Summary of "Reconstruction of open subschemes of elliptic curves in positive characteristic by their geometric fundamental groups under some assumptions"

Akira Sarashina

This is a summary of [2]. We discuss some general properties of elliptic curves over finite fields, and an application of these properties to anabelian geometry in [2].

First we will show a certain general property of elliptic curves over finite fields. Let p be a prime number, let $q = p^n$ $(n \geq 1)$, and E an elliptic curve over $\mathbb{F}_q$ which is defined by a nonsingular Weierstrass form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

where a_1, a_2, a_3, a_4, $a_6 \in \mathbb{F}_q$. Let $\mathcal{O}$ be the identity element of E. Let

$$x : E \to \mathbb{P}^1$$

be the finite morphism of degree 2 such that $x((a, b)) = a$ and $x(\mathcal{O}) = \infty$.

Definition. For any positive integer r, let H_r be the endmorphism of $\mathbb{P}^1$ which makes the following diagram commutative.

$$\begin{array}{ccc} E & \xrightarrow{[r]} & E \\ {\scriptstyle x}\downarrow & & \downarrow{\scriptstyle x} \\ \mathbb{P}^1 & \xrightarrow{H_r} & \mathbb{P}^1 \end{array}$$

Here, $[r]$ stands for the multiplication by r.

For any endmorphism f of E, set

$$E[f] = \{P \in E(\overline{\mathbb{F}}_p) \mid f(P) = \mathcal{O}\}.$$

If $f = [r]$, we write $E[r]$ as $E[[r]]$. The main result of the first part of [2] is the following.

Theorem 1. Let m be a positive integer. Then there exists a positive even integer r which satisfies the following.

$$x(E[m]) \subset H_r(\langle x(E[r]) \setminus \{\infty\} \rangle_{\mathbb{F}_p})$$

Here, $\langle x(E[r]) \setminus \{\infty\} \rangle_{\mathbb{F}_p}$ stands for the $\mathbb{F}_p$-vector subspace generated by $x(E[r]) \setminus \{\infty\}$ in $\overline{\mathbb{F}}_p = \mathbb{A}^1(\overline{\mathbb{F}}_p)$. $\square$

Let $P \in E(\overline{\mathbb{F}}_p)$.

$$x(P) \in H_r(\langle x(E[r]) \setminus \{\infty\} \rangle_{\mathbb{F}_p})$$

holds if and only if we have

$$x([r]^{-1}(P)) \cap \langle x(E[r]) \setminus \{\infty\} \rangle_{\mathbb{F}_p} \neq \phi.$$

This means that at least one of the points of $x([r]^{-1}(P))$ can be written as a linear combination of the points of $x(E[r]) \setminus \{\infty\}$.

In the second part of [2], we consider an application of Theorem 1 to anabelian geometry. Let U_1 and U_2 be nonempty affine open subschemes of elliptic curves $(E_1, \mathcal{O}_1)$ and $(E_2, \mathcal{O}_2)$ over $\overline{\mathbb{F}}_p$ respectively such that

$$\alpha_1 : \pi_1(U_1) \xrightarrow{\sim} \pi_1(U_2).$$

Theorem 2 ([1] Corollary 4.10)**.** We have the following isomorphism of $\mathbb{F}_p$-schemes.

$$E_1 \simeq E_2$$

$\square$

We identify E_1 with E_2 and write $(E, \mathcal{O})$ instead of $(E_1, \mathcal{O}_1)$ and $(E_2, \mathcal{O}_2)$. By a similar argument to [1] Lemma 4.2, α_1 induces an isomorphism

$$\alpha_s : \pi_1([s]^{-1}(U_1)) \xrightarrow{\sim} \pi_1([s]^{-1}(U_2))$$

for each $s > 0$, which makes the following diagram commutative.

$$\begin{array}{ccc} \pi_1([s]^{-1}(U_1)) & \xrightarrow[\alpha_s]{\sim} & \pi_1([s]^{-1}(U_2)) \\ \downarrow & & \downarrow \\ \pi_1(U_1) & \xrightarrow[\alpha_1]{\sim} & \pi_1(U_2) \end{array}$$

Set $S_1 = E \setminus U_1$ and $S_2 = E \setminus U_2$. By [3] Theorem 2.5, α_s induces a bijection

$$\phi_s : [s]^{-1}(S_1) \xrightarrow{\sim} [s]^{-1}(S_2)$$

for each $s > 0$. The group $\mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\}$ acts on E as follows.

$$gP = \begin{cases} P & (g = \overline{0}) \\ -P & (g = \overline{1}) \end{cases}$$

where $g \in \mathbb{Z}/2\mathbb{Z}$ and $P \in E$. We put the following assumption.

(A2) S_1 and S_2 are closed under the action of $\mathbb{Z}/2\mathbb{Z}$ and ϕ_1 preserves this action.

