Hokkaido Mathematical Journal Vol. 10 (1981) p. 209-238

Reduction modulo $\mathfrak{P}$ of Shimura curves

By Yasuo MORITA

(Received May 21, 1980)

0-1. Let F be a totally real algebraic number field of finite degree g, and let B be a division quaternion algebra over F such that $B\otimes_{\boldsymbol{Q}}\boldsymbol{R}$ is isomorphic to the product of $M_2(\boldsymbol{R})$ and $g-1$ copies of the division quaternion algebra $\boldsymbol{H}$ over $\boldsymbol{R}$. Let G be the algebraic F-group satisfying $G_F=B^{\times}$, let G_A be the adelization of G, and let G_{A+} be the subgroup of G_A consisting of all elements whose projections to $M_2(\boldsymbol{R})$ have positive determinants. Let $G_{\infty+}$ and G_0 be the archimedean part and the finite part of G_{A+}, let $G_{\boldsymbol{Q}+}=G_{A+}\cap G_F$, and let $\mathcal{Z}$ be the family consisting of all subgroups S of G_{A+} such that S has the form $S=G_{\infty+}\cdot S_0$ with an open compact subgroup S_0 of G_0.

For each $S\in\mathcal{Z}$, let $\Gamma_S=S\cap G_{\boldsymbol{Q}+}$, and we regard Γ_S as a subgroup of $GL(2,\boldsymbol{R})$. Then Γ_S acts on the complex upper half plane $\mathfrak{H}$ in the usual way, and $\Gamma_S\backslash\mathfrak{H}$ is a complete non-singular curve. Let ν be the reduced norm of B, and let k_S be the abelian extension of F corresponding to the subgroup $\nu(S)\cdot F^{\times}$ of $F_A^{\times}$ by class field theory. Then Shimura constructed an algebraic curve V_S defined over k_S and a holomorphic map φ_S of $\mathfrak{H}$ onto V_S inducing $\Gamma_S\backslash\mathfrak{H}\cong V_S$, satisfying certain algebraic and arithmetic conditions (cf. 1-1).

Let p be a prime number, and let $\mathfrak{P}$ be an extension of p to a place of $\bar{\boldsymbol{Q}}$. Then we shall show that *V_S has good reduction at $\mathfrak{P}$ if* (i) *$\mathfrak{P}$ does not divide the discriminant $D(B/F)$ of B and* (ii) *the "level" of S is prime to p.* (For the exact statement, see Main Theorem 1 in 1-2.) Furthermore, as was conjectured in Shimura [24], 2. 9, we shall *construct a system of curves over finite fields* satisfying several conditions (see Main Theorem 3).

0-2. The exact statements of our main results are in § 1. The proof starts in § 2 and ends in § 3.

In 1-1, we quote the result of Shimura [24] in our case. In 1-2, the main results are stated. In 1-3, a summary of the proof of Shimura's result is given. In 2-1, we quote from Mumford [14] the existence of the fine moduli scheme for polarized abelian schemes with level structures. In 2-2 and 2-3, we construct moduli spaces for families of PEL-sturctures by making use of Mumford's moduli (cf. Theorem 1 in 2–3).

Let $S\in\mathcal{Z}$, $\mathfrak{P}$ and p be as in 0–1. Then we can construct a discrete subgroup $\Gamma_{S_\mathfrak{p}}(\mathfrak{p}=\mathfrak{P}\cap F)$ of $PSL(2, \boldsymbol{R})\times PGL(2, F_\mathfrak{p})$ as in Ihara [8]. Hence, by the result of Ihara [8], we have the zeta function $Z(\Gamma_{S_\mathfrak{p}}; u)$ for the group $\Gamma_{S_\mathfrak{p}}$. In 3–1, we calculate $Z(\Gamma_{S_\mathfrak{p}}; u)$ in the terminology of isolated fixed points (cf. Proposition 1).

Now we assume that S is a congruence subgroup of the form $S(b, c)$ (cf. 1–3) such that c is prime to p. Then, as in Shimura [24], we can construct families of PEL-structures parametrized by $V_{T(x)}(x\in G_{A+}, T(x)= x^{-1}S(b, c)\,x)$. We choose *a finite number of families* $\Sigma(\Omega_i)$ $(i\in I)$ parametrized by $V_i=V_{T(x_i)}$ so that we have a classification of the set consisting of the isomorphism classes of $\tilde{\mathcal{Q}}=\mathcal{Q}$ modulo $\mathfrak{P}$ of elements $\mathcal{Q}$ of $\bigcup_i\Sigma(\Omega_i)$ such that $\tilde{\mathcal{Q}}$ can be defined over $\bar{\boldsymbol{F}}_p$ (cf. [13] and 3–2). Let (S_i, ψ_i) be the moduli for the PEL-type Ω_i constructed in § 2. Then S_i is an irreducible quasi-projective scheme over the integer ring $\mathfrak{r}_c$ of a finite extension K_c of $k_{T(x_i)}$ (cf. 3–2), $\mathfrak{P}$ is *unramified* in K_c/F, and there exists a one-to-one birational morphism of V_i to the generic fibre of S_i.

Let K_c^* be a quadratic extension of K_c such that K_c^* is normal over F and $\mathfrak{P}|K_c$ remains prime in K_c^*/K_c. Let $\tilde{K}_c^*$ be the residue field of $\mathfrak{P}|K_c^*$. Then we calculate in 3–2 the congruence zeta function $Z(u)$ of $\bigcup_i S_i\times_{Spec(\mathfrak{r}_c)} Spec\,(\tilde{K}_c^*)$ by making use of the result of [13] and the result of 3–1, and show that $Z(u)$ *is* $\prod_i Z_i(u)$, *where each* $Z_i(u)$ *has the form of the congruence zeta function of a complete non-singular curve defined over* $\tilde{K}_c^*$ *whose genus is equal to the genus of* V_i (cf. Proposition 2).

Let $\mathfrak{r}_{c\mathfrak{P}}^*$ be the valuation ring of $\mathfrak{P}|K_c^*$, and let $S_i'=S_i\times_{Spec(\mathfrak{r}_c)} Spec\,(\mathfrak{r}_{c\mathfrak{P}}^*)$. Let $\varphi_i: S_i''\to S_i'$ be the normalization of S_i' in the function field at the generic point of S_i'. Then, by making use of Proposition 2, we prove in 3–3 that S_i'' *is smooth projective, there exists an isomorphism* j_i'' *of* V_i *to the general fibre of* S_i'', *and these* S_i'' *and* j_i'' *satisfy the conditions* (ii) *and* (iii) *of Main Theorem* 1 (cf. Proposition 3).

In 3–4, we prove Main Theorem 1 by making use of Proposition 3. In 3–5, we show that Main Theorem 2 follows from Main Theorem 1. In 3–6, by modifying these arguments, we prove Main Theorem 3.

0–3. (1) In 1972, the author proved these results for the case of $F=\boldsymbol{Q}$. In 1974, by a recomendation of G. Shimura, he generalized the results to the present case. But he once gave up the publication of this paper, because he changed his field in 1974. It is due to a strong recommendation of Y. Ihara that he finished writing this paper. So the author would like to thank to Professors G. Shimura and Y. Ihara. He would like to apologize for the delay of the publication.

(2) It seems that there are several methods to prove our main results. For example, it is likely that we can prove the smoothness directly by studying PEL-structures over Artinian rings. But we present here the original proof, because it is one proof and it is an interesting proof, though it is a little complicated.

Notation and terminology

Since we quote often the results of Shimura [24], we use his notation and terminology. Further we use the standard notation and terminology of EGA.

We denote by $\boldsymbol{Z}$, $\boldsymbol{Q}$, $\boldsymbol{R}$, $\boldsymbol{C}$, $\boldsymbol{F}_q$, respectively, the ring of rational integers, the rational number field, the real number field, the complex number field, the finite field with q elements. If F is an algebraic number field of finite degree, we denote by $\mathfrak{r}_F$ the ring of algebraic integers in F, and by $F_A^\times$ the group of ideles of F. Further $F_\infty^\times$ denotes the archimedean part of $F_A^\times$, $F_{\infty+}^\times$ the identity component of $F_\infty^\times$, $F_+^\times$ the subset of $F^\times$ consisting of the elements whose projections to $F_\infty^\times$ belong to $F_{\infty+}^\times$, and F_{ab} the maximal abelian extension of F. For every $u\in F_A^\times$, we denote by $[u, F]$ the element of the Galois group $\mathrm{Gal}(F_{ab}/F)$ canonically associated with u by class field theory. For a positive integer c, we write $u\equiv 1 \bmod_0 (c)$ if, for every non-archimedean prime v of F, the v-component u_v of u is a v-unit, and $(u_v-1)/c$ is a v-integer. For any ideal $\mathfrak{p}$ of $\mathfrak{r}_F$, we denote by $\mathfrak{r}_{F_\mathfrak{p}}$ the $\mathfrak{p}$-adic completion of $\mathfrak{r}_F$, and by $F_\mathfrak{p}$ $\mathfrak{r}_{F_\mathfrak{p}}\otimes_{\boldsymbol{Z}}\boldsymbol{Q}$.

Let V be a vector space over $\boldsymbol{Q}$, and let G be the $\boldsymbol{Q}$-algebraic group $\boldsymbol{GL}(\boldsymbol{V})$. Let $\mathfrak{m}$ be a $\boldsymbol{Z}$-lattice in V, and $x\in G_A$. Put $V_p=V\otimes_{\boldsymbol{Q}}\boldsymbol{Q}_p$, $\mathfrak{m}_p=\mathfrak{m}\otimes_{\boldsymbol{Z}}\boldsymbol{Z}_p$ for every rational prime p. Let x_p be the p-component of x. Then $V/\mathfrak{m}$ is canonically isomorphic to the direct sum of all $V_p/\mathfrak{m}_p$, and the multiplication by x_p defines an isomorphism of $V_p/\mathfrak{m}_p$ to $V_p/\mathfrak{m}_p x_p$. Hence $\mathfrak{m}x=\bigcap_p (V\cap \mathfrak{m}_p x_p)$ is a $\boldsymbol{Z}$-lattice and x defines an isomorphism of $V/\mathfrak{m}$ to $V/\mathfrak{m}x$. Hence, for an element u of $V/\mathfrak{m}$, we denote by ux the corresponding element of $V/\mathfrak{m}x$. If c is a positive integer, we write $x\equiv 1 \bmod_0 (\mathfrak{m}, c)$ if $\mathfrak{m}x=\mathfrak{m}$ and $\mathfrak{m}_p(x_p-1)\subseteqq c\mathfrak{m}_p$ for all p.

§ 1. The main results

1-1. Canonical models of Shimura. Let F be a totally real algebraic number field of degree $g<\infty$, B a *division* quaternion algebra over F, $\mathfrak{o}$

a maximal order of B, and $D(B/F)$ the discriminant of B over F. Let $\tau_{01}, \cdots, \tau_{0g}$ be all isomorphisms of F into $\boldsymbol{R}$. We assume that (i) F is a subfield of $\boldsymbol{R}$; (ii) $\tau_{01}=\mathrm{id}.$ on F; (iii) $B\otimes_F \boldsymbol{R}\cong M_2(\boldsymbol{R})$; (iv) $B\otimes_{F,\tau_{0\nu}}\boldsymbol{R}$ is isomorphic to the division quaternion algebra $\boldsymbol{H}$ over $\boldsymbol{R}$ for each $\nu\geqq 2$, where we construct the tensor product by $\tau_{0\nu}$: $F\to\boldsymbol{R}$.

For any prime v of F, let B_v be the v-adic completion of B. Let G be the F-group satisfying $G_F=B^\times$, and let G_A be the adelization of $B^\times$. Since G_A is a subset of $\prod_v B_v$, any element x of G_A can be written as $x=(x_v)$. Let $v_{\infty\nu}\,(1\leqq\nu\leqq g)$ be the archimedean prime of F corresponding to $\tau_{0\nu}$, and, for any $x\in G_A$, let $x_{\infty\nu}$ be the $v_{\infty\nu}$-component of x. Similarly let G_v be the group of F_v-valued points of G, and let $G_{\infty\nu}=G_{v_{\infty\nu}}$. Let $\nu(x)$ and $\mathrm{tr}\,(x)$ be the reduced norm and the reduced trace of $x\in B$ (or $x\in B_v$, or $x\in B_A$). Let $G_{\infty 1}^+$ be $\{x\in G_{\infty 1}|\nu(x)>0\}$, and let $G_{\infty+}$ (resp. G_{A+}) be $G_{\infty 1}^+\times G_{\infty 2}\times\cdots\times G_{\infty g}$ (resp. $\{x\in G_A|\nu(x_{\infty 1})>0\}$). Put $G_0=\{x\in G_A|\,x_{\infty 1}=\cdots=x_{\infty g}=1\}$ and $G_{Q+}=B^\times\cap G_{A+}$. Then $G_A=G_{\infty+}\cdot G_0$ and $G_{Q+}=\{x\in B|\nu(x)>0\}$.

Let $\mathfrak{H}$ be the complex upper half plane. We fix an isomorphism $B\otimes_F\boldsymbol{R}\cong M_2(\boldsymbol{R})$. Then $G_{\infty 1}^+$ can be identified with the group $GL^+(2,\boldsymbol{R})$. Hence an element γ of G_{Q+} acts on $\mathfrak{H}$ in the natural manner.

Let $\mathcal{Z}$ be the set of all subgroups S of G_{A+} of the form $S=S_0\cdot G_{\infty+}$ with open compact subgroups S_0 of G_0. For each $S\in\mathcal{Z}$, let $\Gamma_S=S\cap G_{Q+}$. Then Γ_S (modulo its center) is a Fuchsian group. Let k_S be the subfield of F_{ab} corresponding to the subgroup $F^\times\cdot\nu(S)$ of $F_A^\times$ by class field theory. For each element x of G_A, let $\sigma(x)$ be the element $[\nu(x)^{-1},F]$ of $\mathrm{Gal}\,(F_{ab}/F)$.

Let M be a totally imaginary quadratic extension of F contained in $\boldsymbol{C}$, and let f be an F-linear isomorphism of M into B. Then $f(M^\times)$ has a unique common fixed point z on $\mathfrak{H}$. We normalize f by

$$\left(\frac{d}{dw}\right)\big[f(a)(w)\big]_{w=z}=\bar{a}/a\qquad\text{for all}\quad a\in M^\times\,,$$

where the bar is the complex conjugation. We call such an embedding f a *normalized embedding*, and denote by (M,f,z) such a triple.

Now the main result of Shimura [24] in this case can be given in the following manner:

THEOREM C. *There exists a system*

$$\big\{V_S,\varphi_S,J_{TS}(x)\,(S,T\in\mathcal{Z}\,;\;x\in G_{A+})\big\}$$

satisfying the following conditions:

(i) *V_S is a projective nonsingular curve defined over k_S.*

(ii) *φ_S is a holomorphic map of $\mathfrak{H}$ to V_S, and induces an isomorphism of $\Gamma_S\backslash\mathfrak{H}$ onto V_S.*

(iii) *$J_{TS}(x)$, defined if $xSx^{-1}\subseteqq T$, is a morphism of V_S onto $V_T^{\sigma(x)}$ rational over k_S, and has the following three properties:*

($\mathrm{iii_a}$) *$J_{SS}(x)$ is the identity map of V_S if $x\in S$;*

($\mathrm{iii_b}$) *$J_{TS}(x)^{\sigma(y)}\circ J_{SR}(y)=J_{TR}(xy)$;*

($\mathrm{iii_c}$) *$J_{TS}(\alpha)[\varphi_S(z)]=\varphi_T(\alpha(z))$ if $\alpha\in G_{Q+}$ and $z\in\mathfrak{H}$.*

(iv) *Let (M,f,z) be a triple consisting of a normalized embedding $f: M\to B$ and the fixed point z of $f(M^\times)$ on $\mathfrak{H}$. Then f induces a homomorphism of $M_A^\times$ into G_{A+}. Let c be an element of $M_A^\times$. Then, for any $S\in\mathcal{Z}$, the point $\varphi_S(z)$ is rational over M_{ab}, and satisfies*

$$\varphi_S(z)^{[c,M]}=J_{ST}\left(f(c)^{-1}\right)\left[\varphi_T(z)\right],$$

where $T=f(c)S\cdot f(c)^{-1}$.

Remark. By Shimura [24], 2.55, (iv) implies that $M\cdot k_S(\varphi_S(z))$ is the class field over M corresponding to the subgroup $\{v\in M_A^\times \mid f(v)\in f(M^\times)\cdot S\}$ of $M_A^\times$.

1-2. The main results. Let S be an element of $\mathcal{Z}$. Let P_S be the set consisting of all ideals $\mathfrak{q}$ of k_S such that (i) $\mathfrak{q}$ does not divide $D(B/F)$ and (ii) there exists $x_{Sp}\in G_{Q+}$ such that S contains $x_{Sp}^{-1}\mathfrak{o}_p^\times x_{Sp}$, where $p=\mathfrak{q}\cap \boldsymbol{Q}$ and $\mathfrak{o}_p$ is the p-adic completion of $\mathfrak{o}$. It is obvious that almost all prime ideals of k_S belong to P_S. Let $\mathfrak{r}_{S_\mathfrak{q}}$ be the valuation ring of $\mathfrak{q}\in P_S$, let $\tilde{k}_{S_\mathfrak{q}}$ be the residue field of $\mathfrak{q}$, and let $\mathfrak{r}_S$ be the intersection of all $\mathfrak{r}_{S_\mathfrak{q}}(\mathfrak{q}\in P_S)$. For each $\mathfrak{q}\in P_S$, let $\mathfrak{p}$ (resp. $\mathfrak{P}$) be the restriction of $\mathfrak{q}$ to F (resp. an extension of $\mathfrak{q}$ to a place of $\bar{\boldsymbol{Q}}$). Let $\mathscr{B}$ be the set consisting of all points z on $\mathfrak{H}$ such that there exist a totally imaginary quadratic extension M of F contained in $\boldsymbol{C}$, and a normalized embedding f of M into B satisfying (a) z is the common fixed point of $f(M^\times)$. Let $\mathscr{C}(\mathfrak{p})$ be the subset of $\mathscr{B}$ satisfying (b) $\mathfrak{p}$ is decomposed in M and (c) f induces an embedding of $\mathfrak{r}_{M_\mathfrak{p}}\cong\mathfrak{r}_{F_\mathfrak{p}}\oplus\mathfrak{r}_{F_\mathfrak{p}}$ into $\mathfrak{o}_\mathfrak{p}$. For given $S\in\mathcal{Z}$ and $\mathfrak{q}\in P_S$, if x_{Sp} and x'_{Sp} satisfy the condition (ii), then $x_{Sp}^{-1}x'_{Sp}\in\mathfrak{o}_\mathfrak{p}^\times$. Hence $x_{Sp}^{-1}\mathscr{C}(\mathfrak{p})$ does not depend on a special choice of x_{Sp}.

