J. Math. Sci. Univ. Tokyo
21 (2014), 355–372.

Honda Theory for Formal Groups of Abelian Varieties over $\mathbb{Q}$ of GL_2-Type

By Yuken Miyasaka and Hirokazu Shinjo

Abstract. Honda proved that two formal groups attached to an elliptic curve E over $\mathbb{Q}$ are strongly isomorphic over $\mathbb{Z}$, where one of them is obtained from the formal completion along the zero section of the Néron model over $\mathbb{Z}$ and another is obtained from the L-series attached to the l-adic Galois representations on E. In this paper, we generalize his theorem to abelian varieties over $\mathbb{Q}$ of GL_2-type. As an application, we give a method to calculate the coefficients of the L-series attached to an algebraic curve over $\mathbb{Q}$ with a Jacobian variety of GL_2-type.

1. Introduction

1.1. Setting

Let A be an abelian variety defined over $\mathbb{Q}$ of dimension g, and $\mathrm{End}(A)$ the ring of endomorphisms of A defined over $\mathbb{Q}$. Suppose that A is an abelian variety of GL_2-type, that is, there is an isomorphism θ between a number field F with $[F:\mathbb{Q}] = g$ and the endomorphism algebra $\mathrm{End}^0(A) := \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ of A over $\mathbb{Q}$:

$$\theta : F \xrightarrow{\sim} \mathrm{End}^0(A).$$

Then F is either a totally real field or a totally imaginary quadratic extension of a totally real field, i.e., a CM-field. Let $\mathcal{O}_F$ be the ring of integers of F, and suppose that $\theta(\mathcal{O}_F) \subset \mathrm{End}(A)$. For a finite set S_0 of prime numbers, we denote by $\mathbb{Z}[S_0^{-1}]$ the ring obtained from $\mathbb{Z}$ by inverting all primes in S_0. Let S_{b} be the set of primes of bad reduction for A. Choose a finite set of primes S_{p} such that $\mathcal{O}_F \otimes_{\mathbb{Z}} \mathbb{Z}[S_{\mathrm{p}}^{-1}]$ is a principal ideal ring. Set $S := S_{\mathrm{b}} \cup S_{\mathrm{p}}$.

2010 *Mathematics Subject Classification.* 11G10, 14K22.

Key words: Formal group, abelian variety of GL_2-type, complex multiplication, L-series.

1.2. Main theorem

We construct two formal groups attached to A by a different manner: one is $\hat{A}$, which is obtained from the formal completion along the zero section of the Néron model $\mathscr{A}$ over $\mathbb{Z}$ for A and a basis of the space of invariant differential forms of $\mathscr{A}^0$ (which is constructed in §2.1). Another is $\hat{L}$, which is obtained from the L-series attached to the λ-adic representations of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on A (which is constructed in §2.2). We prove that formal groups $\hat{A}$ and $\hat{L}$ are strongly isomorphic over $\mathbb{Z}[S^{-1}]$ (§3, Theorem 2.2).

If $\dim A = 1$, this theorem is Honda's original result ([6]). In papers of Hill [5] and Honda [7], $\hat{A}$ and $\hat{L}$ are shown to be isomorphic over $\mathbb{Z}$ in this case. For any $g > 1$, Theorem 2.2 was proved by Deninger and Nart [4] when F is a totally real field. Our proof of Theorem 2.2 works in the case where F is not only a totally real field, but also a CM-field. Sairaiji has given a generalization of the result of Honda [6] to $\mathbb{Q}$-*curves* with complex multiplication ([11, 13]) and to *building blocks* defined over finite abelian extensions of $\mathbb{Q}$ ([12]).

Theorem 2.2 has an application to a problem to compute the coefficients of L-series attached to an algebraic curve over $\mathbb{Q}$. We give a method to calculate them by the "Hasse-Witt matrix" of the reduced curves when its Jacobian variety is of GL_2-type. (§3, Corollary 3.2. It gives a generalization of Honda [6, Corollary3].)

This paper is organized as follows: in section 2 we construct two formal groups $\hat{A}$ and $\hat{L}$ mentioned above, and prove that they are strongly isomorphic over $\mathbb{Z}[S^{-1}]$. In section 3, we give a method to calculate the coefficients of L-series attached to an algebraic curve over $\mathbb{Q}$ with a Jacobian variety of GL_2-type, by using our main theorem and applying a result of S.Kobayashi and T.Yamazaki. We also give numerical examples for certain hyperelliptic curves of genus two defined over $\mathbb{Q}$. Section 4 is devoted to a review of the Honda theory for formal groups.

Acknowledgment. The authors would like to thank Professor Takao Yamazaki for his continuous support and invaluable suggestions.

2. Construction of Formal Groups and Main Theorem

We keep the same notation as in §1.1. All results and terminology on formal groups we use in this section are summarized in Section 4.

2.1. Construction of $\hat{A}$

Let $\mathscr{A}$ be the Néron model over $\mathbb{Z}$ for A and $\mathscr{A}^0$ the connected component of $\mathscr{A}$. Since $\mathscr{A}^0$ is smooth of finite type over $\mathbb{Z}$, the space of invariant differentials $\omega_{\mathscr{A}^0/\mathbb{Z}}$ is a free $\mathbb{Z}$-module of rank g. We fix a basis $\{\omega_i\}_{i=1}^g$ of $\omega_{\mathscr{A}^0/\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Z}[S^{-1}]$ as $\mathcal{O}_F \otimes_{\mathbb{Z}} \mathbb{Z}[S^{-1}]$-module. This basis $\{\omega_i\}_{i=1}^g$ induces an isomorphism of formal group schemes:

$$\hat{\mathscr{A}} \otimes \mathbb{Z}[S^{-1}] \overset{\cong}{\to} \mathrm{Spf}\, \mathbb{Z}[S^{-1}][[\mathbf{x}]], \quad \mathbf{x} = (x_1, x_2, \dots, x_g), \tag{2.1}$$

where $\hat{\mathscr{A}}$ is the formal completion along the zero section of the Néron model $\mathscr{A}$ over $\mathbb{Z}$ for A. Let $\hat{A}(\mathbf{x}, \mathbf{y})$ be the g-dimensional formal group over $\mathbb{Z}[S^{-1}]$ for $\hat{\mathscr{A}} \otimes \mathbb{Z}[S^{-1}]$ obtained from the isomorphism (2.1), and let $f(\mathbf{x})$ be its logarithmic function, that is, $\hat{A}(\mathbf{x}, \mathbf{y}) = f^{-1}(f(\mathbf{x}) + f(\mathbf{y}))$. Let R be the faithful representation of $\mathcal{O}_F$ into the ring of $g \times g$ matrices $M_g(\mathbb{Z})$:

