$\operatorname{RIMS-1702}$

On a problem of Matsumoto and Tamagawa concerning monodromic fullness of hyperbolic curves: Genus zero case

By

Yuichiro HOSHI

July 2010



京都大学 数理解析研究所

RESEARCH INSTITUTE FOR MATHEMATICAL SCIENCES KYOTO UNIVERSITY, Kyoto, Japan

ON A PROBLEM OF MATSUMOTO AND TAMAGAWA CONCERNING MONODROMIC FULLNESS OF HYPERBOLIC CURVES: GENUS ZERO CASE

YUICHIRO HOSHI

JULY 2010

ABSTRACT. In the present paper, we discuss a problem concerning monodromic fullness of hyperbolic curves over number fields posed by M. Matsumoto and A. Tamagawa in the case where a given hyperbolic curve is *of genus* 0.

CONTENTS

Introduction	1
Notations and Conventions	3
Proofs of main results	4
References	9

INTRODUCTION

Write Primes for the set of all prime numbers. In [4], M. Matsumoto and A. Tamagawa posed the following problem concerning monodromic fullness of hyperbolic curves over number fields (cf. [4], Problem 4.1):

> Let *X* be a hyperbolic curve over a number field [where we refer to the discussion entitled "Curves" (respectively, "Numbers") in "Notations and Conventions" concerning the term "hyperbolic curve" (respectively, "number field")]. Then are the following three conditions equivalent?

- (MT₁) X is quasi-Primes-monodromically full (cf. [2], Definition 2.2, (iii)).
- (MT₂) There exists a prime number *l* such that *X* is *l*monodromically full (cf. [2], Definition 2.2, (i)).
- (MT₃) There exists a *finite* subset $\Sigma \subseteq \mathfrak{Primes}$ of \mathfrak{Primes} such that X is ($\mathfrak{Primes} \setminus \Sigma$)-monodromically full.

2000 Mathematics Subject Classification. 14H30.

YUICHIRO HOSHI

Note that this is an *analogue for hyperbolic curves* of the equivalences " $(1) \Leftrightarrow (2) \Leftrightarrow (3)$ " in the following result due to J. P. Serre (cf. [5]):

Let *E* be an elliptic curve over a number field k, \overline{k} an algebraic closure of k, and $G_k \stackrel{\text{def}}{=} \text{Gal}(\overline{k}/k)$. Moreover, for each prime number l, write $T_l(E)$ for the l-adic Tate module of *E*. Then the following four conditions are equivalent:

- (0) *E* does not admit complex multiplication over \overline{k} .
- (1) For any prime number l, the image of the pro-lGalois representation $G_k \rightarrow \operatorname{Aut}(T_l(E))$ is an *open* subgroup of $\operatorname{Aut}(T_l(E))$.
- (2) There exists a prime number l such that the pro-lGalois representation $G_k \rightarrow \operatorname{Aut}(T_l(E))$ is surjective.
- (3) There exists a *finite* subset $\Sigma \subseteq \mathfrak{Primes}$ of \mathfrak{Primes} such that if $l \notin \Sigma$, then the pro-*l* Galois representation $G_k \to \operatorname{Aut}(T_l(E))$ is *surjective*.

In the present paper, we discuss the above problem due to M. Matsumoto and A. Tamagawa in the case where the given hyperbolic curve X is *of genus* 0. More concretely, we prove the following two results.

Theorem A. Let k be a number field. Then there exists a split (where we refer to the discussion entitled "Curves" in "Notations and Conventions" concerning the term "split") hyperbolic curve of type (0, 4) over k which satisfies (MT₃), hence also (MT₂), but does not satisfy (MT₁). Moreover, for any positive integer r > 4, there exists a split hyperbolic curve of type (0, r) over k which satisfies (MT₂) but does not satisfy (MT₁).