The main results of this paper are the following three theorems:

Main Theorem 1. *Let (V_S,φ_S) be as in Theorem C. Then there exist a smooth projective scheme W_S over $Spec(\mathfrak{r}_S)$ and an isomorphism j_S of V_S onto the generic fibre $W_{S0}=W_S\times_{Spec(\mathfrak{r}_S)}Spec(k_S)$ of W_S with the following properties:*

For any $\mathfrak{q}\in P_S$, *let* $\widetilde{W}_{S_\mathfrak{q}}=W_S\times_{Spec(\mathfrak{r}_S)} Spec(\tilde{k}_{S_\mathfrak{q}})$. *Then*

(i) $\widetilde{W}_{S_\mathfrak{q}}$ *is an absolutely irreducible projective nonsingular curve defined over* $\tilde{k}_{S_\mathfrak{q}}$.

(ii) *Reduction* modulo $\mathfrak{P}$ *induces a surjection of* $(j_S\circ\varphi_S)(\mathscr{B})$ *to the set* $\mathscr{I}(\widetilde{W}_{S_\mathfrak{q}})$ *of all* $\bar{\boldsymbol{F}}_p$*-valued points of* $\widetilde{W}_{S_\mathfrak{q}}$. *Furthermore it induces an injection* $i_{S\mathfrak{P}}$ *of* $(j_S\circ\varphi_S)(x_{S\mathfrak{p}}^{-1}\mathscr{C}(\mathfrak{p}))$ *into* $\mathscr{I}(\widetilde{W}_{S_\mathfrak{q}})$.

(iii) *Let* $\mathscr{I}_{ss}(\widetilde{W}_{S_\mathfrak{q}})$ *be the complement of* $(i_{S\mathfrak{P}}\circ j_S\circ\varphi_S)(x_{S\mathfrak{p}}^{-1}\mathscr{C}(\mathfrak{p}))$ *in* $\mathscr{I}(\widetilde{W}_{S_\mathfrak{q}})$. *Then* $\mathscr{I}_{ss}(\widetilde{W}_{S_\mathfrak{q}})$ *is a finite set. Let* z *be an element of* $\mathscr{B}$, *and let* (M,f,z) *be the corresponding triple. Then* $(j_S\circ\varphi_S)(z)$ modulo $\mathfrak{P}$ *belongs to* $\mathscr{I}_{ss}(\widetilde{W}_{S_\mathfrak{q}})$ *iff* $\mathfrak{p}$ *is not decomposed in* M. *Furthermore, for any element* w *of* $\mathscr{I}_{ss}(\widetilde{W}_{S_\mathfrak{q}})$ *and for any totally imaginary quadratic extension* M *of* F *contained in* $\boldsymbol{C}$ *such that* $\mathfrak{p}$ *is not decomposed in* M, *there exists a nomalized embedding* f *of* M *into* B *such that one has*

$$(j_S\circ\varphi_S)(z) \text{ modulo } \mathfrak{P}=w$$

with the unique common fixed point z *of* $f(M^\times)$.

MAIN THEOREM 2. *Let* W_S, j_S, P_S *etc. be as in Main Theorem* 1. *Let* T *be an element of* $\mathcal{Z}$, *and let* x *be an element of* G_{A+} *such that* (i) $xSx^{-1}\subseteqq T$, (ii) $\mathfrak{q}$ *belongs to* P_S *and* (iii) $\nu(x)$ *belongs to* $\nu(S)\cdot F_\mathfrak{p}^\times\cdot F^\times$. *Then the rational map* $j_T^{\sigma(x)}\circ J_{TS}(x)\circ j_S^{-1}$ *induces a morphism of* $W_{S_\mathfrak{q}}=W_S\times_{Spec(\mathfrak{r}_S)} Spec(\mathfrak{r}_{S_\mathfrak{q}})$ *to* $W_T^{\sigma(x)}\times_{Spec(\mathfrak{r}_T^{\sigma(x)})} Spec(\mathfrak{r}_{S_\mathfrak{q}})$.

REMARK. As in Shimura [24], 2.23, *we can prove the congruence relation for* $\widetilde{W}_{S_\mathfrak{q}}$ *if* $\mathfrak{q}$ *belongs to* P_S. In particular, we have *an affirmative answer to Question* 6.2.8 *of Ihara* [30] *for such* $\mathfrak{q}$ (cf. ibid., § 6).

Let $\mathfrak{p}$ be a prime ideal of F which does not divide $D(B/F)$. Let $G^{(\mathfrak{p})}$ be the subgroup of G_{A+} consisting of all elements x such that $\nu(x)$ belongs to the closure of $F_\mathfrak{p}^\times\cdot F^\times\cdot F_{\infty+}^\times$ in $F_A^\times$. Let $\mathcal{Z}^{(\mathfrak{p})}$ be the subset of $\mathcal{Z}$ consisting of all S such that there exists $x_{S_\mathfrak{p}}\in G_{Q+}$ satisfying $S\supseteqq x_{S_\mathfrak{p}}^{-1}\mathfrak{o}_\mathfrak{p}^\times x_{S_\mathfrak{p}}$. Let $\mathfrak{P}$ be an extension of $\mathfrak{p}$ to a place of $\bar{\boldsymbol{Q}}$. For any element S of $\mathcal{Z}^{(\mathfrak{p})}$, let $\tilde{k}_S$ be the residue field of $\mathfrak{P}|k_S$, and let g_S be the genus of V_S. For any $x\in G^{(\mathfrak{p})}$, let $\widetilde{\sigma(x)}$ be $\sigma(x)$ modulo $\mathfrak{P}\in\mathrm{Gal}(\bar{\boldsymbol{F}}_p/\tilde{F})$. Let $\mathscr{B}_s$ (resp. $\mathscr{B}_{ss}$) be the set consisting of all points $z\in\mathfrak{H}$ such that there exists a normalized embedding $f: M\to B$ satisfying (i) z is the common fixed point of $f(M^\times)$ and (ii) $\mathfrak{p}$ is decomposed in M (resp. $\mathfrak{p}$ is not decomposed in M). Further, for a given totally imaginary quadratic extension M of F contained in $\boldsymbol{C}$, let $\mathscr{B}(M)$ be the subset of $\mathscr{B}$ consisting of all $z\in\mathfrak{H}$ such that there exists a normalized embedding f of M into B satisfying $f(M^\times)z=z$. Then we have

MAIN THEOREM 3. *There exists a system*

$$\left\{\tilde{V}_S, \tilde{\varphi}_S, \tilde{J}_{TS}(x)\,(S, T\in\mathcal{Z}^{(\mathfrak{p})}\,;\; x\in G^{(\mathfrak{p})})\right\}$$

satisfying the following conditions:

(i) $\tilde{V}_S$ *is an absolutely irreducible projective nonsingular curve defined over* $\tilde{k}_S$ *with genus* g_S.

(ii) $\tilde{\varphi}_S$ *is a surjective map of* $\Gamma_S\backslash\mathscr{B}$ *onto the set of all* $\bar{\boldsymbol{F}}_p$*-valued points of* $\tilde{V}_S$. $\tilde{\varphi}_S$ *induces a bijective map of* $\Gamma_S\backslash x_S^{-1}\mathscr{C}(\mathfrak{p})$ *to* $\tilde{\varphi}_S(\mathscr{B}_s)$, *and a surjective map of* $\mathscr{B}(M)$ *to* $\tilde{\varphi}_S(\mathscr{B}_{ss})$ *for each* M *such that* $\mathfrak{p}$ *is not decomposed in* M/F. *Furthermore* $\tilde{\varphi}_S(\mathscr{B}_{ss})$ *is a finite set.*

(iii) $\tilde{J}_{TS}(x)$, *defined if* $xSx^{-1}\subseteqq T$, *is a separable morphism of* $\tilde{V}_S$ *to* $\tilde{V}_T^{\widetilde{\sigma(x)}}$ *rational over* $\tilde{k}_S$, *and has the following properties*:

(iii$_a$) $\tilde{J}_{SS}(x)$ *is the identity map of* $\tilde{V}_S$ *if* $x\in S$;

(iii$_b$) $\tilde{J}_{TS}(x)^{\widetilde{\sigma(y)}}\circ\tilde{J}_{SR}(y)=\tilde{J}_{TR}(xy)$;

(iii$_c$) $\tilde{J}_{TS}(\alpha)[\tilde{\varphi}_S(z)]=\tilde{\varphi}_T(\alpha(z))$ *if* $\alpha\in G_{\boldsymbol{Q}+}$ *and* $z\in\mathscr{B}$.

(iv) *Let* z *be an element of* $\mathscr{B}$, *and let* $(M,f\,z)$ *be the corresponding triple. Let* c *be an element of* $M_A^\times$ *such that* $[c, M]$ *belongs to the decomposition group of* $\mathfrak{P}\cap M$, *and let* $[c, M]\bmod\mathfrak{P}$ *be the action of* $[c, M]$ *on the residue field* $\widetilde{M}_{ab}$ *of* $\mathfrak{P}|M_{ab}$. *Then, for any* $S\in\mathcal{Z}^{(\mathfrak{p})}$, *the point* $\tilde{\varphi}_S(z)$ *is rational over* $\widetilde{M}_{ab}$, *and satisfies*

$$\tilde{\varphi}_S(z)^{[c,M]\bmod\mathfrak{P}}=\tilde{J}_{ST}\big(f(c)^{-1}\big)\big[\tilde{\varphi}_T(z)\big],$$

where $T=f(c)\,S\,f(c)^{-1}$.

REMARK. The Main Theorems for the case of the elliptic modular groups (i.e. the case of $B=M_2(\boldsymbol{Q})$) is known and due to Y. Ihara (cf. Ihara [8]). In fact, the author started this reserch by trying to generalize the results of Chapter 5 of [8]. Though our theorems are formulated in a slightly different way from the theorems in [8], it is well-known that the both formulations are essentially equivalent. We used the present formulation simply because this formulation is easier in quoting results from Shimura [24].

We note that, by generalizing Ihara's method, G. Shimura proved the theorems in the case when $p=\mathfrak{p}\cap\boldsymbol{Q}$ is completely decomposed in $F/\boldsymbol{Q}$ or p remains prime in $F/\boldsymbol{Q}$ for almost all such $\mathfrak{p}$. The key point in his proof was the fact that the bijectivity of $i_{S\mathfrak{P}}$ to $\mathscr{I}(\widetilde{W}_{S_q})\backslash\mathscr{I}_{ss}(\widetilde{W}_{S_q})$ follows from the surjectivity or the injectivity of it if good reduction of V_S is assumed. On the other hand, we are going to prove the bijectivity of it at first, and prove good reduction of V_S from the bijectivity. It should be noted that our proof of the bijectivity is essentially the same as Shimura's proof, though it is technically more difficult.

REMARK. In a series of papers published in Canadian Journal of Mathematics, R. P. Langlands studied the zeta-functions of the Shimura varieties obtained from a totally indefinite quaternion algebra. In his case, there exist canonical families of abelian varieties, so that it is not necessary to decend the fields of rationality of the varieties. But his papers suggest the way how to treat the general higher dimensional Shimura varieties.

REMARK. The author heard from Y. Ihara and M. Ohta that each of them can prove the good reduction of the Shimura curve V_S if (i) $\mathfrak{P}$ does not divide $D(B/F)$ and (ii) the level of S is prime to $\mathfrak{p}$ (cf. Ihara-Miki [32] for Ihara's proof).

1-3. Outline of the proof of Theorem C. The rest of § 1 will be used to summarize the proof of Theorem C. More precisely, 1-3 is a summary of Shimura [24], § 6 in our case. It will be used in proving the main theorems in § 3.

Let K be a totally imaginary quadratic extension of F contained in $\boldsymbol{C}$, and let $\tau_1=\mathrm{id.}, \cdots, \tau_g$ be isomorphisms of K into $\boldsymbol{C}$ satisfying $\tau_\nu|F=\tau_{0\nu}$ for each $\nu=1, \cdots, g$. Let L be the quaternion algebra $B\otimes_F K$ over K, and let ρ be a positive involution of L. Let v be an invertible element of L such that $v^\rho=-v$, and we assume $B=\{x\in L|x'=vx^\rho v^{-1}\}$, where $x\to x'$ denotes the main involution of L. It is obvious that ρ induces the complex conjugation on K.

Let Φ be a representation of $L_{\boldsymbol{R}}=L\otimes_{\boldsymbol{Q}}\boldsymbol{R}$ by complex matrices such that the restriction of Φ to K is equivalent to $2(\tau_1+\tau_1\rho+2\sum_{\nu=2}^{g}\tau_\nu)$. We denote $\Phi|K$ by the same letter Φ. Let $\omega_\nu: L_{\boldsymbol{R}}\to M_2(\boldsymbol{C})$ be a representation satisfying $\omega_\nu(a)=a^{\tau_\nu}1_2$ for any $a\in K$. It is known that, for any given K, $\tau_1, \cdots, \tau_g$ and $\omega_1, \cdots, \omega_g$, there exist a positive involution ρ of L and an invertible element v of L such that $v^\rho=-v$, $B=\{x\in L|x'=vx^\rho v^{-1}\}$ and the complex hermitian matrix $-\sqrt{-1}\,\omega_\nu(v)$ has the signature $(1, -1)$ or $(1, 1)$ according as $\nu=1$ or $\nu>1$.

Let $T(x, y)$ be the L-valued ρ-anti-hermitian form on L defined by $T(x, y)=xvy^\rho$ for x, $y\in L$, and let $G(T)$ be the group of all similitudes of T. Let G^* be the $\boldsymbol{Q}$-algebraic group satisfying $G_{\boldsymbol{Q}}^*=G(T)$, and let $\nu: G^*\to F^\times$ be the homomorphism such that $\nu(x)$ is the multiplier of the similitude for any $x\in G_{\boldsymbol{Q}}^*$. Let $G_{\infty+}^*$ be the identity component of $G_\infty^*=G_{\boldsymbol{R}}^*$, let G_A^* be the adelization of G^*, and let G^*_{A+} be the subgroup of G^*_A consisting of all elements x such that the projection of x to G^*_∞ belongs to $G^*_{\infty+}$. It is obvious that G^*_Q contains G_F. (In fact, it is known that $G(T)=K^\times\cdot B^\times$.)

Let $\mathscr{D}$ be the unit ball $\{z\in \boldsymbol{C}\,|\,|z|<1\}$. Shimura defined an action of $G^*_{\infty+}$ on $\mathscr{D}$ in [22], and proved that there is a holomorphic isomorphism j of $\mathfrak{H}$ to $\mathscr{D}$ satisfying $j(\alpha(z))=\alpha(j(z))$ for any $z\in\mathfrak{H}$ and $\alpha\in G_{\infty+}$. Therefore *we identify* $\mathfrak{H}$ *and* $\mathscr{D}$ *and make* $G^*_{\infty+}$ *act on* $\mathfrak{H}$.

For every $\boldsymbol{Z}$-lattice $\mathfrak{N}$ in L, and for every positive integer a, put

$$\Gamma^*(\mathfrak{N}, a)=\left\{\gamma\in G^*_Q\,\middle|\,\nu(\gamma)=1, \mathfrak{N}\gamma=\mathfrak{N}, \ \mathfrak{N}(1-\gamma)\subseteqq a\mathfrak{N}\right\}.$$

Let $\mathfrak{o}$ be as before (i. e. a maximal order of B). Put $\mathfrak{M}=\mathfrak{r}_K\otimes_{\mathfrak{r}_F}\mathfrak{o}\subseteqq L$. For every positive integer a, put

$$S(\mathfrak{o}, a)=\left\{x\in G_{A+}\,|\,x_p\in\mathfrak{o}_p^\times, \mathfrak{o}_p(x_p-1)\subseteqq a\mathfrak{o}_p \quad \text{for all prime number } p\right\}.$$

For any two positive integers b and c, put

$$S(b, c)=S(\mathfrak{o}, c)\cdot\left\{x\in S(\mathfrak{o}, b)\,\middle|\,\nu(x)=1\right\}.$$

It is known that, for a given integer a, there exist two integers b and c satisfying the following three conditions:

(i) $c\boldsymbol{Z}\subseteqq b\boldsymbol{Z}\subseteqq a\boldsymbol{Z}$;

(ii) Put $E=\mathfrak{r}_F^\times$. Then, for every $u\in G_A$ and $v\in K_A^\times$

$$E\cdot\Gamma\left(u^{-1}S(b, c)\,u\right)=E\cdot\Gamma^*(v\mathfrak{M}u, b);$$

(iii) For every $u\in G_A$ and $v\in K_A^\times$, $\Gamma^*(v\mathfrak{M}u, b)$ has no element of finite order other than the identity element. *Hereafter we shall consider only such a group* $S(b, c)$. We note here that, by Shimura [24], 6. 4 and [22] 6. 3, and by Chevalley [1], *we can choose* b *and* c *in the following manner*: For any positive integer b satisfying $b\geqq 3$, and for any given integer d which is prime to b, there exists a positive integer c such that c is prime to d and such that the pair (b, c) satisfies the above three conditions for every divisor a of b and for every K, if K has no roots of unity other than ± 1 and there exists a prime ideal of F such that it is ramified in K and it does not divide 2 $D(B/F)$.

