

JOURNAL

de Théorie des Nombres
de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Xavier XARLES

Trivial points on towers of curves

Tome 25, n° 2 (2013), p. 477-498.

<http://jtnb.cedram.org/item?id=JTNB_2013__25_2_477_0>

© Société Arithmétique de Bordeaux, 2013, tous droits réservés.

L'accès aux articles de la revue « Journal de Théorie des Nombres de Bordeaux » (<http://jtnb.cedram.org/>), implique l'accord avec les conditions générales d'utilisation (<http://jtnb.cedram.org/legal/>). Toute reproduction en tout ou partie de cet article sous quelque forme que ce soit pour tout usage autre que l'utilisation à fin strictement personnelle du copiste est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

cedram

Article mis en ligne dans le cadre du
Centre de diffusion des revues académiques de mathématiques
<http://www.cedram.org/>

Trivial points on towers of curves

par XAVIER XARLES

RÉSUMÉ. Afin d'étudier le comportement des points dans une tour de courbes, nous introduisons et étudions les points triviaux sur les tours de courbes, et nous discutons de leur finitude sur les corps de nombres. Nous relierons le problème de prouver que les seuls points rationnels sont les points triviaux à un certain niveau de la tour à la non-existence d'une borne de la gonologie des courbes de la tour, que nous démontrons sous certaines hypothèses.

ABSTRACT. In order to study the behavior of the points in a tower of curves, we introduce and study trivial points on towers of curves, and we discuss their finiteness over number fields. We relate the problem of proving that the only rational points are the trivial ones at some level of the tower, to the unboundeness of the gonality of the curves in the tower, which we show under some hypothesis.

1. Introduction

A typical feature of the solutions of families of diophantine equations (like Fermat's equation) is the existence of some solutions, usually called trivial, in any member of the family, sometimes clear from the context. It is expected also in most cases that for all members of the family with, maybe, a finite number of exceptions, the only solutions are the trivial ones. This paper was intended as an attempt to study such a problem for the case that the family forms a tower of curves. To this end we first need to find an intrinsic definition of the trivial solutions. The idea is that the trivial solutions are the solutions that are always there, so they should be points that exist at all the levels of the tower. And our main goal is to find conditions in order to show when there is a finite number of such trivial points, and also conditions on the existence of bounds for the level of the tower where all the points are trivial. These bounds will be uniform in the sense that when we change the number field the bound changes depending only on the absolute degree of the field.

The author was partially supported by the grant MTM2009-10359.
Classification math. 11G30, 11G20, 11B39, 11D45, 14G25.

The main example we had in mind was the case of the modular towers: consider the curves $X_1(p^n)$ for some fixed prime p , and $n \geq 0$. Then the trivial points should correspond to the cuspidal points. And, moreover, there is a constant $N(p, d)$ depending on p and $d \geq 1$ such that, for any number field K with $[K : \mathbb{Q}] \leq d$, and for any $n \geq N(p, d)$, the only K -rational points of $X_1(p^n)$ are the trivial ones. This result, but for the constant $N(p, d)$ depending also on K , was obtained by Y. Manin in [26]. The stated uniform version was proved by Frey in [17], and it is a consequence of the main theorem of Faltings (see also section 6). Another example was considered by the author in [32] (see also last example in section 2). This paper is, in some sense, a sequel of that paper, with the aim to investigate in detail under which circumstances these type of results generalize. There are other recent papers treating similar problems. For example, the paper [9] studies cases similar to the modular towers, related to the inverse Galois problem (see also [18] for other generalizations), and the paper [14] studies also such (very general) cases but for families indexed by prime numbers.

The paper is organized as follows. In section 2 we introduce the towers of curves and their trivial points, and give some elementary results. In sections 3 and 4 we study the special cases of towers with genus 0 and 1, giving some partial results. In section 5 we give a criterion for proving the finiteness of trivial points of a tower. In section 6 we recall the well-known relation between the unbounded gonality and the existence of uniform bounds (see Theorem 6.3). The rest of the sections are dedicated to the discussion of distinct methods to bound the gonality of a tower: geometric methods, reduction modulo primes and counting points, and methods related to graphs.

This paper contains results concerning towers of curves that the author collected during some years. The content was explained during the “Cuartas Jornadas de Teoría de Números” in Bilbao, in July 2011. I would like to thank the organizers for the invitation to give a talk, which motivated me to write this paper. I wish to express my gratitude also to Enrique González Jiménez, Joan Carles Lario, Francesc Bars, Pete Clark and Brian Conrad for some conversations related to the subject. I am greatly indebted to Bjorn Poonen for answering some doubts concerning the gonality and for his collaboration in proving some results in section 3. Finally, I gratefully acknowledge the many helpful suggestions of an anonymous referee.

2. Notations, generalities and examples

Given a field K , we will denote by \overline{K} a fixed separable closure of K and by G_K the absolute Galois group of K , equal to $\text{Aut}_K(\overline{K})$, the automorphisms of the field \overline{K} fixing the elements of K . Given any scheme V over K , we will denote by \overline{V} the base change of V to \overline{K} .

Definition. Let K be a field. By a **tower of curves** over K we mean an ordered pair of sequences $\mathbf{C} := (\{C_n\}_{n \geq 0}, \{\varphi_n\}_{n \geq 1})$, where, for any $n \geq 0$, a non-negative integer, C_n are smooth projective algebraic curves defined over K and geometrically connected, and, for any positive integer $n > 0$, the $\varphi_n : C_n \rightarrow C_{n-1}$ are non constant morphisms as algebraic curves of degree > 1 .

If $m > n$, we will denote by $\varphi_{m,n}$ the morphism from C_m to C_n obtained composing the morphisms from φ_m to φ_{n+1} . We will denote also by $\varphi_{n,n}$ the identity map on C_n .

Definition. Given two towers of curves $\mathbf{C} = (\{C_n\}_{n \geq 0}, \{\varphi_n\}_{n \geq 1})$ and $\mathbf{C}' = (\{C'_n\}_{n \geq 0}, \{\varphi'_n\}_{n \geq 1})$, a morphism Ψ from \mathbf{C} to \mathbf{C}' is a collection of morphisms $\psi_n : C_n \rightarrow C'_{k_n}$, where $\{k_n\}_{n=0}^\infty$ is a strictly increasing sequence of non-negative integers, such that $\varphi'_{k_n, k_m} \psi_n = \psi_m \varphi_{n,m}$ if $n \geq m$. A special case is when \mathbf{C} is a subtower of \mathbf{C}' , i.e $C_n = C'_{k_n}$ and ψ_n is the identity, for some progression $k_0 < k_1 < k_2 < \dots$. An isomorphisms of towers will mean that the maps ψ_n are isomorphisms and $k_n = n$ for all $n \geq 0$.

Given a smooth projective algebraic curve C over a field K , we will denote by $g(C)$ the genus of C , and by $\gamma(C)$ the gonality of C over the field K , which is the minimum degree of a rational map to \mathbb{P}^1 .

Note that, given a tower of curves, we have by Hurwitz's theorem that $g(C_n) \geq g(C_{n-1})$ for any n . The same fact for the gonality is not so easy; one can find a proof of this result for example in Proposition A1 in [29] (see Proposition 6.1).

Definition. Given a tower of curves \mathbf{C} , we define the genus $g(\mathbf{C})$ to be $\lim_{n \rightarrow \infty} g(C_n)$, and the gonality $\gamma(\mathbf{C})$ as $\lim_{n \rightarrow \infty} \gamma(C_n)$.

Lemma 2.1. *For any tower \mathbf{C} , the genus can only be $g(\mathbf{C}) = 0, 1$ or ∞ .*

Proof. This is again a consequence of Hurwitz's theorem: if there exists a curve C_n in the tower with genus $g(C_n) > 1$, then $g(C_{m+1}) > g(C_m)$ for all $m \geq n$, so $g(\mathbf{C}) = \infty$. □

Remark. One can construct genus 0 towers easily by fixing rational functions $f_n(x) \in K(x)$ of degree > 1 . Over algebraically closed fields, all genus 0 towers are of this type (see section 3).

Also, to construct genus 1 towers, one can fix elliptic curves E_n and isogenies $\varphi_n : E_n \rightarrow E_{n-1}$. An easy example is given when $E_n = E$ and φ_n is multiplication by some fixed integer number for all $n \geq 0$ (see section 4).

Remark. The analogous result of lemma 2.1 but for the gonality is not true. In fact one can construct towers of curves of a given gonality γ over a field if one knows an algebraic curve C over that field with that gonality: if $f : C \rightarrow \mathbb{P}^1$ is a gonal map, and $g : \mathbb{P}^1 \rightarrow \mathbb{P}^1$ is any map with degree

> 1 , define first $C_0 := \mathbb{P}^1$, $C_1 := C$, $\varphi_1 := f$ and $\psi_1 := f$. Then, define inductively, for $n \geq 1$, the curve C_{n+1} to be the desingularization of a connected component of the fiber product $C_n \times_{\mathbb{P}^1} \mathbb{P}^1$ with respect to the maps ψ_n and g , and the maps $\varphi_{n+1} : C_{n+1} \rightarrow C_n$ and $\psi_{n+1} : C_{n+1} \rightarrow \mathbb{P}^1$ as the natural maps given by the universal property of the fiber product. For a general g the maps φ_n are of degree equal to the degree of g , and the degree of ψ_n equal to the degree of f . Since the gonality of C_n cannot be smaller than the gonality γ of C for $n \geq 1$ (by Proposition 6.1 (6)), and it has a map of the degree γ , the gonality of C_n is equal to γ .