Theorem B. Let k be an imaginary quadratic field and X a hyperbolic curve of type (0, 4) over a subfield k_0 of k such that $X \otimes_{k_0} k$ is split. Then the following four conditions are equivalent:

- (1) There exists a prime number *l* such that *X* is quasi-*l*-monodromically full (cf. [2], Definition 2.2, (iii)).
- (2) There exists a prime number *l* such that X is *l*-monodromically full (cf. [2], Definition 2.2, (i)).
- (3) There exists a finite subset $\Sigma \subseteq \mathfrak{Primes}$ of \mathfrak{Primes} such that X is $(\mathfrak{Primes} \setminus \Sigma)$ -monodromically full.
- (4) \mathfrak{m}_X (cf. [2], Definition 7.10) does not contain any unit of the ring of integers of k, i.e., if $X \otimes_{k_0} k$ is isomorphic to

 $\mathbb{P}^1_k \setminus \{0, 1, \lambda, \infty\}$

— where $\lambda \in k \setminus \{0, 1\}$ *— over* k*, then*

$$\{\lambda,1-\lambda,\frac{\lambda}{\lambda-1}\}\cap\mathfrak{o}_k^\times=\emptyset$$

2

— where \mathfrak{o}_k is the ring of integers of k. In particular, the equivalence " $(MT_2) \Leftrightarrow (MT_3)$ " for such an X holds.

ACKNOWLEDGEMENTS

The author would like to thank Makoto Matsumoto and Akio Tamagawa for inspiring me by means of their problem given in [4]. This research was supported by Grant-in-Aid for Young Scientists (B) (No. 22740012).

NOTATIONS AND CONVENTIONS

Numbers: The notation \mathfrak{P} rimes will be used to denote the set of all prime numbers. The notation \mathbb{Z} will be used to denote the ring of rational integers. If p is a prime number, then the notation \mathbb{F}_p will be used to denote the finite field with p elements and the notation \mathbb{Z}_p will be used to denote the p-adic completion of \mathbb{Z} . We shall refer to a finite extension of the field of rational numbers as a *number field*.

Profinite Groups: If *G* is a profinite group, then we shall write Aut(G) for the group of (continuous) automorphisms of *G*, $Inn(G) \subseteq Aut(G)$ for the group of inner automorphisms of *G*, and

$$\operatorname{Out}(G) \stackrel{\text{def}}{=} \operatorname{Aut}(G) / \operatorname{Inn}(G)$$
.

If, moreover, *G* is *topologically finitely generated*, then one verifies easily that the topology of *G* admits a basis of *characteristic open subgroups*, which thus induces a *profinite topology* on the group Aut(G), hence also a *profinite topology* on the group Out(G).

Curves: Let k be a field and X a scheme over k. For a pair (g, r)of nonnegative integers, we shall say that *X* is a *smooth curve of type* (q,r) over k if there exist a scheme X^{cpt} of dimension 1 which is smooth, proper, and geometrically connected over k and a closed subscheme $D \subseteq X^{cpt}$ of X^{cpt} which is étale and of degree r over k such that the complement of D in X^{cpt} is isomorphic to X over k, and, moreover, a geometric fiber of $X^{\text{cpt}} \rightarrow \text{Spec} k$ is (a necessarily smooth, proper, and connected curve) of genus g. Note that it follows immediately that if X is a smooth curve of type (q, r) over k, then the pair " (X^{cpt}, D) " is uniquely determined up to isomorphism. We shall say that X is a *hyperbolic curve* over k if there exists a pair (q, r)of nonnegative integers such that 2g - 2 + r > 0, and, moreover, X is a smooth curve of type (g, r) over k. We shall say that X is a *tripod* over k if X is a smooth curve of type (0,3) over k. (Thus, any tripod over k is a hyperbolic curve over k.) Suppose that there exists a pair (q, r) of nonnegative integers such that X is a smooth curve of type (q, r) over k. Then we shall say that X is *split* if "D" appearing in the

YUICHIRO HOSHI

definition of the term "smooth curve of type (g, r)" is isomorphic to the disjoint union of r copies of Spec k over k.

PROOFS OF MAIN RESULTS

Let k be a field of characteristic 0 and \overline{k} an algebraic closure of k. Write $G_k \stackrel{\text{def}}{=} \operatorname{Gal}(\overline{k}/k)$ for the absolute Galois group of k determined by the algebraic closure \overline{k} and

$$\mathcal{M} \stackrel{\text{def}}{=} \mathbb{P}^1_k \setminus \{0, 1, \infty\} = \operatorname{Spec} k[t^{\pm 1}, 1/(1-t)]$$

— where t is an indeterminate — for the *split tripod* over k (where we refer to the discussion entitled "Curves" in "Notations and Conventions" concerning the terms "split" and "tripod"). Now we have a natural identification

$$\mathcal{M}(k) \simeq k \setminus \{0, 1\}$$

and an exact sequence of profinite groups

$$1 \longrightarrow \pi_1(\mathcal{M} \otimes_k \overline{k}) \longrightarrow \pi_1(\mathcal{M}) \longrightarrow G_k \longrightarrow 1.$$

Moreover, for each prime number *l*, write

$$\mu_{l^{\infty}} \subseteq \overline{k}^{\,\hat{}}$$

for the subgroup of \overline{k}^{\times} of all *l*-powers roots of unity.

