*/\bar{k} . Since S is Φ -invariant, S' is invariant by the I -conjugate of Φ which is also an open non-compact subgroup of G . Therefore, by the above quoted theorem, both S and S' are the G -invariant S -operator of M^*/\bar{k} . Therefore, $S' = S$, which proves the desired equality. Q.E.D.

4.2. We shall identify the differentials on Z/S and their restrictions to the general fiber Z_η/k . An S -operator on Z_η/k is also called an S -operator on Z/S .

PROPOSITION 5. Let Z_s^0 be an irreducible component of Z_s with multiplicity one, and let ξ, ζ be any elements $\neq 0$ of $D(Z/S)$. Then $\langle\xi, \zeta\rangle$ is finite at the generic point of Z_s^0 .

PROOF. Since $\langle\xi, \zeta\rangle = \langle a\xi, b\zeta\rangle$ for any $a, b \in k^\times$, and since Z_s^0 is of multiplicity one in Z_s , we may assume that ξ and ζ are neither zero nor infinite at the generic point of Z_s^0 . But then, $w_1 = \xi/\zeta$, w_1^{-1} , and $w_{i+1} = dw_i/\zeta$ ($i \geq 1$) are all finite at the generic point of Z_s^0 . Therefore,

$$\langle\xi, \zeta\rangle = \frac{2w_1w_3 - 3w_2^2}{w_1^2} \cdot \zeta^2$$

is finite there, too. Q.E.D.

An S -operator S on X/S is called π -integral if $S\langle\xi\rangle_{x_s} \neq \infty$. This definition is independent of the choice of the differential ξ ($\neq 0$) of X/S , since $S\langle\xi\rangle - S\langle\zeta\rangle = \langle\xi, \zeta\rangle$ and $\langle\xi, \zeta\rangle_{x_s} \neq \infty$, by the above proposition. If S is π -integral, and $\xi, \zeta \in D(X/S)$ are such that $\xi_{x_s} = \zeta_{x_s} \neq 0, \infty$, then $S\langle\xi\rangle_{x_s} = S\langle\zeta\rangle_{x_s}$; in fact, $(S\langle\xi\rangle - S\langle\zeta\rangle)_{x_s} = \langle\xi, \zeta\rangle_{x_s} = \langle\xi_{x_s}, \zeta_{x_s}\rangle = 0$. Therefore, each π -integral S -operator S on X/S defines an S -operator

S_* on the special fiber X_*/F_q , by $S_*\langle\xi_{X_*}\rangle = S\langle\xi\rangle_{X_*}$. We shall call S_* the reduction of S (modulo π).

If $W_* \rightarrow X_*$ is any finite separable covering of X_* , each S -operator S_* on X_* can be uniquely lifted to an S -operator on W_* , for which we shall use the same symbol, S_* .

THEOREM 4. (i) *The S -operator S^X is π -integral, and its reduction S_*^X is an inner S -operator with respect to ω_1 , a $(q-1)$ -th root of ω on a finite separable covering of X_* :*

$$S_*^X\langle\omega_1\rangle = 0.$$

(ii) *Conversely, when $q=p$ and p is a prime element of \mathfrak{o} , a differential ω_1 of degree one on a finite separable covering of X_* satisfying the two equalities $S_*^X\langle\omega_1\rangle = 0$ and $\gamma\omega_1 = \omega_1$ (cf. Theorem 1) is unique up to F_p^\times -multiples, and thus ω is characterized uniquely by these two equalities for its $(p-1)$ -th root ω_1 .*