$$R : \mathcal{O}_F \hookrightarrow M_g(\mathbb{Z}) \tag{2.2}$$

such that for any $c \in \mathcal{O}_F$

$$\theta(c)^* \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_g \end{pmatrix} = R(c) \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_g \end{pmatrix},$$

where $\theta(c)^*$ is the endomorphism of $\omega_{\mathscr{A}^0/\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Z}[S^{-1}]$ induced by $\theta(c)$. Then the endomorphism $[c]_{\hat{A}}(\mathbf{x})$ of the formal group $\hat{A}$ induced by $c \in \mathcal{O}_F$ is written by $[c]_{\hat{A}}(\mathbf{x}) = f^{-1}(R(c) f(\mathbf{x}))$.

2.2. Construction of $\hat{L}$

Let l be a prime number and put $F_l := F \otimes_{\mathbb{Q}} \mathbb{Q}_l$. Using the isomorphism θ, the Tate module $V_l(A)$ is free of rank 2 as F_l-module with F_l-linear $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-action, since the actions of F and $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on $V_l(A)$ commute. Let F_λ be the completion of F at a prime λ dividing l, then $V_\lambda(A) := V_l(A) \otimes_{F_l} F_\lambda$ is a two-dimensional vector space over F_λ with F_λ-linear $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-action. This $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-action gives a λ-adic representation ρ_λ of A

$$\rho_\lambda : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}_{F_\lambda}(V_\lambda(A)) \cong \mathrm{GL}_2(F_\lambda).$$

It is shown in [14, (11.10.1)] that the characteristic polynomial of the Frobenius of $p \notin S_{\mathrm{b}}$ $(p \neq l)$ associated with ρ_λ have coefficients in $\mathcal{O}_F$. The coefficients are independent of the choice of λ and l. The following is given by Ribet [10]:

LEMMA 2.1 ([10, Lemma 3.1]). *There exists a finite order character* $\varepsilon : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to F^*$ *such that* $\det_{F_\lambda} \rho_\lambda = \varepsilon\chi_l$ *for each* λ*, where* χ_l *is the* l*-adic cyclotomic character. If* F *is a totally real field, the character* ε *is trivial.*

For a prime $p \notin S_{\mathrm{b}}$ $(p \neq l)$ and a Frobenius $\sigma_p \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, it follows from Lemma 2.1

$$\begin{aligned} L_p(A, F, X) &:= \det_{F_\lambda}(1 - \sigma_p X \mid V_\lambda(A)) \\ &= 1 - a_p X + \varepsilon_p p X^2. \end{aligned}$$

with $a_p \in \mathcal{O}_F$ and $\varepsilon_p := \varepsilon(\sigma_p) \in \mathcal{O}_F^*$. For the faithful representation $R : \mathcal{O}_F \hookrightarrow M_g(\mathbb{Z})$ chosen in (2.2), we define the formal Dirichlet series

$$\sum_{n \geq 1} \frac{A_n}{n^s} := \prod_{p \notin S_{\mathrm{b}}} (I_g - R(\bar{a}_p)p^{-s} + R(\bar{\varepsilon}_p)p^{1-2s})^{-1}, \quad A_n \in M_g(\mathbb{Z}).$$

Here $^-$ is the complex conjugation (resp. the identity) on F if F is a CM-field (resp. a totally real field). Let $\ell(\mathbf{x})$ be the formal power series

$$\ell(\mathbf{x}) := \sum_{n \geq 1} \frac{A_n}{n} \mathbf{x}^n \in \mathbb{Q}[[\mathbf{x}]]_0^g,$$

and $\hat{L}(\mathbf{x}, \mathbf{y})$ the g-dimensional formal group over $\mathbb{Q}$ whose logarithmic function is given by $\ell(\mathbf{x})$, namely

$$\hat{L}(\mathbf{x}, \mathbf{y}) := \ell^{-1}(\ell(\mathbf{x}) + \ell(\mathbf{y})).$$

The formal group $\hat{L}$ is actually defined over $\mathbb{Z}$ and for each prime $p \notin S_{\mathrm{b}}$ it is of type $pI_g - R(\bar{a}_p)T + R(\bar{\varepsilon}_p)T^2$. (See Theorem 4.3 in Section 4.)

2.3. Main theorem and Proof

THEOREM 2.2. *The formal groups $\hat{A}$ and $\hat{L}$ are strongly isomorphic over $\mathbb{Z}[S^{-1}]$.*

Before beginning the proof of Theorem 2.2, we give a key lemma about the ring of endomorphisms of a special fiber of $\mathscr{A}$. Fix a prime $p \notin S_{\mathrm{b}}$. Let $\mathscr{A}_p$ be the special fiber $\mathscr{A} \otimes_{\mathbb{Z}} \mathbb{F}_p$ of $\mathscr{A}$, and $\mathrm{End}(\mathscr{A}_p)$ be the ring of endomorphisms of $\mathscr{A}_p$ defined over $\mathbb{F}_p$. Put $\mathrm{End}^0(\mathscr{A}_p) := \mathrm{End}(\mathscr{A}_p) \otimes_{\mathbb{Z}} \mathbb{Q}$. Let π be the p-th power Frobenius endomorphism of $\mathscr{A}_p$. By Tate [16, Theorem 1], $\mathbb{Q}(\pi)$ is the center of $\mathrm{End}^0(\mathscr{A}_p)$. By the composed map

$$F \xrightarrow{\theta} \mathrm{End}^0(A) \hookrightarrow \mathrm{End}^0(\mathscr{A}_p), \tag{2.3}$$

we regard F as a subfield of $\mathrm{End}^0(\mathscr{A}_p)$. Since π commutes with all elements, $F(\pi)$ is a commutative subfield of $\mathrm{End}^0(\mathscr{A}_p)$.

LEMMA 2.3. *The following holds in* $\mathrm{End}\,\mathscr{A}_p$*:*

$$p - \bar{a}_p \pi + \bar{\varepsilon}_p \pi^2 = 0. \tag{2.4}$$

PROOF. For the proof, we slightly modify the argument of Deninger-Nart [4, Proposition 2.3].