Let (K, Φ) be as before, and let (K', Φ') be the reflex of (K, Φ) in the sense of Shimura [24], 1. 3. Hence $K'=\boldsymbol{Q}$ if $F=\boldsymbol{Q}$. Put $K'=H$. Let a, b, c be as before, and put $S=S(b, c)$. Let H_c be the class field over H corresponding to the subgroup $H^\times\cdot\{h\in H_A^\times\,|\,h\equiv 1 \bmod_0(c)\}$ of $H_A^\times$. Then it is known that H_c contains $k_S\cdot H$.

Let $\mathfrak{M}$ be as before, and let $\mathfrak{N}$ be a $\boldsymbol{Z}$-lattice in L of the form $\mathfrak{N}=f\mathfrak{M}p$ with $f\in K_A^\times$ and $p\in G_A$. Let us now consider a PEL-type

$$\Omega=(L, \Phi, \rho\,;\ \kappa T, \mathfrak{N}\,;\ q_1, \cdots, q_s)\,,$$

where the q_i are elements of $L/\mathfrak{N}$ and κ is a totally positive element of F such that $b^{-1}\mathfrak{N}/\mathfrak{N}=\sum_{i=1}^{s}\boldsymbol{Z}q_i$ and $\mathrm{tr}_{L/\boldsymbol{Q}}(\kappa T(\mathfrak{N}, \mathfrak{N}))=\boldsymbol{Z}$. Since L, Φ, ρ and T are common to all these PEL-structures, we write simply $\Omega=(\kappa, \mathfrak{N}, \{q_i\})$. We construct a family $\Sigma(\Omega)=\{\mathcal{Q}_z|z\in\mathfrak{H}\}$ of PEL-structures

$$\mathcal{Q}_z=(A_z, \mathcal{C}_z, \theta_z\,;\ t_{1z}, \cdots, t_{sz})$$

by means of the parametrizing function $\mathfrak{y}$ as in Shimura [23], 6. 4, common to all Ω of this type.

By Shimura [24], 6. 6, there exists a subfield k_Ω of H_c with the following property: Let $\mathcal{Q}$ be a PEL-structure of type Ω, and let σ be an automorphism of $\boldsymbol{C}$. Then $\mathcal{Q}^\sigma$ is of type Ω iff σ is the identity mapping on k_Ω. Further Shimura constructed in [21] a fibre system of PEL-structures

$$\mathcal{F}=\left\{V, W, h, f, Y, S(a), f_1, \cdots, f_s\right\}$$

and a holomorphic map φ of $\mathfrak{H}$ onto V with the following properties: (i) V is a projective nonsingular curve; (ii) $h: W\to V$ defines a projective abelian scheme with $f: V\to W$ as the unit section; (iii) Y is an effective Cartier divisor relatively ample with respect to h; (iv) $S(a)$ is defined for every element a of the left order of $\mathfrak{N}$, and $\theta: a\to S(a)$ gives an injection of this order into the endomorphism ring of the abelian scheme $h: W\to V$; (v) The f_i $(i=1, \cdots, s)$ are the b-section points of $h: W\to V$; (vi) For every PEL-structure $\mathcal{Q}$ of type Ω, there exists exactly one point u of V such that $\mathcal{Q}$ is isomorphic to the fibre $\mathcal{Q}_u$ on u; (vii) Every element of $\mathcal{F}$ is defined over k_Ω; (viii) φ induces an isomorphism of $\Gamma(\mathfrak{N}, b)\backslash\mathfrak{H}$ to V such that $\mathcal{Q}_z\in\Sigma(\Omega)$ is isomorphic to $\mathcal{Q}_{\varphi(z)}$ for each $z\in\mathfrak{H}$. Note that $\mathcal{Q}_{\varphi(z)}$ is defined over $k_\Omega(\varphi(z))$ and $k_\Omega(\varphi(z))$ is the field of moduli of $\mathcal{Q}_z$.

Let $\tau_1, \cdots, \tau_g$ be as before. If $F\neq\boldsymbol{Q}$, then let Φ_0 be a representation of K such that $\Phi_0\sim\sum_{\nu=2}^{g}\tau_\nu$. Let (K', Φ_0') be the reflex of (K, Φ_0) and put $\pi=\det\Phi_0'$. Then we have $N_{H/F}(y)\,\pi(y)\,\pi(y)^\rho=N_{H/\boldsymbol{Q}}(y)$ for every $y\in H=K'$. If $F=\boldsymbol{Q}$, then let $\pi(a)=1$ for any $a\in\boldsymbol{Q}=K'$.

Let x be an element of $\mathcal{G}_{H+}=\{x\in G_{A+}|\nu(x)\in N_{H/F}(H_A^\times)\cdot F^\times\cdot F_{\infty+}^\times\}$, and let d be an element of $H_A^\times$ such that $\nu(x)/N_{H/F}(d)\in F^\times\cdot F_{\infty+}^\times$. Put $\sigma=[d^{-1}, H]$. Then Ω^σ is equivalent to $\Omega'=(\mu(\pi(d)\,x)^{-1}x, \pi(d)\,\mathfrak{N}x, \{\pi(d)\,q_i x\})$, where $\mu(\pi(d)\,x)$ is defined in the following manner: Since $N_{H/F}(d)\,\pi(d)\,\pi(d)^\rho=N_{H/\boldsymbol{Q}}(d)\in\boldsymbol{Q}_A^\times$, let $\nu(\pi(d)x)=\pi(d)\pi(d)^{\rho}\nu(x)=abc$ with $a\in \boldsymbol{Q}_A^{\times}$, $b\in F_+^{\times}$ and $c\in F_{\infty+}^{\times}$. Let a_1 be the positive integer which generates the ideal associated with a. Then put $\mu(\pi(d)x)=a_1 b\in F_+^{\times}$ (cf. Shimura [24], 6. 2).

Let $S=S(b,c)$, $\mathfrak{N}=f\mathfrak{M}p$, $\Omega=(\kappa,\mathfrak{N},\{q_i\})$, $\Sigma(\Omega)$, $\mathscr{F}=\{V,W,h,f,S(a),f_1,\cdots,f_s\}$, φ etc. be as before. Put $T=p^{-1}S(b,c)p$, $\bar{V}_T=V$ and $\bar{\varphi}_T=\varphi$. Then $\bar{\varphi}_T$ induces an isomorphism of $\Gamma_T\backslash\mathfrak{H}$ onto $\bar{V}_T$.

Let x, d, σ and Ω' be as before. Put $U'=x^{-1}Tx$. Then we have $\mathscr{F}'=\{V',W',h',f',Y',S'(a),f_1',\cdots,f_s'\}$ and φ' for Ω'. Put $\bar{V}_U=V'$ and $\bar{\varphi}_U=\varphi'$. Since Ω^{σ} is equivalent to Ω', it is known that there exists a biregular morphism J of $\bar{V}_U$ to $\bar{V}_T^{\sigma}$, rational over k_{Ω}, such that, for any automorphism τ of $\boldsymbol{C}$ which induces σ on k_{Ω}, and for any $\mathscr{Q}_w\in\Sigma(\Omega)$ and $\mathscr{Q}_z'\in\Sigma(\Omega')$, the equality $\varphi(w)^{\tau}=J(\varphi'(z))$ holds iff $\mathscr{Q}_w^{\tau}$ is isomorphic to $\mathscr{Q}_z'$. Since k_{Ω} is contained in H_c, $\bar{V}_T$, $\bar{V}_U$ and J are defined over H_c.

It is known that $(\bar{V}_T,\bar{\varphi}_T)$ does not depend on a special choice of f, p and $\{q_i\}$, and that J depends only on the coset xU and the effect of $[d^{-1},H]$ on H_c (cf. Shimura [24], 6. 10, 6. 11, 6. 12). Hence we put $J=\bar{J}(x,d)$. Then we have the following:

(i) Let T, x, d, U be as before. Let $y\in\mathscr{G}_{H+}$ and $e\in H_A^{\times}$ satisfying $\nu(y)/N_{H/F}(e)\in F^{\times}F_{\infty+}^{\times}$. Put $R=y^{-1}Uy$ and $\tau=[e^{-1},H]$. Then

$$\bar{J}_{TR}(xy,de)=\bar{J}_{TU}(x,d)^{\tau}\circ\bar{J}_{UR}(y,e);$$

(ii) Let T be as before, and let α be an element of $G_{\boldsymbol{Q}+}$. Put $U=x^{-1}Tx$. Then

$$\bar{J}_{TU}(\alpha,1)\left[\bar{\varphi}_U(z)\right]=\bar{\varphi}_T\left(\alpha(z)\right).$$

Let $\mathscr{W}_{bc}$ be the subfamily of $\mathscr{Z}$ consisting of all $p^{-1}S(b,c)p$ with $p\in G_A$, where we assume that b and c satisfy the previous conditions. Then we have a system

$$\left\{\bar{V}_T,\bar{\varphi}_T,\bar{J}_{TU}(x,d)\right\}$$

for T, $U\in\mathscr{W}_{bc}$, $x\in\mathscr{G}_{H+}$ and $d\in H_A^{\times}$ such that $U=x^{-1}Tx$ and $\nu(x)/N_{H/F}(d)\in F^{\times}F_{\infty+}^{\times}$. Shimura constructed the canonical system of Theorem C by taking quotients and descending the field of rationality of these systems. In particular, he proved that *this system is biregularly equivalent over H_c to the subsystem*

$$\left\{V_T,\varphi_T,J_{TU}(x)\,(T\in\mathscr{W}_{bc},x\in\mathscr{G}_{H+},U=x^{-1}Tx)\right\}$$

of the canonical system.

§ 2. Moduli spaces

2-1. Mumford's moduli. Let S be a locally noetherian scheme, and let $\mathscr{M}_{g,d,N}(S)$ be the set consisting of all isomorphism classes of all triple $(X, \omega, \{\sigma_j\})$ such that (i) X is a projective g-dimensional abelian scheme over S, (ii) ω is a plarization of X of degree d^2, and (iii) $\{\sigma_1, \cdots, \sigma_{2g}\}$ is a level N-structure of X over S, all in the sense of Mumford [14]. Then $\mathscr{M}_{g,d,N}$ defines a contravariant functor from the category of locally noetherian schemes to the category of sets.

Now assume that $N \geqq 3$. Then Mumford proved in [14] that $\mathscr{M}_{g,d,N}$ *is represented by a scheme* $M = M_{g,d,N}$ *which is quasi-projective over Spec* $(\boldsymbol{Z})$. In other words, there exists an element $(Z, \Omega, \{\Sigma_j\})$ of $\mathscr{M}_{g,d,N}(M)$ such that, for any locally noetherian scheme S and for any $(X, \omega, \{\sigma_j\}) \in \mathscr{M}_{g,d,N}(S)$, there exists a unique morphism $F: S \rightarrow M$ such that $(X, \omega, \{\sigma_j\})$ is isomorphic to the pull back $(Z, \Omega, \{\Sigma_j\}) \times_M S$ of $(Z, \Omega, \{\Sigma_j\})$ by F.

2-2. Embedding of Shimura's moduli into Mumford's moduli $\boldsymbol{M}$. Let $\Omega = (L, \Phi, \rho; T, \mathfrak{M}; v_1, \cdots, v_u)$ be a PEL-type in the sense of Shimura [21], 3. 1. Let N be a natural number satisfying $N \geqq 3$, and *we assume that* $\{v_1, \cdots, v_u\}$ *is a basis of the* $\boldsymbol{Z}/N\boldsymbol{Z}$*-module* $N^{-1}\mathfrak{M}/\mathfrak{M}$. Let $U(T)$ be the unitary group of the ρ-anti-hermitian form T, and let $\mathscr{H}$ be the bounded symmetric domain which is the quotient space of $U(T)_{\boldsymbol{R}}$ by a maximal compact subgroup. Let

$$\Gamma^*(T, N) = \left\{\alpha \in U(T) \,\middle|\, \mathfrak{M}\alpha = \mathfrak{M}, \left(\sum_{i=1}^{u} \boldsymbol{Z} v_i\right)(1-\alpha) \subseteqq \mathfrak{M}\right\},$$

and *we assume that either* $\dim(\mathscr{H}) > 1$ *or* $\Gamma^*(T, N) \backslash \mathscr{H}$ *is compact.* Then, by Theorem 5. 3 of Shimura [21], there exist an algebraic number field k_Ω, a holomorphic map φ of $\mathscr{H}$ to a quasi-projective non-singular variety V defined over k_Ω, and a fibre system of PEL-structures

$$\mathscr{F} = \left\{V, W, h, f, Y, S(a), f_1, \cdots, f_u\right\}$$

on V defined over k_Ω and satisfying the eight conditions in 1-3.

Let $h: W \rightarrow V$ be as above. Then, by Theorem 6. 14 of Mumford [14], $h: W \rightarrow V$ is a projective abelian scheme over V with $f: V \rightarrow W$ as its identity. Since Y is an effective relative Cartier divisor (cf. the proof of Theorem 5. 3 of Shimura [21]), Y defines a V-homomorphism $\omega: W \rightarrow \hat{W}$. Since ω induces on each geometric fibre W_s of π the homomorphism $\varphi_{Y_s}: u \rightarrow Cl(Y_{su} - Y_s)$ with a positive non-degenerate divisor Y_s, Y defines a relatively ample invertible sheaf on $h: W \rightarrow V$ (cf. EGA, III, 4. 7. 1). Hence ω is a polarization.

Therefore

$$\mathscr{F}' = \{V, W, h, f, \omega, f_1, \cdots, f_u\}$$

is an element of $\mathscr{M}_{g,d,N}(V)$ with $u=2g$ and $\deg(\omega)=d^2$. Since $N \geqq 3$, *there exists a unique morphism* $F_0: V \rightarrow M = M_{g,d,N}$ *such that* $\mathscr{F}'$ *is isomorphic to the pull back* $(Z, \Omega, \{\Sigma_j\}) \times_M V$ *of the universal polarized abelian scheme* $(Z, \Omega, \{\Sigma_j\})$ *to* V *by the map* F_0.

Put $k=k_\Omega$, $\mathfrak{r}_k=\mathfrak{r}_{k_\Omega}$, $M_k=M\times_{Spec(\boldsymbol{Z})} Spec(k)$ and $M_\mathfrak{r}=M\times_{Spec(\boldsymbol{Z})} Spec(\mathfrak{r}_k)$. Since $\mathscr{F}'$ is rational over k_Ω, F_0 induces a morphism $F: V \rightarrow M_k$. Since M_k is an M-scheme, we may regard F as a morphism of V to M.

Let t be a generic point of V. Then the fibre of h at t gives a PEL-structure $\mathscr{Q}_t=(A_t, \mathscr{C}_t, \theta_t; f_{jt})$ of type Ω, hence also an element $\mathscr{P}_t=(A_t, \mathscr{C}_t; f_{jt})$ of $\mathscr{M}_{g,d,N}(Spec(k_\Omega(t)))$. Obviously $\mathscr{P}_t$ is isomorphic to the fibre of $(Z, \Omega, \{\Sigma_j\}) \times_{Spec(\boldsymbol{Z})} Spec(k_\Omega)$ at $F(t)$.

Let $\mathfrak{p}$ be a discrete valuation with quotient field K, and let $\mathscr{Q}=(A, \mathscr{C}, \theta; f_j)$ be a PEL-structure of type Ω defined over K. Then, by Shimura-Taniyama [25], III, 11 and by Serre-Tate [19], § 1, $\mathscr{Q}$ has good reduction at $\mathfrak{p}$ iff $\mathscr{P}=(A, \mathscr{C}; f_j)$ has good reduction at $\mathfrak{p}$, and there exists at most one prolongation of $\mathscr{Q}$ to an object over the valuation ring of $\mathfrak{p}$. Hence, by the valuative criterion (cf. EGA, II, 7. 3. 8), F is a proper morphism. In particular, $F(V)$ is a closed subscheme of M_k.

Let $U_0=F(V)$, *and let* U *be the Zariski closure of* U_0 *in* $M_\mathfrak{r}$. Then U is irreducible and quasi-projective over $Spec(\mathfrak{r}_k)$. Hence, for any geometric point w' of U, there exists a valuation $\mathfrak{p}$ of $k_\Omega(t)$ such that (i) the valuation ring R of $\mathfrak{p}$ contains $\mathfrak{r}_k$ and (ii) w' is reduction modulo $\mathfrak{p}$ of $w=F(t)$. Since w' is a point of U, $\mathscr{P}_t=(A_t, \mathscr{C}_t; f_{jt})$ and $\mathscr{Q}_t=(A_t, \mathscr{C}_t, \theta_t; f_{jt})$ have good reduction at $\mathfrak{p}$. Here, by Lemma 2 of Shimura-Taniyama [25], III, 9. 3, we may assume that $\mathfrak{p}$ is discrete (but may not be of rank one). Therefore, for any geometric point w' of U, there exists a discrete place $\mathfrak{p}$ of $k_\Omega(t)$ such that (i) the generic PEL-structure $\mathscr{Q}_t=(A_t, \mathscr{C}_t, \theta_t; f_{jt})$ of type Ω has good reduction at $\mathfrak{p}$ and (ii) $(A_t, \mathscr{C}_t; f_{jt}) \bmod \mathfrak{p}$ is the polarized abelian scheme with level N-structure corresponding to w'.

2-3. Moduli spaces of families of PEL-structures. Let the notation and assumptions be as in 2-2. *Let* $\mathscr{S}_0$ *be the set consisting of all isomorphism classes of all* PEL-*structures of type* Ω. For any element $\mathscr{Q}$ of $\mathscr{S}_0$ and for any place $\mathfrak{p}$ of any field of definition of $\mathscr{Q}$ such that (i) the valuation ring of $\mathfrak{p}$ contains $\mathfrak{r}_k$, (ii) the residue characteristic of $\mathfrak{p}$ is prime to the level N, and (iii) $\mathscr{Q}$ has good reduction at $\mathfrak{p}$, we denote by $\mathscr{Q} \bmod \mathfrak{p}$ reduction modulo $\mathfrak{p}$ of the PEL-structure $\mathscr{Q}$.

