数理解析研究所講究録 1267 巻 2002 年 157-166

ON CURVE CORRESPONDENCES

by

Fedor Bogomolov and Yuri Tschinkel

ABSTRACT. — We study correspondences between algebraic curves defined over the algebraic closure of $\mathbb{Q}$ or $\mathbf{F}_p$.

Contents

Introduction

The following lecture notes are based on the paper [**1**].

A set $\mathcal{C}$ of (complete) algebraic curves over a field F will be called *dominating* if for *every* curve C' over F there exists a curve $C \in \mathcal{C}$ and a finite étale cover $\tilde{C} \to C$ surjecting onto C'. An algebraic curve C over a F will be called *universal* if the set $\mathcal{C} = \{C\}$ is dominating.

THEOREM 1.1 (Belyi). — *Every algebraic curve C defined over a number field admits a surjective map onto $\mathbb{P}^1$ which is unramified outside* $(0, 1, \infty)$.

In 1978 Manin pointed out that Belyi's theorem implies the following

PROPOSITION 1.2. — [4] *The set of modular curves is dominating.*

There are many other dominating sets of curves, for example the set of hyperelliptic curves or of all curves with function field $\overline{\mathbb{Q}}(z, \sqrt[n]{z(1-z)})$ (for $n \in \mathbb{N}$). Of course, one is interested in finding *small* dominating sets.

QUESTION 1.3. — Does there exist a universal algebraic curve over $\overline{\mathbb{Q}}$? Does there exist a number $n \in \mathbf{N}$ such that every curve defined over $\overline{\mathbb{Q}}$ admits a surjective map onto $\mathbf{P}^1$ with ramification only over $(0, 1, \infty)$ and such that all local ramification indices are $\leq n$? Is every curve of genus ≥ 2 universal?

The above questions are also related to the structure of the action of the Galois group action $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$, for $[K : \mathbb{Q}] < \infty$, on the completion $\hat{\pi}_1(C_K)$. Different results about this action have been obtained by Y. Ihara, H.Nakamura and M. Matsumoto (see [8], [9]). An affirmative answer to our conjecture (question) means that the above action of the group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is very similar for different hyperbolic curves over $\overline{\mathbb{Q}}$.

It is natural to consider the following simple model situation: instead of $\overline{\mathbb{Q}}$ we look at $\overline{\mathbf{F}}_p$ (an algebraic closure of the finite field $\mathbf{F}_p$).

THEOREM 1.4. — *Let $p \geq 5$ be a prime number and C a hyperelliptic curve over $\overline{\mathbf{F}}_p$ of genus $g(C) \geq 2$. Then C is universal.*

A byproduct of our work on the above questions was the discovery of the following geometric fact, which could be interpreted as a step towards a converse to the universality question:

PROPOSITION 1.5. — *Every hyperbolic hyperelliptic curve C (over an arbitrary algebraically closed field of characteristic $\neq 2, 3$) has a finite étale cover $\tilde{C}$ which surjects onto the genus 2 curve C_0 given by $\sqrt[6]{z(1-z)}$. In particular, if C_0 is universal then every hyperelliptic curve of genus ≥ 2 is universal.*

Acknowledgments. The first author was partially supported by the NSF. The second author was partially supported by the NSF and the Clay foundation.

2. Finite characteristic constructions

Here we work over an algebraic closure $\overline{\mathbf{F}}_p$ of the finite field $\mathbf{F}_p$ (with $p \geq 5$). We show that there exists at least one universal curve.

Let

$$C_0 \xrightarrow{\iota_0} E_0 \xrightarrow{\pi_0} \mathbb{P}^1$$

be a sequence of double covers induced by:

$$\sqrt[6]{z(z-1)} \to \sqrt[3]{z(z-1)} \to z.$$

Let C be an arbitrary curve with a generic covering $\sigma : C \to \mathbb{P}^1$ such that its branch locus does not contain $(0, 1, \infty)$. Consider the diagram

$$\begin{tikzcd} C \arrow[d, "\sigma"'] & C_1 \arrow[l] \arrow[d] & C_2 \arrow[l] \arrow[dd] \\ \mathbb{P}^1 & E_0 \arrow[l] \arrow[d, "\varphi"'] & \\ & E_0 & C_0 \arrow[l] \end{tikzcd}$$

