# COUNIFORMIZATION OF CURVES OVER NUMBER FIELDS

*by*

Fedor Bogomolov and Yuri Tschinkel

Abstract. — We study correspondences between projective curves over $\bar{\mathbb{Q}}$.

## Contents

## 1. Introduction

In this note we investigate correspondences between (geometrically irreducible) algebraic curves over number fields. Let $C, C'$ be two such curves. We say that $C$ lies over $C'$ and write

$$C \Rightarrow C'$$

if there exist an étale cover $\tilde{C} \to C$ and a dominant map $\tilde{C} \to C'$. In particular, every curve lies over $\mathbb{P}^1$. Clearly, if $C \Rightarrow C'$ and $C' \Rightarrow C''$ then $C \Rightarrow C''$. We say that a curve $C'$ is *minimal* for some class of curves $\mathcal{C}$ if every $C \in \mathcal{C}$ lies over $C'$.

Let

$$\mathsf{C}_n \,:\, y^n = x^2 + 1 \tag{1.1}$$

and $\mathcal{C}$ be the set of such curves. For all $n, m \in \mathbb{N}$ we have $\mathsf{C}_{mn} \Rightarrow \mathsf{C}_n$. Belyi's theorem [1] implies that for every curve $C'$ defined over a number field there exists a curve $\mathsf{C} = \mathsf{C}_n \in \mathcal{C}$ such that $\mathsf{C} \Rightarrow C'$ (see [3] for a simple proof of this corollary). A natural extremal statement is:

Conjecture 1.1. — The curve $\mathsf{C}_6$ lies over every curve $C$ over $\bar{\mathbb{Q}}$.

Every hyperelliptic curve $C$ of genus $\mathsf{g}(C) \geq 2$ lies over $\mathsf{C}_6$ (see Proposition 2.4 or [3]). The conjecture would imply that any hyperbolic hyperelliptic curve lies over any other curve. Our main result towards the above conjecture is

Theorem 1.2. — *For every $m \geq 6$ and every $n \in \{2, 3, 5\}$ the curve $\mathsf{C}_m$ lies over $\mathsf{C}_{mn}$.*

The relevance of such geometric constructions to number theory comes from a theorem of Chevalley-Weil: if $\pi : \tilde{C} \to C$ is an unramified map of proper algebraic curves over a number field $K$ then there exists a *finite* extension $\tilde{K}/K$ such that $\pi^{-1}(C(K)) \subset \tilde{C}(\tilde{K})$. Therefore, if $C \Rightarrow C'$ then Mordell's conjecture (Faltings' theorem) for $C$ follows from Mordell's conjecture for $C'$. Our constructions allow us, at least in the case of hyperelliptic curves, to control the degree and discriminant of the field $\tilde{K}$ in terms of the coefficients defining the curve. In particular, "effective" Mordell for $\mathsf{C}_6$ implies effective Mordell for every hyperelliptic curve (see also [11], [9],[6]).

The proof of this theorem uses certain special properties of modular curves and related elliptic curves. In the construction of unramified covers we need to exhibit maps from various intermediate curves onto $\mathbb{P}^1$ or elliptic curves with simultaneous restrictions on the local ramification indices and the branching points. This is very close, in spirit, to Belyi's theorem which says that every projective algebraic curve defined over $\bar{\mathbb{Q}}$ has a map onto $\mathbb{P}^1$ ramified in $0, 1, \infty$. In fact, there are many such maps. Our technique involves optimizing the choice of these maps by trading the freedom to impose ramification conditions for the degree of the map.

An example of this is given in Section 4 where we prove the first part of Belyi's theorem (reduction to $\mathbb{Q}$-rational branching) under the restriction that the only prime dividing the local ramification indices is 2.

**Acknowledgments.** The first author was partially supported by the NSF Grant DMS-0404715. The second author was partially supported by the NSF Grant DMS-0100277.

## 2. Minimal curves

NOTATIONS 2.1. — For a surjective morphism of curves $\pi : C' \to C$ of degree $d$ we denote by $\mathrm{Bran}(\pi) \subset C$ the branching locus of $\pi$. For $c \in \mathrm{Bran}(\pi)$ put

$$\mathsf{d}_c := (2^{d_2}, 3^{d_3}, \ldots), \ \sum_i i d_i \leq d,$$

where $d_i$ is the number of points in $\pi^{-1}(c)$ with local ramification index $i$. Let

$$\mathrm{RD}(\pi) = \{\mathsf{d}_c\}_{c \in \mathrm{Bran}(\pi)}$$

be the *ramification datum.*

EXAMPLE 2.2. — Let $z^n : \mathbb{P}^1 \to \mathbb{P}^1$ be the $n$-power map $z \mapsto z^n$. Then $\mathrm{Bran}(z^n) = \{0, \infty\}$ and $\mathrm{RD}(z^n) = \{(n)_0, (n)_\infty\}$.

NOTATIONS 2.3. — Let $E$ be an elliptic curve over $\bar{\mathbb{Q}}$ with a fixed $0 \in E$, $E[n]$ the set of $n$-torsion points and

$$E[\infty] := \cup_{n=1}^{\infty} E[n] \subset E(\bar{\mathbb{Q}})$$

the set of all torsion points of $E$. Usually, we write $\sigma : x \to -x$ for the standard involution on $E$ and

$$\pi = \pi_\sigma \ : \ E \to E/\sigma = \mathbb{P}^1$$

for the induced map. When we specify the elliptic curve by the branching locus we write $E = E(\mathrm{Bran}(\pi))$.

PROPOSITION 2.4. — *The curves* $\mathsf{C}_6$ *and* $\mathsf{C}_8$ *are minimal for the class of hyperbolic hyperelliptic curves.*

*Proof.* — Fix a hyperbolic hyperelliptic curve $C$. Notice that for any such $C$ there exists an étale cover $C_1 \to C$ of degree 2 and a degree two surjection $C_1 \to E$ onto an elliptic curve. For example, we can take $E$ to be any elliptic curve ramified in 4 of the ramification points of the initial hyperelliptic map $C \to \mathbb{P}^1$. Fix such an $E$.