For any prime ideal $\mathfrak{q}$ of $\mathfrak{r}_k$ such that $\mathfrak{q}$ is prime to the level N, we fix an extension $\mathfrak{Q}$ of $\mathfrak{q}$ to a place of $\boldsymbol{C}$. Let $\Omega(\mathfrak{q})$ be the residue field of $\mathfrak{Q}$, and let $\mathscr{S}_{\mathfrak{q}}$ be the set consisting of all isomorphism classes of all $\mathscr{Q}$ mod $\mathfrak{Q}$ ($\mathscr{Q}\in\mathscr{S}_0$). Let

$$\mathscr{S}=\mathscr{S}_0 \coprod \coprod_{\mathfrak{q}} \mathscr{S}_{\mathfrak{q}}\,.$$

Let U be as in 2-2, and let $(X, \omega, \{\sigma_j\})$ be the canonical polarized abelian scheme with level N structure over U (i.e. the inverse image of $(Z, \Omega, \{\Sigma_j\})$ by $U\subsetneq M_{\mathfrak{r}}\to M$). Let $\mathcal{E}=\pi_*(L^{\Delta}(\omega)^3)$ and $\phi_3: X\subsetneq \boldsymbol{P}(\mathcal{E})$ be as in Mumford [14], Proposition 7.5 and Proposition 6.13. Since U is quasi-compact, it follows from Mumford [14], Proposition 7.5 that there exists a finite affine covering $\{U_i\}_{i\in I}$ of U with the following properties: (i) The restriction of $(X, \omega, \{\sigma_j\})$ to each U_i admits a linear rigidification $\phi_i: \boldsymbol{P}(\mathcal{E})\times_U U_i \xrightarrow{\sim} \boldsymbol{P}_m\times U_i$ with $m=6^g d-1$; (ii) There exists a $(U_i\cap U_j)$-valued point g_{ij} of $PGL(m)$ such that $g_{ij}\circ\phi_i|(\boldsymbol{P}(\mathcal{E})\times_U(U_i\cap U_j))=\phi_j|(\boldsymbol{P}(\mathcal{E})\times_U(U_i\cap U_j)$ for any $i, j\in I$. Put $\bar{\phi}_i=\phi_i\circ\phi_3$ for each $i\in I$.

Let $\mathfrak{o}$ be the left order of $\mathfrak{M}$, and let $r_1, \cdots, r_v$ be a $\boldsymbol{Z}$-base of $\mathfrak{o}$. Let Let t be a generic point of V over k_Ω, and put $w=F(t)$. Then, by the definition of U, w is a generic point of U. Let $\mathscr{Q}_t=(A_t, \mathscr{C}_t, \theta_t\,;\, f_{jt})$ be the fibre of $\mathscr{F}$ at t. Then F induces an isomorphism F_t of $(A_t, \mathscr{C}_t\,;\, f_{jt})$ to the fibre of $(X, \omega, \{\sigma_j\})$ at w, rational over $k_\Omega(t)$. Hence $\bar{\phi}_i\circ F_t$ induces an embedding of A_t into $\boldsymbol{P}_m\times U$ for each $i\in J$. Let A_{ti} be the image of this embedding, and let θ_{ti} be the injection of $\mathfrak{o}$ into $\mathrm{End}(A_{ti})$ corresponding to θ_t. Since F_t is rational over $k_\Omega(t)$, all elements of $\theta_{ti}(\mathfrak{o})$ are defined over $k_\Omega(t)$. Let R_{til} be the graph of $\theta_{ti}(r_l)$ for every $l=1, \cdots, v$. By the Segre morphism (cf. EGA, II. 43.1), we may regard R_{til} as a subset of $\boldsymbol{P}_{m(l)'}$ with a certain integer $m(l)'$. Let c_{il} be the Chow point of R_{til}, and let $s_i=c_{i1}\times\cdots\times c_{iv}\times w$. Then s_i is a $k_\Omega(t)$-valued point of $\boldsymbol{P}_{m(1)}\times\cdots\times\boldsymbol{P}_{m(v)}\times U_i$ with certain integers $m(1), \cdots, m(v)$. Let S_i be the Zariski closure of s_i in $\boldsymbol{P}_{m(1)}\times\cdots\times\boldsymbol{P}_{m(v)}\times U_i$.

By the functoriality of the Segre morphism, the $(U_i\cap U_j)$-action g_{ij} on $\boldsymbol{P}_m\times(U_i\cap U_j)$ can be extended to a $(U_i\cap U_j)$-action on $\boldsymbol{P}_{m(l)'}\times(U_i\cap U_j)$ for every $l=1, \cdots, v$. Further it follows from the definition of Chow points that g_{ij} can be extended to a $(U_i\cap U_j)$-action on $\boldsymbol{P}_{m(1)}\times\cdots\times\boldsymbol{P}_{m(v)}\times(U_i\cap U_j)$. It is obvious that this action induces an isomorphism of $S_i\times_{U_i}(U_i\cap U_j)$ onto $S_j\times_{U_j}(U_i\cap U_j)$. Hence we can *glue* $\{S_i\}_{i\in I}$ *and construct a scheme* S. Similarly we glue $\{\boldsymbol{P}_{m(1)}\times\cdots\times\boldsymbol{P}_{m(v)}\times U_i\}_{i\in I}$ and construct a scheme P. Let q be the morphism of S to U which is induced by the projection of $\boldsymbol{P}_{m(1)}\times\cdots\times\boldsymbol{P}_{m(v)}\times U_i$ to U_i. We see that (i) there exist locally free $\mathscr{O}_U$-

modules $\mathcal{E}_1, \cdots, \mathcal{E}_v$ such that P is U-isomorphic to $\boldsymbol{P}(\mathcal{E}_1) \times_U \cdots \times \boldsymbol{P}(\mathcal{E}_v)$ (construct the $\mathcal{E}_j$ from $\mathcal{E}$ by taking direct sums and tensor products), and that (ii) S is a closed U-subscheme of P. Hence q is projective, and S is quasi-projective over $Spec(\mathfrak{r}_k)$.

Let $\mathscr{Q}=(A, \mathscr{C}, \theta; f_j)$ be an element of $\mathscr{S}$. Let w' be the point of U corresponding to $(A, \mathscr{C}; f_j)$. We assume that $(A, \mathscr{C}; f_j)$ is the fibre of $(X, \omega, \{\sigma_j\})$ at w'. Since $N \geqq 3$, $(A, \mathscr{C}; f_j)$ has no automorphism other than the identity map. Hence $\theta: \mathfrak{o} \to \mathrm{End}(A)$ is uniquely determined by the isomorphism class of $(A, \mathscr{C}, \theta; f_j)$. Let $\{U_i\}_{i \in I}$ be as before. We assume that w' is a K-valued point of U_i. Let θ'_i be the injection of $\mathfrak{o}$ into $\mathrm{End}(\bar{\phi}_i(A))$ corresponding to θ. Let R'_{il} be the graph of $\theta'_i(r_l)$ $(l=1, \cdots, v)$, and let c'_{il} be the Chow point of R'_{il}. Put $s'_i = c'_{i1} \times \cdots \times c'_{iv} \times w$.

Since $w=F(t)$ is a generic point of U, w' is a specialization of w. Since $F_t(A_t, \mathscr{C}_t; f_{jt})$ and $(A, \mathscr{C}; f_j)$ are fibers of $(X, \omega; \{\sigma_j\})$ at $w=F(t)$ and w', $F_t(A_t, \mathscr{C}_t; f_{jt}) \to (A, \mathscr{C}; f_j)$ is a specialization over $w \to w'$ in the sense of Shimura [20]. Hence $F_t(A_t, \mathscr{C}_t, \theta_t; f_{jt}) \to (A, \mathscr{C}, \theta; f_j)$ is a specialization over $w \to w'$. By Shimura-Taniyama [25], III, 11. 1, Proposition 12, this specialization induces $R_{til} \to R'_{il}$ for each l. Furthermore, by the definition of specializations of cycles in projective spaces, the specialization induces $c_{il} \to c'_{il}$. Hence there exists a discrete place $\mathfrak{p}$ of $k_\Omega(t)$ such that $s'_i = c'_{i1} \times \cdots \times c'_{iv} \times w'$ is reduction modulo $\mathfrak{p}$ of $s_i = c_{i1} \times \cdots \times c_{iv} \times w$. Since S_i is the Zariski closure of s_i in $\boldsymbol{P}_{m(1)} \times \cdots \times \boldsymbol{P}_{m(v)} \times U_i$, and since w' is a $\boldsymbol{C}$- or $\Omega(\mathfrak{q})$-valued point of U_i, s'_i is a $\boldsymbol{C}$- or $\Omega(\mathfrak{q})$-valued point of S_i. We observe that s'_i determines a $\boldsymbol{C}$- or $\Omega(\mathfrak{q})$-valued point s' of S, and this s' does not depend on a special choice of U_i. Therefore *we have constructed a map* ψ *of* $\mathscr{S}$ *to the set of all* $\boldsymbol{C}$- *or* $\Omega(\mathfrak{q})$-*valued points of* S.

It is obvious that this map ψ commutes with any operation of discrete places and automorphisms of the field K of definition of any element $\mathscr{Q}$ of $\mathscr{S}$ (replace $\mathscr{Q}_t$ and $\mathscr{Q}$ by $\mathscr{Q}$ and $\mathscr{Q}$ mod $\mathfrak{p}$ (or $\mathscr{Q}^\sigma$) and repeat the above arguments). Further it follows from the last remark in 2-2 and Proposition 12 of Shimura-Taniyama [25], III, 11. 1 that ψ is surjective. Since ψ induces an injective map of isomorphism classes of the polarized abelian varieties with level N-structure to U, and since the injection θ of $\mathfrak{o}$ into the endomorphism ring is uniquely determined by the isomorphism class of an element $\mathscr{Q}=(A, \mathscr{C}, \theta; f_j)$ for a given $(A, \mathscr{C}; f_j)$, it follows from the construction of $\mathscr{S}$ and ψ that ψ is injective.

Let V be as before. For an element $\mathscr{Q}$ of $\mathscr{S}_0$, let $\mathfrak{v}(\mathscr{Q})$ be the point on V such that $\mathscr{Q}$ is isomorphic to the fibre of $\mathscr{F}$ at $\mathfrak{v}(\mathscr{Q})$. Then $(V, \mathfrak{v})$

satisfies the conditions of Theorem 6.2 of Shimura [21]. Put $S_0=S\times_{Spec(\mathfrak{r})} Spec(k_\Omega)$. Then, by Theorem 6.7 of Shimura [21], there exists a one-to-one morphism j of V onto S_0 such that j is defined over k_Ω and $\phi(\mathscr{Q})=j(\mathfrak{v}(\mathscr{Q}))$ for any $\mathscr{Q}\in\mathscr{S}_0$. Therefore we have proved:

THEOREM 1. *Let the* PEL-*structure* Ω *be as in* 2–2, *and let* V, $\mathfrak{v}$, k_Ω, $\mathfrak{r}_k$, $\mathscr{S}_0$, *the* $\mathfrak{q}$, *the* $\Omega(\mathfrak{q})$ *and* $\mathscr{S}$ *be as before. Then there exist a scheme* $S=S(\Omega)$, *a map* $\phi=\phi_\Omega$ *of* $\mathscr{S}$ *to the set of geometric points of* S, *and a morphism* $j=j_\Omega$ *of* V *to* S *with the following properties*:

(i) S *is irreducible and quasi-projective over* $Spec(\mathfrak{r}_k)$.

(ii) ϕ *induces a bijective map of* $\mathscr{S}$ *to the set* $\{\boldsymbol{C}$*-valued points of* $S\}$ $\coprod\coprod_{\mathfrak{q}}\{\Omega(\mathfrak{q})$*-valued points of* $S\}$.

(iii) *Let* $\mathscr{Q}$ *be an element of* S, *and let* $\mathfrak{p}$ (*resp.* σ) *be a discrete place* (*resp. an automorphism*) *of the field of definition of* $\mathscr{Q}$ *such that* $\mathscr{Q}\bmod\mathfrak{p}$ (*resp.* $\mathscr{Q}^\sigma$) *belongs to* $\mathscr{S}$. *Then* $\phi(\mathscr{Q}\bmod\mathfrak{p})=\phi(\mathscr{Q})\bmod\mathfrak{p}$ (*resp.* $\phi(\mathscr{Q}^\sigma)=\phi(\mathscr{Q}^\sigma)$) *holds.*

(iv) j *induces a one-to-one morphism of* V *onto* $S_0=S\times_{Spec(\mathfrak{r}_k)} Spec(k_\Omega)$ *defined over* k_Ω *such that* $\phi(\mathscr{Q})=j(\mathfrak{v}(\mathscr{Q}))$ *for any* $\mathscr{Q}\in\mathscr{S}_0$.

REMARK. The condition (iii) implies $k_\Omega(\phi(\mathscr{Q}))$ is the field of moduli for each $\mathscr{Q}\in\mathscr{S}_0$. Hence j is a birational morphism.

REMARK. It is more natural to use Hilbertian schemes instead of Chow points. But we have avoided it simply because our result is enough to prove our main theorems.

§ 3. Proof of the main results

3-1. Zeta functions of Ihara groups. Let the notation and assumptions be as in 1-1. In particular, B is a division quaternion algebra over a totally real algebraic number field F. Let $\mathfrak{p}$ be a prime ideal of F which does not divide the discriminant $D(B/F)$ of B. Let S be an element of $\mathcal{Z}$ containing $\mathfrak{o}_\mathfrak{p}^\times$, and let $\bar{\Gamma}_{S_\mathfrak{p}}=G_{\boldsymbol{Q}+}\cap(S\cdot B_\mathfrak{p}^\times)$. We fix an isomorphism of $B_\mathfrak{p}$ onto $M_2(F_\mathfrak{p})$, and regard $\bar{\Gamma}_{S_\mathfrak{p}}$ as a subgroup of $GL^+(2,\boldsymbol{R})\times GL(2,F_\mathfrak{p})$. Let $\Gamma_{S_\mathfrak{p}}$ be the image of $\bar{\Gamma}_{S_\mathfrak{p}}$ by the natural map of $GL^+(2,\boldsymbol{R})\times GL(2,F_\mathfrak{p})$ to $PGL^+(2,\boldsymbol{R})\times PGL(2,F_\mathfrak{p})$. Then, by Proposition 1 of Ihara [8], Vol. 1, p. 174, $\Gamma_{S_\mathfrak{p}}$ is a discrete subgroup of $PGL^+(2,\boldsymbol{R})\times PGL(2,F_\mathfrak{p})$ such that (i) the quotient $\Gamma_{S_\mathfrak{p}}\backslash PGL^+(2,\boldsymbol{R})\times PGL(2,F_\mathfrak{p})$ is compact and (ii) the projection of $\Gamma_{S_\mathfrak{p}}$ to each component of $PGL^+(2,\boldsymbol{R})\times PGL(2,F_\mathfrak{p})$ contains a dense subgroup of $PSL(2,\boldsymbol{R})$ or $PSL(2,F_\mathfrak{p})$. Hereafter *we assume that* $\Gamma_{S_\mathfrak{p}}$ *is contained in* $PSL(2,\boldsymbol{R})\times PSL(2,F_\mathfrak{p})$. Let $\Gamma=\Gamma_{S_\mathfrak{p}}$ and $\Gamma^0=\Gamma_S(=\Gamma_{S_\mathfrak{p}}\cap\mathfrak{o}_\mathfrak{p}^\times)$.

Since Γ is a subgroup of $PSL(2, \boldsymbol{R})$, Γ acts on $\mathfrak{H}$ in the usual manner. Let z be a point of $\mathfrak{H}$, and let $\Gamma_z=\{\gamma\in\Gamma|\gamma z=z\}$. If Γ_z is an infinite group, then we denote by $\{z\}_\Gamma$ the Γ-equivalence class of $z\in\mathfrak{H}$. Let $\mathscr{P}(\Gamma)$ be the set of all such Γ-equivalence classes $\{z\}_\Gamma$.

Let z be a point of $\mathfrak{H}$ with an infinite group Γ_z. Then, by Ihara [8], Vol. 1, p. 17, Corollary, Γ_z is the product of a finite group and an infinite cyclic group. Let γ_z be a generator of the infinite cyclic part of Γ_z, and let $\{\rho_z, \rho_z^{-1}\}$ be the set of eigen values of γ_z. Then ρ_z belongs to $F_\mathfrak{p}$ and ρ_z is not a $\mathfrak{p}$-adic unit (cf. ibid., Vol. 1, p. 17, Corollary). Hence we define the *degree* $\deg\{z\}_\Gamma$ of $\{z\}_\Gamma$ by the absolute value of the $\mathfrak{p}$-adic order of ρ_z. Put

$$Z(\Gamma\,;\, u)=\prod_{P\in\mathscr{P}(\Gamma)}(1-u^{\deg P})^{-1}.$$

Then the following theorem is a special case of Theorem 1 of Ihara [8], Vol. 1, p. 21.

THEOREM Z. *Let the notation and assumptions be as above. We assume further that Γ is torsion free. Then $Z(\Gamma\,;\, u)$ has the following form*:

$$Z(\Gamma\,;\, u)=\frac{\prod_{i=1}^{g}(1-\rho_i u)(1-\rho_i' u)}{(1-u)(1-q^2u)}\times(1-u)^{(q-1)(g-1)},$$

where q is the number of the residue field of $\mathfrak{p}$ (i.e. $q=N\mathfrak{p}$), g is the genus of $\Gamma^0\backslash\mathfrak{H}$, and the ρ_i and ρ_i' are algebraic integers satisfying $\rho_i\rho_i'=q^2$, $|\rho_i|$, $|\rho_i'|\leqq q^2$ and $\rho_i\neq 1$, q^2.