Definition 1. Let *l* be a prime number.

(i) We shall write

$$\Delta^{\{l\}}$$

for the maximal pro-*l* quotient of $\pi_1(\mathcal{M} \otimes_k \overline{k})$.

(ii) Since the closed subgroup $\pi_1(\mathcal{M} \otimes_k \overline{k}) \subseteq \pi_1(\mathcal{M})$ of $\pi_1(\mathcal{M})$ is *normal*, conjugation by elements of $\pi_1(\mathcal{M})$ naturally determines continuous homomorphisms

$$\pi_1(\mathcal{M}) \longrightarrow \operatorname{Aut}(\Delta^{\{l\}}) ; G_k \longrightarrow \operatorname{Out}(\Delta^{\{l\}})$$

— where we refer to the discussion entitled "Profinite Groups" in "Notations and Conventions" concerning the profinite topologies of $Aut(\Delta^{\{l\}})$ and $Out(\Delta^{\{l\}})$. We shall write

$$\widetilde{\rho}^{\{l\}}$$
 ; $\rho^{\{l\}}$

for the above continuous homomorphisms, respectively. It follows immediately from the various definitions involved that these homomorphisms fit into the following commutative diagram of profinite groups

— where the horizontal sequences are *exact*; moreover, since $\Delta^{\{l\}}$ is *center-free*, the left-hand vertical arrow factors as the composite of the natural *surjection* $\pi_1(\mathcal{M} \otimes_k \overline{k}) \twoheadrightarrow \Delta^{\{l\}}$ and the natural *isomorphism* $\Delta^{\{l\}} \xrightarrow{\sim} \text{Inn}(\Delta^{\{l\}})$.

(iii) We shall write

$$\pi_1(\mathcal{M}) \twoheadrightarrow \Phi^{\{l\}}$$
 (respectively, $G_k \twoheadrightarrow G_k^{\text{tpd-}l}$)

for the quotient of $\pi_1(\mathcal{M})$ (respectively, G_k) by the kernel of the homomorphism $\tilde{\rho}^{\{l\}}$ (respectively, $\rho^{\{l\}}$). Thus, the commutative diagram in (ii) determines an exact sequence of profinite groups

$$1 \longrightarrow \Delta^{\{l\}} \longrightarrow \Phi^{\{l\}} \longrightarrow G_k^{\text{tpd-}l} \longrightarrow 1$$

(iv) We shall write

$$k^{\operatorname{tpd-}l} \, (\subseteq \overline{k})$$

for the algebraic extension of k corresponding to the quotient $G_k \twoheadrightarrow G_k^{\text{tpd-}l}$, i.e., $G_k^{\text{tpd-}l} = \text{Gal}(k^{\text{tpd-}l}/k)$.

Remark 2. In [3], the notation $\Delta_{\mathcal{M}/k}^{\{l\}}$ (respectively, $\tilde{\rho}_{\mathcal{M}/k}^{\{l\}}$; $\rho_{\mathcal{M}/k}^{\{l\}}$; $\Phi_{\mathcal{M}/k}^{\{l\}}$; $\Gamma_{\mathcal{M}/k}^{\{l\}}$) was used to denote the object $\Delta^{\{l\}}$ (respectively, $\tilde{\rho}^{\{l\}}$; $\rho^{\{l\}}$; $\rho^{\{l\}}$; $\Phi^{\{l\}}$; $G_k^{\{l\}}$) defined in Definition 1 of the present paper (cf. [3], Definition 1).

Lemma 3. Let *l* be a prime number and $\lambda \in k \setminus \{0, 1\}$. Then the following three conditions are equivalent:

(1) The split hyperbolic curve of type (0, 4) over k

 $\mathbb{P}^1_k \setminus \{0, 1, \lambda, \infty\}$

is l-monodromically full (*respectively*, quasi-*l*-monodromically full) [*cf.* [2], *Definition* 2.2].