Using the composed map (2.3), one can also define the F_λ-vector space $V_\lambda(\mathscr{A}_p)$ in the same manner as §2.2 for a prime $l \neq p$ and $\lambda \mid l$. Since p is a prime number of good reduction for A, the F_λ-vector space $V_\lambda(\mathscr{A}_p)$ is of dimension 2, and we have

$$V_\lambda(A) \cong V_\lambda(\mathscr{A}_p).$$

We denote by $V_\lambda(\pi)$ the endomorphism of $V_\lambda(\mathscr{A}_p)$ induced by $\sigma_p : V_\lambda(A) \to V_\lambda(A)$. We denote by $P(X)$ the monic polynomial $X^2 L_p(A, F, X^{-1})$ in $\mathcal{O}_F[X]$. Then we have

$$\begin{aligned} P(X) &= \det{}_{F_\lambda}(X - V_\lambda(\pi) \mid V_\lambda(\mathscr{A}_p)) \\ &= X^2 - a_p X + \varepsilon_p p \end{aligned}$$

We consider two cases.

Case $\pi \notin F$. It is shown in [15, Proposition 2] that $d = [E : \mathbb{Q}]$ divides $2 \dim \mathscr{A}_p$ where E is a number field in $\mathrm{End}^0 \mathscr{A}_p$. Thus $[F(\pi) : F] = 2$, since we have $[F : \mathbb{Q}] = \dim \mathscr{A}_p = g$. Take the minimal polynomial $Q(X)$ of π over F:

$$Q(X) = X^2 - a'_p X - c'_p \quad \in F[X].$$

Let $C(F)$ be the centralizer of F in $\mathrm{End}^0(\mathscr{A}_p)$. Then the natural $\mathbb{Q}$-algebra map

$$C(F) \to \mathrm{End}_{F_\lambda}(V_\lambda(\mathscr{A}_p))$$

sends π to $V_\lambda(\pi)$. Since $Q(\pi) = 0$, we have $Q(V_\lambda(\pi)) = 0$. On the other hand, $P(V_\lambda(\pi)) = 0$ in $\mathrm{End}_{F_\lambda}(V_\lambda(\mathscr{A}_p))$. Hence monic polynomials Q and P share a root. Since Q is irreducible over F, we have

$$Q(X) = P(X).$$

Therefore we have $a'_p = a_p$, $c'_p = \varepsilon_p p$, and

$$Q(\pi) = \pi^2 - a_p \pi + \varepsilon_p p = 0. \tag{2.5}$$

Case $\pi \in F$. Put $Q(X) := (X - \pi)^2$. Since $\pi \in F \hookrightarrow F_\lambda$, the action of $V_\lambda(\pi)$ is a scalar multiple on $V_\lambda(\mathscr{A}_p)$. Hence

$$P(X) = (X - V_\lambda(\pi))^2.$$

Since Q and P share the same root, we have $Q(X) = P(X)$. Therefore we have $2\pi = a_p$, $\pi^2 = \varepsilon_p p$, and

$$Q(\pi) = \pi^2 - a_p \pi + \varepsilon_p p = 0. \tag{2.6}$$

In either case, by multiplication of $\bar{\varepsilon}_p$ on equations (2.5) and (2.6), we obtain

$$\bar{\varepsilon}_p \varepsilon_p p - \bar{\varepsilon}_p a_p \pi + \bar{\varepsilon}_p \pi^2 = 0.$$

Using Lemma 2.4 bellow and the fact that $\bar{\varepsilon}_p \varepsilon_p = 1$, we obtain the equation (2.4) in $\mathrm{End}^0(\mathscr{A}_p)$. Since $\theta(\mathcal{O}_F) \subset \mathrm{End}(A) \hookrightarrow \mathrm{End}(\mathscr{A}_p)$, the equation (2.4) also holds in $\mathrm{End}(\mathscr{A}_p)$. □

LEMMA 2.4 (Ribet, [10, Proposition 3.4]). *For a prime number p of good reduction for A, the following holds:*

$$a_p = \varepsilon_p \bar{a}_p.$$

PROOF OF THEOREM 2.2. By §2.1 the formal group $\hat{A}$ is defined over $\mathbb{Z}[S^{-1}]$, and by §2.2 the formal group $\hat{L}$ is defined over $\mathbb{Z}$. In order to prove that they are strongly isomorphic over $\mathbb{Z}[S^{-1}]$, it suffices to show that they are strongly isomorphic over $\mathbb{Z}_p$ for every $p \notin S$ (since a strongly isomorphism between $\hat{A}$ and $\hat{L}$ is unique if it exists. See also Theorem 4.1 in Section 4). Fix a prime $p \notin S$. It follows from §2.1 and Lemma 2.3 that

$$f^{-1}(pf(\mathbf{x}) - R(\bar{a}_p)f(\mathbf{x}^p) + R(\bar{\varepsilon}_p)f(\mathbf{x}^{p^2})) \equiv 0 \mod p.$$

Since $\hat{A}(\mathbf{x}, \mathbf{y})$ is defined over $\mathbb{Z}[S^{-1}]$, it follows from [7, Lemma 4.2] that

$$pf(\mathbf{x}) - R(\bar{a}_p)f(\mathbf{x}^p) + R(\bar{\varepsilon}_p)f(\mathbf{x}^{p^2}) \equiv 0 \mod p.$$

This implies that the formal group $\hat{A}(\mathbf{x}, \mathbf{y})$ is of type $pI_g - R(\bar{a}_p)T + R(\bar{\varepsilon}_p)T^2$. Together with §2.2, we see that both the formal groups $\hat{A}$ and $\hat{L}$ have the same type. Therefore they are strongly isomorphic over $\mathbb{Z}_p$. This completes the proof of Theorem 2.2. □