Definition. Given a tower of curves $\mathbf{C} = (\{C_n\}_{n \geq 0}, \{\varphi_n\}_{n \geq 1})$ defined over K , the K -trivial points of \mathbf{C} in the level $n \geq 0$ are

$$\mathbf{C}(K)_n := \{P \in C_n(K) \mid \forall m \geq n \exists P_m \in C_m(K) \text{ such that } \varphi_{m,n}(P_m) = P\}.$$

If $d \geq 1$ is an integer, the K -trivial points of \mathbf{C} in the level $n \geq 0$ and degree d are

$$\mathbf{C}^{(d)}(K)_n := \bigcup_{L \subset \bar{K}, [L:K] \leq d} \mathbf{C}(L)_n.$$

Finally, the trivial points of \mathbf{C} in level n are

$$\mathbf{C}^{(\infty)}(K)_n := \bigcup_{d \geq 1} \mathbf{C}^{(d)}(K)_n.$$

So the trivial points in level n are the points that are L -trivial in level n for some finite extension L/K .

In the case of level 0 we will frequently omit it from the notation.

Observe that over an algebraically closed field the trivial points of a tower of curves in the level n is equal to all the rational points of the curve C_n . So these definitions are only interesting in fields K whose algebraic closure has infinite degree over K . In this paper we will consider only number fields or finite fields.

Observe also that the K -rational trivial points in level n are equal to the image in $C_n(K)$ of the natural map

$$\varprojlim_n C_n(K) \rightarrow C_n(K),$$

where the projective limit is taken with respect to the maps φ_n .

The main problem we are interested on is the finiteness of K -trivial and of trivial points. This finiteness is independent of the level, and one can reduced also to a subtowers, as the following result shows, whose proof is straightforward and we will omit.

Lemma 2.2. *Let $\mathbf{C} = (\{C_n\}_{n \geq 0}, \{\varphi_n\}_{n \geq 1})$ be a tower of curves over some field K .*

- (1) For any $d \in \{0, 1, \dots, \infty\}$, and any $n \geq m$, the natural map $\varphi_{n,m} : \mathbf{C}^{(d)}(K)_n \rightarrow \mathbf{C}^{(d)}(K)_m$ is surjective.
- (2) $d \in \{0, 1, \dots, \infty\}$, and any $n \geq m$, $\mathbf{C}^{(d)}(K)_n \subseteq \varphi_{n,m}^{-1}(\mathbf{C}^{(d)}(K)_m)$.
- (3) If \mathbf{C}' is a subtower of \mathbf{C} , i.e. $C'_n = C_{k_n}$ and ψ_n is the identity, for some progression $k_0 < k_1 < k_2 < \dots$, then $\mathbf{C}'^{(d)}(K)_n = \mathbf{C}^{(d)}(K)_{k_n}$ for all $n \geq 0$ and all $d \in \{0, 1, \dots, \infty\}$.

We end this section by giving some examples of towers of curves.

Example 1. Consider a prime number p . The p -**Fermat tower** will be the tower with curves C_n given by planar homogeneous equations $X_0^{p^n} + X_1^{p^n} = X_2^{p^n}$, and maps $\varphi_n(X_0, X_1, X_2) = [X_0^p : X_1^p : X_2^p]$, all defined over the rational field \mathbb{Q} (or a general number field). One can show that the only trivial points of the tower are the “trivial solutions” $[a_0 : a_1 : a_2]$ with $a_0 a_1 a_2 = 0$.

Example 2. Consider a prime number p . The p -**modular tower** will be the tower with curves $C_n := X_1(p^n)$ and natural maps φ_n . If the ground field is a number field or a finite field, then the only trivial points of the tower are the so-called cuspidal points, a result that can be deduced from the well-known finiteness of the set of torsion points of any elliptic curve over such a field.

Example 3. Consider the homogeneous polynomial $f_0 := X_0^2 + X_1^2 - X_2^2$, and $C_n \subset \mathbb{P}^{n+2}$ be the curves defined over \mathbb{Q} as the zero set of the polynomials f_0, f_1, \dots, f_n , where $f_n := f_0(X_n, X_{n+1}, X_{n+2})$. For any field K , the K -rational points of C_n are in bijection with the Fibonacci type sequences of squares of length $n + 2$, that is sequences $\{a_0, a_1, a_2, \dots, a_n\}$ such that $a_{n+2} = a_{n+1} + a_n$ and all the elements a_i are squares in K . We will call this tower the **Square Fibonacci tower**. This tower of curves is similar the tower of curves studied in [32], which is defined as above but with $f_0 := X_0^2 - 2X_1^2 + X_2^2$.

Observe that we have four points $[\pm 1, 0, \pm 1, 1] \in C_1(\mathbb{Q})$. One can show that C_1 is isomorphic to the elliptic curve E with Cremona Reference 32a2, and that $E(\mathbb{Q})$ has only four points. So $C_1(\mathbb{Q}) = \{[\pm 1, 0, \pm 1, 1]\}$, thus $C_2(\mathbb{Q}) = \emptyset$ and, hence, $\mathbf{C}(\mathbb{Q})_0 = \emptyset$.

Using the results in section 6 one can show that the degree 2 points over \mathbb{Q} of the curve C_2 , which has genus 5 and gonality 4 (see section 7), inject inside the jacobian $\text{Jac}(C_2)$. Using results as in [19, 20], one can show that the jacobian is isogenous to the product of 5 elliptic curves, with Cremona references 32a2,32a2,48a1,96a1 and 96b1. All of them have rank 0 and four rational points, so $\text{Jac}(C_2)$ is finite and computable. Using this result we conclude that

$$C_2(\mathbb{Q})^{(2)} = \{[\sqrt{-1}, \pm 1, 0, \pm 1, \pm 1], [\pm 1, 0, \pm 1, \pm 1, \sqrt{2}]\},$$

which can be used to show that $C_3(\mathbb{Q})^{(2)} = \emptyset$ and hence $\mathbf{C}(K)_0^{(2)} = \emptyset$.

We do not know if $\mathbf{C}(K)_0^{(d)} = \emptyset$ for some $d \geq 3$ (but we do know these sets are finite using the results in section 6) or if $\mathbf{C}(K)_0^\infty = \emptyset$, or even finite. We conjecture that $\mathbf{C}(K)_0^\infty = \emptyset$.

Conjecture 2.3. *The Square Fibonacci tower has no trivial points over any number field. Hence, the curves given by the system of equations*

$$X_0^2 + X_1^2 = X_2^2, X_1^2 + X_2^2 = X_3^2, \dots, X_n^2 + X_{n+1}^2 = X_{n+2}^2$$

inside \mathbb{P}^{n+2} have no rational points for any number field K and for n large enough (in terms of the degree of K/\mathbb{Q}).

3. Genus 0 Towers

Consider a tower of curves \mathbf{C} with genus 0. It is well known that a genus 0 curve is either isomorphic to the projective line \mathbb{P}^1 (and if and only if it has a rational point in your field), or isomorphic to a conic curve (see for example Theorem A.4.3.1. in [21]). In this second case, there exists some degree 2 extension of the field where the curve gets isomorphic to \mathbb{P}^1 .

Definition. Given an enumerated set $\mathcal{F} := \{f_n(x) \in K(x)\}_{n \geq 1}$ of rational functions with degree > 1 , consider the tower of curves $\mathbf{C}_{\mathcal{F}}$ defined as $C_n := \mathbb{P}^1$ and $\varphi_n = f_n(x)$ for all $n \geq 0$. The special case that $f_n = f$ for all n will be denoted by \mathbf{C}_f .

The next lemma, which in part goes at least all the way back to Witt, was communicated to me by Bjorn Poonen.

Lemma 3.1. *Let C and C' be genus 0 curves over a field K , and f be a non-constant morphisms from C to C' . Suppose that $C'(K) = \emptyset$. Then C and C' are isomorphic (and the degree of f is odd).*

Proof. It is well known that the genus 0 curves C without K -rational points correspond to conics without points, so to quaternion algebras over K , hence they give elements x_C of order 2 in the Brauer group $\text{Br}(K)$ of K . The existence of the map f says us that C has no rational points. We will see that $\text{deg}(f)x_C = x_{C'}$ in $\text{Br}(K)$, hence $\text{deg}(f)$ is odd and $x_C = x_{C'}$, so C is isomorphic to C' . Observe that we have a natural map

$$\mathbb{Z} \cong \text{Pic}(\bar{C})^{G_K} \rightarrow H^1\left(G_K, \frac{K(\bar{C})^*}{\bar{K}^*}\right) \rightarrow H^2(G_K, \bar{K}^*) = \text{Br}(K)$$

sending 1 to x_C , given by the natural connecting homomorphisms, which is functorial. On the other hand, the natural map $\text{Pic}(\bar{C}')^{G_K} \rightarrow \text{Pic}(\bar{C})^{G_K}$ is the multiplication by the degree of f . Hence the result is deduced from the commutativity of the natural diagram, which is easy. \square

As a consequence of this lemma and the results cited above, we get the following classification.