PROOF. (i) Let ξ be any element of $D(X/S)$ with $\xi_{X_*} \neq 0, \infty$, and put $S^X\langle\xi\rangle = F \cdot \xi^2$ ($F \in R(X)$). We have

$$S^Y\langle\varphi_1^*(\xi)\rangle - S^Y\langle\varphi_2^*(\xi)\rangle = \langle\varphi_1^*(\xi), \varphi_2^*(\xi)\rangle,$$

so that

$$(1) \quad \left(1 - \frac{\varphi_2^*(F \cdot \xi^2)}{\varphi_1^*(F \cdot \xi^2)}\right) \varphi_1^*(F \cdot \xi^2) = \langle\varphi_1^*(\xi), \varphi_2^*(\xi)\rangle,$$

in view of Proposition 4. Now since $\nu \geq 1$ (Proposition 1), $\varphi_2^*(\xi)/\varphi_1^*(\xi)$ is identically zero on Π ; hence the first factor on the left side of (1) is a Π -adic unit. On the other hand, by Proposition 5, the right side of (1) is finite at the generic point of Π . Therefore, $\varphi_1^*(F \cdot \xi^2)$ is finite at the generic point of Π ; therefore, $S^X\langle\xi\rangle$ is also finite there. Therefore, S^X is π -integral.

To prove that $S_*^X\langle\omega_1\rangle = 0$, let c be as in §2, take an element $f \in \mathcal{O}_{X, X_*}$ such that $R(X_*)/F_q(F_{X_*})$ is finite separable, put $f_1 = \varphi_1^*(f)$, $f_2 = \varphi_2^*(f)$, and let ζ be the restriction of $c^{-1} \cdot df_2$ to Π , considered as a differential on X_* . Then

$$\omega_1 = ((df_1)_{X_*}/\zeta)^{q/(q-1)} \cdot \zeta.$$

Since the p -th power elements are differential-constants in characteristic p , it suffices to prove that $S_*^X\langle\zeta\rangle = 0$. But $S_*^X\langle\zeta\rangle = S^Y\langle c^{-1} \cdot df_2 \rangle_\Pi$ (In fact, if η is any differential on X with $\eta_{X_*} = \zeta$, then $\varphi_1^*(\eta)_\Pi = (c^{-1} df_2)_\Pi$; hence $S_*^X\langle\zeta\rangle = S^X\langle\eta\rangle_{X_*} = S^Y(\varphi_1^*(\eta))_\Pi = S^Y\langle c^{-1} df_2 \rangle_\Pi$). So, it suffices to prove $S^Y\langle c^{-1} df_2 \rangle_\Pi = 0$. But $S^Y\langle c^{-1} df_2 \rangle = S^Y\langle df_2 \rangle =$

$\varphi_2^*(\rho)$ with $\rho = S^X \langle df \rangle$. Since S^X is π -integral and $\nu \geq 1$, it follows immediately that $S^Y \langle c^{-1} df_2 \rangle_{\Pi} = 0$. Therefore, $S_*^X \langle \omega_1 \rangle = 0$.

(ii) Suppose that a differential ω_1^* on some finite separable covering of X , satisfies the two equations $S_*^X \langle \omega_1^* \rangle = 0$ and $\gamma \omega_1^* = \omega_1^*$. Then $\langle \omega_1, \omega_1^* \rangle = 0$, and ω_1^* is non-exact. Therefore, by Proposition 2 of [9], ω_1^*/ω_1 is a p -th power of some rational function A on some finite separable covering of X_s ; $\omega_1^* = A^p \omega_1$. But since $\gamma(A^p \omega_1) = A \cdot \gamma(\omega_1) = A \cdot \omega_1$, this implies $A^{p-1} = 1$. Q.E.D.

4.3. Suppose that $q = p$ and p is a prime element of \mathfrak{o} . Then ω is uniquely characterized by the two equations $S_*^X \langle \omega_1 \rangle = 0$ and $\gamma \omega_1 = \omega_1$ for its $(p-1)$ -th root ω_1 (Th. 4(ii)). This gives an effective method for calculating the explicit formula for ω , provided that S^X is calculable. Unfortunately, as far as we know, the canonical S -operator is calculable only when the corresponding fuchsian group is commensurable with a triangular group.