Let π be a prime element of $\mathfrak{p}$, and let

$$\Gamma^l=\Gamma\cap PSL(2, \mathfrak{r}_{F_\mathfrak{p}})\begin{pmatrix}\pi^l & 0\\ 0 & \pi^{-l}\end{pmatrix}PSL(2, \mathfrak{r}_{F_\mathfrak{p}})$$

for each non-negative integer l. Then, by the theory of elementary divisors, Γ is the disjoint union of the Γ^l $(l=0, 1, 2, \cdots)$. Let $\{z\}_\Gamma$ be an element of $\mathscr{P}(\Gamma)$, and let γ_z be as before. We define the *length* $l\{z\}_{\Gamma^0}$ of the Γ^0-equivalence class of z by the integer l satisfying $\gamma_z\in\Gamma^l$. Then, by Theorem 2 of Ihara [8], Vol. 2, p. 27, $P=\{z\}_\Gamma$ contains exactly $\deg P$ Γ^0-equivalence classes $\{z\}_{\Gamma^0}$ with $l\{z\}_{\Gamma^0}=\deg P$, and the degree of any other Γ^0-equivalence class is greater than $\deg P$.

Let z, γ_z, ρ_z be as before. Then $M_z=F(\rho_z)$ is a totally imaginary quadratic extension of F contained in $\boldsymbol{C}$, and $\mathfrak{p}$ is decomposed in M_z. Further $\rho_z\mapsto\gamma_z$ or $\rho_z^{-1}\mapsto\gamma_z$ induces a normalized F-linear isomorphism of M_z into B.

Conversely, let M be a totally imaginary quadratic extension of F contained in $\boldsymbol{C}$, and let f be a normalized F-linear isomorphism of M into B such that $\mathfrak{p}$ is decomposed in M as $\mathfrak{p}=\mathfrak{q}\bar{\mathfrak{q}}$. Since S is an open subgroup of G_{A+} containing $G_{\infty+}\cdot\mathfrak{o}_{\mathfrak{p}}^{\times}$, there exist a positive integer d and an element γ of $\bar{\Gamma}=G_{\boldsymbol{Q}+}\cap(SG_{\mathfrak{p}})$ such that γ is contained in $f(M^{\times})$ and $f^{-1}(\gamma)$ generates the ideal $(\mathfrak{q}\bar{\mathfrak{q}}^{-1})^{d}$. Since any power of γ fixes the unique common fixed point z of $f(M^{\times})$, Γ_z is an infinite group. It is easy to see that $\deg\{z\}_{\Gamma}$ is the smallest integer d such that $(\mathfrak{q}\bar{\mathfrak{q}}^{-1})^{d}=f^{-1}(\gamma)\,\mathfrak{r}_M$ with $\gamma\in F_{\mathfrak{p}}^{\times}(f(M^{\times})\cap SB_{\mathfrak{p}}^{\times})$. Furthermore, since $l\{z\}_{\Gamma^0}$ is the smallest positive integer l satisfying $\pi^{l}\gamma_z\in\mathfrak{o}_{\mathfrak{p}}$, $l\{z\}_{\Gamma^0}=\deg\{z\}_{\Gamma}$ holds iff $f(\mathfrak{q}^{2d})\subseteqq\mathfrak{o}_{\mathfrak{p}}$. This condition is satisfied iff f induces an optimal embedding of $\mathfrak{r}_{M_{\mathfrak{p}}}\cong\mathfrak{r}_{F_{\mathfrak{p}}}\oplus\mathfrak{r}_{F_{\mathfrak{p}}}$ into $\mathfrak{o}_{\mathfrak{p}}$.

Let $\mathscr{C}(\mathfrak{p})$ be as in 1–2. Hence $\mathscr{C}(\mathfrak{p})$ is the set consisting of all points z on $\mathfrak{H}$ such that (i) there exist a totally imaginary quadratic extension M of F contained in $\boldsymbol{C}$, and a normalized F-linear embedding f of M into B such that z is the unique common fixed point of $f(M^{\times})$, (ii) $\mathfrak{p}$ is decomposed in M as $\mathfrak{p}=\mathfrak{q}\bar{\mathfrak{q}}$, and (iii) f induces an injection of $\mathfrak{r}_{M_{\mathfrak{p}}}\cong\mathfrak{r}_{F_{\mathfrak{p}}}\oplus\mathfrak{r}_{F_{\mathfrak{p}}}$ into $\mathfrak{o}_{\mathfrak{p}}$. *Let $\mathscr{C}(S,\mathfrak{p})$ be the set of all Γ_S-equivalence classes of all $z\in\mathscr{C}(\mathfrak{p})$.* For every $P=\{z\}_{\Gamma_S}$ of $\mathscr{C}(S,\mathfrak{p})$, let $\deg P$ be the smallest positive integer d such that there exists an element γ of $F_{\mathfrak{p}}^{\times}(f(M^{\times})\cap SB_{\mathfrak{p}}^{\times})$ satisfying $f^{-1}(\gamma)\,\mathfrak{r}_M=(\mathfrak{q}\bar{\mathfrak{q}}^{-1})^{d}$. Then we have proved:

PROPOSITION 1. *Let the notation and assumptions be as above. For every positive integer m, let*

$$N_m=\sum_{\substack{P\in\mathscr{C}(S,\mathfrak{p})\\ \deg P|m}}\deg P.$$

Then we have

$$\log Z(\Gamma_{S_{\mathfrak{p}}}\,;\,u)=\sum_{m=1}^{\infty}\frac{N_m}{m}u^m.$$

COROLLARY. *Let N_m be as in Proposition* 1. *We assume that $\Gamma_{S_{\mathfrak{p}}}$ is torsion free. Then*

$$\exp\left\{\sum_{m=1}^{\infty}\frac{N_m}{m}u^m\right\}(1-u)^{-(q-1)(g-1)}=\frac{\prod_{i=1}^{g}(1-\rho_i u)(1-\rho_i' u)}{(1-u)(1-q^2u)},$$

where g, q, ρ_i, ρ_i' are as in Theorem Z.

3-2. Calculation of congruence zeta functions, I. Let the notation and assumptions be as in § 1. Hence K is a totally imaginary quadratic extension of F contained in $\boldsymbol{C}$, $\tau_1,\cdots,\tau_g$ are extensions of $\tau_{01},\cdots,\tau_{0g}$, and

$L=B\otimes_F K$. Let $\mathfrak{p}$ be a prime ideal of F which does not divide $D(B/F)$. Let p be the prime number divisible by $\mathfrak{p}$, and let $p=\mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_t^{e_t}$ ($\mathfrak{p}_1=\mathfrak{p}$) be the factorization of p in F. Let $\mathfrak{P}$ be an extension of $\mathfrak{p}$ to a place of $\overline{\boldsymbol{Q}}$. *We assume hereafter that* (a) *each* $\mathfrak{p}_i$ $(i=1,\cdots,t)$ *is decomposed in* K *as* $\mathfrak{p}_i=\mathfrak{P}_i\overline{\mathfrak{P}}_i$, (b) $\tau_1=\mathrm{id}.$ *and none of the* $\overline{\mathfrak{P}}_i^{\tau_\nu}$ $(i=1,\cdots,t,\ \nu=1,\cdots,g)$ *is contained in* $\mathfrak{P}$, (c) K *has no root of unity other than* ± 1, (d) K *is generated over* $\boldsymbol{Q}$ *by* $\sum_{\nu=2}^{g} x^{\tau_\nu}$ *for all* $x\in K$ *if* $F\neq\boldsymbol{Q}$, *and* (e) *there exists a prime ideal of* F *which is ramified in* K *and which does not divide* $2D(B/F)$. By the proof of Shimura [22], Proposition 7.6, for a given natural number m, there exist infinitely many $(K,\tau_1,\cdots,\tau_g)$ satisfying (a)$\sim$(e) and (f) all prime divisors of m are completely decomposed in K/F. We note that (d) implies $K'=K$ if $F\neq\boldsymbol{Q}$ (cf. Shimura [22], 5.14.7).

Let $\mathfrak{M}=\mathfrak{r}_K\otimes_{\mathfrak{r}_F}\mathfrak{o}$, and let $S(b,c)$ be as in 1-3. Hence *we assume that* $S(b,c)$ *satisfies the conditions* (i)$\sim$(iii) *in* 1-3. Since $\Gamma^*(\mathfrak{M},b)$ is torsion free, $b\geqq 3$. Hence the condition (iii) implies that Γ_S $(S=S(b,c))$ is torsion free. *We assume further that* (iv) c *is prime to* p *and* (v) $\Gamma_{S_\mathfrak{p}}$ *is contained in* $PSL(2,\boldsymbol{R})\times PSL(2,F_\mathfrak{p})$ (cf. [1]). Then the condition (iv) implies that $S(b,c)\supset\mathfrak{o}_p^\times$. Hence we can apply the result of 3-1 to the group $\Gamma_{T_\mathfrak{p}}(T=x^{-1}S(b,c)\,x)$ for any element x of G_{A+} whose projection to G_p belongs to $\mathfrak{o}_p^\times$.

Let K_c be the class field over K which corresponds to $K^\times\cdot\{h\in K_A^\times\,|\,h\equiv 1 \bmod_0(c)\}$ of $K_A^\times$ by class field theory. Let $\mathfrak{P}_c$ be the restriction of $\mathfrak{P}$ to K_c, let $\mathfrak{r}_c$ be the maximal order of K_c, let $\tilde{K}_c$ be the residue field of $\mathfrak{P}_c$, and let f be the residue degree of $\mathfrak{P}_c/\mathfrak{p}$. Then K_c is normal over F, $\mathfrak{P}$ is unramified in K_c/F, and $\mathfrak{p}^f$ is generated by an element ε of $F_+^\times$ satisfying $\varepsilon\equiv 1 \bmod^* c$. *Let* K_c^* *be a quadratic extension of* K_c *such that* K_c^* *is normal over* F *and* $\mathfrak{P}_c$ *remains prime in* K_c^*/K_c. Let $\mathfrak{P}_c^*=\mathfrak{P}|K_c^*$, let $\mathfrak{r}_c^*$ be the valuation ring of $\mathfrak{P}_c^*$, and let $\tilde{K}_c^*$ be the residue field of $\mathfrak{P}_c^*$.

Put $U=\{x\in G_{A+}\,|\,\mathfrak{o}x=\mathfrak{o}\}$. Let $\boldsymbol{X}=\{x_1,\cdots,x_h\}$ be a set of representatives of $U\backslash G_{A+}/G_{\boldsymbol{Q}+}$, and let $\boldsymbol{F}=\{f_1,\cdots,f_{h'}\}$ be a set of representatives of $\{x\in K_A^\times\,|\,x\mathfrak{r}_K=\mathfrak{r}_K\}\cdot F_A^\times\backslash K_A^\times/K$. *We assume that* $x_1,\cdots,x_h,f_1,\cdots,f_{h'}$ *are prime to* cp. Then $f_\mu\mathfrak{M}x_\lambda/bf_\mu\mathfrak{M}x_\lambda=\mathfrak{M}/b\mathfrak{M}$ for any $f_\mu\in\boldsymbol{F}$ and $x_\lambda\in\boldsymbol{X}$. For any $f_\mu\in\boldsymbol{F}$ and $x_\lambda\in\boldsymbol{X}$, let $\beta_{\lambda\mu}$ be a totally positive element of F satisfying

$$\mathrm{tr}_{L/\boldsymbol{Q}}\left\{\beta_{\lambda\mu}T(f_\mu\mathfrak{M}x_\lambda,\ f_\mu\mathfrak{M}x_\lambda)\right\}=\boldsymbol{Z}\,.$$

Put $\Gamma_\lambda=\{\gamma\in x_\lambda^{-1}\mathfrak{o}x_\lambda\,|\,N_{B/F}(\gamma)=1\}$, and let $\mathfrak{T}_\lambda(b)=\{t \bmod \mathfrak{M}x_\lambda\,|\,t\in L,\ b^{-1}\mathfrak{M}x_\lambda=\mathfrak{M}x_\lambda+\mathfrak{M}x_\lambda t\}/\Gamma_\lambda$. Let $\mathfrak{T}(b)$ be the disjoint union of the $\mathfrak{T}_\lambda(b)\,(\lambda=1,\cdots,h)$. Let $\{s_1,\cdots,s_v\}$ be a $\boldsymbol{Z}$-basis of $\mathfrak{M}$, *let* $\Omega_{\lambda\mu t}=(\beta_{\lambda\mu},f_\mu\mathfrak{M}x_\lambda,\{f_\mu s_j x_\lambda t\})$ *be as in* 1-3 *for any* $x_\lambda\in\boldsymbol{X}$, $f_\mu\in\boldsymbol{F}$ *and* $t\in\mathfrak{T}_\lambda(b)$, *and let* $\Sigma(b)$ *be the union of all the* *families* $\Sigma(\Omega_{\lambda\mu t})$. Then $\Omega_{\lambda\mu t}$ is not equivalent to $\Omega_{\lambda'\mu't'}$ if $(\lambda,\mu,t)\neq(\lambda',\mu',t')$. For every triple (λ,μ,t), we fix a set of representatives of $\{\gamma\in\Gamma_\lambda|\gamma\equiv 1 \bmod_0(x_\lambda^{-1}\mathfrak{o}x_\lambda, b)\}\backslash\mathscr{C}(\mathfrak{p})$. Let $\mathscr{C}^*_{\lambda\mu t}(b,\mathfrak{p})$ be the subset of $\Sigma(\Omega_{\lambda\mu t})$ consisting of all $\mathscr{Q}_z$ such that z belongs to the representatives, and let $\mathscr{C}^*(b,\mathfrak{p})$ be the disjoint union of all $\mathscr{C}^*_{\lambda\mu t}(b,\mathfrak{p})$ $(\lambda=1,\cdots,h,\ \mu=1,\cdots,h',\ t\in\mathfrak{T}_\lambda(b))$.

Let $\mathfrak{P}$ be as before. We extend $\mathfrak{P}$ to a place of $\boldsymbol{C}$ and denote it by the same $\mathfrak{P}$. Let $\mathscr{Q}$ be any element of $\Sigma(b)$. If $\mathscr{Q}$ has good reduction at $\mathfrak{P}$, we denote by $\widetilde{\mathscr{Q}}$ reduction modulo $\mathfrak{P}$ of $\mathscr{Q}$. Let $\mathscr{F}^*_{\lambda\mu t}(b,\mathfrak{p})$ be the set consisting of all isomorphism classes of $\widetilde{\mathscr{Q}}(\mathscr{Q}\in\Sigma(\Omega_{\lambda\mu t}))$ such that $\widetilde{\mathscr{Q}}$ can be defined over a finite field, and let $\mathscr{F}^*(b,\mathfrak{p})$ be the union of all $\mathscr{F}^*_{\lambda\mu t}(b,\mathfrak{p})$. Then, by *the results of* [13], (i) reduction modulo $\mathfrak{P}$ induces an injection ι of $\mathscr{C}^*(b,\mathfrak{p})$ to $\mathscr{F}^*(b,\mathfrak{p})$, and (ii) the number of elements of $\mathscr{F}^*(b,\mathfrak{p})\backslash\iota\{\mathscr{C}^*(b,\mathfrak{p})\}$ is finite, and equal to $\sum_\lambda|\boldsymbol{F}|\ |\mathfrak{T}_\lambda(b)|(N_{F/\boldsymbol{Q}}(\mathfrak{p})-1)(g_{b\lambda}-1)$, where $|*|$ denotes the cardinality of $*$ and $g_{b\lambda}$ is the genus of $\Gamma^*(\mathfrak{M}\mathrm{x}_\lambda, b)\backslash\mathfrak{H}=\{\gamma\in\Gamma_\lambda|\gamma\equiv 1 \bmod^0 (x_\lambda^{-1}\mathfrak{o}x_\lambda, b)\}\backslash\mathfrak{H}$. Further, (iii) for any element $\widetilde{\mathscr{Q}}$ of $\mathscr{F}^*(b,\mathfrak{p})\backslash\iota\{\mathscr{C}^*(b,\mathfrak{p})\}$ and for any totally imaginary quadratic extension M of F contained in $\boldsymbol{C}$ such that $\mathfrak{p}$ is not decomposed in M, there exists a triple (M,f,z) such that (a) f is a normalized F-linear isomorphism of M into B, (b) z is the unique common fixed point of $f(M^\times)$, (c), at least for one (λ,μ,t), the element $\mathscr{Q}_z\in\Sigma(\Omega_{\lambda\mu t})$ has good reduction at $\mathfrak{P}$ and $\mathscr{Q}_z$ modulo $\mathfrak{P}$ is isomorphic to $\widetilde{\mathscr{Q}}$. Furthermore, (iv) for any totally imaginary quadratic extension M of F contained in $\boldsymbol{C}$, and for any such triple (M,f,z), reduction modulo $\mathfrak{P}$ of $\mathscr{Q}_z\in\Sigma(\Omega_{\lambda\mu t})$ belongs to $\{\mathscr{C}^*(b,\mathfrak{p})\}$ (resp. $\mathscr{F}^*(b,\mathfrak{p})\backslash\iota\{\mathscr{C}^*(b,\mathfrak{p})\}$) iff $\mathfrak{p}$ is decomposed in M/F (resp. $\mathfrak{p}$ is not decomposed in M/F).

Let $\Omega_{\lambda\mu t}$ be as above. Since $b\geqq 3$, we can apply Theorem 1 to this PEL type $\Omega_{\lambda\mu t}$. Let $\mathscr{S}(\Omega_{\lambda\mu t})$ and $S(\Omega_{\lambda\mu t})$ be as in Theorem 1. Let $I=\{i=(\lambda,\mu,t)|1\leqq\lambda\leqq h,\ 1\leqq\mu\leqq h',\ t\in\mathfrak{T}_\lambda(b)\}$, and put $\Omega_i=\Omega_{\lambda\mu t}$, $k_i=k_{\Omega_i}$, $\mathfrak{r}_i=\mathfrak{r}_{k_i}$, $\mathscr{S}_i=\mathscr{S}(\Omega_i)$, $S_i=S(\Omega_i)$ and $\phi_i=\phi_{\Omega_i}$. Then the $k_i(i\in I)$ are contained in K_c.