We use the following simple fact about elliptic curves: Let $\pi : E \to \mathbb{P}^1$ be an elliptic curve. Then $\pi(E[3])$ is (projectively equivalent to) the union of one point from $\mathrm{Bran}(\pi)$ and $\{1, \zeta, \zeta^2, \infty\} \subset \mathbb{P}^1$ (where $\zeta$ is a fixed third root of 1). Similarly, $\pi(E[4])$ is (projectively equivalent to)

$$\mathrm{Bran}(\pi) = \{\lambda, \lambda^{-1}, -\lambda, -\lambda^{-1}\} \cup \{1, -1, i, -i, 0, \infty\} \subset \mathbb{P}^1.$$

Now consider the natural (multiplication by $m$) isogeny

$$\varphi_m : E \to E$$

where $m = 3$ or 4. The map $\varphi_m$ is 2-ramified in $E[m]$, for $m = 3, 4$.

Consider the diagram

$$\begin{tikzcd}
C & C_1 \arrow[l] \arrow[d, "\iota_1"'] & C_2 \arrow[l, "\tau_2"'] \arrow[d, "\iota_2"'] \arrow[r, equal] & C_2 \arrow[d, "\sigma_2"'] & C_3 \arrow[l, "\tau_3"'] \arrow[d, "\iota_3"'] & C_4 \arrow[l, "\tau_4"'] \arrow[d, "\iota_4"'] & C_5 \arrow[l, "\tau_5"'] \arrow[d] \\
 & E & E \arrow[l, "\varphi_m"] \arrow[r, "\pi"'] & \mathbb{P}^1 & E_m \arrow[l, "\pi_m"] & E_m \arrow[l, "\varphi_m"] & \mathsf{C}_{2m}. \arrow[l, "\iota_m"]
\end{tikzcd}$$

Here

- $\mathrm{Bran}(\pi_3) = \{1, \zeta, \zeta^3, \infty\} \subset \mathrm{Bran}(\sigma_2)$;
- $\mathrm{Bran}(\pi_4) = \{1, -1, i, -i\} \subset \mathrm{Bran}(\sigma_2)$;
- $\iota_m : \mathsf{C}_{2m} \to E_m = \mathsf{C}_m$ is the standard map, it is ramified in two points (whose difference is) in $E_m[m]$;
- $C_2$ is an irreducible component of the fiber product $C_1 \times_E E$;
- $\sigma_2 = \pi \circ \iota_2$;
- $C_3 := C_2 \times_{\mathbb{P}^1} E_m$;
- $C_4$ is an irreducible component of $C_3 \times_{E_m} E_m$;
- $C_5 := C_4 \times_{E_m} \mathsf{C}_{2m}$;

Observe that for $q \in \mathrm{Bran}(\pi_m)$ the local ramification indices in the preimage $\sigma_2^{-1}(q)$ are all even. Therefore, $\tau_3$ is *unramified* and $\iota_3$ has even local ramification indices over (the preimage of) $q \in \{\pi(E[m]) \setminus \mathrm{Bran}(\pi_m)\}$ (such a point exists). Note that $q \in \mathrm{Bran}(\pi)$. The map $\iota_4$ is ramified over the preimages $(\pi_m \circ \varphi_m)^{-1}(q)$, with even local ramification indices, which implies that $\tau_5$ is unramified. Finally, $C_5$ has a dominant map onto $\mathsf{C}_{2m}$ and is unramified over $C_4$ (and consequently, $C_1$). This shows that every hyperelliptic curve lies over $\mathsf{C}_{2m}$, for $m = 3, 4$. □

Theorem 2.5. — *For all $m \geq 6$ and $n \in \{2, 3\}$ one has*

$$\mathsf{C}_m \Rightarrow \mathsf{C}_{mn}.$$

*Proof.* — We first assume that $m = 2n$ is even and $\geq 8$, since $\mathsf{C}_6 \Rightarrow \mathsf{C}_8$. First we show that $C := \mathsf{C}_m$ lies over $\mathsf{C}_{2m}$. Consider the diagram:

$$\begin{tikzcd}
\mathsf{C}_{2n} \arrow[d, "\iota_0"'] & C_1 \arrow[l, "\tau_1"'] \arrow[d, "\iota_1"'] & C_2 \arrow[l, "\tau_2"'] \arrow[d, "\iota_2"'] & C_3 \arrow[l, "\tau_3"'] \arrow[d, "\iota_3"'] \arrow[r, equal] & C_3 \arrow[d, "\iota_3'"'] & C_4 \arrow[l, "\tau_4"'] \arrow[d] \\
\mathbb{P}^1 & \mathbb{P}^1 \arrow[l, "z^n"] & E \arrow[l, "\pi"] & E \arrow[l, "\varphi_2"] \arrow[r, "\pi'"'] & \mathbb{P}^1 & \mathsf{C}_{4n}. \arrow[l, "\theta"]
\end{tikzcd}$$

Here

- $\pi$ is a double cover whose branch locus consists of 3 points in the preimage of 1 under $z^n$ and the preimage of 0;
- $C_1$ is the fiber product $\mathsf{C}_{2n} \times_{\mathbb{P}^1} \mathbb{P}^1$, note that $\tau_1$ is unramified and that $\iota_1$ is evenly ramified over all points in Bran$(\pi)$;
- $C_2 = C_1 \times_{\mathbb{P}^1} E$, note that $\tau_2$ is unramified since $\iota_1$ has ramification of order two over 0 and even ramification over all $\zeta_n \in \mathbb{P}^1$;
- $\tau_3$ is unramified;
- since $n \geq 4$, the map $\iota_2$ has ramification points of order $2n$ and $\iota_3$ is branched with ramification index $2n$ over all points in $E[2]$;
- $\pi'$ is the map such that Bran$(\pi') = \pi'(E[2])$, then $\iota_3' := \pi' \circ \iota_3$ is $4n$-ramified over all points in Bran$(\pi')$;
- $\theta$ is the map branched in three of the above points, in particular, $\tau_4$ is unramified.