We shall carry out the calculation under the following assumptions (a)~(d):

- (a) $q = p \neq 2$, and p is a prime element of \mathfrak{o} ;
- (b) $X = \text{Spec } \mathfrak{o}[t] \cup \text{Spec } \mathfrak{o}[t^{-1}]$ (t : a variable);
- (c) Δ is a triangular group, with three points of ramifications at $t=0, 1, \infty$.

Let e_0, e_1, e_∞ be the ramification indices at $t=0, 1, \infty$, of the covering $\varphi_{1C} \circ u_Y: \mathcal{H} \rightarrow X_C$, so that $2 \leq e_i \leq \infty$ and $\sum e_i^{-1} < 1$.

- (d) For each $i=0, 1, \infty$, there exists $\varepsilon_i = \pm 1$ such that

$$p \equiv \varepsilon_i \pmod{e_i}, \quad \sum \frac{p - \varepsilon_i}{e_i} \equiv 0 \pmod{2}.$$

Put

$$g_i = \frac{p - \varepsilon_i}{e_i}, \quad \delta_i = \frac{1}{2}(p - 1 - g_i) \quad (i=0, 1, \infty),$$

and

$$A^* = \frac{1}{2}(1 + p + g_0 + g_1 + g_\infty), \quad B^* = \frac{1}{2}(1 + p + g_0 + g_1 - g_\infty), \quad C^* = 1 + g_0.$$

Then each g_i is a non-negative integer ($g_i=0$ if and only if $e_i=\infty$), and A^*, B^*, C^* are positive integers. Moreover, it holds that

$$(2) \quad 1 \leq C^* \leq B^* \leq A^* \leq p, \quad \frac{1}{2}(p+1) \leq A^*.$$

In fact, $p - A^* + 1 = \frac{1}{2}(p+1 - g_0 - g_1 - g_\infty)$ is positive by $\sum e_i^{-1} < 1$, and is an integer,

⁹⁾ This congruence should be neglected when $e_i = \infty$.

so that $p \geq A^*$. In the same manner, we obtain $B^* \geq C^*$. The rest of (2) is obvious. Put

$$u(t) = f(A^*, B^*; C^*; t) = 1 + \frac{A^* \cdot B^*}{1 \cdot C^*} t + \frac{A^*(A^*+1)B^*(B^*+1)}{1 \cdot 2 \cdot C^*(C^*+1)} t^2 + \dots,$$

a finite hypergeometric series of degree $p - A^*$ (as a polynomial of t) and in characteristic p . It satisfies the Gaussian differential equation:

$$(3) \quad t(1-t) \frac{d^2 u}{dt^2} + (C^* - (A^* + B^* + 1)t) \frac{du}{dt} - A^* B^* u = 0; \quad (\text{in characteristic } p).$$

Since $1 \leq C^* \leq B^* \leq A^* \leq p$, the space of solutions of (3) in the separable closure \mathcal{L} of $F_p(t)$ is one-dimensional over \mathcal{L}^p ([9] § 1.6). If we put $C'' = A^* + B^* + 1 - C^* - p = 1 + g_1$, then $1 \leq C'' \leq B^* \leq A^* \leq p$, and replacing C^* by C'' in (3) gives an equation for $u(1-t)$. Therefore, $u(1-t)$ is an $\mathcal{L}^{\times p}$ -multiple of $f(A^*, B^*; C''; t)$, but since $u(1-t)$ and $f(A^*, B^*; C''; t)$ are polynomials over F_p of degree $p - A^* < p$, we conclude that $u(1-t)$ is an F_p^{\times} -multiple of $f(A^*, B^*; C''; t)$. In particular, $u(0)u(1) \neq 0$. Moreover, $u(t)$ has no multiple roots. This follows exactly in the same manner as in Igusa [5] (which was for the case of $A^* = B^* = \frac{1}{2}(p-1)$, $C^* = 1$). Namely, if $u(t)$ had a multiple root λ , then $u(\lambda) = \frac{du}{dt}(\lambda) = 0$; hence $\frac{d^2 u}{dt^2}(\lambda) = 0$ by (3) (since $\lambda \neq 0, 1$). By differentiating (3), we obtain successively $\frac{d^3 u}{dt^3}(\lambda) = \dots = 0$, which is a contradiction since $u(t)$ is a non-zero polynomial of a degree less than p .