The local ramification indices of the map $C_1 = C \times_{\mathbb{P}^1} E_0 \to \mathbb{P}^1$ are ≤ 2. Since *all* $\overline{\mathbf{F}}_p$-points of the elliptic curve E_0 are torsion points there exists a suitable multiplication map φ mapping all ramification points of C_1 over E_0 to 0. Taking the composition of $C_1 \to E_0$ with this map we get a surjection $C_1 \to E_0$, ramified only over the zero point in E_0 and such that all local ramification indices are at most 2. Any irreducible component of $C_2 := C_0 \times_{E_0} C_1$ satisfies the conclusion of Theorem 1.4.

REMARK 2.1. — The natural idea to employ group actions (e.g., multiplication by n, factorizing by the additive group or actions of $\mathrm{SL}_2(\mathbf{F}_q)$)

to "collect" ramification points of coverings has appeared in various contexts. For a recent application (using $\mathbb{G}_m$) to a proof of a positive characteristic analogue of Belyi's theorem see [**12**].

LEMMA 2.2. — *Let C be a smooth complete curve and E a curve of genus 1. There exist a curve C_1 and a diagram*

$$C \xleftarrow{\tau_1} C_1 \xrightarrow{\iota_1} E,$$

with surjective τ_1, ι_1 such that all ramification points of ι_1 lie over a single point of E and all of its local ramification indices are equal to 2.

Proof. — Choose a generic map $\sigma : C \to \mathbb{P}^1$ and a double cover $\pi : E \to \mathbb{P}^1$ such that the branch loci $\mathrm{Bran}(\sigma)$ and $\mathrm{Bran}(\pi)$ on $\mathbb{P}^1$ are disjoint. The product $C_1 := C \times_{\mathbb{P}^1} E$ is an irreducible curve which is a double cover of C and which surjects onto E with local ramification indices ≤ 2. As above we find an unramified cover $\varphi : E \to E$ such that the composition $\varphi \circ \iota_1 : C_1 \to E$ is ramified only over one point in E and the local ramification indices are still equal to 2. □

COROLLARY 2.3. — *Assume that an unramified covering $\tilde{C}$ of C surjects onto an elliptic curve E and that there exists a point $q \in E$ such that* all *local ramification indices of $\tilde{C} \to E$ over q are divisible by 2. Then C is universal.*

COROLLARY 2.4 (Theorem 1.4). — *Every hyperelliptic curve C over $\overline{\mathbb{F}}_p$ (with $p \geq 5$) of genus ≥ 2 is universal.*

Proof. — Consider the standard projection $\sigma : C \to \mathbb{P}^1$ (of degree 2). Let $\pi : E \to \mathbb{P}^1$ be a double cover such that $\mathrm{Bran}(\pi)$ is contained in $\mathrm{Bran}(\sigma)$. Then the product $\tilde{C} = C \times_{\mathbb{P}^1} E$ is an unramified double cover of C. Moreover, $\tilde{C}$ is a double cover of E with ramification at most over the preimages in E of the points in $\mathrm{Bran}(\sigma) \setminus \mathrm{Bran}(\pi)$. Apply Corollary 2.3. □

In *finite* characteristic, there are many other (classes of) universal curves. For example, cyclic coverings with ramification in 3 points, hyperbolic modular curves, etc. Thus it seems plausible to formulate the following

CONJECTURE 2.5. — Any smooth complete curve C of genus $g(C) \geq 2$ defined over $\overline{\mathbf{F}}_p$ (for $p \geq 2$) is universal.

3. Geometric constructions

Let (E, q_0) be an elliptic curve, q_1 a torsion point of order two on E and $\pi : E \to \mathbb{P}^1$ the quotient with respect to the involution induced by q_1. Let n be an odd positive integer and $\varphi_{n,E} : \mathbb{P}^1_2 \to \mathbb{P}^1_1$ the map induced by

$$\begin{tikzcd} E \arrow[r, "\pi"] \arrow[d, "\phi_n"'] & \mathbb{P}^1_2 \arrow[d, "\varphi_{n,E}"] \\ E \arrow[r, "\pi"'] & \mathbb{P}^1_1. \end{tikzcd}$$

Any quadruple $r = \{r_1, ..., r_4\}$ of four distinct points in $\varphi_{n,E}^{-1}(\pi(q_0))$ defines a genus 1 curve E_r (the double cover of $\mathbb{P}^1$ ramified in these four points).