- (2) The k-rational point of M naturally corresponding to λ ∈ k \ {0,1} is *l*-monodromically full (respectively, quasi-*l*-monodromically full) [cf. [3], Definition 3].
- (3) The image of the composite

$$G_k \longrightarrow \pi_1(\mathcal{M}) \longrightarrow \Phi^{\{l\}}$$

— where the first arrow is the outer homomorphism induced by $\lambda \in k \setminus \{0, 1\} \simeq \mathcal{M}(k)$ — is $\Phi^{\{l\}}$ (respectively, is an **open** subgroup of $\Phi^{\{l\}}$).

Proof. The equivalence " $(1) \Leftrightarrow (2)$ " follows from the second equivalence in [3], Remark 4. The equivalence " $(2) \Leftrightarrow (3)$ " follows from [3], Proposition 4, (iv).

Definition 4 (cf. [1], §2.3; 2.5). Let *l* be an odd prime number.

(i) We shall write

 \mathbb{S}_l

for the minimal set of finite subsets of $\mathbb{P}^1_{\overline{k}}(\overline{k}) \simeq \overline{k} \cup \{\infty\}$ which satisfies the following three conditions:

- (1) $\{0, 1, \infty\} \in \mathbb{S}_l$.
- (2) If $S \in \mathbb{S}_l$, then $\{a \in \overline{k} \mid a^l \in S\} \cup \{\infty\} \in \mathbb{S}_l$.
- (3) If $S \in \mathbb{S}_l$, and ϕ is an automorphism of $\mathbb{P}^1_{\overline{k}}$ over \overline{k} such that $\{0, 1, \infty\} \subseteq \phi(S)$, then $\phi(S) \in \mathbb{S}_l$.
- (ii) We shall write

$$\mathbb{E}_l \subseteq \overline{k}^{\times}$$

for the subgroup of \overline{k}^{\times} generated by the elements of $S \setminus \{0, \infty\}$ for all $S \in \mathbb{S}_l$.

Some of main results of [1] are as follows.

Proposition 5. Let *l* be an odd prime number. Then the following hold:

(i) $k^{\operatorname{tpd}-l} = k(\mathbb{E}_l).$

(ii)
$$(\mathbb{E}_l)^l = \mathbb{E}_l$$

(iii)
$$\mu_{l^{\infty}} \subseteq \mathbb{E}_l$$
.

Proof. This follows from [1], Theorems A and B.

Lemma 6. Let *l* be an odd prime number. Then $l \in \mathbb{E}_l$.

Proof. It follows from condition (1) of Definition 4, (i), that $\{0, 1, \infty\} \in S_l$. Thus, it follows from condition (2) of Definition 4, (i), that

 $S \stackrel{\text{def}}{=} \{0, 1, \zeta_l, \zeta_l^2, \cdots, \zeta_l^{l-1}, \infty\} \in \mathbb{S}_l$

— where $\zeta_l \in \overline{k}$ is an *l*-th root of unity. Now since the automorphism ϕ of $\mathbb{P}^1_{\overline{k}}$ over \overline{k} given by " $t \mapsto 1 - t$ " satisfies that $\{0, 1, \infty\} \subseteq \phi(S)$, it follows from condition (3) of Definition 4, (i), that

$$\phi(S) = \{1, 0, 1 - \zeta_l, 1 - \zeta_l^2, \cdots, 1 - \zeta_l^{l-1}, \infty\} \in \mathbb{S}_l.$$

Therefore,

$$l = \prod_{i=1}^{l-1} \left(1 - \zeta_l^i\right) \in \mathbb{E}_l.$$

This completes the proof of Lemma 6.

Lemma 7. Let l be a prime number. Suppose that $\mu_{l^{\infty}} \subseteq k$. For each positive integer n, write

$$C_{l^n} \stackrel{\text{def}}{=} \operatorname{Spec} k[x^{\pm 1}, y^{\pm 1}]/(x^{l^n} + y^{l^n} + 1) \longrightarrow \mathcal{M}$$

— where x and y are indeterminates — for the finite étale Galois $(\mathbb{Z}/l^n\mathbb{Z})^{\oplus 2}$ covering of \mathcal{M} given by " $t \mapsto x^{l^n}$ " and

$$\pi_1(\mathcal{M}) \twoheadrightarrow Q_l \simeq \mathbb{Z}_l^{\oplus 2}$$

for the quotient of $\pi_1(\mathcal{M})$ determined by the C_{l^n} 's. Then the quotient $\pi_1(\mathcal{M}) \twoheadrightarrow Q_l$ factors through the quotient $\pi_1(\mathcal{M}) \twoheadrightarrow \Phi^{\{l\}}$.