THEOREM 5. Under the assumptions (a)~(d), we have

$$\omega = c_0 \cdot \frac{u(t)^2}{t^{2\delta_0}(1-t)^{2\delta_1}} (dt)^{p-1};$$

where c_0 is an element of F_p^{\times} given by the coefficient of t^{p-1} in the polynomial $t^{2\delta_0}(1-t)^{2\delta_1}u(t)^{p-2}$.

PROOF. The classical formula for the canonical S -operator with respect to the triangular groups (cf. e.g. [9] § 2.4) gives

$$S^X \langle \xi \rangle = \langle \xi, dt \rangle + \frac{at^2 + bt + c}{t^2(1-t)^2} (dt)^2; \quad (\xi \in D(X/S), \xi \neq 0),$$

where a, b, c are rational numbers defined by

$$a+1 = e_{\infty}^{-2}, \quad a+b+c+1 = e_1^{-2}, \quad c+1 = e_0^{-2}.$$

Therefore, by Theorem 4(ii), ω_1 is characterized (up to F_p^{\times} -multiples) by the two

equations

$$(4) \quad \langle \omega_1, dt \rangle = -\frac{at^2+bt+c}{t^2(1-t)^2}(dt)^2; \quad (\text{in characteristic } p),$$

and $\gamma\omega_1 = \omega_1$. Put

$$v(t) = t^{-\delta_0}(1-t)^{-\delta_1}u(t), \quad \omega'_1 = v(t)^{-2}dt.$$

Then since $u(t)$ satisfies (3), $v(t)$ satisfies

$$\frac{d^2v}{dt^2} = \frac{1}{4} \cdot \frac{at^2+bt+c}{t^2(1-t)^2} \cdot v.$$

Therefore, (4) is valid when ω_1 is replaced by ω'_1 . (In fact, define $\rho_i \in F_p$ by $\rho_i \equiv \varepsilon_i e_i^{-1} \pmod{p}$. Then, we have the following congruences mod p ;

$$g_i \equiv -\rho_i, \quad \delta_i \equiv \frac{1}{2}(\rho_i - 1); \quad a+1 \equiv \rho_\infty^2, \quad a+b+c+1 \equiv \rho_1^2, \quad c+1 \equiv \rho_0^2,$$

and

$$A^* \equiv \frac{1}{2}(1-\rho_0-\rho_1-\rho_\infty), \quad B^* \equiv \frac{1}{2}(1-\rho_0-\rho_1+\rho_\infty), \quad C^* \equiv 1-\rho_0.$$

Therefore, the calculation of [9] §1.6 is applicable.)

We claim now that

$$(5) \quad \gamma(v(t)^{-2}dt) = c'_0 dt$$

with some constant $c'_0 \in F_p$. To check this, put $y(t) = u(t)^p v(t)^{-2} = t^{2\delta_0}(1-t)^{2\delta_1}u(t)^{p-2}$, and $H^* = \deg u(t) = p - A^*$. Then $y(t)$ is a polynomial of degree $p(H^*+1) + g_\infty - 1$, which is strictly smaller than $p(H^*+2) - 1$. Therefore, $\gamma(y(t)dt) = z(t)dt$ with some polynomial $z(t)$ of degree at most H^* . But since $\gamma(v(t)^{-2}dt) = u(t)^{-1}z(t)dt$, it suffices to show that $z(t)$ is divisible by $u(t)$. So, it suffices to show that $\gamma(v(t)^{-2}dt)$ has no poles at the roots λ of $u(t)$. Let λ be a root of $u(t)$. Since it is a simple root, the pole of $v(t)^{-2}dt$ at λ is of order 2. So, it is enough to show that the residue of $v(t)^{-2}dt$ at λ is zero, or equivalently, that

$$\frac{d \log}{dt} \{t^{2\delta_0}(1-t)^{2\delta_1}u(t)^{-2}(t-\lambda)^2\}_{t=\lambda} = 0.$$