PROPOSITION 3.1. — *Let $\iota : C \to E$ be a finite cover such that all local ramification indices over q_0 are even. Then there exists an unramified cover $\tau_r : C_r \to C$ dominating E_r and having only even local ramification indices over some point in E_r.*

Proof. — Assume that $n \geq 3$ and consider the following diagram

$$\begin{tikzcd}
C & C_2 \arrow[l, "\tau_2"'] & C_r \arrow[l, "\tau_r"'] \\
E \arrow[u, phantom] & E \arrow[l, "\varphi_n"'] & E_r \\
\mathbb{P}^1_1 & \mathbb{P}^1_2 \arrow[l, "\phi_{n,E}"'] & \mathbb{P}^1_2,
\arrow[from=1-1, to=2-1, "\iota"'] \arrow[from=1-2, to=2-2, "\iota_2"] \arrow[from=1-3, to=2-3, "\iota_r"]
\arrow[from=2-1, to=3-1, "\pi"'] \arrow[from=2-2, to=3-2, "\pi"] \arrow[from=2-3, to=3-3, "\pi_r"]
\end{tikzcd}$$

where E_r is a double cover of $\mathbb{P}^1_2$ ramified in any quadruple of points in the preimage $\phi^{-1}_{n,E}(\pi(q_0))$ and C_r is any irreducible component of $C_2 \times_{\mathbb{P}^1_2} E_r$. Any point $q_r \in E_r$ such that q_r is not contained in the ramification locus of π_r (that is, its image in $\mathbb{P}^1_2$ is distinct from $r_1, ..., r_4$) has the claimed property. $\square$

REMARK 3.2. — Iterating this procedure (and adding isogenies) we obtain many elliptic curves E' which are dominated by curves having an unramified cover onto E.

DEFINITION 3.3. — *We will say that $E' \leq E$ if there exists a diagram*

$$E' \xrightarrow{\pi'} \mathbb{P}^1 \xleftarrow{\pi} E$$

such that

- *π' is a double cover;*
- *for all $p \in \pi^{-1}(\mathrm{Bran}(\pi')) \subset E$ the local ramification indices are ≤ 2;*
- *for all $p, p' \in \pi^{-1}(\mathrm{Bran}(\pi'))$ the cycle $(p - p')$ is torsion in the Jacobian of E.*

REMARK 3.4. — It would be interesting to know if for any two elliptic curves E' and E over $\overline{\mathbb{Q}}$ there exists a cycle

$$E' = E_1 \leq E_2 \leq \cdots \leq E_n = E$$

connecting them. Of course, isogenous curves are connected by such a

We will now show that *any* elliptic curve over *any* algebraically closed field of characteristic zero can be connected in this way to E_0.

Consider the family of elliptic curves on $\mathbb{P}^2$ given by

$$E_\lambda \;:\; x^3 + y^3 + z^3 + \lambda xyz = 0.$$

For each λ the set $E_\lambda[3]$ of 3-torsion points of E_λ is precisely

$$\mathsf{T} := \left\{ \begin{array}{lll} (1:0:1), & (1:0:-\zeta), & (1:0:-\zeta^2), \\ (0:1:1), & (0:1:-\zeta), & (0:1:-\zeta^2), \\ (1:1:0), & (1:-\zeta:0), & (1:-\zeta^2:0) \end{array} \right\},$$

(here ζ is a primitive cubic root of 1). The projection

$$\begin{array}{rccc} \pi \;: & \mathbb{P}^2 & \to & \mathbb{P}^1 \\ & (x:y:z) & \mapsto & (x+z:y) \end{array}$$

respects the involution $x \to z$ on $\mathbb{P}^2$. Denote by π_λ the restriction of π to E_λ. Clearly, π_λ exhibits each E_λ as a double cover of $\mathbb{P}^1$ and π_λ has only simple double points for all λ. Moreover,

$$\pi(\mathsf{T}) = \{(0:1), (1:-\zeta), (1:-\zeta^2), (1:-1), (1:0)\}$$

and for all λ there exists a (non-empty) set $S_\lambda \subset \mathrm{Bran}(\pi_\lambda) \subset \mathbb{P}^1$ such that $\pi_\lambda^{-1}(S_\lambda) \subset \mathsf{T}$. Let $\pi_0' \;:\; E_0' \to \mathbb{P}^1$ be a double cover ramified in 4 points in $\pi(\mathsf{T})$.