Now we assume that $m$ is odd, $m \geq 5$ and consider the diagram:

$$\begin{tikzcd}
\mathsf{C}_m \arrow[d, "\iota_0"'] & C_1 \arrow[l, "\tau_1"'] \arrow[d, "\iota_1"'] \arrow[r, equal] & C_1 \arrow[d, "\iota_1'"'] & C_2 \arrow[l, "\tau_2"'] \arrow[d, "\iota_2"'] & C_3 \arrow[l, "\tau_3"'] \arrow[d, "\iota_3"'] \\
\mathbb{P}^1 & \mathbb{P}^1 \arrow[l, "z^m"] \arrow[r, "\psi_1"'] & \mathbb{P}^1 & \mathbb{P}^1 \arrow[l, "\psi_2"] & E. \arrow[l, "\pi"]
\end{tikzcd}$$

Here

- $\psi_1 : z \mapsto (z+z^{-1})/2$, then $\iota_1' = \psi_1 \circ \iota_1 : C_1 \to \mathbb{P}^1$ is 2-ramified over -1, $2m$-ramified over 1 and $m$-ramified over $\xi_i := (\zeta_m^i + \zeta_m^{-i})/2$;
- $\psi_2 = \sqrt[m]{(z-\xi_1)/(z-\xi_2)}$, it has 2-ramification over all $m$ preimages of $-1$ and $2m$-ramification over the preimages of 1;
- $\pi$ is a double cover ramified over (arbitrary) 4 points in the preimage of $-1$ under $\psi_2$, then $\iota_3 : C_3 \to E$ is $m$-ramified over all other points and we can continue as above.

Now we show that $\mathsf{C}_m$ lies over $\mathsf{C}_{3m}$ ($m$ even, this suffices for our purposes). Consider:

$$\begin{tikzcd}
\mathsf{C}_{2n} \arrow[d, "\iota_0"'] & C_1 \arrow[l, "\tau_1"'] \arrow[d, "\iota_1"'] & C_2 \arrow[l, "\tau_2"'] \arrow[d, "\iota_2"'] & C_3 \arrow[l, "\tau_3"'] \arrow[d, "\iota_3"'] \arrow[r, equal] & C_3 \arrow[d, "\iota_3'"'] & C_4 \arrow[l, "\tau_4"'] \arrow[d, "\iota_4"'] & C_5 \arrow[l, "\tau_5"'] \arrow[d, "\iota_5"'] \arrow[r, equal] & C_5 \arrow[d] & C_6 \arrow[l, "\tau_6"'] \arrow[d] \\
\mathbb{P}^1 & \mathbb{P}^1 \arrow[l, "z^n"] & E \arrow[l, "\pi"] & E \arrow[l, "\varphi_6"] \arrow[r, "\pi'"'] & \mathbb{P}^1 & E_0 \arrow[l, "\pi_0"] & E_0 \arrow[l, "\varphi_3"] \arrow[r, "\theta_0"'] & \mathbb{P}^1 & \mathsf{C}_{6n} \arrow[l]
\end{tikzcd}$$

Here

- $\pi$ is a double cover whose branch locus consists of 3 points in the preimage of 1 under $z^n$ and the preimage of 0;
- $C_1 = \mathsf{C}_{2n} \times_{\mathbb{P}^1} \mathbb{P}^1$, note that $\tau_1$ is unramified and that $\iota_1$ is evenly ramified over all points in $\mathrm{Bran}(\pi)$;
- $C_2$ is the fiber product $C_1 \times_{\mathbb{P}^1} E$, note that $\tau_2$ is unramified since $\iota_1$ has ramification of order two over 0 and even ramification over all $\zeta_n \in \mathbb{P}^1$;
- $\tau_3$ is unramified;
- since $n \geq 4$, the map $\iota_2$ has ramification points of order $2n$ and $\iota_3$ is branched with ramification index $2n$ over all points in $E[6]$;
- $\pi' : E \to \mathbb{P}^1$ is the map such that $\mathrm{Bran}(\pi') = \pi'(E[2])$, then $\iota_3' = \pi' \circ \iota_3$ is $4n$-ramified over all points of $\mathrm{Bran}(\pi')$;

– $\mathrm{Bran}(\pi_3) = \pi'(E[3]) \setminus \pi'(0)$ and the fiber product $C_4 = C_3 \times_{\mathbb{P}^1} \mathsf{C}_3$ is unramified over $C_3$, since the all the preimages of $\mathrm{Bran}(\pi_3)$ in $C_3$ have even ramifications (for $\iota_3$);
– note that there is a point $q_0 \in E_0$ such that every point in $\iota_4^{-1}(q_0) \in C_4$ has ramification of order $2n$ (for example, take a point $q$ of order exactly 6 in $E$ and take any $q_0 \in \pi_0^{-1}(\pi'(q)) \in E_0$).
– the fiber product $C_5 = C_4 \times_{E_0} E_0$ is unramified over $C_4$ and the map $\iota_5$ has ramification of order $2n$ over all points in $E_0[3]$;
– now let $\theta_0$ be the triple cover of $\mathbb{P}^1$ ramified in three points of order 3 in $E_0$, the composition of $\theta_0$ with $\iota_5$ exhibits $C_5$ as a cover of $\mathbb{P}^1$ so that all local ramification indices over three points in $\mathbb{P}^1$ are multiples of $6n$;
– finally, the fiber product $C_6 = C_5 \times_{\mathbb{P}^1} \mathsf{C}_{6n}$ is unramified over $C_5$.

□

Proposition 2.6. — *We have*

$$\mathsf{C}_6 \Rightarrow \mathsf{C}_5.$$

*Proof.* — Consider the standard action of the alternating group $\mathfrak{A}_5$ on $\mathbb{P}^1$. Choose any $\mathfrak{A}_4 \subset \mathfrak{A}_5$ and let $p_1, \dots, p_{12}$ be the $\mathfrak{A}_4$-orbit of a point fixed by an element of order 5 in $\mathfrak{A}_5$. By Klein (see [7], Ch. 1, 12, p. 58-59), there exists a polynomial identity

$$108t^4 - w^3 + \chi^2 = 0,$$

where

$$\chi \in H^0(\mathbb{P}^1, \mathcal{O}(p_1 + \cdots + p_{12})), t \in H^0(\mathbb{P}^1, \mathcal{O}(6)) \quad \text{and} \quad w \in H^0(\mathbb{P}^1, \mathcal{O}(8))$$

(the zeroes of $t$ give the vertices of the octahedron, of $w$ the vertices of the cube and of $\chi$ the vertices of the icosahedron). An Euler characteristic computation shows that the map $w^3/\chi^2 : \mathbb{P}^1 \to \mathbb{P}^1$ is branched over exactly three points with $\mathrm{RD} = \{(3^8), (4^6), (2^{12})\}$.