3. Application to L-Series of Algebraic Curves

3.1. Coefficients of L-series of curves

Let C be a smooth projective, geometrically connected curve over $\mathbb{Q}$ of genus $g > 1$ with a rational point $\infty \in C(\mathbb{Q})$. Let J be its Jacobian variety and $\mathcal{J}$ the Néron model over $\mathbb{Z}$ of J. Suppose that J is of GL_2-type, that is, there exists a number field F with $[F : \mathbb{Q}] = g$ such that F is isomorphic to the endomorphism algebra $\mathrm{End}^0(J)$ of J over $\mathbb{Q}$. Suppose that $\theta(\mathcal{O}_F) \subset \mathrm{End}(J)$, where $\mathcal{O}_F$ is the ring of integer of F. For a prime number p of good reduction for J, define the local L-series attached to the λ-adic representation of J by

$$L_p(C, F, X) := \det{}_{F_\lambda}(1 - \sigma_p X \mid V_\lambda(J)) = 1 - a_p X + p\varepsilon_p X^2,$$

where $a_p, \varepsilon_p \in \mathcal{O}_F$ (see §2.2). The ordinary local L-series $L_p(C, X)$ attached to the curve C is a finite product of the above local L-series:

$$L_p(C, X) = \prod_{\iota : F \hookrightarrow \mathbb{C}} \iota(L_p(C, F, X)),$$

where ι runs on all embeddings from F into $\mathbb{C}$. It is well-known that one obtain the coefficients of $L_p(C, X)$ by counting up rational points of the reduction of C at p. In this subsection, we introduce another method to obtain the coefficients of $L_p(C, X)$ for large prime numbers p. More precisely, by using Theorem 2.2 and applying a result of S.Kobayashi and T.Yamazaki, we show that a_p is computable for large primes p by calculating the *Hasse-Witt matrix* of the reduction of C at p.

Let $W_\infty(C)$ be the *Weierstrass gap sequence* of C at ∞:

$$\begin{aligned} W_\infty(C) :&= \{n \in \mathbb{Z}_{>0} \mid H^0(C, \mathcal{O}_C((n-1)\infty)) = H^0(C, \mathcal{O}_C(n\infty))\} \\ &= \{\mu_1, \mu_2, \dots, \mu_g\}, \quad \text{where } \mu_i \in \mathbb{Z} \text{ and } \mu_1 = 1 < \mu_2 < \cdots < \mu_g. \end{aligned}$$

By definition of the Weierstrass gap sequence and the Serre duality, for a local parameter t at ∞ there exists a basis $\omega_1, \omega_2, \dots, \omega_g$ of $H^0(C, \Omega^1_{C/\mathbb{Q}})$ such that

$$\omega_i(t) = \left(\sum_{j=\mu_i}^{\infty} c_{i,j} t^j \right) \frac{dt}{t} \tag{3.1}$$

with $c_{i,j} \in \mathbb{Q}$ satisfying $c_{i,\mu_j} = \delta_{i,j}$(Kronecker's delta). Such a basis is called the *Hermite basis* with respect to the local parameter t. Take the $\mathbb{Q}$-linear map $\Psi : \mathrm{End}(H^0(C, \Omega^1_{C/\mathbb{Q}})) \to M_g(\mathbb{Q})$ by such the Hermite basis. Now we assume the following:

(**A1**) The composition of following maps lies inside the matrices with integral coefficients:

$$\begin{aligned} \mathcal{O}_F \xrightarrow{\theta} \quad & \mathrm{End}(J) \xrightarrow{\text{pull-back}} \mathrm{End}(H^0(J, \Omega^1_{J/\mathbb{Q}})) \\ \xrightarrow{\Lambda^*} \mathrm{End}(H^0(C, \Omega^1_{C/\mathbb{Q}})) \quad & \xrightarrow{\Psi} \quad M_g(\mathbb{Q}), \end{aligned} \tag{3.2}$$

where Λ^* is obtained from the Abel-Jacobi map $\Lambda : C \to J$ with respect to the base point ∞. Let us denote by R the composed map from $\mathcal{O}_F$ to $M_g(\mathbb{Z})$ in (3.2)

The assumption (**A1**) means that a basis $\{\eta_i\}$ of $H^0(J, \Omega^1_{J/\mathbb{Q}})$ such that $\Lambda^*(\eta_i) = \omega_i$ is regarded as a $\mathbb{Z}$-basis of $H^0(\mathcal{J}, \Omega^1_{\mathcal{J}/\mathbb{Z}})$ and it gives a basis of the space of invariant differentials $\omega_{\hat{\mathcal{J}}/\mathbb{Z}}$ by the formal completion. Thus from the argument in §2.1, the Hermite basis $\omega_1, \omega_2, \ldots, \omega_g$ determines a g-dimensional formal group $\hat{J}$ for J, and from the proof of Theorem 2.2 (§2.3) it is of type $p - R(\bar{a}_p)T + R(\bar{\varepsilon}_p)T^2$ for each prime number of good reduction.

From now on, we fix a good prime $p \geq 2g$. We consider the smooth projective curve $X := C \otimes \mathbb{Q}_p$ over the p-adic number field $\mathbb{Q}_p$. Let $\mathfrak{X}$ be the smooth projective model over $\mathbb{Z}_p$ of X and $Y := \mathfrak{X} \otimes \mathbb{F}_p$ the special fiber of $\mathfrak{X}$. We write $\widetilde{\infty} \in Y(\mathbb{F}_p)$ for the reduction of $\infty \in X(\mathbb{Q}_p)$. We assume the following:

(**A2**) $W_\infty(X) = W_{\widetilde{\infty}}(Y)$.

Then from [8, §4] one can choose a local parameter t at ∞ such that all coefficients $c_{i,j}$ of the expansion (3.1) of the Hermite basis with respect to the local parameter t belong to $\mathbb{Z}_p$. We write H_p for the $(g \times g)$-matrix $(c_{i,p\mu_j})_{1 \leq i,j \leq g} \in M_g(\mathbb{Z}_p)$. (Here $H_p \mod p \in M_g(\mathbb{F}_p)$ is called *Hasse-Witt matrix* of Y.) Then the following is proved by Kobayashi-Yamazaki:

Theorem 3.1 ([8, Theorem 4.5]). *Let us assume* (**A2**). *There exist* $(g \times g)$*-matrices* $\mathbf{e}^{(k)} \in M_g(\mathbb{Z}_p)$ $(k \in \mathbb{Z}_{\geq 0})$ *with* $\mathbf{e}^{(0)} = I_g$ *and* $\mathbf{e}^{(1)} = H_p$ *such that the formal power series*

$$l(\mathbf{x}) = \sum_{k=0}^{\infty} \frac{\mathbf{e}^{(k)}}{p^k} \mathbf{x}^{p^k} \in \mathbb{Q}_p[[\mathbf{x}]]_0^g, \quad \mathbf{x} = {}^t(x_1, x_2, \ldots, x_g)$$

gives a logarithmic function of a formal group over $\mathbb{Z}_p$ *which is strongly isomorphic to* $\hat{J}/\mathbb{Z}_p$.