This is equivalent to

$$\delta_0\lambda^{-1} + \delta_1(\lambda-1)^{-1} - \sum_{\mu \neq \lambda} (\lambda-\mu)^{-1} = 0,$$

where μ runs over all roots $\neq \lambda$ of $u(t)$. But

$$\sum_{\mu \neq \lambda} (\lambda - \mu)^{-1} = a_2/a_1,$$

where $u(t + \lambda) = a_1 t + a_2 t^2 + \dots$; hence $a_1 = \frac{du}{dt}(\lambda)$, $a_2 = \frac{1}{2} \cdot \frac{d^2 u}{dt^2}(\lambda)$. But by (3), we obtain

$$\lambda(1 - \lambda) \frac{\frac{d^2 u}{dt^2}(\lambda)}{\frac{du}{dt}(\lambda)} + (C^* - (A^* + B^* + 1)\lambda) = 0;$$

whence

$$\begin{aligned} \sum_{\mu \neq \lambda} (\lambda - \mu)^{-1} &= - \frac{(A^* + B^* + 1)\lambda - C^*}{2\lambda(\lambda - 1)} \\ &= \delta_0 \lambda^{-1} + \delta_1 (\lambda - 1)^{-1}. \end{aligned}$$

This settles (5).

Now since $z(0) = c_0$ and $u(0) = 1$, we obtain $c'_0 = c_0$. On the other hand, since $1 \leq C^* \leq B^* \leq A^* \leq p$, $v(t)^{-2} dt$ is non-exact [9] (§ 1.5. Cor. of Prop. 4, and § 1.6). Therefore, $c_0 \neq 0$. Now put

$$\omega_1^* = c_0^{p/(p-1)} v(t)^{2/(p-1)} dt = (c_0^{1/(p-1)} v(t)^{2/(p-1)})^p \cdot \omega_1'.$$

Then by the second equality, ω_1^* also satisfies (4); and by (5), ω_1^* is invariant by γ . Therefore, $\omega_1 = \omega_1^*$ (up to F_p^\times -multiples). Therefore, $\omega = c_0^p v(t)^2 (dt)^{p-1} = c_0 v(t)^2 (dt)^{p-1}$.

Q.E.D.

In the elliptic modular case [8], ω can be calculated by putting $\{e_0, e_1, e_\infty\} = \{3, 2, \infty\}$ in Theorem 5 for $p \neq 2, 3$, and individually using Theorem 4(ii) for $p = 2, 3$. The differentials $\omega_1^{(p-1)/2}$ (for $p \neq 2$) and ω_1 (for $p = 2$) coincide (up to the signs for $p \neq 2$) with the differentials given in [6]. Other similar examples, e.g., for $\{e_0, e_1, e_\infty\} = \{3, 2, 7\}, \{3, 2, 10\}$ based on the Shimura congruence relations [20] (but not for all p), can be calculated directly from Theorem 5.

Bibliography

- [1] Deligne, P. and D. Mumford, The irreducibility of the space of curves of given genus, Publ. I.H.E.S. 36, 1969.
- [2a] Deligne, P., Formes modulaires et représentations l -adiques, Sémin. Bourbaki 21^e ann. n° 355, 1969.
- [2b] Deligne, P. and M. Rapoport, Les schémas de modules de courbes elliptiques, Modular functions of one variable II, Proc. Intern. Summer School, Univ. Antwerp, 1972, Springer Lecture Note No. 349, pp. 143-316.
- [3] Dwork, B., " p -adic cycles", Publ. I.H.E.S. 37, 1969.
- [4] Grothendieck, A., et J. Dieudonné, "Éléments de géométrie algébrique I-IV".
- [5] Igusa, J., Class number of a definite quaternion with prime discriminant, Proc. Nat.