Consider

$$\begin{tikzcd}
\mathsf{C}_6 & \mathsf{C}_{24} \arrow[l, "\tau_0"'] \arrow[d, "\iota_0"'] & C_1 \arrow[l, "\tau_1"'] \arrow[r, equal] \arrow[d, "\iota_1"'] & C_1 \arrow[d, "\iota_1'"'] & C_2 \arrow[l, "\tau_2"'] \arrow[d, "\iota_2"'] & C_3 \arrow[l, "\tau_3"'] \arrow[d, "\iota_3"'] & C_4 \arrow[l, "\tau_4"'] \arrow[d] \\
 & \mathbb{P}^1 & \mathbb{P}^1 \arrow[l, "w^3/\chi^2"] \arrow[r, "\xi_5"'] & \mathbb{P}^1 & \mathbb{P}^1 \arrow[l, "\pi_2"] & \mathbb{P}^1 \arrow[l, "\pi_3"] & \mathsf{C}_{30} \arrow[l]
\end{tikzcd}$$

Here

- $\mathrm{RD}(\iota_0) = \{(24^1), (12^2), (24)^1\}$ and $\tau_0$ is unramified;
- all local ramification indices of $\iota_1$ over all zeroes of $\chi$ are divisible by 12.
- $\xi_5 : \mathbb{P}^1 \to \mathbb{P}^1/\mathfrak{A}_5$, the map $\iota_1$ is branched in three points $q_0, q_1, q_\infty$: over $q_0$ all local ramification indices are even, over $q_1$ - divisible by 3 and over $q_\infty$ - divisible by 60;
- $\pi_2$ is a double cover branched $q_0$ and $q_\infty$, $\iota_2$ is branched in three points $r_0, r_1, r_\infty$ so that all local ramification indices of $\iota_2$ over $r_0, r_1$ are divisible by 3 and over $r_\infty$ divisible by 30;
- $\pi_3$ is a triple cover, branched in three points so that all local ramification indices of $\iota_3$ are divisible by 30;
- the standard map $\mathsf{C}_{30} \to \mathbb{P}^1$ is ramified over 3 points with $\mathrm{RD} = \{(30^1), (15^2), (30^1)\}$.

Thus $\mathsf{C}_6 \Rightarrow \mathsf{C}_{30} \Rightarrow C_5$, as claimed. □

Theorem 2.7. — *For all $m, p \in \mathbb{N}$ one has*

$$\mathsf{C}_{5m} \Rightarrow \mathsf{C}_{5^p m}.$$

*Proof.* — Let $\pi : E_5 \to \mathbb{P}^1$ be a degree 5 map from an elliptic curve, given by a rational function $f \in \mathbb{C}(E_5)$ with $\mathrm{div}(f) = 5(q_0 - q_\infty)$, and $q_0, q_\infty \in E_5$. Assume that $\pi$ has cyclic degree 5 ramification over $0 = \pi(q_0)$ and $\infty = \pi(q_\infty)$ and that the (unique) remaining degenerate fiber of $\pi$ contains two points with local ramification equal to 2 and one point $q_1$ where $\pi$ is unramified. (Such a curve can be given as a quotient of the modular curve $X(10)$.)

Note that $5q_0 = 5q_1 = 5q_\infty$ in $\mathrm{Pic}(E_5)$. Since $\mathsf{C}_5 \Rightarrow \mathsf{C}_{20}$ it suffices to consider the diagram

$$\begin{tikzcd}
\mathsf{C}_{20n} \arrow[d] & C_1 \arrow[l, "\tau_1"'] \arrow[d, "\iota_1"'] & C_2 \arrow[l, "\tau_2"'] \arrow[d, "\iota_2"'] \arrow[r, equal] & C_2 \arrow[d, "\iota_2'"'] & C_3 \arrow[l, "\tau_3"'] \arrow[d, "\iota_3"'] \\
\mathbb{P}^1 & E_5 \arrow[l, "\pi"] & E_5 \arrow[l, "\phi_5"] \arrow[r, "\pi"'] & \mathbb{P}^1 & \mathsf{C}_{25n}. \arrow[l, "\theta"]
\end{tikzcd}$$

Here

- $C_1 = \mathsf{C}_{20n} \times_{\mathbb{P}^1} E_5$, and $\tau_1$ has cyclic ramification of order 20 over $q_1$;

- $C_2$ is (an irreducible component of) the fiber product $C_1 \times_{E_5} E_5$;
- $\iota_2' = \pi \circ \iota_2$ has cyclic $100n$ ramifications over $0, \infty$ and only even local ramification indices over 1;
- $\theta$ is the composition of the standard map $\mathsf{C}_{25n} \to \mathbb{P}^1$ with a degree two map $\mathbb{P}^1 \to \mathbb{P}^1$ (given by $x \mapsto (x + 1/x) + 1$), so that $\theta$ has the following ramification: a unique degree 50 cyclic ramification point over 0, two cyclic ramification points of degree 25 over $\infty$ and only degree two local ramifications over 1.

Then the (irreducible component of the) fiber product $C_3$ is unramified over $C_2$. □

Corollary 2.8. — *The subset of minimal curves in the class $\{\mathsf{C}_n\}$ is infinite: if the only prime divisors of $n$ are 2,3 or 5 then $\mathsf{C}_n$ is minimal.*

Example 2.9. — Let

$$X(7) \,:\, x^3y + y^3z + z^3x = 0$$

be Klein's quartic plane curve of genus 3. It is easy to see that $X(7) \Leftrightarrow \mathsf{C}_7$: $X(7)$ is isomorphic to the curve $y^7 = x^2(x+1)$ while $\mathsf{C}_7$ is isomorphic to $y^7 = x(x+1)$. Thus their fiber product over $\mathbb{P}^1$ is unramified for both projections.

## 3. A graph on the set of elliptic curves

Axiomatizing the constructions of Section 2, we are lead to consider a certain directed graph structure on the set $\mathcal{E}$ of all elliptic curves defined over $\bar{\mathbb{Q}}$, defined as follows: Write

$$E \rightharpoondown E', \quad \text{resp.} \quad E \rightleftharpoons E',$$

if $\mathrm{Bran}(E', \pi')$ is projectively equivalent to a set of four points in $\pi(E[\infty])$, resp. if $E, E'$ are isogenous. Here $\pi$ and $\pi'$ are the standard double covers over $\mathbb{P}^1$. Note that the set

$$\pi(E[\infty]) \subset \mathbb{P}^1(\bar{\mathbb{Q}}),$$

depends (up to the action of $\mathrm{PGL}_2$ on $\mathbb{P}^1$) only on $E$ and not on the choice of $0 \in E$.