Corollary 3.2. *Let us assume* (**A1**) *and* (**A2**). *Then we have*

$$R(\bar{a}_p) \equiv H_p \mod p. \tag{3.3}$$

Proof. From Theorem 3.1, it follows that the logarithmic function $l(\mathbf{x})$ is of type v for some special element v. Equivalently, there exists a

special element $v \in M_g(\mathbb{Z}_p)[[T]]$ such that $v * l(\mathbf{x}) \equiv 0 \mod p$. Thus if we write $v = pI_g + B_1T + B_2T^2 + \cdots$, we have

$$H_p \equiv -B_1 \mod p.$$

Since $\hat{J}$ is of type $p - R(\bar{a}_p)T + R(\bar{\varepsilon}_p)T^2$ by the assumption (**A1**), it follows that $B_1 \equiv -R(\bar{a}_p) \mod p$. Therefore we get (3.3). □

From the congruence (3.3), one can find some possible values for a_p by calculating the Hasse-Witt matrix H_p. In addition, we know that for any embedding $\iota : F \hookrightarrow \mathbb{C}$, the absolute value of $\iota(a_p)$ is bounded by $2\sqrt{p}$ (so-called, the *Weil bound*):

$$|\iota(a_p)| \leq 2\sqrt{p}.$$

Thus we can uniquely determine a_p for large prime numbers p from H_p. We give some numerical examples below.

3.2. Example 1

For a hyperelliptic curve C over $\bar{\mathbb{Q}}$ given by an equation of the form $y^2 = f(x) \in \bar{\mathbb{Q}}[x]$ such that $f(x)$ is a separable polynomial of degree 5 or 6, every automorphism of C is given by the coordinate transformation M_U:

$$M_U : (x, y) \mapsto \left(\frac{ax + b}{cx + d}, \frac{(ad - bc)y}{(cx + d)^3} \right)$$

for a suitable matrix $U = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\bar{\mathbb{Q}})$. Note that $M_U \circ M_V = M_{VU}$ for $U, V \in \mathrm{GL}_2(\bar{\mathbb{Q}})$. We write M_U^* for the induced endomorphism by M_U of the Jacobian variety of C.

We consider the hyperelliptic curve C_a over $\mathbb{Q}$ given by

$$y^2 = x(x - 1)(x^3 - (3 + a)x^2 + ax + 1), \quad a \in \mathbb{Z},$$

which is defined by Cardona, González, Lario and Rio [2]. Set $V = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$. Then M_V defines an automorphism of C_a. It satisfies that $(2M_V^* + 1)^2 = -3$ in $\mathrm{End}(J)$.

THEOREM 3.3 ([2, Proposition 3.2]). *The $\mathbb{Q}$-algebra map*

$$\theta : \mathbb{Q}(\zeta) \to \mathrm{End}^0(J), \quad \zeta \mapsto M_V^*$$

is an isomorphism, where ζ is a primitive 3-rd root of unity.

Let ∞ denote the point at infinity of C_a. Then we see that $W_\infty(C_a) = \{1, 3\}$ and that the (**A2**) is satisfied for each prime of good reduction. We take the local parameter t at ∞ as x^2/y. Then the Hermite basis ω_1, ω_2 with respect to t is presented by

$$\omega_1 = -\frac{1}{2}\left(\frac{x+a+4}{y}\right)dx = (t + c_{1,5}t^5 + c_{1,7}t^7 + \cdots)\frac{dt}{t}$$
$$\omega_2 = -\frac{dx}{2y} = (t^3 + c_{2,5}t^5 + c_{2,7}t^7 + \cdots)\frac{dt}{t}$$

where $c_{i,j} \in \mathbb{Z}[a]$. By computing the composition of the maps (3.2), we obtain a faithful map $R : \mathbb{Z}[\zeta] \to M_2(\mathbb{Z})$ as

$$\zeta \mapsto \begin{pmatrix} -a-5 & a^2+9a+21 \\ -1 & a+4 \end{pmatrix},$$

then the assumption (**A1**) is satisfied when a is integer. Therefore Corollary 3.2 can be applied to this case.

We consider the case that $a = 0$. Then the representation R is given by

$$R : \zeta \mapsto \begin{pmatrix} -5 & 21 \\ -1 & 4 \end{pmatrix},$$

and each prime $p \neq 2, 3$ is a good reduction prime. We apply our method to the case that $p = 59$, for example. Then we compute

$$R(\bar{a}_{59}) \equiv H_{59} \equiv \begin{pmatrix} 44 & 4 \\ 56 & 12 \end{pmatrix} \equiv R(3\zeta) \mod 59,$$

where the first congruence follows from Corollary 3.2. Thus $\bar{a}_{59} \equiv 3\zeta \mod 59$. The Weil bound says that

$$|a_{59}| \leq 2\sqrt{59} = 15.3\ldots.$$

Hence $\bar{a}_{59}$ should be 3ζ. (In particular, we have $a_{59} = 3\zeta^2$.) Moreover, from Lemma 2.4, we also get $\varepsilon_{59} = a_{59}/\bar{a}_{59} = \zeta$. Hence we have

$$L_{59}(C_0, \mathbb{Q}(\zeta), X) = 1 - 3\zeta^2 X + 59\zeta X^2$$

and

$$\begin{aligned} L_{59}(C_0, X) &= (1 - 3\zeta^2 X + 59\zeta X^2)(\overline{1 - 3\zeta^2 X + 59\zeta X^2}) \\ &= 1 + 3X - 50X^2 + 177X^3 + 4489X^4. \end{aligned}$$

The local L-series $L_p(C_0, X)$ for other primes are presented in TABLE 1. The first and second columns in this table are lists of primes p such that $17 \leq p \leq 71$ and the Hasse-Witt matrix for each prime p. The corresponding value of a_p for each p is given in the third column.