Lemma 3.2. *Let K be a field, and let \mathbf{C} be a genus 0 tower of curves. Then*

- (1) *If $\mathbf{C}(K)_0 \neq \emptyset$, then there exists a set $\mathcal{F} := \{f_n(x) \in K(x)\}_{n \geq 1}$ of rational functions and an isomorphism $\mathbf{C} \cong \mathbf{C}_{\mathcal{F}}$.*
- (2) *There always exists some degree 2 extension L/K , an enumerated set $\mathcal{F} := \{f_n(x) \in L(x)\}_{n \geq 1}$ and an isomorphism $\mathbf{C} \otimes_K L \cong \mathbf{C}_{\mathcal{F}}$ defined over L .*

Proof. If $\mathbf{C}(K)_0 \neq \emptyset$, then there are points $P_n \in C_n(K)$ for all n , hence all the curves C_n are isomorphic to \mathbb{P}^1 . But then the maps φ_n give us endomorphisms of \mathbb{P}^1 , so rational functions f_n . The same is true if $C_n(K) \neq \emptyset$ for all $n \geq 0$.

Now, suppose there exists $n \geq 0$ such that $C_n(K) = \emptyset$. Using the previous lemma, we get that C_m is isomorphic to C_n for all $m \geq n$, and all isomorphic to a fixed conic C .

To end the proof, we only need to observe that for any conic C over a field there exists some degree 2 extension L/K such that $C(L) \neq \emptyset$; if $C(K) = \emptyset$, and it is defined by a polynomial $f(x, y) \in K[x, y]$, take any $a \in K$. Then $f(x, a) \in K[x]$ is a degree 2 irreducible polynomial which defines the desired extension L . □

Now we are going to study the finiteness of K -trivial points when K is a number field. Hence we can and will assume that $\mathbf{C}(K)_0 \neq \emptyset$. We will only get results for towers of the form \mathbf{C}_f using the theory of heights.

Remark. For the towers of the form \mathbf{C}_f , with $f(x) \in K(x)$, observe that $\mathbf{C}(K)_n = \mathbf{C}(K)_0$ for all n , and it contains the set of periodic points of f : the points $P \in \mathbb{P}^1(K)$ such that $f^N(P) = P$ for some $N \geq 1$.

Theorem 3.3. *Let K be a number field and let $f(x) \in K(x)$ be a rational function of degree $d > 1$. Then*

- (1) *For every $e \geq 1$, the set of trivial points of degree e and level 0 $\mathbf{C}_f(K)_0^{(e)}$ is equal to the set of periodic points of f of degree e .*
- (2) *The set of K -rational trivial points $\mathbf{C}_f(K)_0$ is finite.*

Proof. Recall that Northcott theorem (Proposition B.4.2.(b) in [21]) states that the set of preperiodic points (points P such that $f^N(P)$ is periodic for some $N \geq 1$) is finite, and in particular the set of periodic points is finite too. Hence part (2) follows from part (1) and it suffices to show that every trivial point is periodic.

Consider the canonical height function $h_f : \mathbb{P}^1(\overline{K}) \rightarrow \mathbb{R}$ associated to f (see for example [21], Theorem B.4.1.). Then $h_f(f(P)) = dh_f(P)$ for any $P \in \mathbb{P}^1(\overline{K})$, where $d > 1$ is the degree of f . If $P \in \mathbf{C}_f(K)_0^{(e)}$, there exists a finite extension L of K of degree $\leq e$, and points $P_n \in \mathbb{P}^1(L)$ such that $f^n(P_n) = P$. For these points we have $h_f(P) = h_f(f_n(P_n)) = d^n h_f(P_n)$.

Suppose that $h_f(P) \neq 0$. Then $h_f(P_n) = d^{-n}h_f(P) < d^{-n+1}h_f(P) = h_f(P_{n-1})$, so all these real numbers are distinct. Thus the set $\{P_n \mid n \geq 0\}$ is an infinite set of points of $\mathbb{P}^1(L)$ and with bounded canonical height h_f , hence with bounded absolute (logarithmic) height, which is not possible (see [21], theorem B.2.3). So $h_f(P) = 0$ and hence P is preperiodic by Proposition B.4.2.(a) in [21]. Now, if P is preperiodic but not periodic, the set $\{P_n \mid n \geq 0\}$ is an infinite set of preperiodic points all defined over L , which is again no possible, by Northcott theorem. \square

Observe that the finiteness of the set of K -rational trivial points of degree $e > 1$ will follow from the same result on the periodic points, which is a conjecture (see for example conjecture 3.15 in [31]).

Question 1. Are there genus 0 towers (of the form $\mathbf{C}_{\mathcal{F}}$) over a number field K having an infinite number of K -rational trivial points?

Concerning the trivial points of the genus 0 towers, it is easy to construct examples such that there are infinitely many of them, and towers with only a finite number of them, as shown in the next two examples.

Example 4. Consider the special case $f(x) = x^2$ and $K = \mathbb{Q}$. Then the set of trivial points $\mathbf{C}_{x^2}^{(\infty)}(K)_0$ of \mathbf{C} in level 0 is equal to the set of periodic points for x^2 , which is the set of n -roots of unity for odd $n \geq 1$ (and $x = 0$ and ∞), hence infinite:

$$\mathbf{C}_{x^2}^{(\infty)}(\mathbb{Q})_0 = \{\xi \in \overline{\mathbb{Q}} \mid \exists N \geq 1 \text{ odd such that } \xi^N = 1\} \cup \{0, \infty\}.$$

Example 5. Take the genus 0 tower $\mathbf{C}_{\mathcal{F}}$ defined by $\mathcal{F} := \{f_n(x) = x^{n+1} \in K(x)\}$, where K is any number field. Then the set of trivial points of \mathbf{C} in level 0 is equal to

$$\mathbf{C}_{\mathcal{F}}^{(\infty)}(K)_0 = \{0, 1, \infty\}.$$

To show these, observe that $\alpha \in K$ is a K -rational trivial point if and only if α has a n th root for all $n \geq 1$. But the only such numbers are 0 and 1 in any number field. This last result can be shown proving first that the absolute logarithmic height of α must be 0 (if $\alpha \neq 0$) as in the proof of the Theorem 3.3, so α must be a root of unity. But the only root of unity which is a n th root of unity for all $n \geq 1$ is 1.

4. Genus 1 Towers

First of all, observe that, if we have a tower \mathbf{C} of genus 1 curves over a field K such that there is a trivial point $P \in \mathbf{C}(K)_0$, we can use this point in order to get an explicit description of the tower.

Lemma 4.1. *Consider a tower $\mathbf{C} = (\{C_n\}_{n \geq 0}, \{\varphi_n\}_{n \geq 1})$ of genus 1 curves over a field K , and suppose there is a point $P \in \mathbf{C}(K)_0$. Then the tower \mathbf{C} is isomorphic to a tower $\mathcal{E} := (\{E_n\}_{n \geq 0}, \{\phi_n\}_{n \geq 1})$ where the E_n are elliptic curves and the $\phi_n : E_n \rightarrow E_{n-1}$ are isogenies.*

Proof. Let us fix a point $P_n \in C_n(K)$ such that $\varphi_n(P_n) = P_{n-1}$. Consider the elliptic curve $E_n := \text{Jac}(C_n)$, and the Abel-Jacobi map $\iota_n : C_n \rightarrow E_n$ given by sending the point $P_n \in C_n(K)$ to 0, which is an isomorphism of curves. The maps $\phi_n := \iota_{n-1}\varphi_n\iota_n^{-1}$ are non-constant morphisms of curves between E_n and E_{n-1} which send the 0 point to the 0 point. Hence they are isogenies. \square

Definition. Given an elliptic curve E over a field, denote by $\mathcal{O} := \text{End}_K(E)$ the ring of endomorphisms of E over K as elliptic curve (if E has no complex multiplication, and K has characteristic 0, then $\mathcal{O} \cong \mathbb{Z}$). Given a progression $\mathcal{A} := \{a_n \in \mathcal{O} \mid n = 0, 1, \dots\}$ of elements with degree > 1 , consider the tower of curves $\mathbf{C}_{E,\mathcal{A}}$ defined as $C_n := E$ for all $n \geq 0$ and φ_n equal to the a_n for all $n \geq 1$. The special case that $a_n = a$ for all n will be denoted by $\mathbf{C}_{E,a}$.

Corollary 4.2. *Let $\mathbf{C} = (\{C_n\}_{n \geq 0}, \{\varphi_n\}_{n \geq 1})$ be a tower of genus 1 curves over a number field K such that $\mathbf{C}(K)_0 \neq \emptyset$. Then there is an elliptic curve E defined over K and a progression $\mathcal{A} := \{a_n\}$ such that the tower $\mathbf{C}_{E,\mathcal{A}}$ is isomorphic to a subtower of \mathbf{C} .*

Proof. By applying the lemma we are reduced to the case that the C_n are elliptic curves and the φ_n are isogenies. A well-known result of Faltings' (see [15]) implies that there is a finite number of elliptic curves isogenous to a given one over a number field. Hence in the set of elliptic curves C_n , there are infinitely many of them isomorphic to a given elliptic curve E . The result is now easily deduced. \square

Now we can prove the finiteness of the K -rational trivial points.