LEMMA 3.5. — *Let $\iota \;:\; C \to E_\lambda$ be a double cover such that over at least one point in* $\mathrm{Bran}(\iota)$ *the local ramification indices are even. Then there exists an unramified cover $\tilde{C} \to C$ and a surjective morphism $\tilde{\iota} \;:\; \tilde{C} \to E_0'$ such that over at least one point in* $\mathrm{Bran}(\tilde{\iota}) \subset E_0'$ *all local ramification indices of $\tilde{\iota}$ are even.*

Proof. — Consider the diagram

$$\begin{tikzcd} E_\lambda \arrow[d, "\varphi_3"'] & C_1 \arrow[l, "\iota"'] \arrow[d] \\ E_\lambda \arrow[d, "\pi_\lambda"'] & C \arrow[l] \\ \mathbb{P}^1 & \end{tikzcd}$$

Then $C_1 \to \mathbb{P}^1$ has even local ramification indices over all points in $\pi(\mathsf{T})$. It follows that

$$\tilde{C} := C_1 \times_{\mathbb{P}^1} E_0' \to E_0'$$

has even local ramification indices over the preimages of the fifth point in $\pi(\mathsf{T})$, as claimed. □

NOTATIONS 3.6. — Let $\mathcal{C}$ be the class of curves such that there exists an elliptic curve E, a surjective map $\iota : C \to E$ and a point $q \in \mathrm{Bran}(\iota)$ such that all local ramification indices in $\iota^{-1}(q)$ are even.

EXAMPLE 3.7. — Any hyperelliptic curve of genus ≥ 2 belongs to $\mathcal{C}$. More generally, $\mathcal{C}$ contains any curve C admitting a map $C \to \mathbb{P}^1$ with even local ramification indices over at least 5 points in $\mathbb{P}^1$.

PROPOSITION 3.8. — *For any $C \in \mathcal{C}$ there exists an unramified cover $\tilde{C} \to C$ surjecting onto C_0 (with $C_0 \to \mathbb{P}^1$ given by $\sqrt[6]{z(1-z)}$).*

Proof. — Look at the diagram

$$\begin{tikzcd} C_1 \arrow[d, "\iota_1"'] & C_2 \arrow[l, "\tau_2"'] \arrow[d, "\iota_2"'] \arrow[r, equal] & C_2 \arrow[d, "\sigma_2"'] & C_3 \arrow[l, "\tau_3"'] \arrow[d, "\iota_3"'] & C_4 \arrow[l, "\tau_4"'] \arrow[d, "\iota_4"'] & C_5 \arrow[l, "\tau_5"'] \arrow[d] \\ E & E \arrow[l, "\varphi_3"] \arrow[r, "\pi"'] & \mathbb{P}^1 & E_0 \arrow[l, "\pi_0"] & E_0 \arrow[l, "\varphi_3"] & C_0. \arrow[l, "\iota_0"] \end{tikzcd}$$

Here

- $C_1 := C \in \mathcal{C}$ with $\iota_1 : C_1 \to E = E_\lambda$ as in 3.6;
- C_2 is an irreducible component of the fiber product $C_1 \times_E E$;

- $\sigma_2 = \pi \circ \iota_2$;
- $C_3 := C_2 \times_{\mathbb{P}^1} E_0$;
- C_4 is an irreducible component of $C_3 \times_{E_0} E_0$;
- $C_5 := C_4 \times_{E_0} C_0$.