Definition 3.1. — *Let $E'$ be an elliptic curve. A curve $C'$ is called $(E', n)$-minimal if for every cover $\iota'' : C'' \to E'$ such that all local ramification indices over at least one point in* $\mathrm{Bran}(\iota'')$ *are divisible by $n$ one has $C'' \Rightarrow C'$.*

Remark 3.2. — Note that every curve $\iota' : C' \to E'$ such that

- $\mathrm{Bran}(\iota') \subset E'[\infty]$;
- all local ramification indices of $\iota'$ divide $n$.

is $(E', n)$-minimal.

Consider the standard action of the icosahedral group $\mathfrak{A}_5$ on $\mathbb{P}^1$. Let

- $\kappa_5 : \mathsf{H}_5 \to \mathbb{P}^1$ be the hyperelliptic curve branched in the 12 five-invariant points;
- $\kappa_3 : \mathsf{H}_3 \to \mathbb{P}^1$ the hyperelliptic curve branched in the 20 three-invariant points;
- $\iota_5 : \mathsf{C}_5 \to \mathbb{P}^1$ the standard curve from (1.1);
- $\iota : \mathsf{C} \to \mathbb{P}^1$ the degree 4 cover ramified over the primitive 5th roots $\{\zeta^i\}$ of 1, with local ramification indices equal to 2; we have $\mathsf{g}(\mathsf{C}) = 2$.

Proposition 3.3. — *We have*

$$\mathsf{H}_5 \Leftrightarrow \mathsf{H}_3 \Leftrightarrow \mathsf{C}_5 \Leftrightarrow \mathsf{C}.$$

*Proof*. — First of all, $\mathsf{H}_5 \Rightarrow \mathsf{C}_5$, since 6 of the 12 points are projectively equivalent to $\mathrm{Bran}(\iota_5)$ and hence an unramified degree two cover of $\mathsf{H}_5$ surjects onto $\mathsf{C}_5$. On the other hand, $\mathsf{C}_{30} \Rightarrow \mathsf{H}_5$, since $\kappa_5$ has three ramification points with indices $2, 3, 10$.

Similarly, $\mathsf{C}_{30} \Rightarrow \mathsf{H}_3$, since $\kappa_3$ has $2, 6, 5$ as local ramification indices. On the other hand, $\mathsf{H}_3/\mathfrak{C}_5$ is an elliptic curve, and the quotient map is branched at 4 points with ramification indices equal to 5. Hence $\mathsf{H}_3 \Rightarrow \mathsf{C}_5$. Since $\kappa_5$ is two-ramified over the 5-th roots of unity plus 0, we have $\mathsf{C}_5 \Rightarrow \mathsf{C}$.

Finally, let $R$ be the fiber product of five degree 2-covers $\mathbb{P}^1 \to \mathbb{P}^1$ ramified over, $\zeta^i, \zeta^{i+1}$, for $i = 1, \dots, 5$. Then $R \to \mathbb{P}^1$ is a Galois cover, consisting of two components $R_1, R_2$, each of genus 5, each ramified over $\mathbb{P}^1$ with degree 16 $(32 - 8 \cdot 5 = -8)$. The natural action of the cyclic group $\mathfrak{C}_5$ on $R_1$ has two invariant points (among the preimages of $0, \infty$), hence $R_1/\mathfrak{C}_5$ is an elliptic curve and, consequently, $R_1 \Rightarrow \mathsf{C}_5$. At the same time, $R_1 \Leftrightarrow \mathsf{C}$. □

Note that $\mathsf{C}$ is $(E(\zeta,\zeta^2,\zeta^3,\zeta^4),2)$-minimal, since its 2-ramifications lies over points of finite order. Similarly, $X(7)$ is 2-minimal with respect to $E_7$.

Proposition 3.4. — *Let $C'$ be an $(E',n)$-minimal curve and $E \rightharpoondown E'$. Let $\iota : C \to E$ be a cover such that there exists an $e \in E$ with the property that for all $c \in \iota^{-1}(e)$ the local ramification indices are divisible by $n$. Then $C \Rightarrow C'$.*

*Proof.* — As in Section 2. □

Remark 3.5. — Proposition 3.4 explains why we are interested in *minimal* elements of the graph $\mathcal{E}$: curves $E'$ such that for every curve $E$ there is a finite chain

$$E \rightharpoondown E^1 \cdots \rightharpoondown E'$$

ending at $E'$. We have shown that $\mathcal{E}$ has a minimal element

$$E_0 = \mathsf{C}_3 : \;\; y^3 = x^2 + 1,$$

(for any $E$ the curve $E_0$ is ramified over the images of torsion points of order 3 of $E$ in $\mathbb{P}^1$). Thus any curve isogenous to $E_0$ is also minimal as is any curve $E'$ with $E_0 \rightharpoondown E'$. In particular, every curve $\iota : C \to E_0$ such that $\mathrm{Bran}(\iota) \subset E_0[\infty]$ with local ramification indices equal to products of powers of two and three is minimal in the sense of Section 2.

Remark 3.6. — Note that $\mathcal{E}$ does not have a *maximal* element, that is, a curve $E$ such that for every elliptic curve $E'$ there is a chain

$$E \rightharpoondown E_1 \rightharpoondown \ldots \rightharpoondown E',$$

(in the class $\mathcal{E}$). This follows from the observation that the Galois groups of fields obtained by adjoining torsion points are contained in iterated extensions of subgroups $\mathrm{GL}_2(\mathbb{Z}/m)$. In particular, fields with simple Galois groups (over the ground field) which have no faithful two-dimensional representations over $\mathbf{F}_p$, for every prime $p$, cannot be realized.

