Anabelian geometry of curves over algebraically closed fields of positive characteristic: the case of one-punctured elliptic curves (Algebraic Number Theory and Related Topics 2017)

AUTHOR(S):

Sarashina, Akira

CITATION:

Sarashina, Akira. Anabelian geometry of curves over algebraically closed fields of positive characteristic: the case of one-punctured elliptic curves (Algebraic Number Theory and Related Topics 2017). 数理解析研究所講究録別冊 2020, B83: 235-241

ISSUE DATE:

2020-10

URL:

http://hdl.handle.net/2433/260702

RIMS Kôkyûroku Bessatsu
B83 (2020), 235–241

Anabelian geometry of curves over algebraically closed fields of positive characteristic: the case of one-punctured elliptic curves

By

Akira Sarashina*

Abstract

This article is an announcement of the author's recent work on anabelian geometry over algebraically closed fields of positive characteristic. We review some known results in this area and give a sketch of the proof of the main result which concerns reconstruction of curves of $(1,1)$-type by their geometric fundamental groups.

§ 1. Étale fundamental groups of curves

In this section, we review some properties of étale fundamental groups of curves over a field which is not necessarily of positive characteristic or algebraically closed. First we define some notations.

Definition 1.1.
Let k be a field, $\overline{k}$ an algebraic closure of k, and U a scheme geometrically connected and of finite type over k. Let G_k denote the absolute Galois group of k, and $\pi_1(U)$ the étale fundamental group of U (with respect to a suitable choice of base point). We sometimes call $\pi_1(U \times_k \overline{k})$ the geometric fundamental group of U.

Then we have the following short exact sequence of profinite groups

Received March 30, 2018. Revised May 9, 2019.
2010 Mathematics Subject Classification(s): 14H30.
Key Words: *curve, étale fundamental group, positive characteristic.*
Supported by JSPS KAKENHI Grant Number 18J13541.
*RIMS, Kyoto University, Kyoto 606-8502, Japan.
e-mail: sarashin@kurims.kyoto-u.ac.jp

$$1 \longrightarrow \pi_1(U \times_k \overline{k}) \longrightarrow \pi_1(U) \xrightarrow{Pr_U} \pi_1(Spec(k)) \longrightarrow 1.$$
$$\Vert$$
$$G_k$$

In the early 1980s, Grothendieck advocated that $Pr_U : \pi_1(U) \twoheadrightarrow G_k$ should determine the geometry of U when U is an anabelian variety ([3], [2]). This philosophy is called the Grothendieck conjecture nowadays. Grothendieck did not give a definition of anabelian variety, but considered that one-dimensional anabelian varieties are nothing but hyperbolic curves. The following theorem was proved by Nakamura, Tamagawa and Mochizuki in the 1990s.

Theorem 1.2 (Grothendieck conjecture for hyperbolic curves) ([4] Theorem A)**.** *Suppose that k is a sub-p-adic field (i.e. a subfield of finitely generated extension field of $\mathbb{Q}_p$), and U_1 and U_2 are hyperbolic curves over k (i.e. for $i = 1, 2$, U_i is a smooth geometrically connected curve over k such that $2g_i + n_i - 2 > 0$, where g_i stands for the genus of the smooth compactification of U_i and n_i stands for the cardinality of the complement of U_i in its smooth compactification). Let $Isom_{G_k}(\pi_1(U_1), \pi_1(U_2))$ denote the set $\{F \in Isom(\pi_1(U_1), \pi_1(U_2)) | Pr_{U_1} = Pr_{U_2} \circ F\}$. Then the natural map*

$$Isom_{(k\text{-}sch)}(U_1, U_2) \to Isom_{G_k}(\pi_1(U_1), \pi_1(U_2))/Inn(\pi_1(U_2 \times_k \overline{k}))$$

is bijective. □

This theorem especially says that $U_1 \simeq U_2$ over k if $\pi_1(U_1) \simeq \pi_1(U_2)$ over G_k, but this does not hold when k is an algebraically closed field of characteristic 0.

Theorem 1.3 ([1] XII)**.** *Suppose that k is an algebraically closed field of characteristic 0 and that U is a curve over k. Let $\Pi_{g,n}$ be the profinite completion of the group*

$$< \alpha_1, \beta_1, \cdots, \alpha_g, \beta_g, \gamma_1, \cdots, \gamma_n \mid \alpha_1\beta_1\alpha_1^{-1}\beta_1^{-1} \cdots \alpha_g\beta_g\alpha_g^{-1}\beta_g^{-1}\gamma_1 \cdots \gamma_n >,$$

where g is the genus of the smooth compactification of U and n is the cardinality of the complement of U in its smooth compactification. Then we have the following isomorphism: $\pi_1(U) \simeq \Pi_{g,n}$. □

In this situation, the isomorphism class of $\pi_1(U)$ is determined by (g, n). But there are two distinct isomorphism classes of hyperbolic curves which have the same (g, n). For example, observe $\Pi_{0,3} \simeq \Pi_{1,1}$. If k is an algebraically closed field of positive characteristic, this theorem does not hold and geometric fundamental groups have more information.