- Acad. Sci. U.S.A. **44** (1958), 312-314.
- [6] Ihara, Y., An invariant multiple differential attached to the field of elliptic modular functions of characteristic p , Amer. J. Math. **93** (1971), 139-147.
 - [7] Ihara, Y., (a) Modular transforms of p -power degrees and induced multiple differentials of characteristic p (mimeographed note, 1970).
 (b) Non-abelian invariant differentials (mimeographed note, 1971).
 (c) Non-abelian invariant differentials and Schwarzian equations in the p -adic theory of automorphic functions, Proc. U.S.-Japan Seminar in "Modern Methods in Number Theory", 1971 (Available at Univ. Tokyo).
 - [8] Ihara, Y., On modular curves over finite fields, to appear in the Proc. Intern. Colloq. on Discrete Subgroups of Lie Groups (held in Bombay in Jan. 1973).
 - [9] Ihara, Y., Schwarzian equations, J. Fac. Sci. Univ. Tokyo, Sec. IA **21-1** (1974), 97-118.
 - [10] Ihara, Y., (a) On the Congruence Monodromy Problems Vol. 1, 2, Lecture Notes, Univ. Tokyo, 1968, 69.
 (b) Non-abelian class fields over function fields in special cases, Actes, Congrès intern. math., Nice, 1970, Tome I, pp. 381-389.
 - [11] Katz, N., p -adic properties of modular schemes and modular forms, Modular functions of one variable III, Proc. Intern. Summer School, Univ. Antwerp, 1972, Springer Lecture Note No. 350, pp. 69-190.
 - [12] Koike, M., Congruences between modular forms and functions, and applications to the conjecture of Atkin, J. Fac. Sci. Univ. Tokyo, Sec. IA, **20** (1973), 129-169.
 - [13] Lamprecht, E., Restabbildungen von Divisoren I, II, Archiv. Math. **8** (1957), 255-264, ibid. **10** (1959), 428-437.
 - [14] Nagata, M., Local rings, Interscience, No. 13, 1960.
 - [15] Nering, E. D., Reduction of an algebraic function field modulo a prime in the constant field, Ann. of Math. **67** (1958), 590-606.
 - [16] Popp, H., Über das Verhalten des Geschlechts eines Funktionenkörpers einer Variablen bei Konstantenreduktion, Math. Z. **106** (1968), 17-35.
 - [17] Šafarevich, I. R., Lectures on minimal models and birational transformations of two dimensional schemes, Tata Institute Lecture Notes, Bombay, 1966.
 - [18] Serre, J.-P., Congruences et formes modulaires (d'après H.P.F. Swinnerton-Dyer), Sémin. Bourbaki, 1971/72, exposé 416.
 - [19] Serre, J.-P., Formes modulaires et fonctions zêta p -adiques, Modular functions of one variable III, Proc. Intern. Summer School, Univ. Antwerp, 1972, Springer Lecture Note No. 350, pp. 191-268.
 - [20] Shimura, G., On the zeta functions of the algebraic curves uniformized by certain automorphic functions, J. Math. Soc. Japan, **13** (1961), 275-331.
 - [21] Shimura, G., Construction of class fields and zeta functions of algebraic curves, Ann. of Math. **85** (1967), 58-159.
 - [22] Tate, J., A letter to Prof. Dwork, on the p -adic q -invariant of elliptic curves.

(Received March 11, 1974)

Department of Mathematics
 Faculty of Science
 University of Tokyo
 Hongo, Tokyo
 113 Japan