6

Proof. To verify Lemma 7, it is immediate that it suffices to verify the *fact* that for any positive integer *n*, the quotient $\pi_1(\mathcal{M}) \twoheadrightarrow (\mathbb{Z}/l^n\mathbb{Z})^{\oplus 2}$ determined by the finite étale covering $C_{l^n} \to \mathcal{M}$ *factors through* the quotient $\pi_1(\mathcal{M}) \twoheadrightarrow \Phi^{\{l\}}$. Moreover, to verify this *fact*, it follows immediately from [3], Proposition 7, (i), that it suffices to verify that the kernel of the pro-*l* outer Galois representation associated to \mathcal{M}/k (i.e., Ker($\rho^{\{l\}}$)) *coincides with* the kernel of the pro-*l* outer Galois representation associated to C_{l^n}/k . On the other hand, this follows immediately from [3], Proposition 9. This completes the proof of Lemma 7.

Proposition 8. Let *l* be an odd prime number and $\lambda \in k \setminus \{0, 1\}$. If either $\lambda \in \mathbb{E}_l \cap k$ (cf. Definition 4, (ii)) or λ is a **root of unity**, then the split hyperbolic curve of type (0, 4) over k

$$\mathbb{P}^1_k \setminus \{0, 1, \lambda, \infty\}$$

is not quasi-*l*-monodromically full.

Proof. To verify Proposition 8, it follows immediately from Lemma 3, together with the exactness of the sequence appearing in Definition 1, (iii), that, by replacing k by $k^{\text{tpd}-l} \subseteq \overline{k}$, we may assume without loss of generality that $k = k^{\text{tpd}-l}$. Write ϕ for the composite

$$G_k \longrightarrow \pi_1(\mathcal{M}) \longrightarrow Q_l$$

— where the first arrow is the outer homomorphism induced by $\lambda \in k \setminus \{0,1\} \simeq \mathcal{M}(k)$, and the second arrow is the natural surjection from $\pi_1(\mathcal{M})$ to the quotient Q_l defined in the statement of Lemma 7 (cf. Proposition 5, (i), (iii)). Moreover, for each positive integer n, write ϕ_n for the composite of ϕ and the natural surjection $Q_l \twoheadrightarrow Q_l/l^n Q_l (\simeq (\mathbb{Z}/l^n \mathbb{Z})^{\oplus 2})$ and $k_n \subseteq \overline{k}$ for the finite Galois extension of k corresponding to the quotient of G_k determined by the homomorphism ϕ_n . Then it follows immediately from the definition of the finite étale covering $C_{l^n} \to \mathcal{M}$ (where we refer to the statement of Lemma 7 concerning " $C_{l^n} \to \mathcal{M}$ ") that

$$k_n = k(\lambda^{1/l^n}, (1-\lambda)^{1/l^n}).$$

Now I *claim* that for any positive integer n, it holds that $k_n = k((1 - \lambda)^{1/l^n})$. Indeed, if $\lambda \in \mathbb{E}_l$, then it follows immediately from Proposition 5, (i), (ii), that $\lambda^{1/l^n} \in \mathbb{E}_l \subseteq k^{\text{tpd}-l} = k$; in particular, $k_n = k(\lambda^{1/l^n}, (1 - \lambda)^{1/l^n}) = k((1 - \lambda)^{1/l^n})$. On the other hand, if λ is a *root of unity*, then it follows immediately from Proposition 5, (i), (iii), that $\lambda^{1/l^n} \in k(\mu_{l^{\infty}}, \lambda) \subseteq k^{\text{tpd}-l}(\lambda) = k(\lambda)$; in particular, $k_n = k(\lambda^{1/l^n}, (1 - \lambda)^{1/l^n}) = k((1 - \lambda)^{1/l^n})$. This completes the proof of the above *claim*. Now it follows immediately from Lemma 3 that the hyperbolic curve of type (0, 4) over k