§ 2. Anabelian geometry of curves over algebraically closed fields of positive characteristic

In this section, we present the main problem and the statement of the main result of this article. We assume that k is an algebraically closed field of positive characteristic from now on. We use the same symbols as in the previous section. Let p be the characteristic of k.

Theorem 2.1 (Tamagawa[10] Theorem 1.9)**.**
Let U_1 and U_2 be curves over k such that $\pi_1(U_1) \simeq \pi_1(U_2)$. Then (g_1, n_1) is equal to (g_2, n_2). □

This statement does not hold when the characteristic is 0 as we have seen in the previous section.

The main problem of this article is the following conjecture.

Conjecture.
For $i = 1, 2$, let U_i be a curve of (g_i, n_i)-type over k. Suppose that $(g_1, n_1) \neq (1, 0)$ and $\pi_1(U_1) \simeq \pi_1(U_2)$. Then U_1 is isomorphic to U_2 as schemes.

When (g_1, n_1) is equal to $(1, 0)$ (i.e. U_1 is a (proper) elliptic curve over k), $\pi_1(U_1)$ is isomorphic to $\prod_{l \neq p, l:\text{prime}} \mathbb{Z}_l \times \mathbb{Z}_l$ or $\mathbb{Z}_p \times (\prod_{l \neq p, l:\text{prime}} \mathbb{Z}_l \times \mathbb{Z}_l)$ (see [1] X). But there are infinitely many isomorphism classes of elliptic curves. Thus the statement of the conjecture does not hold when (g_1, n_1) is equal to $(1, 0)$.

In this conjecture, it is expected that U_1 is isomorphic to U_2 as schemes, not as k-schemes. Because the étale fundamental group cannot determine the isomorphism class of the curve as a k-scheme. For example, let U be a punctured elliptic curve over k such that the j-invariant $j(U)$ of its smooth compactification is not in $\mathbb{F}_p$ and F the Frobenius map of k. Then, U is not k-isomorphic to $U \times_{k,F} k$ since $j(U) \neq j(U)^p = j(U \times_{k,F} k)$, while, since $U \simeq U \times_{k,F} k$ as schemes, $\pi_1(U)$ is isomorphic to $\pi_1(U \times_{k,F} k)$.

Regarding this conjecture, the following theorems were known.

Theorem 2.2 (Tamagawa[10] Theorem 3.5)**.**
Let U_1 and U_2 be curves over $\overline{\mathbb{F}}_p$ such that $g_1 = 0$ and $\pi_1(U_1) \simeq \pi_1(U_2)$. Then U_1 is isomorphic to U_2 as schemes. □

Theorem 2.3 (Tamagawa[11] Theorem(8.6))**.**
Let U be a curve over $\overline{\mathbb{F}}_p$ such that (g, n) is not equal to $(1, 0)$. Then there are only finitely many isomorphism classes of curves over $\overline{\mathbb{F}}_p$ whose étale fundamental group is isomorphic to $\pi_1(U)$. □

The following generalization of Theorem2.2 is the main result of [8].

Theorem 2.4 ([8] Theorem 4.9)**.**
Let U_1 and U_2 be curves over $\overline{\mathbb{F}}_p$ such that $p \neq 2$, $(g_1, n_1) = (1, 1)$ and $\pi_1(U_1) \simeq \pi_1(U_2)$. Then U_1 is isomorphic to U_2 as schemes.

In the next section, we will give a sketch of the proof of Theorem 2.4.

Remark. We need the assumption $p \neq 2$ in the proof of Theorem 3.3 and Lemma 3.4 (see §3).

Remark. Theorem 1.2 for genus 0 curves over number fields was proved by H. Nakamura (cf.[6]). Then he proved Theorem 1.2 for curves of $(1, 1)$-type, reducing it to the case of genus 0 curves (cf.[5][7]). The proof of Theorem 2.4 borrows various techniques from the proof of Theorem 2.2 in [10], but is not reduced to Theorem 2.2 itself.