3.3. Example 2

We next consider the hyperelliptic curve C_1 defined by the equation

$$C_1 : y^2 = (x^2 + 1)(x^4 - 8x^3 + 2x^2 + 8x + 1).$$

It is the curve in the family of dihedral curves defined by Cardona-Quer [3] (we get it by taking $(1, 1, 0)$ for the parameter (u, v, z) in their notation). The curve C_1 has good reduction at $p \neq 2, 3$. Cardona-Quer proved that automorphisms M_U, M_V generate $\mathrm{Aut}(C_1)$ where M_U, M_V are given by matrices

$$U := \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad V := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Since $U^2 = V^4 = 1$ and $UV^3 = VU$, $\mathrm{Aut}(C_1)$ is isomorphic to the dihedral group D_8.

LEMMA 3.4. *We have*

$$\mathbb{Q}(\sqrt{-1}) \cong \mathrm{End}^0(J)$$

PROOF. It follows from the same procedure as in [2]. We denote by $D := \mathrm{End}_{\bar{\mathbb{Q}}}(J) \otimes \mathbb{Q}$ the algebra of all endomorphisms of J. Since

Table 1.

p	$H_p \pmod p$	a_p	$L_p(C_0, \mathbb{Q}(\zeta), X)$	$L_p(C_0, X)$
17	$\begin{pmatrix} 6 & 0 \\ 0 & 6 \end{pmatrix}$	6	$1 - 6X + 17X^2$	$1 - 12X + 70X^2 - 204X^3 + 289X^4$
19	$\begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix}$	4	$1 - 4X + 19X^2$	$1 - 8X + 54X^2 - 152X^3 + 361X^4$
23	$\begin{pmatrix} 8 & 17 \\ 20 & 12 \end{pmatrix}$	$3\zeta^2$	$1 - 3\zeta^2 X + 23\zeta X^2$	$1 + 3X - 14X^2 + 69X^3 + 529X^4$
29	$\begin{pmatrix} 12 & 24 \\ 3 & 14 \end{pmatrix}$	3ζ	$1 - 3\zeta X + 29\zeta^2 X^2$	$1 + 3X - 20X^2 + 87X^3 + 841X^4$
31	$\begin{pmatrix} 25 & 19 \\ 5 & 11 \end{pmatrix}$	$-5\zeta^2$	$1 + 5\zeta^2 X + 31\zeta X^2$	$1 - 5X - 6X^2 - 155X^3 + 961X^4$
37	$\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$	2	$1 - 2X + 37X^2$	$1 - 4X + 78X^2 - 148X^3 + 1369X^4$
41	$\begin{pmatrix} 26 & 22 \\ 38 & 12 \end{pmatrix}$	$3\zeta^2$	$1 - 3\zeta^2 X + 41\zeta X^2$	$1 + 3X - 32X^2 + 123X^3 + 1681X^4$
43	$\begin{pmatrix} 4 & 22 \\ 1 & 38 \end{pmatrix}$	ζ	$1 - \zeta X + 43\zeta^2 X^2$	$1 + X - 42X^2 + 43X^3 + 1849X^4$
47	$\begin{pmatrix} 36 & 46 \\ 9 & 2 \end{pmatrix}$	9ζ	$1 - 9\zeta X + 47\zeta^2 X^2$	$1 + 9X + 34X^2 + 423X^3 + 2209X^4$
53	$\begin{pmatrix} 47 & 0 \\ 0 & 47 \end{pmatrix}$	-6	$1 + 6X + 53X^2$	$1 + 12X + 142X^2 + 636X^3 + 2809X^4$
59	$\begin{pmatrix} 44 & 4 \\ 56 & 12 \end{pmatrix}$	$3\zeta^2$	$1 - 3\zeta^2 X + 59\zeta X^2$	$1 + 3X - 50X^2 + 177X^3 + 3841X^4$
61	$\begin{pmatrix} 9 & 29 \\ 48 & 4 \end{pmatrix}$	-13ζ	$1 + 13\zeta X + 61\zeta^2 X^2$	$1 - 13X + 108X^2 - 793X^3 + 3721X^4$
67	$\begin{pmatrix} 32 & 13 \\ 60 & 28 \end{pmatrix}$	$7\zeta^2$	$1 - 7\zeta^2 X + 67\zeta X^2$	$1 + 7X - 18X^2 + 496X^3 + 4489X^4$
71	$\begin{pmatrix} 12 & 0 \\ 0 & 12 \end{pmatrix}$	12	$1 - 12X + 71X^2$	$1 - 24X + 286X^2 - 1704X^3 + 5041X^4$

$\mathrm{Aut}(C_1)$ is non-abelian, it follows from [2, Lemma 2.4] that J is isogenous over $\bar{\mathbb{Q}}$ to the square of an elliptic quotient E of C_1. One can check that C_1 has two non-isomorphic elliptic quotients with no complex multiplication. (Indeed, according to [1, §2], we see that j-invariants of the elliptic quotients are $2^6 13^3/3$ and $2^6 7^3/3^2$, respectively. Hence they are non-isomorphic and no-CM.) Therefore, from [9, Chap.5 §1.9], D is isomorphic to $M_2(\mathrm{End}^0_{\bar{\mathbb{Q}}}(E)) \cong M_2(\mathbb{Q})$. Now D coincides with the $\mathbb{Q}$-vector space generated by the image of $\mathrm{Aut}(C_1) \hookrightarrow D \cong M_2(\mathbb{Q})$. Since M_V (resp. M_U) is defined (resp. not defined) over $\mathbb{Q}$ and since $\mathrm{End}(J)$ is the ring of endo-

morphisms of J defined over $\mathbb{Q}$, $\mathrm{End}^0(J) = \mathrm{End}(J) \otimes_{\mathbb{Z}} \mathbb{Q}$ is the $\mathbb{Q}$-vector subspace of D generated by the cyclic subgroup $\langle M_V^* \rangle$. Since $(M_V^*)^2 = -1$, the $\mathbb{Q}$-algebra map $\mathbb{Q}(\sqrt{-1}) \to \mathrm{End}^0(J)$ by associating $\sqrt{-1}$ with M_V^* is an isomorphism. $\square$

Let ∞ denote a point at infinity of C_1. Then we see that $W_\infty(C_a) = \{1, 2\}$ and that the assumption (**A2**) is satisfied for good reduction primes. We take the local parameter t at ∞ as $1/x$. Then the Hermite basis ω_1, ω_2 with respect to t is presented by

$$\begin{aligned} \omega_1 &= \frac{4-x}{y}dx = (t + c_{1,3}t^3 + c_{1,4}t^4 + \cdots)\frac{dt}{t}, \\ \omega_2 &= -\frac{1}{y}dx = (t^2 + c_{2,3}t^3 + c_{2,4}t^4 + \cdots)\frac{dt}{t}, \end{aligned}$$

where $c_{i,j} \in \mathbb{Z}[2^{-1}]$. By computing the composition of maps (3.2), we obtain a faithful map $R : \mathbb{Z}[\sqrt{-1}] \to M_2(\mathbb{Z})$ as

$$\sqrt{-1} \mapsto \begin{pmatrix} -4 & -17 \\ 1 & 4 \end{pmatrix},$$

Table 2.