(Assumption (A1) appears below.) Under assumption (A2), $[s]^{-1}(S_1)$ and $[s]^{-1}(S_2)$ are closed under the action of $\mathbb{Z}/2\mathbb{Z}$ for any $s > 0$. Let m be a positive integer such that

$$S_1 \subset E[m].$$

By Theorem 1, we can take a positive even integer r such that

$$x(E[m]) \subset H_r(\langle x(E[r]) \setminus \{\infty\}\rangle_{\mathbb{F}_p}).$$

Definition. Let

$$L_{i,r} = \ker(\pi_1([r]^{-1}(U_i)) \to \pi_1(\mathbb{P}^1 \setminus T_{i,r}) \to \pi_1(\mathbb{P}^1 \setminus T_{i,r})^{ab,p'}).$$

Here, $T_{i,r} = x([r]^{-1}(S_i))$ $(i = 1, 2)$. Note that we can define the natural surjection $[r]^{-1}(U_i) \to \mathbb{P}^1 \setminus T_{i,r}$ because $[r]^{-1}(S_1)$ and $[r]^{-1}(S_2)$ are closed under the action of $\mathbb{Z}/2\mathbb{Z}$.

Then we put the following assumption, which depends on r.

(A3(r)) $\alpha_r(L_{1,r}) = L_{2,r}$

We can assume the following conditions by replacing the open immersions $U_1 \to E$ and $[r]^{-1}(U_1) \to E$ with suitable ones.

- $\mathcal{O} \in S_1, \mathcal{O} \in S_2$ and $\phi_r(\mathcal{O}) = \mathcal{O}$.
- ϕ_r preserves the action of $\mathbb{Z}/2\mathbb{Z}$.

(Assumption (A3(r)) is used in the proof of the second condition.) So there is a bijection $\psi_r : T_{1,r} \to T_{2,r}$ which makes the following diagram commutative.

$$\begin{array}{ccc} [r]^{-1}(S_1) & \xrightarrow[\phi_r]{\sim} & [r]^{-1}(S_2) \\ \downarrow{\scriptstyle x} & & \downarrow{\scriptstyle x} \\ T_{1,r} & \xrightarrow[\psi_r]{\sim} & T_{2,r} \end{array}$$

The condition

$$P \in H_r(\langle x(E[r]) \setminus \{\infty\}\rangle_{\mathbb{F}_p})$$

implies that there is a linear relation

$$x(Q) = \sum_{\mu \in x(E[r]) \setminus \{\infty\}} a_\mu \mu$$

for some $Q \in [r]^{-1}(P)$ and some a_μ $(\mu \in x(E[r]) \setminus \{\infty\})$. Then we have an equality

$$x(\phi_r(Q)) = \sum_{\mu \in x(E[r]) \setminus \{\infty\}} a_\mu \psi_r(\mu)$$

because of assumption (A3(r)) and [1] Theorem 3.3. By [3] Corollary 1.10, α_1 naturally induces an isomorphism

$$\theta : \pi_1(E) \simeq \pi_1(E)$$

which makes the following diagram commutative.

$$\begin{array}{ccc} \pi_1(U_1) & \xrightarrow{\sim} & \pi_1(U_2) \\ \downarrow & & \downarrow \\ \pi_1(E) & \xrightarrow[\theta]{\sim} & \pi_1(E) \end{array}$$

We put the following assumption.

(A1) θ is contained in the image of the map $\pi_1 : Aut_{\mathbb{F}_p}(E) \to Aut(\pi_1(E))$.

We can replace the open immersions $U_i \to E$ $(i = 1, 2)$ with suitable ones and prove the following condition by using assumption (A1).

- $\phi_s|_{E[s]} = id|_{E[s]}$ for any $s > 0$

Hence $\psi_r|_{x(E[r])} = id|_{x(E[r])}$ holds. So we have the following equality.

$$x(Q) = \sum_{\mu \in x(E[r]) \setminus \{\infty\}} a_\mu \mu = \sum_{\mu \in x(E[r]) \setminus \{\infty\}} a_\mu \psi_r(\mu) = x(\phi_r(Q))$$

This implies that

$$x(P) = x(\phi_1(P)).$$

By applying the above argument to all the points of S_1 (note that r does not depend on the choice of P), we have the following theorem, which is the main result of [2].

Theorem 3. Let $p \geq 3$ be a prime number, U_1 and U_2 nonempty affine open subschemes of an elliptic curve $(E, \mathcal{O})$ respectively over $\overline{\mathbb{F}}_p$ such that

$$\pi_1(U_1) \simeq \pi_1(U_2).$$

We assume that

$$\mathcal{O} \in S_1,$$
$$\mathcal{O} \in S_2$$

and

$$\phi_1(\mathcal{O}) = \mathcal{O}.$$

Let m be a positive integer such that $S_1 \subset E[m]$, r a positive even integer such that

$$x(E[m]) \subset H_r(\langle x(E[r]) \setminus \{\infty\} \rangle_{\mathbb{F}_p}).$$

We assume (A1), (A2) and (A3(r)). Then

$$U_1 \simeq U_2$$

holds. □

References

[1] A. Sarashina. Reconstruction of one-punctured elliptic curves in positive characteristic by their geometric fundamental groups. *manuscripta mathematica*, Vol. 163, No. 1, pp. 201–225, 2020.

[2] A. Sarashina. Reconstruction of open subschemes of elliptic curves in positive characteristic by their geometric fundamental groups under some assumptions. *Thesis*, 2020.

[3] A. Tamagawa. On the fundamental groups of curves over algebraically closed fields of characteristic > 0. *Internat. Math. Res. Notices*, Vol. 1999, No. 16, pp. 853–857, 1999.