§ 3. Sketch of the proof of the Theorem 2.4

Let E_1 and E_2 be elliptic curves over $\overline{\mathbb{F}}_p$, $\mathcal{O}_1$ and $\mathcal{O}_2$ closed points of E_1 and E_2 respectively such that $\pi_1(E_1 \backslash \{\mathcal{O}_1\}) \simeq \pi_1(E_2 \backslash \{\mathcal{O}_2\})$. We always consider that E_1 and E_2 are equipped with the group structure with respect to $\mathcal{O}_1$ and $\mathcal{O}_2$, respectively.

Our goal is to prove that $E_1 \backslash \{\mathcal{O}_1\} \simeq E_2 \backslash \{\mathcal{O}_2\}$ (as schemes), which is equivalent to $E_1 \simeq E_2$. Let λ_1 and λ_2 be λ-invariants of E_1 and E_2 respectively, in their Legendre form (Recall that $p \neq 2$). It suffices to show that the minimal polynomial of λ_1 over $\mathbb{F}_p$ is identical to that of λ_2 (Here we use the assumption that $k = \overline{\mathbb{F}}_p$). To prove this, we use the additive structure of elliptic curves in combination with the additive structure on $\mathbb{P}^1(k) \backslash \{\infty\} = k$. We prove that the additive structure of the elliptic curves is determined by π_1 in Lemma 3.2 (Note that $E_i = \cup_{m>0} E_i[m]$ by the assumption that $k = \overline{\mathbb{F}}_p$). We prove that the additive structure on $\mathbb{P}^1 \backslash \{\infty\}$ is determined by π_1 in Theorem 3.3.

Lemma 3.1 (Tamagawa[10] Theorem 2.5)**.**
Let U be a curve over an algebraically closed field k of positive characteristic, and X the smooth compactification of U. Then the set of cusps $X \backslash U$ can be recovered group-theoretically from $\pi_1(U)$ as a quotient set of the set of inertia subgroups. □

We will consider étale covers of $E_1 \backslash \{\mathcal{O}_1\}$ and $E_2 \backslash \{\mathcal{O}_2\}$, and calculate some invariants of the cusps.

Lemma 3.2 ([8] Lemma 4.2 and the proof of Theorem 4.9)**.**
Let m be a positive integer.

(1) *We can identify* $\pi_1(E_1\backslash E_1[m])$ *(resp.* $\pi_1(E_2\backslash E_2[m])$*) with a certain subgroup of* $\pi_1(E_1\backslash\{\mathcal{O}_1\})$ *(resp.* $\pi_1(E_2\backslash\{\mathcal{O}_2\})$*), such that* $\pi_1(E_1\backslash\{\mathcal{O}_1\}) \simeq \pi_1(E_2\backslash\{\mathcal{O}_2\})$ *restricts to* $\pi_1(E_1\backslash E_1[m]) \simeq \pi_1(E_2\backslash E_2[m])$.

(2) *The natural bijection* $\varphi_m : E_1[m] \simeq E_2[m]$ *induced by* $\pi_1(E_1\backslash E_1[m]) \simeq \pi_1(E_2\backslash E_2[m])$ *(cf. Lemma3.1) is a group isomorphism.*

□

We may assume that m is a multiple of 4 and E_1 (resp. E_2) $\subset \mathbb{P}^2$ is defined by $y^2 = x(x-1)(x-\lambda_1)$ (resp. $y^2 = x(x-1)(x-\lambda_2)$) such that

$$(\varphi_m((0,0)), \varphi_m((1,0)), \varphi_m((\lambda_1,0)), \varphi_m(\infty)) = ((0,0),(1,0),(\lambda_2,0),\infty).$$

If the minimal polynomial of λ_1 over $\mathbb{F}_p$ is equal to that of λ_2, there is an isomorphism $\psi : k \simeq k$ such that $\psi(\lambda_1) = \lambda_2$, then $E_1\backslash\{\mathcal{O}_1\}$ and $(E_2\backslash\{\mathcal{O}_2\}) \times_{k,\psi} k$ are expressed by the same polynomial and the cusps are ∞. Thus, Theorem 2.4 holds. To prove the above hypothesis on the minimal polynomials, we use the group structure on $E_1[m]$ and $E_2[m]$ and the additive structure on $k = \mathbb{P}^1(k)\backslash\{\infty\}$. Let $x_1 : E_1 \to \mathbb{P}^1$ (resp. $x_2 : E_2 \to \mathbb{P}^1$) be the projection to the x-axis (with respect to the above embedding E_1 (resp. E_2) $\subset \mathbb{P}^2$). This projection induces a homomorphism $\pi_1(E_1\backslash E_1[m]) \to \pi_1(\mathbb{P}^1\backslash x_1(E_1[m]))$ (resp. $\pi_1(E_2\backslash E_2[m]) \to \pi_1(\mathbb{P}^1\backslash x_2(E_2[m]))$) and a map $E_1[m] \to x_1(E_1[m])$ (resp, $E_2[m] \to x_2(E_2[m])$).