Corollary 4.3. *Let $\mathbf{C} = (\{C_n\}_{n \geq 0}, \{\varphi_n\}_{n \geq 1})$ be a tower of genus 1 curves over a number field K . Then, for all $n \geq 0$ and all $d \geq 1$, the set of K -trivial points of \mathbf{C} in the level $n \geq 0$ and degree d is finite.*

Proof. Observe that it is sufficient to know the result for an isomorphic subtower by Lemma 2.2. Hence, by using the previous results, we are reduced to the case that $\mathbf{C} = \mathbf{C}_{E,\mathcal{A}}$ for some elliptic curve E and some progression $\mathcal{A} := \{a_n\}$ of natural numbers, or of elements in a quadratic imaginary order in the CM case, and also to the case $n = 0$.

Consider a point $P \in \mathbf{C}^{(d)}(K)_0$. Let L/K be an extension of degree d such that $P \in \mathbf{C}(L)_0$. Such an element in $\mathbf{C}(L)_0$ is a point $P \in E(L)$ that is divisible by $b_n := a_0 a_1 \cdots a_n$ for all n , hence by its norm to \mathbb{Z} . But $E(L)$ is finitely generated, so P must be torsion. Thus $\mathbf{C}(L)_0 \subset E(L)_{tors}$, the torsion subgroup, which is finite, which proves the case $d = 1$. In general, we get that

$$\mathbf{C}^{(d)}(K)_0 \subset \bigcup_{L \subset \overline{K}, [L:K] \leq d} E(L)_{tors},$$

which is again finite, as we are going to show.

First, we prove that there exists an integer $N(d, K, E)$, depending on d , K and E , such that all points in $E(L)_{tors}$ for L/K of degree d have order dividing $N(d, K, E)$. Fix L/K of degree d and let $N_L \geq 1$ be an integer such that $E(L)_{tors} = E(L)[N_L]$. Now, take a good reduction prime \wp with residual characteristic p . Let $N_{L,p} := p^{-\text{ord}_p(N_L)} N_L$ be the prime to p -part of N_L . Then the reduction map modulo \wp gives an injection $E(L)[N_{L,p}] \hookrightarrow E_\wp(\ell_{\wp'})$, where E_\wp is the reduction of E at \wp , \wp' is a prime above \wp and $\ell_{\wp'}$ is the residue field of L at \wp' (see for example [30], Proposition VII.3.1). Hence $N_{L,p}$ is bounded above by a constant depending only on the number of elements of $\ell_{\wp'}$ by the Weil bound. One can give then a bound $M(p, d, d_K)$, depending only on d , p and the absolute degree d_K of K , such that $N_{L,p}$ divides $M(p, d, d_K)$. Considering then two primes \wp_1 and \wp_2 with distinct characteristics p_1 and p_2 we get the result; just take $N(d, K, E)$ to be the least common multiple of $M(p_i, d, d_K)$ for $i = 1$ and 2 .

Using this result, one gets finally that

$$\bigcup_{L \subset \overline{K}, [L:K] \leq d} E(L)_{tors} \subset E(\overline{K})[N(d, K, E)]$$

which is finite, with order $N(d, K, E)^2$. □

Remark. Using Merel’s result in [27], one can show that there exists a bound of $\bigcup_{L \subset \overline{K}, [L:K] \leq d} E(L)_{tors}$, for any E elliptic curve over a number field L , which depends only on d and the absolute degree of K , which in particular implies the result in the last part of the proof.

On the other hand, it is not true in general that the set of all trivial points of a genus 1 tower is finite, as shown in this example.

Example 6. The set of all trivial points of the tower $\mathbf{C}_{E,a}$, where E is an elliptic curve defined over a number field K and $a > 1$, is equal to the set of torsion points of $E(\overline{K})$ with order prime with a :

$$\mathbf{C}_{E,N}^{(\infty)}(K) = \{P \in E(\overline{K}) \mid \exists m, [m](P) = 0 \text{ and } (m, a) = 1\}.$$

Finally, let us mention that there are genus 1 towers without trivial points at all, as shown in the next example.

Example 7. Let E be an elliptic curve over a number field K . Suppose that the Galois cohomology group $H^1(K, E)$ contains a non-zero divisible element ψ , or, even less, an element divisible for all powers of a fixed prime p . Now, consider elements $\psi_n \in H^1(K, E)$ such that $p\psi_n = \psi_{n-1}$ and $\psi_0 = \psi$.

Recall that any element $\xi \in H^1(K, E)$ corresponds to a twist C_ξ of the curve E , that is, a genus 1 curve isomorphic to E over the algebraic closure of K (and, hence, with jacobian isomorphic to E over K). Moreover, the multiplication-by- m in the group $H^1(K, E)$ corresponds to a map $\phi_{m\xi}$

between C_ξ and $C_{m\xi}$ such that gives the multiplication-by- m map between the corresponding jacobians (see for example [22] for all this facts).

So we have a tower given by the curves C_{ψ_n} and the maps $\varphi_n := \phi_{p\psi_n}$. Now, the elements ψ_n have order divisible by p^n , hence have index also divisible by p^n (see proposition 5 in [22]), which implies that the curves C_{ψ_n} do not have rational points in any extension with degree $< p^n$. Hence the result.

The proof is completed by showing the existence of such elliptic curves E . In fact, showing the existence of one such E over \mathbb{Q} is sufficient. And this is known: take, for example, any elliptic curve E over \mathbb{Q} with finite number of \mathbb{Q} -rational points, which implies that the Tate-Shafarevich group is also finite (see for example theorem D in [10]).

5. Finiteness of trivial points and reduction

Now we are going to consider towers with genus ∞ , or, equivalently, towers such that there is a curve C_n with genus > 1 . In this case, and when K is a number field, the finiteness of the K -rational trivial points is clear, since, by Faltings' theorem [15], the number of points in $C_n(K)$ is finite. So we are mainly interested in the whole trivial points. Next example will show that there are towers with infinite genus and an infinite number of trivial points.

Example 8. For $n \geq 0$, let C_n be the smooth hyperelliptic curve defined over \mathbb{Q} by the hyperelliptic equation $y^2 = x^{2^n} - 1$, and consider the degree two maps φ_n defined in the affine part by $\varphi_n(x, y) = (x^2, y)$.

Now, take $\xi \in \overline{\mathbb{Q}}$ a root of unity of odd degree, so there exists an odd $N \geq 1$ such that $\xi^N = 1$. Consider the field K_ξ generated by $\sqrt{\xi^i - 1}$, for $i = 1, \dots, N - 1$; it is a finite extension of \mathbb{Q} and, clearly, $(\xi, \sqrt{\xi - 1}) \in C_0(K_\xi)$ is a K_ξ -rational trivial point of the tower.

So, the trivial points of the tower include all the points of this form, and there are an infinite number of them.

Observe that hyperelliptic curves have an infinite number of points of degree ≤ 2 , a result that generalizes to points of degree $\leq d$ for curves of gonality d .

The next question is directly related to the Question 1 on trivial points on genus 0 towers.

Question 2. For $d > 1$, are there towers with infinite genus over a number field K having an infinite number of trivial points of degree $\leq d$?

We will see in the next section that the answer of the question is no when the gonality of the tower is infinite. But before we will give a criterion for a tower to have a finite number of trivial points.

Definition. Let \mathbf{C} be a tower of curves over a number field K and a ring of integers \mathcal{O} (a Dedekind domain, not a field, and with field of fractions K). By a proper model of \mathbf{C} over \mathcal{O} we mean a collection of proper models \mathcal{C}_n of C_n and morphisms $\varphi_{n,\mathcal{O}} : \mathcal{C}_n \rightarrow \mathcal{C}_{n-1}$ such that the generic fiber is $\varphi_{n,\mathcal{O}} \otimes_{\mathcal{O}} K = \varphi_n$. We will denote by $\widetilde{\varphi_{n,\mathcal{O}}} : \mathcal{C}_{n,\mathcal{O}} \rightarrow \mathcal{C}_{n-1,\mathcal{O}}$ the reduction of the morphism modulo some nonzero prime \wp of \mathcal{O} (and we will suppress the \wp in the notation if it is clear from the context).

Observe that for any nonzero prime \wp of \mathcal{O} we have a reduction map $\text{red}_{\wp} : \mathcal{C}_n(\mathcal{O}) \rightarrow \mathcal{C}_{n,\wp}(k_{\wp})$, where k_{\wp} is the residue field \mathcal{O}/\wp . For any $P \in C_n(K) = \mathcal{C}_n(\mathcal{O})$, we have $\text{red}_{\wp}(\varphi_n(P)) = \widetilde{\varphi_n}(\text{red}_{\wp}(P))$.