Let $\leqq$ be a linear order of I, let 1 be the smallest element of I, and, for each $i\in I$, let $\mathscr{S}_i^{**}$ be the subset of $\mathscr{S}_i$ consisting of all elements which are isomorphic to some elements of $\mathscr{S}_j$ with $j\in I$, $j\lneqq i$. Since Ω_i is not equivalent to any Ω_j $(j\neq i)$, $\mathscr{S}_i^{**}$ contains no PEL-structure defined over a field of characteristic 0. It is obvious that $\mathscr{S}_i^{**}$ is stable by $\mathfrak{r}_c$-operations of discrete places and automorphisms. Hence $\phi_i(\mathscr{S}_i^{**})$ defines a closed $\mathfrak{r}_c$-subscheme S_i^{**} of $S_i^*=S_i\times_{Spec(\mathfrak{r}_i)}Spec(\mathfrak{r}_c)$. It is obvious that $S_i^{**}\cap(S_i^*\times_{Spec(\mathfrak{r}_i)}Spec(K_c))=\phi$ and $\phi=\coprod_i\phi_i$ induces a bijective map of $\coprod_i(\mathscr{S}_i\backslash\mathscr{S}_i^{**})$ to $\coprod_i$ {geometric points of $S_i^*\backslash S_i^{**}$}. In particulaı, ϕ induces an injective map of

$\mathscr{S}^*(b,\mathfrak{p})$ to the set $\mathscr{S}(b,\mathfrak{p})$ of all $\bar{\boldsymbol{F}}_p$-valued points of $\coprod_i (S_i^*\backslash S_i^{**})\times_{Spec(\mathfrak{r}_c)} Spec(\tilde{K}_c)$. Since any $\bar{\boldsymbol{F}}_p$-valued point of S_i can lifted to a $\bar{\boldsymbol{Q}}$-valued point of S_i (cf. § 2 and Mumford [15], Chap. 2, § 8, Theorem 1), this map is surjective. Hence $\psi:\mathscr{S}^*(b,\mathfrak{p})\to\mathscr{S}(b,\mathfrak{p})$ is bijective, and commutes with the actions of $\mathrm{Gal}(\bar{\boldsymbol{F}}_p/\tilde{K}_c)$.

Let $\mathscr{C}^*(b,\mathfrak{p})=\coprod_{\lambda,\mu,t}\mathscr{C}^*_{\lambda\mu t}(b,\mathfrak{p})$ and $\iota:\mathscr{C}^*(b,\mathfrak{p})\to\mathscr{S}^*(b,\mathfrak{p})$ be as before. Let $\mathscr{A}$ be an element of $\mathscr{C}^*_{\lambda\mu t}(b,\mathfrak{p})$. Let σ be an element of $\mathrm{Gal}(\bar{\boldsymbol{Q}}/K_c)$ which belongs to the decomposition group of $\mathfrak{P}$, and let $\tilde{\sigma}$ be $\sigma \bmod \mathfrak{P}\in\mathrm{Gal}(\bar{\boldsymbol{F}}_p/K_c)$. Then $\mathscr{A}^\sigma$ belongs to $\mathscr{C}^*_{\lambda\mu t}(b,\mathfrak{p})$ because $K_c\supseteqq k_i$ $(i\in I)$ and $\mathscr{A}$ and $\mathscr{A}^\sigma$ are conjugate over K_c. It follows from the injectivity of ι and ψ that the following six conditions are equivalent: (a) $\psi(\mathscr{A})^\sigma=\psi(\mathscr{A})$; (b) $\psi(\mathscr{A}^\sigma)=\psi(\mathscr{A})$; (c) $\mathscr{A}^\sigma\cong\mathscr{A}$; (d) $\widetilde{\mathscr{A}^\sigma}\cong\widetilde{\mathscr{A}}$; (e) $\psi(\widetilde{\mathscr{A}^\sigma})=\psi(\widetilde{\mathscr{A}})$; (f) $\psi(\widetilde{\mathscr{A}})^{\tilde{\sigma}}=\psi(\widetilde{\mathscr{A}})$. Hence $\psi(\mathscr{A})^\sigma=\psi(\mathscr{A})$ iff $\psi(\widetilde{\mathscr{A}})^{\tilde{\sigma}}=\psi(\widetilde{\mathscr{A}})$. As we noted in 1-3, there exists an isomorphism h_T of the canonical model V_T of $\Gamma_T\backslash\mathfrak{H}$ $(T=x_\lambda^{-1}S(b,c)x_\lambda)$ to $S(\Omega_{\lambda\mu t})\times_{Spec(\mathfrak{r}_i)} Spec(K_c)$ defined over K_c. Hence $\psi(\widetilde{\mathscr{A}})^{\tilde{\sigma}}=\psi(\widetilde{\mathscr{A}})$ iff $(h_T^{-1}\circ\psi)(\mathscr{A}^\sigma)=(h_T^{-1}\circ\psi)(\mathscr{A})$.

Let (z,M,f) be the triple corresponding to an element of $\mathscr{C}^*_{\lambda\mu t}(b,\mathfrak{p})$. Hence M is a totally imaginary quadratic extension of F contained in $\boldsymbol{C}$, f is a normalized F-linear embedding of M into B, and z is the unique common fixed point of $f(M^\times)$ on $\mathfrak{H}$. Let $\mathfrak{p}=\mathfrak{q}\bar{\mathfrak{q}}$ $(\mathfrak{q}\subseteqq\mathfrak{P})$ be the factorization of $\mathfrak{p}$ in M, and let u be the idele of $M_A^\times$ corresponding to $\mathfrak{q}$. Then $[u] \bmod \mathfrak{P}$ generates the Galois group of $\bar{\boldsymbol{F}}_p$ over the residue field $\tilde{F}$ of $\mathfrak{p}$. Hence, for any even power $\sigma=[u]^{2m}$ of $[u]$, $\tilde{\sigma}$ is trivial on $\tilde{K}_c^*$ and $\psi(\widetilde{\mathscr{A}})^{\tilde{\sigma}}=\psi(\widetilde{\mathscr{A}})$ iff $[\tilde{K}_c^*:\tilde{F}]=2f$ divides $2m$ and $\varphi_T(z)^\sigma=\varphi_T(z)$. By 3. 5. 1 (and 3. 7) of Shimura [24], this condition is satisfied iff $f|m$ and $f(u^{2m})=\delta t$ with $\delta\in f(M^\times)$ and $t\in T$. Let ε be as before. Then $\gamma=\varepsilon^{-m/f}\delta=f(\varepsilon^{-m/f}u^{2m})t^{-1}\in f(M^\times)\cap TB_\mathfrak{p}^\times$ and $f^{-1}(\gamma)\mathfrak{x}_M=(\mathfrak{q}\bar{\mathfrak{q}}^{-1})^m$. Conversely, if there exists $\gamma\in f(M^\times)\cap TB_\mathfrak{p}^\times$ such that $f|m$ and $f^{-1}(\gamma)\mathfrak{x}_M=(\mathfrak{q}\bar{\mathfrak{q}}^{-1})^m$, then $\delta=\varepsilon^{m/f}\gamma\in f(M^\times)$ and $t=\gamma^{-1}f(\varepsilon^{-m/f}u^{2m})\in T\mathfrak{o}_\mathfrak{p}^\times=T$. It follows from the definition of $\deg P=\deg\{z\}_\Gamma$ (cf. 3-1) that $[\tilde{K}_c^*(\psi(\widetilde{\mathscr{A}})):\tilde{K}_c^*]=\deg P/(\deg P,f)$.

If $\widetilde{\mathscr{A}}$ is an element of $\mathscr{S}^*(b,\mathfrak{p})\backslash\iota\{\mathscr{C}^*(b,\mathfrak{p})\}$, then, for any totally imaginary quadratic extension M of F contained in $\boldsymbol{C}$ such that $\mathfrak{p}$ remains prime in M/F, let (z,M,f) and $\mathscr{A}_z\in\Sigma(\Omega_{\lambda\mu t})$ be as before. Let σ be the f-th power of the Frobenius automorphism for $\mathfrak{p}\mathfrak{x}_K$. Then σ generates the Galois group of $\bar{\boldsymbol{F}}_p$ over $\tilde{K}_c^*$ and $\mathfrak{p}^f$ is generated by the element ε of $F_+^\times\cap T$. Hence, by Theorem C, $\varphi_T(z)^\sigma=\varphi_T(z)$. Hence $\psi(\mathscr{A})^\sigma=\psi(\mathscr{A})$. Therefore $\psi(\widetilde{\mathscr{A}})$ is rational over $\tilde{K}_c^*$. Since $\mathscr{S}^*(b,\mathfrak{p})\backslash\iota\{\mathscr{C}^*(b,\mathfrak{p})\}$ contains exactly $\sum_\lambda|\boldsymbol{F}|\,|\mathfrak{T}_\lambda(b)|(N_{F/\boldsymbol{Q}}(\mathfrak{p})-1)(g_{b\lambda}-1)$ elements, it follows from the bijectivity of $\psi:\mathscr{S}^*(b,\mathfrak{p})\to$

$\mathscr{T}(b, \mathfrak{p})$ that the number N_m^* of $\boldsymbol{F}_{q^{2fm}}$-rational points ($f=[\tilde{K}_c:\tilde{F}]$) of $\coprod_i (S_i^*\backslash S_i^{**})\times_{Spec(\mathfrak{r}_c)} Spec(\tilde{K}_c^*)$ is given by

$$N_m^* = \sum_{\lambda,\mu,t}\Big[\sum_{\substack{P\in\mathscr{C}(x_\lambda^{-1}Sx_\lambda,\mathfrak{p})\\ \deg P/(\deg P,f)\mid m}} \deg P + \big(N_{F/\boldsymbol{Q}}(\mathfrak{p})-1\big)(g_{b\lambda}-1)\Big].$$

Hence, by the corollary of Proposition 1, we have:

PROPOSITION 2. *The congruence zeta function* $Z(u)=\exp\left\{\sum_{m=1}^{\infty}\frac{N_m^*}{m}u^m\right\}$ *of the algebraic set* $\coprod_i (S_i^*\backslash S_i^{**})\times_{Spec(\mathfrak{r}_c)} Spec(\tilde{K}_c^*)$ *is*

$$\prod_{\lambda=1}^{h}\left\{\prod_{i=1}^{g_{b\lambda}}(1-\rho_{\lambda i}^f u)\big(1-(\rho'_{\lambda i})^f u\big)\Big/(1-u)(1-q^{2f}u)\right\}^{h'|\mathfrak{T}_\lambda(b)|},$$

where the $\rho_{\lambda i}$ *and the* $\rho'_{\lambda i}$ *are the roots of* $Z(\Gamma_{x_\lambda^{-1}Sx_\lambda,\mathfrak{p}};\ u)$ (*cf. Theorem Z*).

3-3. Calculation congruence zeta functions, II. Let $\mathfrak{r}=\mathfrak{r}_{c\mathfrak{P}}^*$ be the valuation ring of $\mathfrak{P}\cap K_c^*$. Let $S_i'=S_i^*\times_{Spec(\mathfrak{r}_c)} Spec(\mathfrak{r}_{c\mathfrak{P}}^*)$ and $S_i'^*=S_i^{**}\times_{Spec(\mathfrak{r}_c)} Spec(\mathfrak{r}_{c\mathfrak{P}}^*)$. It is obvious that $\coprod_i (S_i'\backslash S_i'^*)\times_{Spec(\mathfrak{r})} Spec(\tilde{K}_c^*)$ is a Zariski open $\tilde{K}_c^*$-rational subset of a purely one dimensional $\tilde{K}_c^*$-rational cycle in a projective space. Since $\rho_{\lambda i}\rho'_{\lambda i}=q^2$, the reduced denominator of $Z(u)$ is a power of $(1-u)(1-q^{2f}u)$. It follows from the results of Weil [27] that *each geometrically irreducible component of* $\coprod_i (S_i'\backslash S_i'^*)\times_{Spec(\mathfrak{r})} Spec(\tilde{K}_c^*)$ *is rational over* $\tilde{K}_c^*$. Since $Z(u)$ is the congruence zeta function of a Zariski open subset of a one dimensional cycle, $\rho=\rho_{\lambda i}^f$ or $(\rho'_{\lambda i})^f$ satisfies (i) $|\rho|=1$, or (ii) $|\rho|=q^f$ or (iii) $\rho=p^{2f}$. Since $\rho_{\lambda i}\rho'_{\lambda i}=q^2$, it follows that $|\rho|=1$ holds iff $\rho=1$. Hence no root of the reduced numerator of $Z(u)$ is a root of unity. It follows that *each connected component of* $\coprod_i (S_i'\backslash S_i'^*)\times_{Spec(\mathfrak{r})} Spec(\tilde{K}_c^*)$ *is proper and geometrically irreducible*, and that *no two connected components intersect.* Furthermore no root of the numerator of the congruence zeta function of each component is a root of unity.

Since S_i' is quasi-projective, we can define the Zariski closure $\bar{S}_i'$ of S_i'. Since $S_i'\times_{Spec(\mathfrak{r})} Spec(K_c^*)$ is a geometrically irreducible proper curve, it follows from the *Zariski connection theorem* (cf. EGA, III, 4.3.1) that $\bar{S}_i'\times_{Spec(\mathfrak{r})} Spec(\tilde{K}_c^*)$ is connected. Since the $(S_i'\backslash S_i'^*)\times_{Spec(\mathfrak{r})} Spec(\tilde{K}_c^*)$ are open in $\coprod (S_i'\backslash S_i'^*)\times_{Spec(\mathfrak{r})} Spec(\tilde{K}_c^*)$, each $(S_i'\backslash S_i'^*)\times_{Spec(\mathfrak{r})} Spec(\tilde{K}_c^*)$ is a disjoint union of a finite number of proper geometrically irreducible curves. Hence $(S_i'\backslash S_i'^*)\times_{Spec(\mathfrak{r})} Spec(\tilde{K}_c^*)$ is open and closed in $\bar{S}_i'\times_{Spec(\mathfrak{r})} Spec(\tilde{K}_c^*)$. Therefore $(S_i'\backslash S_i'^*)\times_{Spec(\mathfrak{r})} Spec(\tilde{K}_c^*)$ is either ϕ or $\bar{S}_i'\times_{Spec(\mathfrak{r})} Spec(\tilde{K}_c^*)$. In particular, either $(S_i'\backslash S_i'^*)\times_{Spec(\mathfrak{r})} Spec(\tilde{K}_c^*)=\phi$ or $S_i'^*=\phi$.

Since $S_1'^*=\phi$, and since $S_1'\times_{Spec(\mathfrak{r})} Spec(\tilde{K}_c^*)\neq\phi$ (because each $\mathscr{Q}\in\mathscr{C}^*(b,\mathfrak{p})$ has good reduction at $\mathfrak{P}$ and determines a point of $S_1'\times_{Spec(\mathfrak{r})} Spec(\tilde{K}_c^*)$), it follows that $S_1'\times_{Spec(\mathfrak{r})} Spec(\tilde{K}_c^*)=\bar{S}_1'\times_{Spec(\mathfrak{r})} Spec(\tilde{K}_c^*)$. Hence *$S_1'$ is projective and $S_1'\times_{Spec(\mathfrak{r})} Spec(\tilde{K}_c^*)$ is geometrically irreducible.* Furthermore, by changing the order of I, we observe that each S_i' $(i\in I)$ has the same properties. In particular, any $\mathscr{Q}\in\Sigma(b)$ has good reduction at $\mathfrak{P}$.

Let $\varphi_i: S_i''\to S_i'$ be the normalization of S_i' in the function field at the generic point of S_i'. By EGA, II, 6. 3. 10, φ_i is a finite morphism. Hence S_i'' is projective over $Spec(\mathfrak{r})$. It is obvious that the general fibre of S_i'' is the complete non-singular model of the general fibre of S_i'. Hence there exists an isomorphism j_i'' of $V_T\times_{Spec(k_T)} Spec(K_c^*)$ onto $S_i''\times_{Spec(\mathfrak{r})} Spec(K_c^*)$ with $T=x_\lambda^{-1}S(b,c)\,x_\lambda$. Let $\tilde{S}_{i1}'',\cdots,\tilde{S}_{it}''$ be the irreducible components of $\tilde{S}_i''=S_i''\times_{Spec(\mathfrak{r})} Spec(\tilde{K}_c^*)$, and let $\tilde{\mathfrak{K}}_1,\cdots,\tilde{\mathfrak{K}}_t$ be the function fields at the generic points of $\tilde{S}_{i1}'',\cdots,\tilde{S}_{it}''$. Let e_{ij} (resp. $f_{ijs}r_{ij}$) (resp. r_{ij}) be the multiplicity of $\tilde{S}_{ij}''$ (resp. the separable degree of $\tilde{\mathfrak{K}}_j$ over the function field $\tilde{\mathfrak{K}}$ at the generic point $\tilde{S}_i'=S_i'\times_{Spec(\mathfrak{r})} Spec(\tilde{K}_c^*)$) (resp. the degree $[\tilde{\mathfrak{K}}_j\cap\bar{\boldsymbol{F}}_p:\tilde{\mathfrak{K}}\cap\bar{\boldsymbol{F}}_p]$). Then f_{ijs} is an integer. Let $g(\tilde{S}_i')$ be the genus of $\tilde{\mathfrak{K}}$. Then, by the Hurwitz formula, the genus $g(\tilde{S}_{ij}'')$ of $\tilde{\mathfrak{K}}_j$ satisfies $g(\tilde{S}_{ij}'')-1\geqq f_{ijs}(g(\tilde{S}_i')-1)$. Further, *by the result of Popp* [17],

$$\sum_{j=1}^{t} r_{ij}e_{ij}\left(g(\tilde{S}_{ij}'')-1\right)\leqq g_{b\lambda}-1\,.$$

Hence we have

$$\left(\sum_{j=1}^{t} r_{ij}e_{ij}f_{ijs}\right)\left(g(\tilde{S}_i')-1\right)\leqq g_{b\lambda}-1\,.$$

Since $g_{b\lambda}-1>0$, this implies $g(\tilde{S}_i')-1\leqq g_{b\lambda}-1$.