Theorem 3.3 ([8] Proposition 3.1, Theorem 4.3 and Corollary 4.8)**.**

(1) *The isomorphism* $\pi_1(E_1\backslash E_1[m]) \simeq \pi_1(E_2\backslash E_2[m])$ *preserves the kernels of* $(\pi_1(E_1\backslash E_1[m]) \to \pi_1(\mathbb{P}^1\backslash x_1(E_1[m])) \to (\pi_1(\mathbb{P}^1\backslash x_1(E_1[m])))^{ab,p'}$*) and* $(\pi_1(E_2\backslash E_2[m]) \to \pi_1(\mathbb{P}^1\backslash x_2(E_2[m])) \to (\pi_1(\mathbb{P}^1\backslash x_2(E_2[m])))^{ab,p'}$*) (here,* $(-)^{ab}$ *stands for the abelianization and* $(-)^{p'}$ *stands for the maximal prime to* p *quotient), and the isomorphism* $\varphi_m : E_1[m] \simeq E_2[m]$ *induces a bijection*

$$\overline{\varphi}_m : x_1(E_1[m]) \simeq x_2(E_2[m]).$$

(2) *For any* $a_P \in \mathbb{F}_p$ *(*$P \in x_1(E_1[m])\backslash\{0,\infty\}$*), the linear relation*

$$\sum_{P \in x_1(E_1[m])\backslash\{0,\infty\}} a_P P = 0$$

holds if and only if the linear relation

$$\sum_{P \in x_1(E_1[m])\backslash\{0,\infty\}} a_P \overline{\varphi}_m(P) = 0$$

holds.

□

For any $\alpha_1, \alpha_2, \alpha_3 \in E_1[m]$ such that $x_1(\alpha_1) + x_1(\alpha_2) = x_1(\alpha_3)$, this theorem says that the equation $x_2(\varphi_m(\alpha_1)) + x_2(\varphi_m(\alpha_2)) = x_2(\varphi_m(\alpha_3))$ holds. Lemma 3.2 and Theorem 3.3 imply that both the additive structure on $E_i[m] \subset E_i$ and the additive structure on $x_i(E_i[m])\backslash\{\infty\} \subset k$ can be recovered from $\pi_1(E_i\backslash\{\mathcal{O}_i\})$. The following additive formula for elliptic curves gives a relation between these two additive structures.

Lemma 3.4.
Let F be a field of characteristic $\neq 2$, $\lambda \in F \setminus \{0,1\}$, and $E : y^2 = x(x-1)(x-\lambda)$ an elliptic curve over F with the origin $\mathcal{O} = (\infty, \infty)$. Consider the affine part of the projection $x : E \to \mathbb{P}^1$ as a map:

$$x : E\backslash\{\mathcal{O}\} \to \mathbb{A}^1 = \mathbb{P}^1\backslash\{\infty\}.$$

For each $a \in \mathbb{A}^1(F)$, pick $Q_a \in x^{-1}(a)(\subset E(\overline{F}))$. Then, for $a \in \mathbb{A}^1(F)$ and $b \in \mathbb{A}^1(F)\backslash\{0\}$, we have

(1) $x(Q_a + Q_{a+b}) + x(Q_a - Q_{a+b}) = \frac{4}{b^2}a^3 + (\frac{6}{b} - \frac{4\lambda}{b^2} - \frac{4}{b^2})a^2 + (2 - \frac{4}{b} - \frac{4\lambda}{b} + \frac{4\lambda}{b^2})a + \frac{2\lambda}{b}$.

Moreover, in the special case of $a = \lambda$, $b = 1$, we have

(2) $x(Q_\lambda + Q_{\lambda+1}) = x(Q_\lambda - Q_{\lambda+1}) = \lambda^2$.

Proof .
The formula (1) follows from ([9] Chapter III, Group Law Algorithm 2.3) where $a_1 = a_3 = a_6 = 0$, $a_2 = -1 - \lambda$ and $a_4 = \lambda$. □

Clearly, the right hand side (hence also the left hand sides) of Lemma 3.4 (1) does not depend on the choice of Q_a, Q_{a+b}. Similarly, λ^2 (hence also $x(Q_\lambda + Q_{\lambda+1}), x(Q_\lambda - Q_{\lambda+1})$) does not depend on the choice of $Q_{\lambda+1}$.