Lemma 3.7. — *Let $E \rightharpoondown E'$ be nonisogenous elliptic curves and let $\iota : C \to E$ be a cover, such that $\iota$ has at least one local ramification* *index divisible by $2n$. Then there is a cover $\iota' : C' \to E'$ from a curve $C'$ such that $C \Rightarrow C'$, and* $\mathrm{Bran}(\iota')$ *includes points in $E'(\bar{\mathbb{Q}}) \setminus E'[\infty]$.*

*Proof.* — Consider the diagram

$$\begin{tikzcd}
C \arrow[d, "\iota"'] & C_1 \arrow[l, "\tau_1"'] \arrow[r, equal] \arrow[d, "\iota_1"'] & C_1 \arrow[d] & C' \arrow[l, "\tau'"'] \arrow[d, "\iota'"'] \\
E & E \arrow[l, "\varphi_m"] \arrow[r, "\pi"'] & \mathbb{P}^1 & E'. \arrow[l, "\pi'"]
\end{tikzcd}$$

Here

- $m$ is such that $\mathrm{Bran}(\pi') \subset \pi(E[m])$, it exists since $E \rightharpoondown E'$;
- there exists a point $q \in \pi(E[m]) \setminus \mathrm{Bran}(\pi')$ such that the difference between the two preimages of $q$, under $\pi'$, in $E'$ is of infinite order in $E'(\bar{\mathbb{Q}})$.

This last claim holds since the set

$$\pi(E[\infty]) \cap \pi'(E'[\infty]) \subset \mathbb{P}^1$$

is finite, provided $E$ is nonisogeneous to $E'$. Indeed, consider the map

$$\rho : E \times E' \to \mathbb{P}^1 \times \mathbb{P}^1 \supset \Delta(\mathbb{P}^1)$$

of degree 4, induced by $\pi, \pi'$. For nonisogeneous $E, E'$, the genus of the preimage of the diagonal $C := \rho^{-1}(\Delta(\mathbb{P}^1))$ is $\geq 2$. By a theorem of Raynaud [10], the set

$$C(\bar{\mathbb{Q}}) \cap (E[\infty] \times E'[\infty])$$

is finite (in fact, one can effectively estimate its cardinality). □

Lemma 3.8. — *The set $\pi(E[\infty]) \cap \mathbb{G}_m[\infty] \subset \mathbb{P}^1(\bar{\mathbb{Q}})$ is finite.*

*Proof.* — Follows from McQuillan's generalization of a theorem of Raynaud's (see [8], [10], and also [5]). Consider the map

$$(\theta, z^m) : E \times \mathbb{P}^1 \to \mathbb{P}^1 \times \mathbb{P}^1.$$

Then the preimage of the diagonal $(\theta, z^m)^{-1}(\Delta)$ is an affine open curve $C$ of genus $> 1$. The finiteness of the intersection of $C$ with $(E \times \mathbb{G}_m)_{tors} \subset E \times \mathbb{P}^1$ follows. □

A *cycle* in $\mathcal{E}$ is a finite set of curves $E, E_1, \ldots \in \mathcal{E}$ such that

$$E \rightharpoondown E_1 \rightharpoondown \ldots \rightharpoondown E.$$

Remark 3.9. — Lemma 3.7 shows that each nontrivial cycle for $E$ gives new $(E, n)$-minimal curves, which are $n$-ramified over points of infinite order in $E(\bar{\mathbb{Q}})$.

We now exhibit several such cycles in $\mathcal{E}$.

Lemma 3.10. — *For any $x \in \mathbb{P}^1 \setminus \{0, 1, \infty\}$ one has*

$$E(0, 1, x^2, \infty) \rightharpoondown E(0, 1, x, \infty).$$

*Proof.* — On the curve $E(0, 1, x^2, \infty)$ the preimages of the points $x, -x$ have order 4, since the involution $z \to x^2/z$ maps $0 \to \infty$ and $1 \to x^2$, and has $x, -x$ as invariant points. In particular, by definition,

$$E(0, 1, x^2, \infty) \rightharpoondown E(0, 1, x, \infty) \quad \text{and} \quad E(0, 1, x^2, \infty) \rightharpoondown E(0, 1, -x, \infty).$$

□

Corollary 3.11. — *Let $\zeta = \zeta_{2^n}$ be $2^n$-root of unity. Then*

$$E(0, 1, -1, \infty) \rightharpoondown E(0, 1, \zeta, \infty).$$

Corollary 3.12. — *Let $\ell$ be an odd number. Then*

$$E(0, 1, \zeta_\ell, \infty) \rightharpoondown E(0, 1, \zeta_\ell \cdot \zeta_{2^n}, \infty),$$

*where $\zeta_m$ is an $m$-th root unity.*

*Proof.* — Some $2^m$-th power of $\zeta_\ell \cdot \zeta_{2^n}$ is equal to $\zeta_\ell$. □

Corollary 3.13. — *Let $\ell$ be an odd number. The set*

$$\{E(0, 1, \zeta_\ell^j, \infty)\}$$

*decomposes into $\phi(\ell)/d_\ell$ (nontrivial) cycles of length $d_\ell$, where $\phi$ is the Euler function and $d_\ell$ is the maximal power of 2 dividing $\phi(\ell)$.*

Corollary 3.14. — *For any $x \in \mathbb{P}^1 \setminus \{0, 1, \infty\}$ one has*

$$E(0, 1, (x-1)^2, \infty) \rightharpoondown E(0, 1, x, \infty)$$

*and similarly,*

$$E(0, 1, (2-x)x, \infty) \rightharpoondown E(0, 1, x, \infty).$$

*Proof.* — We use the isomorphism

$$E(0,1,(1-x),\infty) \sim E(0,1,x,\infty).$$

□

## 4. Collecting points

LEMMA 4.1. — *Let $\mathbb{A}^d$ be the complex affine space of dimension $d$. For $x \in \mathbb{A}^d(\mathbb{C})$ let $S_x$ be the affine algebraic variety characterized by the property:*

- *$x \in S_x$ and*
- *for every quadratic polynomial $g \in \mathbb{C}[y], g(y) = g_2y^2 + g_1y + g_0$, and every $a = (a_1, \ldots, a_d) \in S_x$ one has $(g(a_1), \ldots, g(a_d)) \in S_x$.*

*Then $S_x$ is irreducible and is either equal to $\mathbb{A}^d$ or is contained in one of the diagonals $\Delta_{ij} := \{x_i = x_j,\ i \neq j\}$.*

*Proof.* — Note that $S_x$ is built from $x$ as an iteration of vector bundles. At each step we have an irreducible variety. The procedure stabilizes after finitely many steps (by dimension reasons). Thus $S_x$ is irreducible.