Theorem 5.1. *Let \mathbf{C} be a tower of curves over a number field K such that $\Omega := \mathbf{C}(K)_n$ is finite for some $n \geq 0$. Fix a proper model of \mathbf{C} over a ring of integers \mathcal{O} of K , and suppose that for any nonzero prime \wp of \mathcal{O} outside a finite number of primes, there exists $m := m_{\wp} \geq n$ such that $C_m(k_{\wp}) = \text{red}_{\wp}(\varphi_{m,n}^{-1}(\Omega))$, where k_{\wp} is the residue field modulo \wp and red_{\wp} is the reduction map. Then Ω is the set of all trivial points $\mathbf{C}^{(\infty)}(K)_n$ of \mathbf{C} , and hence there is a finite number of them.*

Proof. Let L/K be a finite extension of K , and let \mathcal{O}_L be the ring of integers of L . We are going to show that the set of L -rational trivial points $\mathbf{C}(L)_n$ is equal to Ω . Suppose in the contrary that there is a point $P \in (\mathbf{C}(L)_n \setminus \Omega)$.

Consider a nonzero prime ideal \wp_L of \mathcal{O}_L such that there is a prime ideal \wp of K divisible by \wp_L and with equal residue fields $k_{\wp_L} = k_{\wp}$ (there are an infinite number of them). First, we show that then $\text{red}_{\wp_L}(P) \in \text{red}_{\wp}(\Omega)$. Take $m := m_{\wp}$ and $P_m \in C_m(L)$ such that $\varphi_{m,n}(P_m) = P$. By hypothesis, $\text{red}_{\wp_L}(P_m) \in \text{red}_{\wp}(\varphi_{m,n}^{-1}(\Omega))$. Hence

$$\begin{aligned} \widetilde{\varphi_{m,n}}(\text{red}_{\wp_L}(P_m)) &= \text{red}_{\wp_L}(\varphi_{m,n}(P_m)) = \\ &= \text{red}_{\wp_L}(P) \in \widetilde{\varphi_{m,n}}(\text{red}_{\wp}(\varphi_{m,n}^{-1}(\Omega))) = \text{red}_{\wp}(\Omega). \end{aligned}$$

So, we have an infinite number of primes \wp_L of \mathcal{O}_L such that $\text{red}_{\wp_L}(P) \in \text{red}_{\wp_L}(\Omega)$. Since the set Ω is finite, there should be a point $Q \in \Omega$ and an infinite number of primes \wp_L of \mathcal{O}_L such that $\text{red}_{\wp_L}(P) = \text{red}_{\wp_L}(Q)$. But, given a (proper) curve \mathcal{C} over a Dedekind domain \mathcal{O} and points $P \neq Q \in \mathcal{C}(\mathcal{O})$, the number of primes \wp of \mathcal{O} such that $\text{red}_{\wp}(P) = \text{red}_{\wp}(Q)$ is finite. Hence $P = Q$. □

We will say that a tower of curves has a model of good reduction at some nonzero prime \wp if the models \mathcal{C}_n of C_n have good reduction at \wp (i.e. $\mathcal{C}_{n,\wp}$ are smooth and projective curves). In this case the curves $\mathcal{C}_{n,\wp}$ together with the maps $\widetilde{\varphi_{n,\wp}}$ form a tower of curves over k_{\wp} .

Corollary 5.2. *Suppose that the tower \mathbf{C} has a model with good reduction outside a finite number of primes S of \mathcal{O} . For any prime \wp of good reduction*

of \mathbf{C} , consider the tower of curves $\mathbf{C}_\varphi = (\{\mathbf{C}_{n,\varphi}\}, \{\widetilde{\varphi_{n,\varphi}}\})$, reduction modulo φ of the model. Suppose that there exists n such that $\mathbf{C}(K)_n$ is finite and for any prime φ outside a finite set containing S , $\text{red}_\varphi(\mathbf{C}(K)_n) = \mathbf{C}_\varphi(k_\varphi)_n$. Then $\mathbf{C}^{(\infty)}(K)_n = \mathbf{C}(K)_n$.

5.1. An example related to torsion points on abelian varieties.

Let K be a number field and U/k a smooth geometrically connected algebraic curve over K . Let $\mathcal{A} \rightarrow U$ be an abelian scheme of dimension $g \geq 1$, defined over K . Given a prime number p and a $n \geq 1$, consider the étale cover $\mathcal{A}[p^n] \rightarrow U$ over U . Let U_n be a connected component of $\mathcal{A}[p^n]$, such that the multiplication-by- p maps $\mathcal{A}[p^n] \rightarrow \mathcal{A}[p^{n-1}]$ give maps $\phi_n : U_n \rightarrow U_{n-1}$ for all $n \geq 2$ in a compatible way. Suppose moreover that $U_n(S) \subset \mathcal{A}[p^n](S)$ consists of points of order exactly p^n , for any S scheme over U_n ; in particular, U_n is not the image of the zero section.

Let C_n be the smooth projective curve associated to U_n , and let $\varphi_n : C_n \rightarrow C_{n-1}$ be the natural maps. Since the U_n are smooth over U , the points $U_n(L)$ can be seen inside $C_n(L)$, for any extension L/K . The points in $U_n(L)$ classify fibers \mathcal{A}_s of the family $\mathcal{A} \rightarrow U$ at the point $s := \text{Spec}(L)$, which is an abelian variety over L , together with a point $P \in \mathcal{A}_s(L)$ of order exactly p^n .

Although the curves C_n are connected, it could happen that they are not geometrically connected; however, they are geometrically connected if $C_n(K) \neq \emptyset$. In any case, we can construct the tower of (not necessarily geometrically connected) curves $\mathbf{C} = (\{C_n\}_{n \geq 0}, \{\varphi_n\}_{n \geq 1})$.

Using that the torsion subgroup of an abelian variety is finite, one can see that the trivial points $\mathbf{C}^{(\infty)}(K)_n$ at level n are contained in $C_n(\overline{K}) \setminus U_n(\overline{K})$, which is well known to be finite.

This result can be shown by observing that the points $P \in U_n(L)$ correspond to a special fiber \mathcal{A}_s , which is an abelian variety over L , together with a point $Q \in \mathcal{A}_s(L)$ of order exactly p^n . This point P is a trivial point if and only if for all $m \geq 1$, there exists a point $Q_m \in \mathcal{A}_s(L)$ such that $[p^m]Q_m = Q$; thus, Q_m has exact order p^{n+m} . Since the cardinal of the group of torsion points of an abelian variety over a number field is finite (a fact that can be proved by reducing modulo some primes ℓ), there is no such a Q_M for $m \gg 1$. So there is no trivial point inside U_n .

Another way to show this result is by reducing modulo some prime φ of K , such that the map $\mathcal{A} \rightarrow U$ has good reduction, and does not divide p (all primes except a finite number of them verify these conditions). Then the tower U_n has good reduction at such a prime. The assertion is deduced from the fact that the cardinal of the group of (torsion) points of an abelian variety over a finite field is finite, which is trivial, and then applying the Corollary 5.2 (observe that the corollary is still valid if the curves in the tower are not necessarily geometrically connected).

6. Genus ∞ Towers, trivial points and gonality

Recall that the gonality $\gamma_K(C)$ of a curve C over a field K is the minimum m such that there exists a morphism $\phi : C \rightarrow \mathbb{P}^1$ of degree m defined over K . In the next proposition we recall some properties of the gonality (see [29] for the proofs).

Proposition 6.1. *Let K be any field, and let C be an smooth and projective curve with genus $g > 1$ and gonality $\gamma_K(C)$. Then*

- (1) $\gamma_K(C) \leq 2g - 2$.
- (2) If $C(K) \neq \emptyset$, then $\gamma_K(C) \leq g$.
- (3) If $K = \bar{K}$ is algebraically closed, then $\gamma_K(C) \leq \lfloor \frac{g+3}{2} \rfloor$.
- (4) If L/K is a field extension, then $\gamma_K(C) \geq \gamma_L(C)$.
- (5) If K is a perfect field, L/K is an algebraic field extension, $\gamma_L(C) > 2$ and $C(K) \neq \emptyset$ then $\gamma_K(C) \leq (\gamma_L(C) - 1)^2$.
- (6) If $f : C \rightarrow C'$ is a non-constant K -morphism then $\gamma_K(C) \leq \deg(f)\gamma_K(C')$ and $\gamma_K(C') \leq \gamma_K(C)$.

The main tool we will use to relate the gonality with the finiteness of trivial points is the following criterion of Frey [17], proved also by Abramovich in his thesis, which is an application of the main result of Faltings in [16].

Theorem 6.2 (Frey). *Let C a curve over a number field K , with gonality $\gamma > 2$ over K , and such that $C(K) \neq \emptyset$. Fix an algebraic closure \bar{K} of K and consider the points of degree d of C ,*

$$C^{(d)}(K) := \bigcup_{[L:K] \leq d} C(L) \subset C(\bar{K})$$

where the union is over all the finite extensions of K inside \bar{K} of degree $\leq d$. Suppose that $2d < \gamma$. Then $C^{(d)}(K)$ is finite.

Using this criterion we can show the following result.

Theorem 6.3. *Let $\mathbf{C}(\{C_n\}_{n \geq 0}, \{\varphi_n\}_{n \geq 1})$ be a tower with infinite gonality. Then, for all $d \geq 1$ and $n \geq 0$, the set of K -trivial points of \mathbf{C} in the level $n \geq 0$ and degree d is finite.*

Moreover, for all $d \geq 1$ there exists a constant n_d (depending on the tower \mathbf{C}) such that, for any extension L/K of degree $\leq d$, and for any $n \geq n_d$, $C_n(L) \subset \mathbf{C}^{(d)}(K)_n$.