Let us return to the proof of Theorem 2.4. For $i = 1, 2$ and $a \in \mathbb{A}^1(\overline{\mathbb{F}}_p)$, pick $Q_a^{(i)} \in x_i^{-1}(a)$. When $Q^{(1)}_{\lambda_1+1}, Q^{(1)}_{\lambda_1^2} \in E_1[m]$, Lemma 3.4 (2) says that $Q^{(2)}_{\lambda_2^2} \in E_2[m]$ and $\overline{\varphi}_m(\lambda_1^2) = \lambda_2^2$. (Recall from Theorem 3.3 (1), we have a bijection $\overline{\varphi}_m : x_1(E_1[m]) \to x_2(E_2[m])$. Note that $Q^{(2)}_{\lambda_2+1} \in E_2[m]$ and $\overline{\varphi}_m(\lambda_1 + 1) = \lambda_2 + 1$ are already known by Theorem 3.3.) Let f_1 (resp. f_2) stand for the minimal polynomial of λ_1 (resp. λ_2) over $\mathbb{F}_p$. Further, by using Lemma 3.4(1) and the induction on the degree, we can prove that $Q^{(1)}_{\lambda_1^2}, \cdots, Q^{(1)}_{\lambda_1^{degf_1}} \in E_1[m]$, $Q^{(2)}_{\lambda_2^2}, \cdots, Q^{(2)}_{\lambda_2^{degf_1}} \in E_2[m]$ and $\overline{\varphi}_m(\lambda_1^2) = \lambda_2^2, \cdots, \overline{\varphi}_m(\lambda_1^{degf_1}) = \lambda_2^{degf_1}$ for suitable m. We can regard $f_1(\lambda_1) = 0$ as a linear relation of $1, \lambda_1, \cdots, \lambda_1^{degf_1}$ over $\mathbb{F}_p$. Therefore we have $f_1(\lambda_2) = 0$ by Theorem 3.3. Similarly, we have $f_2(\lambda_1) = 0$, thus $f_1 = f_2$. This completes the proof of Theorem 2.4. □

References

[1] A. Grothendieck. *Revêtements étales et groupe fondamental (SGA1)*, Vol. 1960/61 of *Séminaire de Géométrie Algébrique*. Institut des Hautes Études Scientifiques, Paris, 1963.

[2] A. Grothendieck. Brief an G. Faltings. In *Geometric Galois actions, 1*, Vol. 242 of *London Math. Soc. Lecture Note Ser.*, pp. 49–58. Cambridge Univ. Press, Cambridge, 1997. With an English translation on pp. 285–293.

[3] A. Grothendieck. Esquisse d'un programme. In *Geometric Galois actions, 1*, Vol. 242 of *London Math. Soc. Lecture Note Ser.*, pp. 5–48. Cambridge Univ. Press, Cambridge, 1997. With an English translation on pp. 243–283.

[4] S. Mochizuki. The local pro-p anabelian geometry of curves. *Invent. Math.*, Vol. 138, No. 2, pp. 319–423, 1999.

[5] H. Nakamura. On Galois rigidity of fundamental groups of algebraic curves (in Japanese). In *Proceedings of the 35th Algebra Symposium held at Hokkaido University in 1989*, pp. 186–199, 1989.

[6] H. Nakamura. Galois rigidity of the étale fundamental groups of punctured projective lines. *J. Reine Angew. Math.*, Vol. 411, pp. 205–216, 1990.

[7] H. Nakamura. On Galois rigidity of fundamental groups of algebraic curves. In *Non-abelian fundamental groups and Iwasawa theory*, Vol. 393 of *London Math. Soc. Lecture Note Ser.*, pp. 56–71. Cambridge Univ. Press, Cambridge, 2012.

[8] A. Sarashina. Reconstruction of one-punctured elliptic curves in positive characteristic by their geometric fundamental groups. *RIMS Preprint, No.1876*, 2017.

[9] Joseph H. Silverman. *The arithmetic of elliptic curves*, Vol. 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986.

[10] A. Tamagawa. On the fundamental groups of curves over algebraically closed fields of characteristic > 0. *Internat. Math. Res. Notices*, No. 16, pp. 853–873, 1999.

[11] A. Tamagawa. Finiteness of isomorphism classes of curves in positive characteristic with prescribed fundamental groups. *J. Algebraic Geom.*, Vol. 13, No. 4, pp. 675–724, 2004.