p	$H_p \pmod p$	a_p	$L_p(C_1, \mathbb{Q}(\sqrt{-1}), X)$	$L_p(C_1, X)$
17	$\begin{pmatrix} 11 & 0 \\ 0 & 11 \end{pmatrix}$	-6	$1 + 6X + 17X^2$	$1 + 12X + 70X^2 + 204X^3 + 289X^4$
19	$\begin{pmatrix} 16 & 11 \\ 15 & 3 \end{pmatrix}$	$-4\sqrt{-1}$	$1 + 4\sqrt{-1}X - 19X^2$	$1 - 22X^2 + 361X^4$
23	$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$	0	$1 + 23X^2$	$1 + 46X^2 + 529X^4$
29	$\begin{pmatrix} 8 & 5 \\ 27 & 21 \end{pmatrix}$	$-2\sqrt{-1}$	$1 + 2\sqrt{-1}X - 29X^2$	$1 - 54X^2 + 841X^4$
31	$\begin{pmatrix} 27 & 0 \\ 0 & 27 \end{pmatrix}$	-4	$1 + 4X + 31X^2$	$1 + 8X + 78X^2 + 248X^3 + 961X^4$
37	$\begin{pmatrix} 8 & 34 \\ 35 & 29 \end{pmatrix}$	$-2\sqrt{-1}$	$1 + 2\sqrt{-1}X - 37X^2$	$1 - 70X^2 + 1369X^4$

then the assumption (**A1**) is satisfied. Therefore Corollary 3.2 is applied for the basis ω_1, ω_2. For each prime p such that $17 \leq p \leq 37$, $H_p \mod p$, a_p and $L_p(C_1, X)$ are given in TABLE 2.

4. Appendix: Formal Groups over $\mathbb{Z}_p$

In this section, we explain the Honda theory for formal groups over the p-adic integer ring.

4.1. Notation

Let R be a commutative ring. Let $R[[\mathbf{x}]] = R[[x_1, x_2, \ldots, x_g]]$ be the ring of formal power series on g-variables $x_1, x_2, \ldots, x_g$. We denote by $R[[\mathbf{x}]]^g$ the set of column vectors ${}^t(\varphi_1(\mathbf{x}), \varphi_2(\mathbf{x}), \ldots, \varphi_g(\mathbf{x}))$ with $\varphi_i \in R[[\mathbf{x}]]$. If $\varphi(\mathbf{x}), \psi(\mathbf{x})$ in $R[[\mathbf{x}]]^g$ coincide in terms of degree strictly less than r, we write $\varphi(\mathbf{x}) \equiv \psi(\mathbf{x}) \mod \deg r$. Let us denote by $R[[\mathbf{x}]]_0$ the set $\{\varphi(\mathbf{x}) \in R[[\mathbf{x}]] \mid \varphi(\mathbf{x}) \equiv 0 \mod \deg 1\}$. We regard $\mathbf{x}$ as the column vector ${}^t(x_1, x_2, \ldots, x_g)$ in $R[[\mathbf{x}]]_0^g$ and $\mathbf{x}^n$ as the column vector ${}^t(x_1^n, x_2^n, \ldots, x_g^n)$. Let $M_g(R)[[T]]$ be the ring of one-variable formal power series with coefficients in the ring of $g \times g$ matrices with elements in R.

4.2. Types of formal groups

We recall the theory "*of types*" for formal groups, which is due to Honda ([6, 7]). Let p be a prime number. For $v = \sum_{n \geq 0} B_n T^n \in M_g(\mathbb{Z}_p)[[T]]$ and $f \in \mathbb{Q}_p[[\mathbf{x}]]_0^g$, we define an element $v * f \in \mathbb{Q}_p[[\mathbf{x}]]_0^g$ by

$$v * f(\mathbf{x}) := \sum_{n \geq 0} B_n f(\mathbf{x}^{p^n}).$$

An element $v = \sum_{n \geq 0} B_n T^n \in M_g(\mathbb{Z}_p)[[T]]$ is called *special* if $B_0 = pI_g$. For a special element v, an element $f \in \mathbb{Q}_p[[\mathbf{x}]]_0^g$ is said to be *of type* v if all coefficients of $v * f$ belong to $p\mathbb{Z}_p$, that is

$$v * f(\mathbf{x}) \equiv 0 \mod p.$$

Let $\hat{F}(\mathbf{x}, \mathbf{y})$ be a g-dimensional formal group defined over $\mathbb{Q}_p$, namely, $\hat{F}(\mathbf{x}, \mathbf{y})$ is a formal power series in $\mathbb{Q}_p[[\mathbf{x}, \mathbf{y}]]_0^g$ satisfying the following con-

dition:

$$\begin{aligned}
&(1)\quad \hat{F}(\mathbf{x},\mathbf{y}) \equiv \mathbf{x}+\mathbf{y} \mod \deg 2,\\
&(2)\quad \hat{F}(\hat{F}(\mathbf{x},\mathbf{y}),\mathbf{z}) = \hat{F}(\mathbf{x},\hat{F}(\mathbf{y},\mathbf{z})),\\
&(3)\quad \hat{F}(\mathbf{x},\mathbf{y}) = \hat{F}(\mathbf{y},\mathbf{x}).
\end{aligned}$$

Then there exists a unique element $f \in \mathbb{Q}_p[[\mathbf{x}]]_0^g$ such that $f(\mathbf{x}) \equiv \mathbf{x} \mod \deg 2$ and $\hat{F}(\mathbf{x},\mathbf{y}) = f^{-1}(f(\mathbf{x})+f(\mathbf{y}))$ ([7, Theorem 1]). Such an element f is called the *logarithmic function* of the formal group $\hat{F}$. For a special element v, a formal group $\hat{F}$ over $\mathbb{Q}_p$ is said to be *of type* v if its logarithmic function is of type v.