Proof. First of all, we show that we can suppose $\mathbf{C}(K)_n \neq \emptyset$ for all $n \geq 0$. Suppose $\mathbf{C}^\infty(K)_m \neq \emptyset$, otherwise the result is clear. Let d be the minimum integer such that $\mathbf{C}^{(d)}(K)_m \neq \emptyset$ for some $m \geq 0$ (and hence for all m , see Lemma 2.2). This implies that there exists an extension L/K of degree d such that $\mathbf{C}(L)_m \neq \emptyset$. But $\mathbf{C}^{(e)}(K)_m \subset \mathbf{C}^{(e)}(L)_m$ for any $e \geq 1$. If $P \in \mathbf{C}^{(e)}(K)_m$, then $P \in \mathbf{C}(M)_m$ for some extension M/K of degree e ,

hence $P \in \mathbf{C}(M')_m$ for M'/M the compositum of M and L , which is an extension of L degree $e' \leq e$. Thus $P \in \mathbf{C}^{(e')}(L)_m \subset \mathbf{C}^{(e)}(L)_m$.

Hence, consider a tower \mathbf{C} of infinite gonality with $\mathbf{C}(K)_n \neq \emptyset$. In order to show $\mathbf{C}^{(d)}(K)_n$ is finite for all $d \geq 1$ and all $n \geq 0$, we can do it for some $n \gg 1$ (in terms of d). Just take n such the gonality of C_n is bigger than $2d$. Since $\emptyset \neq \mathbf{C}(K)_n \subset C_n(K)$, we can apply Frey's Theorem 6.2 to conclude that $C_n^{(d)}(K) \supseteq \mathbf{C}^{(d)}(K)_n$ is finite.

Moreover, continuing with the same hypothesis, since $C_n^{(d)}(K) \setminus \mathbf{C}^{(d)}(K)_n$ is finite, there are a finite number of extensions L/K of degree $\leq d$ such that any point P in $C_n^{(d)}(K) \setminus \mathbf{C}^{(d)}(K)_n$ comes from a point in $C_n(L)$. Since $P \notin \mathbf{C}^{(d)}(K)_n$, there is an integer $n_P \geq n$ such that $P \notin \varphi_{n_P, n}(C_{n_P}(L))$. By considering the maximum n_d of all the integers n_P for $P \in C_n^{(d)}(K) \setminus \mathbf{C}^{(d)}(K)_n$, we get that for all $m \geq n_d$, $C_m^{(d)}(K) = \mathbf{C}^{(d)}(K)_m$, which implies the last claim in the theorem. \square

Corollary 6.4. *If the set $\mathbf{C}^{(\infty)}(K)_m$ is finite for some m , and $\gamma(\mathbf{C}) = \infty$, then for all $d \geq 1$ there exists a constant n_d (depending on the tower \mathbf{C}), such that for any extension L/K of degree $\leq d$ and for any $n \geq n_d$, $C_n(L) \subset \mathbf{C}^{(\infty)}(K)_n$.*

We do not know, however, if all towers with infinite gonality have a finite number of trivial points.

Question 3. Are there towers with infinite gonality over a number field K having an infinite number of trivial points?

7. Gonality in the complete intersection case

Definition. For any $n \geq 1$, let $f_n(X_0, X_1, \dots, X_{n+1})$ be a homogeneous polynomial of degree $d_n > 1$. Consider the curves $C_{n-1} \subset \mathbb{P}^{n+1}$ defined as the zero set of the polynomials f_1, f_2, \dots, f_n . We have a natural map $\varphi_n : C_n \rightarrow C_{n-1}$ given by forgetting the last coordinate: $\varphi_n([x_0 : x_1 : \dots : x_{n+2}]) = [x_0 : x_1 : \dots : x_{n+1}]$. If the polynomials f_n are sufficiently general, then the curves C_n are smooth and complete intersection, and we get a tower of curves. We call these type of towers complete intersection towers.

The main result of this section is that the complete intersection towers have infinite gonality. The main tool is the following theorem by Lazarsfeld (see Exercise 4.12. in [23]), which is a generalization of the well-known fact that a planar curve (so given by an smooth projective model inside \mathbb{P}^2) has gonality larger or equal to the degree of the model minus 1 (and with equality exactly if the curve has a rational point).

Theorem 7.1 (Lazarsfeld). *Let $C \subset \mathbb{P}^n$ be a smooth complete intersection of hypersurfaces of degrees $2 \leq a_1 \leq a_2 \leq \dots \leq a_{r-1}$ over \mathbb{C} . Then $\gamma(C) \geq (a_1 - 1)a_2 \cdots a_{r-1}$.*

Corollary 7.2. *Any complete intersection tower of curves has infinite gonality over any characteristic zero field.*

Proof. Let $a := \min d_n$ and let $n_0 \geq 0$ be such that $d_{n_0} = a$. By the previous theorem, the gonality of the curves C_{n-1} for $n \geq n_0$ is bounded below by

$$\gamma(C_{n-1}) \geq \left(1 - \frac{1}{a}\right) \left(\prod_{i=1}^n d_n\right),$$

hence its limit goes to infinite. □

Observe that, if the degree d_1 is the minimum of all the d_n , and $C_0(K) \neq \emptyset$, then the gonality of C_n over K is in fact equal to $(d_1 - 1) (\prod_{i=2}^n d_n)$, since the map $\varphi_{n,1} : C_n \rightarrow C_0$ has degree $(\prod_{i=2}^n d_n)$, which composed with the map of degree $d_1 - 1$ from C_0 to \mathbb{P}^1 given by the rational point has the desired degree.

Example 9. Fix an homogeneous irreducible polynomial $f(X_0, X_1, X_2)$ of degree $d > 1$ and defined over a number field. Suppose that the curve projective $C_0 \subset \mathbb{P}^2$ defined as the zero set of the polynomials f is non singular and geometrically connected. Consider now the complete intersection tower \mathbf{C}_f of curves $C_{n-1} \subset \mathbb{P}^{n+1}$ defined as the zero set of the polynomials $f_1 := f, f_2 := f(X_1, X_2, X_3), \dots, f_n := f(X_{n-2}, X_{n-1}, X_n)$. Then the curve C_n has gonality $\geq d^n - d^{n-1}$, so the tower has infinite gonality, with equality exactly when $C_0(K) \neq \emptyset$.

Hence, if K is a number field, and by Corollary 6.3, we get that the curves C_n have only the trivial points over a finite extension L/K for n large enough, depending only on the tower and the degree $[L : K]$.

And, in case we know the set of trivial points is finite and computable (for example, by theorem 5.1), we get that the points of the curves C_n over a finite extension L/K for n large enough, depending only on \mathbf{C} and the degree $[L : K]$, by Corollary 6.4.

One can also use the theorem for other type of towers of curves, a generalization of the p^n Fermat tower.

Example 10. Fix an homogeneous irreducible polynomial $f_0(X_0, X_1, X_2)$ of degree $d > 1$ and defined over a number field, and a progression $\{a_n\}_{n \geq 1}$ of integers $a_n \geq 2$. Suppose that the curve projective $C_0 \subset \mathbb{P}^2$ defined as the zero set of the polynomials f_0 is non singular and geometrically connected. Consider now the complete intersection tower \mathbf{C} of curves $C_n \subset \mathbb{P}^2$ defined as the zero set of the polynomial $f_n := f_{n-1}(X_0^{a_n}, X_1^{a_n}, X_2^{a_n})$, and the maps φ_n given by $\varphi_n(X_0, X_1, X_2) = [X_0^{a_n} : X_1^{a_n} : X_2^{a_n}]$. Then the curves C_n are planar curves of degree $da_1a_2 \cdots a_n$, and hence with gonality $\gamma(C_n) \geq da_1a_2 \cdots a_n - 1 \geq 2^n - 1$.

8. Gonality and reduction

The following proposition was shown in [32], proposition 5, and it will allow us to bound by below the gonality by just counting points “modulo p ”.

Proposition 8.1. *Let C be a curve over a number field, and let \wp be a prime of good reduction of the curve, with residue field k_\wp . Denote by C' the reduction of the curve C modulo \wp . Then the gonality $\gamma(C)$ of C satisfies that*

$$\gamma(C_K) \geq \gamma(C'_{k_\wp}) \geq \frac{\#C'(k_\wp)}{\#k_\wp + 1}.$$

Observe that the proposition has two parts: first, that the gonality does not increase under reduction modulo a prime. Second, that the gonality over a finite field is bounded below by the number of points.

Definition. Let K be a number field and let \mathbf{C} be a tower of curves over K . We will say that a prime \wp of the ring of integers \mathcal{O} of K is a prime of good reduction of the tower if there exists a proper model of \mathbf{C} over $\mathcal{O}_{(\wp)}$, the localization of \mathcal{O} at \wp , such that $\mathcal{C}_{n,\wp}$ are smooth and projective curves, and the maps $\widetilde{\varphi_{n,\wp}}$ are non constant.