$$\mathbb{P}^1_k \setminus \{0, 1, \lambda, \infty\}$$

is quasi-l-monodromically full if and only if the image of the composite

$$G_k \longrightarrow \pi_1(\mathcal{M}) \longrightarrow \Phi^{\{l\}}$$

— where the first arrow is the outer homomorphism induced by $\lambda \in k \setminus \{0, 1\} \simeq \mathcal{M}(k)$ — is an *open* subgroup of $\Phi^{\{l\}}$. In particular, it follows from Lemma 7 that if $\mathbb{P}_k^1 \setminus \{0, 1, \lambda, \infty\}$ is *quasi-l-monodromically full*, then the image of ϕ is an *open* subgroup of Q_l . On the other hand, it follows immediately from the above *claim* that for any positive integer *n*, the image of ϕ_n is a *cyclic group*. In particular, the image of ϕ is *not open* in Q_l . Therefore, $\mathbb{P}_k^1 \setminus \{0, 1, \lambda, \infty\}$ is *not quasi-l-monodromically full*. This completes the proof of Proposition 8.

Proof of Theorem A. Let *l* be an odd prime number. Then since $l \in \mathbb{E}_l$ (cf. Lemma 6), it follows immediately from Proposition 8 that the hyperbolic curve of type (0, 4) over *k*

$$X \stackrel{\text{def}}{=} \mathbb{P}^1_k \setminus \{0, 1, l, \infty\}$$

is *not quasi-l-monodromically full*. On the other hand, since neither l, 1 - l, nor l/(l - 1) is a *unit* of the ring of integers of k, it follows from [2], Corollary 7.11, that there exists a *finite* subset $\Sigma \subseteq \mathfrak{Primes}$ of \mathfrak{Primes} such that X is ($\mathfrak{Primes} \setminus \Sigma$)-*monodromically full*. In particular, X satisfies the condition (MT₃) but does not satisfy the condition (MT₁). This completes the proof of the fact that there exists a split hyperbolic curve *of type* (0, 4) over k which *satisfies* (MT₃), hence also (MT₂), but does *not satisfy* (MT₁).

Moreover, let r > 4 be a positive integer and $l' \notin \Sigma$ a prime number. Then it follows from [3], Proposition 2, that there exists an l'-monodromically full k-rational point x (cf. [3], Definition 3) of the (r - 4)-th configuration space of the hyperbolic curve X/k. Since X is l'-monodromically full and x is l'-monodromically full, it follows from [3], Proposition 5, that the split hyperbolic curve Y of type (0, r) determined by x — i.e., the hyperbolic curve obtained by taking the complement in X of the images of r - 4 distinct k-rational points of X determined by x — is l'-monodromically full. In particular, Y satisfies the condition (MT₂). On the other hand, since $Y \subseteq X$, and X is not quasi-l-monodromically full. In particular, Y does not satisfy the condition (MT₁). This completes the proof of the fact that for any positive integer r > 4, there exists a split hyperbolic curve of type (0, r) over k which satisfies (MT₂) but does not satisfy (MT₁).

Proof of Theorem B. The implication " $(4) \Rightarrow (3)$ " follows from [2], Corollary 7.11. The implications " $(3) \Rightarrow (2) \Rightarrow (1)$ " are immediate.

The implication "(1) \Rightarrow (4)" follows from Proposition 8, together with the fact that every unit of the ring of integers of an imaginary quadratic field is a root of unity.

References

- G. Anderson and Y. Ihara, Pro-*l* branched coverings of P¹ and higher circular *l*-units, *Ann. of Math.* (2) 128 (1988), no. 2, 271–293.
- [2] Y. Hoshi, Galois-theoretic characterization of isomorphism classes of monodromically full hyperbolic curves of genus zero, INI preprint NI09074-NAG; see http://www.kurims.kyoto-u.ac.jp/~yuichiro/papers_e.html for a revised version.
- monodromically [3] Y. Hoshi, On full points of configuraof hyperbolic curves, RIMS 1700; tion spaces preprint see http://www.kurims.kyoto-u.ac.jp/~yuichiro/papers_e.html for а revised version.
- [4] M. Matsumoto and A. Tamagawa, Mapping-class-group action versus Galois action on profinite fundamental groups, *Amer. J. Math.* **122** (2000), no. **5**, 1017– 1026.
- [5] J. P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.* **15** (1972), no. **4**, 259–331.

(Yuichiro Hoshi) RESEARCH INSTITUTE FOR MATHEMATICAL SCIENCES, KY-OTO UNIVERSITY, KYOTO 606-8502, JAPAN

E-mail address: yuichiro@kurims.kyoto-u.ac.jp