We proceed by induction on $d$. For $d = 1, 2, 3$ the claim is trivial. Assume the claim holds for all $d' < d$. We may also assume that $S_x \subset \mathbb{A}^n$ is a hypersurface not coinciding with a diagonal $\Delta_{ij}$. Otherwise, the projection of $S_x$ onto the first $d-1$ coordinates $\mathbb{A}^{d-1} \subset \mathbb{A}^d$ would not be surjective and hence, by the inductive assumption, contained in one of the diagonals, which would prove our claim.

We see that $\pi_{d-1} : S_x \to \mathbb{A}^{d-1}$ is a generically finite cover. Let

$$T_{d-1} := \{(t_1, \ldots, t_{d-1})\} \subset \mathbb{A}^{d-1}$$

be such that all $t_j$ are roots of unity of odd order. The set $T_{d-1}$ is Zariski dense in $\mathbb{A}^{d-1}$. It contains a subset $T^0_{d-1}$ which is Zariski dense in $\mathbb{A}^{d-1}$ and has the property that all fibers of $\pi_{d-1}$ over $T^0_{d-1}$ are nonempty and finite.

Note that for each $t = (t_j)_{j=1,\ldots,d-1} \in T^0_{d-1}$ there exists an $n = n_t \in \mathbb{N}$ such that $t_j^{2^n} = t_j$ for all $j = 1, \ldots, d-1$. This implies that the fiber over $t$ is mapped into itself by the map $(a_j)_{j=1,\ldots,d-1} \mapsto (a_j^{2^n})_{j=1,\ldots,d-1}$. In particular, there is a point $b \in \pi_{d-1}^{-1}t$ and an $n' \geq n$ such that is fixed under the map

$$(b_j)_{j=1,\dots,d-1} \mapsto (b^{2^{n'}})_{j=1,\dots,d-1}.$$

We see that $b_j$ are torsion points in $\mathbb{C}^*$, for all $j = 1, \dots, d-1$.

If $S^0 \subset (\mathbb{C}^*)^d$ is an algebraic subvariety and $T \subset S^0 \cap (\mathbb{C}^*)^d$ the subset of torsion points then $S^0$ contains a finite set of translates of subtori by torsion points which contains $T$ (see [5], [12]). If follows that $S_x$ contains a subtorus $(\mathbb{C}^*)^{d-1} \subset (\mathbb{C}^*)^d$ as a Zariski open subvariety.

Thus $S_x \subset \mathbb{A}^d$ is given by an equation

$$\prod_{j\in J} x_j^{n_j} = \prod_{j'\in J'} x_{j'}^{n_{j'}},$$

where $J \cap J' \subset [1, \dots, d]$ and $n_j, n'_j > 0$. The intersection of $S_x$ with every diagonal $\Delta_{ij}$ is a proper subset (by assumption) and therefore (by induction) a finite union of subdiagonals (the intersection $S_x \cap \Delta_{ij}$ is stable under quadratic transformations). We may assume that $J \supset \{x_1, x_2\}$ and consider the diagonal $\Delta_{34} := \{x_3 = x_4\}$ (recall that $d \geq 4$). The resulting equation for $S_x \cap \Delta_{34}$ does not define a subset of a union of diagonals. □

Corollary 4.2. — *Let $K/\mathbb{Q}$ be a field extension of degree $d = r_1 + 2r_2$, with $r_1$ real and $r_2$ (pairs of) complex embeddings, and*

$$K \hookrightarrow R^{r_1} \oplus \mathbb{C}^{2r_2} \hookrightarrow \mathbb{C}^d = \mathbb{A}^d(\mathbb{C})$$

*the corresponding map into the complex affine space. Let $x \in K^*$ be a primitive element (a generator of the field $K$ over $\mathbb{Q}$). For any Zariski closed subset $Z \subset \mathbb{A}^d$ there exists a finite sequence of quadratic polynomials $g_i \in \mathbb{Q}[x]$, $i = 1, \dots, n$, such that $g_1(g_2(\cdots(g_n(x)))) \notin Z$.*

*Proof.* — Since $x$ is primitive, it is not contained in any diagonal in $\mathbb{A}^d$. Therefore, the variety $S_x$ constructed in Lemma 4.1 coincides with $\mathbb{A}^d$. It suffices to observe that the image of $x$ under $\mathbb{Q}$-rational quadratic maps is Zariski dense in $S_x = \mathbb{A}^d$ (at each step of the inductive construction, we get a Zariski dense set of points in the total space of the vector bundle). □

For $q \in \bar{\mathbb{Q}}$ let $\deg(q)$ be the degree of the minimal polynomial $f = f_q(x) \in \mathbb{Q}[x]$ vanishing in $q$ and $K = K_q/\mathbb{Q}$ the field generated by $q$.

Corollary 4.3. — *Let $q \in \bar{\mathbb{Q}}$. Then there exists a sequence of quadratic polynomials $g_i \in \mathbb{Q}[x]$ such that $g := g_1(g_2 \cdots (g_n(x))) \in \mathbb{Q}[x]$ has the property that*

- $\deg(g(q)) = \deg(q)/2^k$, *for some $k \in \mathbb{N}$, and*
- *the derivative of the minimal polynomial $f_{g(q)}(x) \in \mathbb{Q}[x]$ of $g(q) \in \bar{\mathbb{Q}}$ has no multiple roots.*

*Proof.* — The first condition is satisfied, since a $\mathbb{Q}$-rational quadratic maps can diminish the degree of the minimal polynomial at most by a factor of 2. The second condition amounts to a Zariski closed condition on the set of points in $K_q \subset \mathbb{A}^{\deg(q)}(\mathbb{C})$. □

Let $f : \mathbb{P}^1 \to \mathbb{P}^1$ be a rational map and $\mathrm{Ram}(f) = \{q \mid f'(q) = 0\} \subset \mathbb{P}^1$ the set of ramification points.

Theorem 4.4. — *For any finite set $Q \subset \mathbb{P}^1(\bar{\mathbb{Q}})$ there is rational map $f : \mathbb{P}^1 \to \mathbb{P}^1$ such that*

$$\{f(q), q \in Q\} \cup \mathrm{Ram}(f) \subset \mathbb{P}^1(\mathbb{Q}).$$

*Moreover, the only prime dividing a local ramification index of $f$ is 2.*

Remark 4.5. — This is an analog of the first part of Belyi's theorem, with restrictions on the ramification. The proof follows the general line of Belyi's argument.