Corollary 8.2. *Let $\mathbf{C} = (\{C_n\}_{n \geq 0}, \{\varphi_n\}_{n \geq 1})$ be a tower of curves over a number field K . Suppose that there exists a prime \wp of good reduction of the tower, and suppose that*

$$\lim_{n \rightarrow \infty} \#\mathcal{C}_{n,\wp}(k_\wp) = +\infty.$$

Then the tower \mathbf{C} has infinite gonality.

Proof. Using the Proposition 8.1 one gets that

$$\gamma(C_n) \geq \gamma(\mathcal{C}_{n,\wp}) \geq \frac{\#\mathcal{C}_{n,\wp}(k_\wp)}{\#k_\wp + 1},$$

hence the result. □

9. Gonality and Cayley-Schreier graphs

In this section we are going to follow the ideas originating in the work of Zograf [33] and Abramovich [1], and developed in a recent paper of Ellenberg, Hall and Kowalski [14]. The idea is to show that certain étale towers of (possibly affine) curves have infinite gonality if the associated Cayley-Schreier graphs form an expanding family (or, more generally, verify some growing condition in the first non-trivial eigenvalue of the combinatorial laplacian operator).

Suppose that we have a tower of curves \mathbf{C} defined over a number field such that the maps $\varphi_{n,0}$ are étale (i.e. non-ramified) outside a fixed Zarisky closed set Z . So, we have open subsets $U_i = C_i \setminus Z$ of C_i , together with

maps $\varphi_n : U_n \rightarrow U_{n-1}$, which are étale, and the original tower \mathbf{C} is obtained projectivizing the curves U_i (the case $U_i = C_i$ is also considered).

Fix, for all $i \geq 0$, a point x_i in $U_i(\bar{K})$ such that $\varphi_i(x_i) = x_{i-1}$, and a generating set S of the topological fundamental group $G := \pi_1(U_{0\mathbb{C}}, x_0)$. Consider the Cayley-Schreier graphs $\Gamma_i = C(N_i, S)$ associated to the finite quotient sets

$$N_i := G/H_i = \pi_1(U_{0\mathbb{C}}, x_0)/\pi_1(U_{i\mathbb{C}}, x_i).$$

Recall that the graphs $\Gamma_i = C(G/H_i, S)$ have vertex set $V(\Gamma_i) = G/H_i$, and with (possibly multiple) edges from vertex xH_i to vertex sxH_i for all $s \in S$; hence, they are r -regular graphs for $r = |S|$.

Define the combinatorial Laplacian operator of a r -regular graph Γ as $rId - A(\Gamma)$, where $A(\Gamma)$ is the adjacency matrix of Γ . We compute the eigenvalues of Γ , which are positive real numbers, and let $\lambda_1(G)$ to be the smallest non-zero of them.

Observe that there are maps of graphs $\Gamma_i \rightarrow \Gamma_{i-1}$ for all $i \geq 1$, and that such maps are unramified: the preimage of any vertex is formed always by k vertices, where k , the degree of the map, is fixed.

Definition. A tower of graphs is a couple $(\{\Gamma_i\}, \{\phi_i\})$ where Γ_i are graphs for any $i \geq 0$ and $\phi_i : \Gamma_i \rightarrow \Gamma_{i-1}$ are surjective maps of graphs. We say that the tower is unramified if all the maps ϕ_i for $i \geq 1$ are unramified.

Following ideas from the paper [14], we will bound the gonality of the curves C_i by imposing some condition on the first non-zero eigenvalue $\lambda_1(\Gamma_i)$ of the combinatorial laplacian operator on Γ_i .

Theorem 9.1. *Let $\mathbf{C} = (\{C_n\}, \{\varphi_n\})$ be a tower of curves defined over \mathbb{C} such that the maps $\varphi_{n,0}$ are étale outside a fixed Zarisky closed set Z , and with the genus $g(C_0) > 1$. Consider the open subsets $U_i = C_i \setminus Z$ of C_i , together with maps $\varphi_n : U_n \rightarrow U_{n-1}$ and points x_i in $U_i(\bar{K})$ such that $\varphi_i(x_i) = x_{i-1}$. Let $\{\Gamma_i, \phi_i\}$ be the unramified tower of Cayley-Schreier graphs $C(\pi_1(U_{0\mathbb{C}}, x_0)/\pi_1(U_{i\mathbb{C}}, x_i), S)$. Suppose that $\lim_{i \rightarrow \infty} \lambda_1(\Gamma_i)|V(\Gamma_i)| = \infty$. Then $\lim_{i \rightarrow \infty} \gamma(C_i) = \infty$.*

Proof. First of all, observe that, by the Hurwitz’s formula

$$g(C_i) - 1 \geq \deg(\varphi_{i,0})(g(C_0) - 1) \geq \deg(\varphi_{i,0})$$

(where we have equality exactly if $\phi_{i,0}$ are unramified). Now, the degree of $\varphi_{i,0}$ is exactly equal to the index of $\pi_1(U_{i\mathbb{C}}, x_i)$ inside $\pi_1(U_{0\mathbb{C}}, x_0)$, which is equal to the number of vertices of Γ_i . So we get that $g(C_i) - 1 \geq |V(\Gamma_i)|$.

Now, we will find a formula relating the $\lambda_1(\Gamma_i)$ to the gonality of C_i and $g(C_i)$. We will follow the proof of Theorem 8 (b) in [14], and we will only sketch the proof. Since the genus of C_i is > 1 for all i , we can write U_i as $G_i \setminus \mathbb{H}$ for some discrete subgroup of $PSL_2(\mathbb{R})$. The hyperbolic area $\mu_i(U_i)$

is then finite and the Poincaré metric induces a Laplacian operator on the L^2 -space. Following Li and Yau [24], and Abramovich [1], one has that

$$\gamma(C_i) \geq \frac{1}{8\pi} \lambda_1(U_i) \mu(U_i)$$

where $\lambda_1(U_i)$ is the first non-trivial eigenvalue of the laplacian operator $-div(grad)$.

Now, using the Gauss-Bonnet theorem, one gets

$$\mu(U_i) = -2\pi\chi(U_i) \geq -2\pi\chi(C_i) = -4\pi(1 - g(C_i)).$$

Using the comparison principle of Brooks [7] and Burger [8], one gets that there exists a constant $c > 0$, depending only on U_0 and on S , such that

$$\lambda_1(U_i) \geq c\lambda_1(\Gamma_i).$$

Hence, combining all the results, that

$$\gamma(U_i) \geq 2c\lambda_1(\Gamma_i)(g(C_i) - 1) \geq 2c\lambda_1(\Gamma_i)|V(\Gamma_i)|$$

and hence the result. □

We say that a family of graphs is an expander if $\lim_{i \rightarrow \infty} |\Gamma_i| = \infty$ and $\lambda_1(\Gamma_i) \geq c$ for some constant c . We will say that it is esperantist if there exists some constant $A \geq 0$ such that

$$\lambda_1(\Gamma_i) \geq \frac{c}{(\log(2|\Gamma_i|))^A}.$$

Observe that, if our family (in fact, tower) of Cayley-Schreier graphs $\{\Gamma_i\}$ is an expander (or it is esperantist), then they verify a fortiori the hypothesis of the theorem. Hence, the following constructions give towers of curves \mathbf{C} defined over a number field K with infinite gonality. Consider U_0 a smooth geometrically connected algebraic curve over a number field K , and suppose we have an epimorphism of groups $p : \pi_1(U_0(\mathbb{C}), x_0) \rightarrow G$, where the group G is one of the cases below. Take finite-index subgroups H_n of G such that $H_n \subsetneq H_{n-1}$ and $H_0 = G$, and consider the étale coverings $U_n \rightarrow U_0$ associated to the subgroups $p^{-1}(H_n)$. Finally, consider the projectivizations and desingularizations C_n of these curves U_n .

- (1) If G is a finite-index subgroup in $\mathbf{G}(\mathbb{Q}) \cap \mathrm{GL}_m(\mathbb{Z})$, where $\mathbf{G} \subset \mathrm{GL}_m$ is a semisimple algebraic subgroup, defined over \mathbb{Q} , and G has real rank at least 2 (for example, G can be a finite-index subgroup of $\mathrm{SL}_n(\mathbb{Z})$, $n > 3$, or of $\mathrm{Sp}_{2g}(\mathbb{Z})$, $g > 2$) and S is an arbitrary finite set of generators of G , and H_n arbitrary normal subgroups (by property (T) of Kazhdan, see [4]).
- (2) If G is a subgroup of $\mathrm{SL}_n(\mathbb{Z})$ which is Zarisky-dense in SL_d , for $d > 1$, S is an arbitrary finite set of generators of G , p is a prime number sufficiently large (depending on G) and $H_n = p^n \mathrm{SL}_d(\mathbb{Z})$, so $G/H_n \cong \mathrm{SL}_n(\mathbb{Z}/p^n\mathbb{Z})$, by [5] and [6].

- (3) If G is any Zarisky dense subgroup of \mathbf{G}/\mathbb{Z}_p , an arbitrary split semisimple algebraic group, and we consider the tower of Cayley graphs of $\mathbf{G}(\mathbb{Z}/p^n\mathbb{Z})$ with respect to any symmetric set of generators, by the results of Dinai [12],[13] concerning the diameter of this graphs: the diameter is less than $c \log(|\mathbf{G}(\mathbb{Z}/p^n\mathbb{Z})|)^d$, for some constants c and d .