THEOREM 4.1 ([7, Theorem 2-4]). *Let $\hat{F}(\mathbf{x},\mathbf{y})$ be a g-dimensional formal group over $\mathbb{Q}_p$ whose logarithmic function is given by $f \in \mathbb{Q}_p[[\mathbf{x}]]_0^g$.*

1. *The formal group $\hat{F}$ is defined over $\mathbb{Z}_p$ if and only if $\hat{F}$ is of type v for some special element v.*

2. *Let v_1 and v_2 be special elements. Assume that $\hat{F}$ is of type v_1, and let $\hat{G}$ be another formal group over $\mathbb{Z}_p$ of type v_2. Then there exists an element u in $I_g + TM_g(\mathbb{Z}_p)[[T]]$ satisfying $v_1 = uv_2$ if and only if there exists a power series $\varphi(\mathbf{x})$ in $\mathbb{Z}_p[[\mathbf{x}]]_0^g$ satisfying the following*

$$\begin{aligned}
&\text{(i)}\quad \varphi(\hat{F}(\mathbf{x},\mathbf{y})) = \hat{G}(\varphi(\mathbf{x}),\varphi(\mathbf{y})),\\
&\text{(ii)}\quad \varphi(\mathbf{x}) \equiv \mathbf{x} \mod \deg 2.
\end{aligned}$$

We say that $\hat{F}$ is *strongly isomorphic over* $\mathbb{Z}_p$ to $\hat{G}$ if there exists $\varphi(\mathbf{x})$ in $\mathbb{Z}_p[[\mathbf{x}]]_0^g$ satisfying the above (i) and (ii). Note that such a formal power series $\varphi(\mathbf{x})$ is unique if it exists.

COROLLARY 4.2. *Let v_1 and v_2 be special elements of the form $v_1 = pI_g + B_1T + \cdots$ and $v_2 = pI_g + B_1'T + \cdots$. Let $\hat{F}$ and $\hat{G}$ be g-dimensional formal groups over $\mathbb{Z}_p$ of type v_1 and v_2, respectively. If they are strongly isomorphic over $\mathbb{Z}_p$, then we have $B_1 \equiv B_1' \mod p$.*

4.3. Formal groups for L-series

Let $\{A_p, C_p\}_p$ be a set of commuting matrices in $M_g(\mathbb{Z})$ for all prime numbers p. Consider the formal Dirichlet series

$$\sum_{n\geq 1} \frac{A_n}{n^s} := \prod_p (I_g - A_p p^{-s} + C_p p^{1-2s})^{-1},$$

where $A_n \in M_g(\mathbb{Z})$. Put

$$f(\mathbf{x}) := \sum_{n\geq 1} \frac{A_n}{n} \mathbf{x}^n \in \mathbb{Q}[[\mathbf{x}]]_0^g.$$

THEOREM 4.3 ([7, Theorem 8]). *The formal power series*

$$\hat{F}(\mathbf{x}, \mathbf{y}) := f^{-1}(f(\mathbf{x}) + f(\mathbf{y}))$$

is a g-dimensional formal group over $\mathbb{Z}$. For each prime number p, it is of type $pI_g - A_pT + C_pT^2$.

References

[1] Cardona, G., **Q**-*curves and abelian varieties of* GL_2-*type from dihedral genus 2 curves*, Modular curves and abelian varieties, Progr. Math., vol. 224, Birkhäuser, Basel, 2004, 45–52.

[2] Cardona, G., González, J., Lario, J. and A. Rio, On curves of genus 2 with Jacobian of GL_2-type, Manuscripta Mathematica **98** (1999), no. 1, 37–54.

[3] Cardona, G. and J. Quer, Curves of genus 2 with group of automorphisms isomorphic to D_8 or D_{12}, Trans. Amer. Math. Soc. **359** (2007), no. 6,2831–2849.

[4] Deninger, C. and E. Nart, Formal groups and L-series, Comment. Math. Helv. **65** (1990), no. 2, 318–333.

[5] Hill, W., Formal groups and zeta-functions of elliptic curves, Invent. Math. **12** (1971), 321–336.

[6] Honda, T., Formal groups and zeta-functions, Osaka J. Math. **5** (1968), 199–213.

[7] Honda, T., On the theory of commutative formal groups, J. Math. Soc. Japan **22**, (1970), 213–246.

[8] Kobayashi, S. and T. Yamazaki, Torsion points on Jacobian varieties via Anderson's p-adic soliton theory, ArXiv e-prints, (2012), (2012), available at http://adsabs.harvard.edu/abs/2012arXiv1210.5838K.

[9] Mumford, D., *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics, No. 5, Published for the Tata Institute of Fundamental Research, Bombay, 1970.

[10] Ribet, K., *Abelian varieties over* $\mathbf{Q}$ *and modular forms*, Algebra and topology 1992 (Taejŏn), Korea Adv. Inst. Sci. Tech., Taejŏn, 1992, pp. 53–79.

[11] Sairaiji, F., Formal groups of certain $\mathbf{Q}$-curves over quadratic fields, Osaka J. Math. **39** (2002), no. 1, 223–243.

[12] Sairaiji, F., Formal groups of building blocks completely defined over finite abelian extensions of $\mathbf{Q}$, Bull. London Math. Soc. **38** (2006), no. 1, 81–92.

[13] Sairaiji, F., Formal groups of Q-curves with complex multiplication, Rocky Mountain J. Math. **43** (2013), no. 3, 1023–1036.

[14] Shimura, G., Algebraic number fields and symplectic discontinuous groups, Ann. of Math. (2) **86** (1967), 503–592.

[15] Shimura, G. and Y. Taniyama, *Complex multiplication of abelian varieties and its applications to number theory*, Publications of the Mathematical Society of Japan, vol. 6, The Mathematical Society of Japan, Tokyo, 1961.

[16] Tate, J., *Classes d'isogénie des variétés abéliennes sur un corps fini (d'après T. Honda)*, Séminaire Bourbaki. Vol. 1968/69: Exposés 347–363, Lecture Notes in Mathematics, Vol. 179, Springer-Verlag, Berlin, 1971.

(Received February 28, 2014)
(Revised July 1, 2014)

Mathematical Institute
Tohoku University
Sendai 980-8578, Japan
E-mail: sa7m27@math.tohoku.ac.jp
(Yuken Miyasaka)
sb1m23@math.tohoku.ac.jp
(Hirokazu Shinjo)