Let J be the set consisting of all $i\in I$ satisfying $(S_i'\backslash S_i'^*)\times_{Spec(\mathfrak{r})} Spec(\tilde{K}_c^*)\neq\phi$. Then it follows from our calculation of $Z(u)$ in 3-2 that

$$\sum_{i\in J}\left(2g(\tilde{S}_i')-2\right)=\sum_{i\in I}(2g_{b\lambda}-2)\,.$$

Since

$$\begin{aligned}\sum_{i\in J}\left(g(\tilde{S}_i')-1\right)&\leqq\sum_{i\in J}(g_{b\lambda}-1)\\ &=\sum_{i\in I}(g_{b\lambda}-1)-\sum_{i\in I\backslash J}(g_{b\lambda}-1)=\sum_{i\in J}\left(g(\tilde{S}_i')-1\right)-\sum_{i\in I\backslash J}(g_{b\lambda}-1)\,,\end{aligned}$$

we obtain $\sum_{i\in I\backslash J}(g_{b\lambda}-1)\leqq 0$. Since $g_{b\lambda}\geqq 2$, we obtain $I\backslash J=\phi$. Hence $I=J$.

Hence, for any $i\in I$,

$$g(\tilde{S}_i')-1\leqq g_{b\lambda}-1\quad\text{and}\quad\sum_{i\in I}\left(g(\tilde{S}_i')-1\right)=\sum_{i\in I}(g_{b\lambda}-1)\,.$$

It follows that $g(\tilde{S}'_i)-1=g_{b\lambda}-1>0$. Hence

$$\sum_{j=1}^{t} e_{ij} r_{ij} f_{ijs} \leqq 1 .$$

Therefore $t=1$, $e_{i1}=r_{i1}=f_{i1s}=1$. Hence $\tilde{S}''_i=S''_i \times_{Spec(\mathfrak{r})} Spec(\tilde{K}^*_c)$ is geometrically irreducible, the generic point of $\tilde{S}''_i$ is reduced, and φ_i induces a purely inseparable morphism $\tilde{\varphi}_i : \tilde{S}''_i \to \tilde{S}'_i$. Furthermore the genus $g(\tilde{S}''_i)$ of the function field at the generic point of $\tilde{S}''_i$ satisfies

$$g(\tilde{S}'_i)=g(\tilde{S}''_i)=g_{b\lambda} .$$

Hence the effective genus of the special fibre $\tilde{S}''_i=S''_i \times_{Spec(\mathfrak{r})} Spec(\tilde{K}^*_c)$ is equal to the effective genus of the general fibre $S''_i \times_{Spec(\mathfrak{r})} Spec(K^*_c)$. Since the general fibre is non-singular, it is also equal to the arithmetic genus of the general fibre. By the invariance of the Euler-Poincare characteristic (cf. e. g. EGA, III, 7. 94), it follows that the effective genus of the special fibre $\tilde{S}''_i$ is equal to the arithmetic genus of $\tilde{S}''_i$. Hence $\tilde{S}''_i$ is an absolutely irreducible projective non-singular curve defined over $\tilde{K}^*_c$ with genus $g_{b\lambda}=g_T$. Hence S''_i *is smooth and projective over* $Spec(\mathfrak{r}^*_{c\mathfrak{P}})$. In particular, S''_i is a stable curve over $Spec(\mathfrak{r}^*_{c\mathfrak{P}})$ (cf. Deligne-Mumford [3]).

Since $g(\tilde{S}'_i)=g_{b\lambda}$, the numerator of $Z(u)$ has $\sum_{i\in I} 2g_{b\lambda}$ roots ρ with $|\rho|=q^{-f}$. Hence $|\rho_{\lambda i}|=|\rho'_{\lambda i}|=q^f$. Furthermore the congruence zeta function $Z_i(u)$ of each $\tilde{S}'_i$ has the form

$$\prod_{j=1}^{g_{b\lambda}} (1-\rho_{ij}u)(1-\rho'_{ij}u)/(1-u)(1-q^{2f}u)$$

with $|\rho_{ij}|=|\rho'_{ij}|=q^f$, because $Z(u)=\prod_{i\in I} Z_i(u)$, $\tilde{S}'_i$ is geometrically irreducible and $g(\tilde{S}'_i)=g_{\lambda b}$. Since $\tilde{\varphi}_i : \tilde{S}''_i \to \tilde{S}'_i$ is a purely inseparable morphism, the congruence zeta function of $\tilde{S}''_i$ is also equal to $Z_i(u)$. Hence $\tilde{\varphi}_i$ *is one-to-one.* In particular, $\varphi_i^{-1}\circ\psi_i$ induces a bijective map of $\mathscr{T}^*_i(b, \mathfrak{p})$ to the set of all $\bar{\boldsymbol{F}}_p$-valued points of $\tilde{S}''_i$.

Since $I=J$, $(S_i \backslash S'^*_i) \times_{Spec(\mathfrak{r})} Spec(\tilde{K}^*_c) \neq \phi$ for each $i \in I$. Hence $S'^*_i=\phi$ for each $i \in I$. Hence $\mathscr{S}^{**}_i=\phi$ for each $i \in I$. Therefore $\mathscr{T}^*_i(b, \mathfrak{p}) \cap \mathscr{T}^*_j(b, \mathfrak{p})=\phi$ if $i \neq j$. This shows that *the results of* [13], *which we quoted in* 3-2, *hold if we restrict to each* PEL-*type* Ω_i. Therefore, by the bijectivity of $\varphi_i^{-1}\circ\psi_i$, S''_i and j''_i satisfy the conditions (ii)$\sim$(iii) of Main Theorem 1 for $\mathfrak{P}$. Therefore we have proved:

PROPOSITION 3. *There exist a smooth projective scheme* S''_i ($i=(\lambda, \mu, t) \in I$) *over the valuation ring* $\mathfrak{r}$ *of* $\mathfrak{P}|K^*_c$ *and an isomorphism* j''_i *of* $V_T \times_{Spec(k_T)} Spec(K^*_c)$ ($T=x_\lambda^{-1} S(b, c)\, x_\lambda$) *onto the general fibre* $S''_i \times_{Spec(\mathfrak{r})} Spec(K^*_c)$ *of* S''_i

such that S_i'' and j_i'' satisfy the conditions (ii) *and* (iii) *of Main Theorem* 1.

3-4. Proof of Main Theorem 1. Let b and c be positive integers such that $b\geqq 3$, $b|c$ and the pair (b, c) satisfies the conditions (i)$\sim$(iii) in 1-3 for every divisor a of b and for every K such that K has no roots of unity other than ± 1 and there exists a prime ideal of F such that it is ramified in K and does not divide $2D(B/F)$. Let $S=S(b, c)$ be as in 1-3, and let P_S be as in 1-2.

Since $S(b, c)\subseteqq S(\mathfrak{o}, b)$, an ideal $\mathfrak{q}$ of k_S belongs to P_S only if $\mathfrak{q}$ does not divide b. In this case, $\{x\in S(\mathfrak{o}, b)|\nu(x)=1\}$ contains $\{x_p\in\mathfrak{o}_p^\times|\nu(x)=1\}$, where $p=\mathfrak{q}\cap \boldsymbol{Q}$. Hence $S(b, c)\supseteqq \mathfrak{o}_p^\times$ iff $\mathfrak{q}\nmid b$ and $\nu(\{x_p\in\mathfrak{o}_p^\times|\mathfrak{o}_p(x_p-1)\subseteqq c\mathfrak{o}_p\})=\mathfrak{r}_{Fp}^\times$. Let $\mathfrak{p}=\mathfrak{q}\cap F$. Since $\mathfrak{p}\nmid D(B/F)$, $\nu(\{x_\mathfrak{p}\in\mathfrak{o}_\mathfrak{p}^\times|\mathfrak{o}_\mathfrak{p}(x_\mathfrak{p}-1)\subseteqq c\mathfrak{o}_\mathfrak{p}\})=\mathfrak{r}_{F_\mathfrak{p}}^\times$ iff $\mathfrak{p}$ does not divide c. Therefore $\mathfrak{q}\in P_S$ iff $\mathfrak{q}$ does not divide $cD(B/F)$. We note that $\mathfrak{q}$ *is unramified in k_T/F* in this case.

Let $\mathfrak{q}$ be an element of P_S, $\mathfrak{p}=\mathfrak{q}\cap F$, and let $\Gamma_{S_\mathfrak{p}}$ be as in 3-1. We assume that $\Gamma_{S_\mathfrak{p}}$ is contained in $PSL(2, \boldsymbol{R})\times PSL(2, F_\mathfrak{p})$. Then we claim that there exist a smooth projective scheme $W_{S_\mathfrak{q}}$ over the valuation ring $\mathfrak{r}_\mathfrak{q}=\mathfrak{r}_{S_\mathfrak{q}}$ of $\mathfrak{q}$ and an isomorphism $j_{S_\mathfrak{q}}$ of V_S onto $W_{S0}=W_{S_\mathfrak{q}}\times_{Spec(\mathfrak{r}_\mathfrak{p})} Spec(k_S)$ satisfying the conditions (i)$\sim$(iii) of Main Theorem 1 for this $\mathfrak{q}$ and for any extension $\mathfrak{P}$ of $\mathfrak{q}$ to an place of $\bar{\boldsymbol{Q}}$.

Let K, $\tau_1, \cdots, \tau_g$, L, $\mathfrak{p}_1, \cdots, \mathfrak{p}_t$, $\mathfrak{P}_1, \cdots, \mathfrak{P}_t$, etc. be as in 3-2. Hence we assume that the conditions (a)$\sim$(e) are satisfied. Let $\boldsymbol{X}=\{x_1, \cdots, x_h\}$, $\boldsymbol{F}=\{f_1, \cdots, f_{h'}\}$, $\mathfrak{T}_\lambda(b)$, $\mathfrak{T}(b)$, $I=\{i=(\lambda, \mu, t)\}$, the Ω_i etc. be as in 3-2. Let K_c be as before, and let K_c^* be a quadratic extension of K_c such that K_c^* is normal over F and $\mathfrak{P}|K_c$ remains prime in K_c^*/K_c. Let S_i'' and j_i'' be as in Proposition 3 for $S(b, c)$. We assume that $x_\lambda=1$ and $f_\mu=1$ for $1=(\lambda, \mu, t)$. Then S_1'' is a smooth projective scheme over the valuation ring $\mathfrak{r}$ of the restriction of $\mathfrak{P}$ to K_c^*, and j_1'' is an isomorphism of $V_S\times_{Spec(k_S)} Spec(K_c^*)$ onto the general fibre S_{10}'' of S_1''. Furthermore, S_1'' and j_1'' satisfy the conditions (ii) and (iii) of Main Theorem 1 for these $\mathfrak{q}$ and $\mathfrak{P}$

Let σ be an element of $\mathrm{Gal}(K_c^*/k_S)$. Then there exists an isomorphism $J_0(\sigma)$ of S_{10}'' to $(S_{10}'')^\sigma$, and these $J_0(\sigma)$ satisfy the cocycle condition for descent. Since the $(S_1'')^\sigma$ are stable curves over $\mathfrak{r}$, each $J_0(\sigma)$ extends to an isomorphism $J(\sigma)$ of S_1'' to $(S_1'')^\sigma$ (cf. Deligne-Mumford [3]). Since $Spec(\mathfrak{r})$ is etale over $Spec(\mathfrak{r}_\mathfrak{q})$, these $J(\sigma)$ give a descent deta. Hence, by the result of Grothendieck [6], 190, there exist a scheme $W_{S_\mathfrak{q}}$ over $Spec(\mathfrak{r}_\mathfrak{q})$ and an isomorphism j_S' of S_1'' to $W_{S_\mathfrak{q}}\times_{Spec(\mathfrak{r}_\mathfrak{q})} Spec(\mathfrak{r})$. Since $Spec(\mathfrak{r})\rightarrow Spec(\mathfrak{r}_\mathfrak{q})$ is faithfully flat and quasi-compact, and since S_1'' is smooth and proper over $Spec(\mathfrak{r})$, $W_{S_\mathfrak{q}}$ is proper and smooth over $Spec(\mathfrak{r}_\mathfrak{q})$. Since the general fibre of $W_{S_\mathfrak{q}}$ is an absolutely irreducible projective non-singular curve with genus g_S, the special fibre has the same property. Since the special fibre is projective, $W_{S_\mathfrak{q}}$ is projective over $Spec(\mathfrak{r}_\mathfrak{q})$ (cf. EGA, III, 4.7.1). Hence $W_{S_\mathfrak{q}}$ and $j_{S_\mathfrak{q}}=j'_S\circ j''_1$ satisfy the required conditions. Therefore the claim is proved.

Let T be any element of $\mathcal{Z}$. For each $\mathfrak{q}\in P_T$, let $\mathfrak{P}$ be as in 1-2. Since the problem is local, if, for each $\mathfrak{q}$, there exist a smooth projective scheme W^* over the valuation ring of $\mathfrak{q}$ and an isomorphism j^* of the canonical model V_T for T to the general fibre of W^* satisfying the conditions (i)$\sim$(iii) of Main Theorem 1 for $\mathfrak{P}$, then Main Theorem 1 holds for T. Let x_{Tp} be as in 1-2. If W^* and j^* satisfy these conditions for $x_{Tp}Tx_{Tp}^{-1}$ and $\mathfrak{q}$, then W^* and $j^*\circ x_{Tp}$ satisfy the conditions for T and $\mathfrak{q}$. Hence we assume that $T\supseteqq\mathfrak{o}_p^\times$, and prove the existence of such W^* and j^*.

Let $U=\{x\in G_{A+}|\mathfrak{M}x=\mathfrak{M}\}$. Then U is an element of $\mathcal{Z}$. Let $R=\bigcap_{x\in T}x(T\cap U)x^{-1}$ (cf. [24], 3.11). Then R is a normal subgroup of T satisfying $T\cap U\supseteqq R\supseteqq\mathfrak{o}_p^\times$. Since $R\supseteqq\mathfrak{o}_p^\times$ and $R\in\mathcal{Z}$, there exists a pair (b, c) of positive integers such that (a) $R\supseteqq S(b, c)$ and (b) (b, c) satisfies the conditions at the beginning of 3-4 for $\mathfrak{q}$ (cf. [1]). It is obvious that $S=S(b, c)$ is a normal subgroup of R.

Since S is normal in R, Γ_S is normal in Γ_R. Hence $V'_R=V_R\times_{Spec(k_R)} Spec(k_S)$ can be regarded as the quotient of V_S by $G=\{J_{SS}(\gamma)|\gamma\in\Gamma_R$ modulo $\Gamma_S\}$. Let $\mathfrak{r}_S=\mathfrak{r}_{S_{\mathfrak{q}^*}}$ and $\mathfrak{r}_R$ be the valuation rings of $\mathfrak{q}^*=\mathfrak{P}|k_S$ and $\mathfrak{P}|k_R$. Then there exist a smooth projective scheme $W_{S_{\mathfrak{q}^*}}$ over $Spec(\mathfrak{r}_S)$ and an isomorphism $j_{S_{\mathfrak{q}^*}}$ of V_S to the general fibre W_{S0} of $W_{S_{\mathfrak{q}^*}}$, and these $W_{S_{\mathfrak{q}^*}}$ and $j_{S_{\mathfrak{q}^*}}$ satisfy the conditions (ii) and (iii) of Main Theorem 1. Since $W_{S_{\mathfrak{q}^*}}$ is a stable curve, the $J_{SS}(\gamma)$ $(\gamma\in\Gamma_R/\Gamma_S)$ can be extended to elements of $\mathrm{Aut}(W_{S_{\mathfrak{q}^*}})$ Let W'^*_R be the quotient of $W_{S_{\mathfrak{q}^*}}$ by this finite group G (cf. Mumford [14] and Grothendieck [6], 212).

Since $W_{S_{\mathfrak{q}^*}}$ is of finite type over $Spec(\mathfrak{r}_S)$, W'^*_R is of finite type over $Spec(\mathfrak{r}_S)$. Since $W_{S_{\mathfrak{q}^*}}\to W'^*_R$ is surjective, W'^*_R is proper over $Spec(\mathfrak{r}_S)$ (cf. EGA, II, 5.53). Since $W_{S_{\mathfrak{q}^*}}\to W'^*_R$ is faithfully flat, and since $W_{S_{\mathfrak{q}^*}}\to Spec(\mathfrak{r}_S)$ is flat, $W'^*_R\to Spec(\mathfrak{r}_S)$ is flat (cf. EGA, IV, 2.2.13). Since $W_{S_{\mathfrak{q}^*}}$ is smooth over $Spec(\mathfrak{r}_S)$, $W_{S_{\mathfrak{q}^*}}$ is normal. Hence W'^*_R is normal. In particular, the general fibre W'^*_{R0} of W'^*_R is non-singular. Furthermore, *by the results of Lamprecht* [11] (cf. Definition 3, Satz 2 and Korollar 5), and by the definition of W'^*_R, the special fibre of W'^*_R is non-singular. Hence all geometric fibres of W'^*_R are non-singular. Since W'^*_R is flat over $Spec(\mathfrak{r}_S)$, W'^*_R is smooth over $Spec(\mathfrak{r}_S)$. Therefore W'^*_R is smooth and projective over $Spec(\mathfrak{r}_S)$. It is obvious that there is an isomorphism j'^*_R of V'_R to the general fibre of

$W_R'^*$, and that these V_R', φ_R, $j_R'^*$ and $W_R'^*$ satisfy the conditions (ii) and (iii) of Main Theorem 1.

Let σ be an element of $\mathrm{Gal}(k_S/k_R)$. Then there exists an isomorphism $J_0(\sigma)$ of V_R' to $V_R'^\sigma$, and these $J_0(\sigma)$ satisfy the cocycle condition for descent. Since the $(W_R'^*)^\sigma$ are stable curves over $Spec(\mathfrak{r}_S)$, each $J_0(\sigma)$ extends to an isomorphism $J(\sigma)$ of $W_R'^*$ to $(W_R'^*)^\sigma$. Since $F \subseteqq k_T \subseteqq k_S \subseteqq K_c$, $Spec(\mathfrak{r}_S)$ is etale over $Spec(\mathfrak{r}_R)$. Hence the $J(\sigma)$ give a descent deta for $Spec(\mathfrak{r}_S) \to Spec(\mathfrak{r}_R)$. Hence, by the result of Grothendieck [6], there exist a smooth projective scheme W_R^* over $Spec(\mathfrak{r}_R)$ satisfying $W_R^* \times_{Spec(\mathfrak{r}_R)} Spec(\mathfrak{r}_S) \cong W_R'^*$, and an isomorphism j_R^* of V_R to the general fibre of W_R^*. It is obvious that W_R^* and j_R^* satisfy the conditions (ii) and (iii) of Main Theorem 1.