To show some of these cases, one needs to know that there is a relation between the first non-trivial eigenvalue of the combinatorial laplacian operator and the diameter (longest shortest path between any to pair of vertices) for any (regular) graph Γ . For example, Diaconis and Saloff-Coste [11] showed that

$$\lambda_1(C(G, S)) \geq \frac{1}{|S|\text{diam}(C(G, S))^2},$$

if $C(G, S)$ is a Cayley Graph associated to a finite group G with symmetric set of generators S . Hence, if e have normal subgroups $H_i \trianglelefteq G$ inside a group G , with $H_i \subseteq H_{i-1}$, the hypothesis of the theorem is verified if

$$\lim_{i \rightarrow \infty} \frac{|G/H_i|}{\text{diam}(C(G/H_i, S))^2} = +\infty$$

On the other hand, it is easy to construct towers of curves not verifying the growing condition on the first non-trivial eigenvalue of the combinatorial laplacian operator (and having bounded gonality), as in the following trivial example.

Example 11. Consider the tower of curves \mathbf{C}_{x^2} , so with $C_n = \mathbb{P}^1$ and maps given by $\varphi_n(x) = x^2$. Of course this tower has no infinite gonality. These maps φ_n are unramified outside $x = 0$ and ∞ , so they give unramified selfmaps of $U_i = \mathbb{G}_m = \mathbb{P}^1 \setminus \{0, \infty\}$. Choose, for example, $x_n := 1 \in C_n(\mathbb{Q})$. Then one has that $\pi_1(U_{i\mathbb{C}}, x_i) \cong \mathbb{Z}$, and for the set $S := \{1, -1\}$, we get that the Cayley-Schreier graphs

$$C(\pi_1(U_{0\mathbb{C}}, x_0)/\pi_1(U_{i\mathbb{C}}, x_i), S) = C(\mathbb{Z}/2^n\mathbb{Z}, \{\pm 1\}) = \Gamma_{2^n}$$

where Γ_n denotes the cycle graph form by a cycle with n vertices and n edges. It is well known that the eigenvalues of the combinatorial laplacian operator for these cycle graphs are $\lambda_k(\Gamma_n) := 2 - 2 \cos(2k\pi/n)$ for $k = 0, \dots, n - 1$. Hence,

$$\lim_{i \rightarrow \infty} \lambda_1(\Gamma_{2^i})|V(\Gamma_{2^i})| = \lim_{i \rightarrow \infty} 2^i(2 - 2 \cos\left(\frac{\pi}{2^{i-1}}\right)) = 0.$$

Finally, we would like to mention that there is another completely different relation of the gonality with graph theory, developed by Baker and Norine [3] and specially by Baker in [2]. Suppose K is a field complete with respect to a discrete valuation, and let C be a curve over K having a regular

semistable model over the ring of integers of K . Consider Γ the dual graph of the reduction of X , where the vertexes are the irreducible components, and the edges correspond to the intersection points. Then, there is a notion of gonality for a finite graph and the gonality of C is bounded below by the gonality of Γ (see Corollary 3.2 in [2]). Using this result it is not difficult to construct towers of (Mumford) curves over \mathbb{Q}_p having infinite gonality. All these results are also related to tropicalizations of algebraic curves, and how to bound the gonality from the tropicalization.

References

- [1] ABRAMOVICH, D., *A linear lower bound on the gonality of modular curves*, International Math. Res. Notices **20** (1996), 1005–1011.
- [2] BAKER, M., *Specialization of Linear Systems from Curves to Graphs*, Algebra and Number Theory **2**, no. 6 (2008), 613–653.
- [3] BAKER, M., NORINE, S., *Riemann-Roch and Abel-Jacobi Theory on a Finite Graph*, Advances in Mathematics, **215** (2007), 766–788.
- [4] BEKKA, B., DE LA HARPE, P., VALETTE, A., *Kazhdan's property (T)*, New Mathematical Monographs, 11, Cambridge University Press, 2008.
- [5] BOURGAIN, J., GAMBURD, A. *Expansion and random walks in $SL_d(\mathbb{Z}/p^n\mathbb{Z})$: I*, J. Eur. Math. Soc. **10**, (2008), 987–1011.
- [6] BOURGAIN, J., GAMBURD, A. *Expansion and random walks in $SL_d(\mathbb{Z}/p^n\mathbb{Z})$: II*, J. Eur. Math. Soc. **11**, 1057–1103 (2009)
- [7] BROOKS, R., *On the angles between certain arithmetically defined subspaces of \mathbb{C}^n* , Annales Inst. Fourier **37** (1987), 175–185.
- [8] BURGER, M., *Estimations de petites valeurs propres du laplacien d'un revêtement de variétés riemanniennes compactes*, C.R. Acad. Sc. Paris **302** (1986), 191–194.
- [9] CADORET, A., TAMAGAWA, A., *Uniform boundedness of p -primary torsion of abelian schemes*, Invent. Math., **188** (2012), 83–125.
- [10] ÇIPERIANI, M., STIX, J., *Weil-Châtelet divisible elements in Tate-Shafarevich groups*, arXiv:1106.4255.
- [11] DIACONIS, P., SALOFF-COSTE, L., *Comparison Techniques for Random Walk on Finite Groups*, Ann. Probab. **21**, no. 4 (1993), 2131–2156.
- [12] DINAI, O., *Poly-log diameter bounds for some families of finite groups*, Proc. Amer. Math. Soc. **134** (2006), 3137–3142.
- [13] DINAI, O. *Diameters of Chevalley groups over local rings*, arXiv:1201.4686.
- [14] ELLENBERG, J., HALL, C., KOWALSKI, E., *Expander graphs, gonality and variation of Galois representations*, Duke Math. J. **161**, no. 4 (2012), 1233–1275.
- [15] FALTINGS, G., *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. math. **73** (1983), 349–366.
- [16] FALTINGS, G., *Diophantine approximation on abelian varieties*, Annals of Math. **133** (1991), 549–576.
- [17] FREY, G., *Curves with infinitely many points of fixed degree*, Israel J. Math. **85** (1994), no. 1-3, 79–83.
- [18] FRIED, M. D., *Introduction to modular towers: generalizing dihedral group-modular curve connections*, in Recent developments in the inverse Galois problem (Seattle, WA, 1993), 111–171, Contemp. Math., 186, Amer. Math. Soc., Providence, RI, 1995.
- [19] GONZÁLEZ-JIMÉNEZ, E., XARLES, X., *On symmetric square values of quadratic polynomials*, Acta Arithmetica **149**, 145–159 (2011).
- [20] GONZÁLEZ-JIMÉNEZ, E., XARLES, X., *Five squares in arithmetic progression over quadratic fields*, to appear in Rev. Mat. Iberoamericana.
- [21] HINDRI, M., SILVERMAN, J.H., *Diophantine Geometry, An introduction*. Graduate Texts in Mathematics 201. Springer-Verlag, New York, 2000.

- [22] LANG, S., TATE, J., *Principal homogeneous spaces over abelian varieties*, Amer. J. Math. **80**, (1958), 659–684.
- [23] LAZARUSFELD, R., *Lectures on Linear Series, With the assistance of Guillermo Fernández del Busto*. IAS/Park City Math. Ser., 3, Complex algebraic geometry (Park City, UT, 1993), 161–219, Amer. Math. Soc., Providence, RI, 1997.
- [24] LI, P. AND YAU, S.T., *A new conformal invariant and its applications to the Willmore conjecture and the first eigenvalue of compact surfaces* Invent. math. **69** (1982), 269–291.
- [25] LUBOTZKY, A., *Discrete groups, expanding graphs and invariant measures*, Progress in Math. 125, Birkhäuser 1994.
- [26] MANIN, Y., *A uniform bound for p -torsion in elliptic curves*, Izv. Akad. Nauk. CCCP **33**, (1969), 459–465.
- [27] MEREL, L., *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, Invent. Math. **124** (1996), no. 1–3, 437–449.
- [28] MOHAR, B., *Eigenvalues, diameter, and mean distance in graphs*, Graphs Combin. **7** (1991) 53–64.
- [29] POONEN, B. *Gonality of modular curves in characteristic p* , Math. Res. Lett. **14** (2007), no. 4, 691–701.
- [30] SILVERMAN, J.H., *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics 106, Springer-Verlag, 1986.
- [31] SILVERMAN, J.H., *The Arithmetic of Dynamical Systems*, Graduate Texts in Mathematics 241, Springer-Verlag, 2007.
- [32] XARLES, X. *Squares in arithmetic progression over number fields*, J. Number Theory **132** (2012) 379–389.
- [33] ZOGRAF, P. *Small eigenvalues of automorphic Laplacians in spaces of cusp forms*, Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov (LOMI) **134** (1984), 157–168; translation in Journal of Math. Sciences **36**, Number 1, 106–114.

Xavier XARLES
Departament de Matemàtiques
Universitat Autònoma de Barcelona
08193 Bellaterra, Barcelona, Spain
E-mail: xarles@mat.uab.cat