Observe that for $q \in \mathrm{Bran}(\pi_0)$ the local ramification indices in the preimage $(\iota_2 \circ \pi)^{-1}(q)$ are all even. Therefore, τ_3 is *unramified* and ι_3 has even local ramification indices over (the preimage of) $q_5 \in \{\pi(\mathrm{T}) \setminus \mathrm{Bran}(\pi_0)\}$ (the 5th point). The map ι_4 is ramified over the preimages $(\pi_0 \circ \varphi_3)^{-1}(q_5)$, with even local ramification indices, which implies that τ_5 is unramified. Finally, C_5 has a dominant map onto C_0 and is unramified over C_4 (and consequently, C_1). □

REMARK 3.9. — As one of the corollaries we obtain that for any (hyperbolic) hyperelliptic curve C the group $\hat{\pi}_1(C_K)$, together with the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$, has $\hat{\pi}_1(C_0)$, with $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$-action, as a quotient (for some finite extension $[K : \mathbb{Q}] < \infty$). Thus we can universally estimate from below the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ on $\hat{\pi}_1(C_K)$, for any hyperellipic curve C.

REMARK 3.10. — The above construction also shows that for every hyperelliptic curve C there exists a chain of abelian étale covers with groups

$$\mathbb{Z}/2, \mathbb{Z}/3 \oplus \mathbb{Z}/3, \mathbb{Z}/2, \mathbb{Z}/2$$

(of total degree 72) such that the resulting curve $\tilde{C}$ admits a degree 4 surjective map onto C_0. In particular, Mordell's conjecture (Faltings' theorem) for C follows from Mordell's conjecture for C_0. Implementing this construction over the rings of integers one can find effective bounds on the number (and height) of K-rational points on C in terms the number (and height) of K'-rational points in C_0, where K' is a finite extension of K, determined by the geometry of C over the integers $\mathfrak{o}_K$.

The fact that there is some interaction between the arithmetic of different curves has been noted previously. Moret-Bailly and Szpiro showed (see **[12]**, **[10]**) that the proof of an *effective* Mordell conjecture for *one* (hyperbolic) curve (for example, C_0) implies the ABC-conjecture, which in turn implies an effective Mordell conjecture for *all* (hyperbolic) curves (Elkies **[5]**). Here *effective* means an explicit bound on the height of a

K-rational point on the curve for all number fields K. Again, Belyi's theorem is used in an essential way.

References

[1] F. Bogomolov, Yu. Tschinkel, *Unramified correspondences*, alg-geom 0202223, (2002).

[2] G. V. Belyi, *Galois extensions of a maximal cyclotomic field*, Izv. Akad. Nauk SSSR Ser. Mat. **43**, (1979), no. 2, 267–276, 479.

[3] G. V. Belyi, *Another proof of the Three Points theorem*, Preprint MPI 1997-46 at http://www.mpim-bonn.mpg.de, (1997).

[4] F. Bogomolov, D. Husemoller, *Geometric properties of curves defined over number fields*, Preprint MPI 2000-1 at http://www.mpim-bonn.mpg.de, (2000).

[5] N. Elkies, *ABC implies Mordell*, Intern. Math. Res. Notices **7**, (1991), 99–109.

[6] R. Hain, M. Matsumoto, *Tannakian fundamental groups associated to Galois groups*, alg-geom 0010210, (2000).

[7] R. Hain, M. Matsumoto, *Weighted completion of Galois groups and Galois actions on the fundamental group of* $\mathbb{P}^1 - \{0, 1, \infty\}$, alg-geom 0006158, (2000).

[8] M. Matsumoto, *Arithmetic fundamental groups and moduli of curves*, School on Algebraic Geometry (Trieste, 1999), 355–383, ICTP Lect. Notes, 1, Abdus Salam Int. Cent. Theoret. Phys., Trieste, 2000.

[9] M. Matsumoto, A. Tamagawa, *Mapping-class-group action versus Galois action on profinite fundamental groups*, Amer. Journ. Math. **122**, (2000), no. 5, 1017–1026.

[10] L. Moret-Bailly, *Hauteurs et classes de Chern sur les surfaces arithmétiques*, Astérisque **183**, (1990), 37–58.

[11] M. Saidi, *Revêtements modérés et groupe fondamental de graphe de groupes*, Compositio Math. **107**, (1997), no. 3, 319–338.

[12] L. Szpiro, *Discriminant et conducteur des courbes elliptiques*, Astérisque **183**, (1990), 7–18.