*Proof.* — We proceed by induction on $m := \max(\deg(q))$, for $q \in Q$. Observe, that for all $f \in \mathbb{Q}[x]$ and all $q \in \bar{\mathbb{Q}}$ we have

$$\deg(f(q)) \leq m.$$

Assume that $m = 2^k$ and let $r \in Q$ be a point with minimal polynomial $f = f_q$ of degree $m$. If $f' \in \mathbb{Q}[x]$ has no multiple roots, then $f(Q) \bigcap \mathrm{div}_0(f')$ has fewer points of degree $m$: $f$ maps $q$ to zero and the zeroes of $f'$ have degree $< m$. Moreover, the local ramification indices of $f$ are powers of 2. If $f'$ has multiple roots, we apply a sequence of $\mathbb{Q}$-rational quadratic maps as in Corollary 4.3, to replace $q$ by $q' := g_1(g_2 \cdots (g_n(q)))$ so that the derivative of the minimal polynomial $f_{q'}(x) \in \mathbb{Q}[x]$ of $q'$ has no multiple roots. The local ramification indices of a sequence of quadratic maps are powers of 2.

Now assume that $2^{k-1} < m < 2^k$, for some $k \in \mathbb{N}$, and put $s = 2^k - m$. Identify the space $F_m$ of monic degree $d$ polynomials with the affine space

$$\mathbb{A}^d = \{f_0 + f_1 x + \cdots f_{d-1}x^{d-1} + x^d\}$$

and consider the following $\mathbb{Q}$-variety:

$$X \subset F_m \times F_s \times \mathbb{A}^s = \{(a_1, \ldots, a_s)\},$$

given by

$$(f \cdot g)'(a_j) = 0, \quad \text{for all} \ \ j = 1, \ldots, s. \tag{4.1}$$

For fixed $f \in F_m$ and $a \in \mathbb{A}^s$ we get a system of non-homogeneous linear equations, where the variables are the coefficients of $g$. For generic, in Zariski topology on $F_m \times \mathbb{A}^s$, choices of $f$ and $a$ we get a unique solution, and a $\mathbb{Q}$-birational parametrization of $X$ by $F_m \times \mathbb{A}^s = \mathbb{A}^{m+s}$ (here we use $m > s$). Thus the set of $\mathbb{Q}$-rational triples $(f, g, a)$ subject to the equations (4.1) is Zariski dense in $X$.

The natural $\mathbb{Q}$-rational projection

$$X \quad \to \quad F_m \times F_s$$

is surjective (this can be checked over $\mathbb{C}$). In particular, $X(\mathbb{Q})$ is Zariski dense in $X$. The preimage $Z \subset X$ of the subset of those $(f, g)$ where $(fg)'$ and $g$ have multiple roots is a proper subvariety.

Applying $\mathbb{Q}$-rational quadratic maps as in Lemma 4.1, if necessary, we find a generic $f = f_q \in F_m(\mathbb{Q})$ and, by the argument above, a generic $g \in F_s(\mathbb{Q})$ such that there is a point $(f, g, a) \in (X \setminus Z)(\mathbb{Q})$ over $(f, g)$.

The map $h := fg : \mathbb{P}^1 \to \mathbb{P}^1$ has the following properties:

- $h(q) = 0$ and $Q$ has stricly fewer points of degree $m$;
- by construction, $(fg)'$ has at least $s$ distinct $\mathbb{Q}$-rational roots so that the degree of points added to $Q$ (the zeroes of $(fg)'$) is strictly less than $m$;
- all local ramification indices are powers of 2.

This concludes the induction and the proof of the theorem. □

Remark 4.6. — A similar statement holds over function fields of any characteristic ($\neq 2$). Using the techniques from [4] one can show the following result: for any affine algebraic variety $X$ over an algebraically closed field there exist a proper finite map $\pi : X \to \mathbb{A}^n$ and a linear projection $\lambda : \mathbb{A}^n \to \mathbb{A}^{n-1}$ such that $\pi$ is ramified only in the sections of $\lambda$ and the local ramification indices are powers of 2.

REMARK 4.7. — The methods of Belyi of collecting $\mathbb{Q}$-points on $\mathbb{P}^1$ produce ramification indices which depend on all pairwise differences between the coordinates of the points (for an exposition, see [2], Chapter 10). They cannot be applied in the construction of maps with restricted ramification.

## References

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

[2] F. BOGOMOLOV and T. PETROV – *Algebraic curves and one-dimensional fields*, Courant Lecture Notes in Mathematics, vol. 8, New York University Courant Institute of Mathematical Sciences, New York, 2002.

[3] F. BOGOMOLOV and Y. TSCHINKEL – "Unramified correspondences", Algebraic number theory and algebraic geometry, Contemp. Math., vol. 300, Amer. Math. Soc., Providence, RI, 2002, p. 17–25.

[4] F. A. BOGOMOLOV and T. G. PANTEV – "Weak Hironaka theorem", *Math. Res. Lett.* **3** (1996), no. 3, p. 299–307.

[5] E. BOMBIERI and U. ZANNIER – "Algebraic points on subvarieties of $\mathbf{G}_m^n$", *Internat. Math. Res. Notices* (1995), no. 7, p. 333–347.

[6] N. D. ELKIES – "*ABC* implies Mordell", *Internat. Math. Res. Notices* (1991), no. 7, p. 99–109.

[7] F. KLEIN – *Lectures on the icosahedron and the solution of equations of the fifth degree*, revised ed., Dover Publications Inc., New York, N.Y., 1956.

[8] M. MCQUILLAN – "Division points on semi-abelian varieties", *Invent. Math.* **120** (1995), no. 1, p. 143–159.

[9] L. MORET-BAILLY – "Hauteurs et classes de Chern sur les surfaces arithmétiques", *Astérisque* (1990), no. 183, p. 37–58, Séminaire sur les Pinceaux de Courbes Elliptiques (Paris, 1988).

[10] M. RAYNAUD – "Courbes sur une variété abélienne et points de torsion", *Invent. Math.* **71** (1983), no. 1, p. 207–233.

[11] L. Szpiro – "Discriminant et conducteur des courbes elliptiques", *Astérisque* (1990), no. 183, p. 7–18, Séminaire sur les Pinceaux de Courbes Elliptiques (Paris, 1988).

[12] S. Zhang – "Positive line bundles on arithmetic varieties", *J. Amer. Math. Soc.* **8** (1995), no. 1, p. 187–221.