Since R is a normal subgroup of T, and since $F \subseteqq k_T \subseteqq k_R \subseteqq K_c$, we can repeat the above arguments and construct W_T^* and j_T^* from W_R^* and j_R^*. Then these W_T^* and j_T^* satisfy the required conditions. Therefore *Main Theorem* 1 *holds in the general case.*

3-5. Proof of Main Theorem 2. Let the notation and assumptions be as in Main Theorem 2. Put $R = x^{-1}Tx$. Then $R \supseteqq S$ and $J_{TS}(x) = J_{TR}(x) \circ J_{SR}(1)$. Hence *the proof of Main Theorem* 2 *is reduced to the cases* (i) $x=1$ *and* (ii) $xSx^{-1} = T$.

We assume $x=1$ *and* $S \subseteqq T$. Then $j_T \circ J_{TS}(1) \circ j_S^{-1}$ induces a morphism of the general fibre W_{S0} of W_S to the general fibre W_{T0} of W_T. Let G_0 be the graph of this morphism. Since $x=1$, $\mathfrak{q}_T = \mathfrak{P} | k_T$ and $\nu(x) = 1$. Since $S \subseteqq T$, $\mathfrak{q} \in P_S$ implies $\mathfrak{q}_T = \mathfrak{q} | k_T \in P_T$. We assume $x_{Sp} = x_{Tp}$. Let G be the Zariski closure of G_0 in $W_S \times_{Spec(\mathfrak{r}_{S_\mathfrak{q}})} \{W_T \times_{Spec(\mathfrak{r}_T)} Spec(\mathfrak{r}_{S_\mathfrak{q}})\}$. Put $\tilde{G} = G \times_{Spec(\mathfrak{r}_{S_\mathfrak{q}})} Spec(\tilde{k}_{S_\mathfrak{q}})$. Then $\tilde{G}$ is reduction modulo $\mathfrak{q}$ of G_0. Since reduction modulo $\mathfrak{q}$ preserves intersection multiplicities, $\tilde{G}$ (considered as a cycle) can be written as $\tilde{G}_0 + \sum_{i=1}^{N} \tilde{G}_i$, where $\tilde{G}_0$ is a graph of a rational map $\tilde{f}$ and each $\tilde{G}_i$ has the form $u_i \times \{W_T \times_{Spec(\mathfrak{r}_T)} Spec(\tilde{k}_{S_\mathfrak{q}})\}$. Let v be any point of $(i_{T\mathfrak{P}} \circ j_T \circ \varphi_T)(x_{Sp}^{-1}\mathscr{C}(\mathfrak{p}))$ such that $(i_{T\mathfrak{P}} \circ j_T \circ \varphi_T)^{-1}(v) \in \mathfrak{H}$ is not fixed by Γ_T. Then, by (ii) of Main Theorem 1, there exist exactly $\rho = [\Gamma_T : \Gamma_S]$ (the index as transformation groups) different points $w_1, \cdots, w_\rho$ of $(i_{S\mathfrak{P}} \circ j_S \circ \varphi_S)(x_{Sp}^{-1}\mathscr{C}(\mathfrak{p}))$ which correspond to v by the correspondence $\tilde{G}$. Since there exists such a point v, the separable degree of $\tilde{f}$ is at least ρ. Since the degree of the rational map $J_{TS}(1)$ is ρ, and since reduction modulo $\mathfrak{q}$ preserves intersection multiplicities, it follows that $\tilde{G} = \tilde{G}_0$ and $\tilde{f}$ is separable. Since $\widetilde{W}_{S_\mathfrak{q}}$ is a complete non-singular curve, $\tilde{f}$ is a morphism.

Let g be the projection of G to $W_{S_\mathfrak{q}}$. Then, by the above result, $g^{-1}(y)$ is a finite set for any point y of $W_{S_\mathfrak{q}}$. It is obvious that g is a birational morphism and $W_{S_\mathfrak{q}}$ is normal. Therefore, by EGA, III, 4. 4. 9, g is an isomorphism. Hence, by EGA, I, 5. 3. 11, G is a graph of a morphism. Hence $j_T \circ J_{TS}(1) \circ j_S^{-1}$ *can be extended to a morphism of* $W_{S_\mathfrak{q}}$ *to* $W_T \times_{Spec(\mathfrak{r}_T)} Spec(\mathfrak{r}_{S_\mathfrak{q}})$.

Next *we assume* $xSx^{-1}=T$. Let $\mathfrak{q}$ and $\nu(x)$ be as in the theorem. Then $\sigma(x)$ belongs to the decomposition group of $\mathfrak{q}=\mathfrak{P}|k_S$. Since $k_T=k_S$ in this case, $W_T^{\sigma(x)} \times_{Spec(\mathfrak{r}_T^{\sigma(x)})} Spec(\mathfrak{r}_{S_\mathfrak{q}})$ is well-defined. Since $xSx^{-1}=T$, it follows from Shimura [24], 2. 6 that $J_{TS}(x)$ is a biregular isomorphism defined over k_S. Since W_S and W_T are stable curves, *the isomorphism* $j_T^{\sigma(x)} \circ J_{TS}(x) \circ j_S^{-1}$ *can be extended to an isomorphism of* $W_{S_\mathfrak{q}}$ *to* $W_T^{\sigma(x)} \times_{Spec(\mathfrak{r}_T^{\sigma(x)})} Spec(\mathfrak{r}_{S_\mathfrak{q}})$. Therefore we have completed the proof of Main Theorem 2.

3-6. Proof of Main Theorem 3. Let $\mathfrak{p}$, $\mathfrak{P}$, $\mathcal{Z}^{(\mathfrak{p})}$, $G^{(\mathfrak{p})}$ etc. be as in 1-2. Let $\mathcal{Z}^{(p)}$ be the subset of $\mathcal{Z}^{(\mathfrak{p})}$ consisting of all S such that there exists $x_{Sp} \in G_{Q+}$ satisfying $S \supseteqq x_{Sp}^{-1} \mathfrak{o}_p^\times x_{Sp}$. Then *the assertions of Main Theorem* 3 *concerning for this subfamily* $\mathcal{Z}^{(p)}$ *follow immediately from Theorem C and Main Theorems* 1 *and* 2. Hence *the main task of the proof of Main Theorem* 3 *is in extending* $\mathcal{Z}^{(p)}$ *to* $\mathcal{Z}^{(\mathfrak{p})}$.

Let $(K, \tau_1, \cdots, \tau_g)$ be as in 3-2. Let $p=\mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_t^{e_t}$ and $\mathfrak{p}_1=\mathfrak{p}$ be as in 3-2. By our assumption, *each* $\mathfrak{p}_j$ *is decomposed as* $\mathfrak{p}_j=\mathfrak{P}_j\overline{\mathfrak{P}}_j$, $\mathfrak{P}_j \neq \overline{\mathfrak{P}}_j$ *in* K/F. Let b, c, $S(b, c)$, Ω_i, $\Sigma(\Omega_i)$ etc. be as in 3-2. Let $\tilde{\mathscr{P}}=(\tilde{A}, \tilde{\mathscr{C}}, \tilde{\theta}\,; \tilde{t}_1, \cdots, \tilde{t}_v)$ be reduction of $\mathscr{P} \in \Sigma(\Omega_i)$ modulo $\mathfrak{P}$. Let λ_j be the $\overline{\mathfrak{P}}_j$-multiplication of $(\tilde{A}, \tilde{\theta})$. Then, by the result of [13], λ_2, λ_3, $\cdots$, λ_t are *separable* isogenies.

Let m be a positive integer such that the $\mathfrak{p}_j^{e_jm}$ and the $\mathfrak{P}_j^{e_jm}$ are principal ideals. Put $\mathfrak{b}=b\overline{\mathfrak{P}}_2^{e_2m}\cdots\overline{\mathfrak{P}}_t^{e_tm}$, $\mathfrak{b}_0=b\mathfrak{p}_2^{e_2m}\cdots\mathfrak{p}_t^{e_tm}$, $\mathfrak{c}=c\overline{\mathfrak{P}}_2^{e_2m}\cdots\overline{\mathfrak{P}}_t^{e_tm}$, $\mathfrak{c}_0=c\mathfrak{p}_2^{e_2m}\cdots\mathfrak{p}_t^{e_tm}$. Define $S(\mathfrak{b}_0, \mathfrak{c}_0)$, $\mathfrak{T}_\lambda(\mathfrak{b})$, $\Sigma(\mathfrak{b})$, $\tilde{\mathscr{C}}(\mathfrak{b}, \mathfrak{p})$, $\mathscr{F}(\mathfrak{b}, \mathfrak{p})$ etc. in the obvious manner. Then, replacing b, c and H_c by $\mathfrak{b}_0$, $\mathfrak{c}_0$ and H_{cp^m}, the results of 1-3 hold. Furthermore, replacing $\mathfrak{T}_\lambda(b)$, $\Sigma(b)$, $\tilde{\mathscr{C}}(b, \mathfrak{p})$, $\mathscr{F}(b, \mathfrak{p})$ etc. by new objects, the results of [13], which we quoted in 3-2, hold without any further cahnge (cf. [13], the remark after Theorem 3).

Let $\mathfrak{r}$ be the valuation ring of $\mathfrak{P}|K_{cp^m}$. Since the $\mathfrak{b}$-multiplication of $(\tilde{A}, \tilde{\theta})$ is a separable isogeny, the group of the $\mathfrak{b}$-section points is etale. Hence, repeating the arguments in § 2, we can construct a moduli scheme for Ω_i over $Spec(\mathfrak{r})$. Then, repeating the same arguments, the results in 3-2~3-3 hold. Let $T=x^{-1}S(\mathfrak{b}_0, \mathfrak{c}_0)\,x$ $(x \in G_A)$. Then there exist a smooth projective scheme S_T'' over $Spec(\mathfrak{r})$ and an isomorphism j_T'' of $V_T \times_{Spec(k_T)} Spec(K_{cp^m})$ to the general fibre S_{T0} of S_T such that S_T and j_T'' satisfy the conditions (ii) and (iii) of Main Theorem 1.

Let T be an element of $\mathcal{Z}^{(\mathfrak{p})}$. Then, repeating the arguments in 3-4, we can show that *there exist a smooth projective scheme* W'_T *over* $Spec(\mathfrak{r})$ *and an isomorphism* j'_T *of* $V'_T = V_T \times_{Spec(k_T)} Spec(K_{cp^m})$ *satisfying the conditions* (ii) *and* (iii) *of Main Theorem* 1. Furthermore, repeating the arguments in 3-5, we see that $j_T'^{\sigma(x)} \circ J_{TS}(x) \circ j_S'^{-1}$ ($x \in G^{(\mathfrak{p})}$, $T, S \in \mathcal{Z}^{(\mathfrak{p})}$, $xSx^{-1} \subseteqq T$) induces a morphism of W'_S to $W_T'^{\sigma(x)}$. Let $\tilde{K}$ be the residue field of $\mathfrak{P}|K_{cp^m}$. Let $\tilde{V}'_T = W'_T \times_{Spec(\mathfrak{r})} Spec(\tilde{K})$, $\tilde{J}'_{TS}(x) = (j_T'^{\sigma(x)} \circ J_{TS}(x) \circ j_S'^{-1}) \times_{Spec(\mathfrak{r})} Spec(\tilde{K})$, and let $\tilde{\varphi}'_T$ be the composition of $j'_T \circ \varphi_T$ and reduction modulo $\mathfrak{P}$. Obviously $\tilde{V}'_T$ is an absolutely irreducible projective non-singular curve with genus g_T.

For any $\sigma \in \mathrm{Gal}(K_{cp^m}/k_T)$, let $J_0(\sigma)$ be the conjugation map of V'_T to $V_T'^{\sigma}$. Then the $J_0(\sigma)$ satisfy the cocycle condition. Since W'_T and $W_T'^{\sigma}$ are stable curves, each $J_0(\sigma)$ can be extended to an isomorphism $J(\sigma)$ of W'_T to $(W'_T)^{\sigma}$. If σ is an element of the decomposition group of $\mathfrak{P}$, then $J(\sigma)$ induces an isomorphism $\tilde{J}(\sigma)$ of $\tilde{V}'_T$ to $(\tilde{V}'_T)^{\sigma}$. Obviously such $\tilde{J}(\sigma)$ satisfy the cocycle condition. Hence, by the result of Weil [26], *there exist an absolutely irreducible projective non-singular curve defined over* $\tilde{k}_T$ *and an isomorphism* j''_T *of* $\tilde{V}'_T$ *to* $\tilde{V}_T$ *defined over* $\tilde{K}$. Let $\tilde{\varphi}_T = j''_T \circ \tilde{\varphi}'_T$ and $\tilde{J}_{TS}(x) = j''_T \circ \tilde{J}'_{TS} \circ (j''_S)^{-1}$. Then *the conditions* (i) *and* (ii) *of Main Theorem* 3 *are satisfied by* $\tilde{V}_T$ *and* $\tilde{\varphi}_T$. Furthermore, it follows from Theorem C and our construction of $\tilde{V}_T$ and $\tilde{\varphi}_T$ that *the condition* (iii) *of Main Theorem* 3 *is also satisfied.* Therefore we have completed the proof of Main Theorems 1, 2, 3.

References

[1] C. CHEVALLEY: Deux théorèmes d'arithmétique, J. Math. Soc. Japan, **3** (1951), 36-44.

[2] M. DEURING: Reduktion algebraischer Funktionenkörper nach Primdivisoren des Konstantenkörpers, Math. Z, **47** (1942), 643-654.

[3] P. DELIGNE and D. MUMFORD: The irreducibility of the space of curves of given genus, Publ. Math. I. H. E. S., **36** (1969).

[4] A. GROTHENDIECK: Eléments de géométrie algébrique, Publ. Math. I. H. E. S., **4** (1960), **8** (1961), **11** (1961), **17** (1963), **20** (1964), **24** (1965), **28** (1966), **32** (1967). *Referred to as* EGA.

[5] A. GROTHENDIECK: Séminaire de géométrie algébrique, 1960/61. Notes from I. H. E. S.

[6] A. GROTHENDIECK: Fondements de la géométrie algébrique, collected Bourbaki talks. Paris 1962.

[7] J. IGUSA: Kroneckerian model of fields of elliptic modular functions, Amer. J. Math., **81** (1959), 561-577.

[8] Y. IHARA: On congruence monodromy problems, Lecture notes at Univ. of Tokyo, Vol. 1 (1968), Vol. 2 (1969), Tokyo.

[9] Y. IHARA: Some fundamental groups in arithmetic of algebraic curves over finite fields, Proc. National Academy of Sci., **72** (1975), 3281-3284.

[10] M. LICHTENBAUM: Curves over discrete valuation rings, Amer. J. Math., **90** (1968), 380-405.

[11] E. LAMPRECHT: Restabbildungen von Divisoren, Arch. Math., **8** (1957), 255–265.

[12] Y. MORITA: On potential good reduction of abelian varieties, J. Fac. Sci. Univ. Tokyo, Sec IA, **22** (1975), 437–447.

[13] Y. MORITA: Classification of abelian varieties parametrized by reduction modulo $\mathfrak{P}$ of a Shimura curve, Proc. Japan Acad., Vol. **56**, Ser. A (1980), 338–341.

[14] D. MUMFORD: Geometric invariant theory, Erg. d. Math., Neue Forge, **34**, Springer-Verlag, Berlin-Heidelberg-New York, 1965.

[15] D. MUMFORD: Introduction to algebraic geometry, Lecture notes at Harvard University.

[16] A NERON: Modeles minimaux des variétés abéliennes sur les corps locaux et globaux, Publ. Math. I. H. E S., **21** (1964).

[17] H. POPP: Über des Verhalten des Geschlechts eines Funktionenkörpers einer Variablen bei Konstantenreduktion, Math. Z, **106** (1968), 17–35.

[18] I. SAFAREVICH: Lectures on minimal models, Tata Institute Lecture notes, Bombay, 1966.

[19] J.-P. SERREand J. TATE: Good reduction of abelian varieties, Ann. of Math., **88** (1969), 492–517.

[20] G. SHIMURA: Reduction of algebraic varieties with respect to a discrete valuation of the base field, Amer. J. Math., **77** (1955), 134–176.

[21] G. SHIMURA: Moduli and fibre systems of abelian varieties, Ann. of Math., **83** (1966), 294–333.

[22] G. SHIMURA: Construction of class fields and zeta functions of algebraic curves, Ann. of Math., **85** (1967), 58–159.

[23] G. SHIMURA: Algebraic number fields and symplectic discontinous groups, Ann. of Math., **86** (1967), 503–592.

[24] G. SHIMURA: On canonical models of arithmetic quotients of bounded symmetric domains, Ann. of Math., **91** (1970), 144–222.

[25] G. SHIMURA and Y. TANIYAMA: Complex multiplication of abelian varieties and its applications to number theory, Publ. Math. Soc. Japan, **6** (1961).

[26] A. WEIL: The field of definition of a variety, Amer. J. Math., **78** (1956), 509–524.

[27] A. WEIL: Sur les courbes algébriques et les variétés qui s'en déduisent, Hermann, Paris, 1948.

[28] A. WEIL: Varietés abéliennes et courbes algébriques, Hermann, Paris, 1948.

[29] Y. IHARA: Non-abelian class fields over function fields in special cases, Actes de Congres Internat. Math., Nice, 1970, Tome 1, 381–389.

[30] Y. IHARA: Congruence relations and Shimura curves, Proc, Symp. Pure Math., Amer. Math. Soc., **33** (1979), 291–311.

[31] Y. IHARA: Congruence relations and Shimura curves, II, J. Fac. Sci. Univ. Tokyo, Sec. IA, **25** (1979), 301–361.

[32] Y. IHARA and H. MIKI: Criteria related to potential unramifiedness and reduction of unramified coverings of curves, J. Fac. Sci. Univ. Tokyo, Sec. IA, **22** (1975), 237–254.

Department of Mathematics
Hokkaido University
Sapporo 060, Japan