C. R. Acad. Sci. Paris, Ser. I 356 (2018) 911–915

Contents lists available at ScienceDirect

C. R. Acad. Sci. Paris, Ser. I

www.sciencedirect.com

Number theory

ABC and the Hasse principle for quadratic twists of hyperelliptic curves

ABC et le principe de Hasse pour les tordues de courbes hyperelliptiques

Pete L. Clark, Lori D. Watson

Department of Mathematics, University of Georgia, Athens, GA 30606, United States

ARTICLE INFO

Article history:
Received 8 May 2018
Accepted after revision 13 July 2018
Available online 3 August 2018

Presented by the Editorial Board

ABSTRACT

Conditionally on the ABC conjecture, we apply work of Granville to show that a hyperelliptic curve $C_{/\mathbb{Q}}$ of genus at least three has infinitely many quadratic twists that violate the Hasse Principle iff it has no $\mathbb{Q}$-rational hyperelliptic branch points.

RÉSUMÉ

En supposant la conjecture ABC, nous utilisons un travail de Granville pour montrer qu'une courbe hyperelliptique $C_{/\mathbb{Q}}$ de genre au moins trois a une infinité de tordues quadratiques, qui violent le principe de Hasse si et seulement si elle n'a pas de point de branchement hyperelliptique rationnel sur $\mathbb{Q}$.

1. Introduction

Let $C_{/\mathbb{Q}}$ be an algebraic curve. (All our curves will be *nice*: smooth, projective and geometrically integral.) An involution ι on C is an order 2 automorphism of $C_{/\mathbb{Q}}$. For any quadratic field $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$, there is a curve $\mathcal{T}_d(C,\iota)_{/\mathbb{Q}}$, the quadratic twist of C by ι and $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$. After extension to $\mathbb{Q}(\sqrt{d})$, the curve $\mathcal{T}_d(C,\iota)$ is canonically isomorphic to $C_{/\mathbb{Q}(\sqrt{d})}$, but the $\mathrm{Aut}(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) = \langle\sigma_d\rangle$ action on $C(\mathbb{Q}(\sqrt{d}))$ is "twisted by ι", meaning that $\sigma_d : P \in C(\mathbb{Q}(\sqrt{d})) \mapsto \iota(\sigma_d(P))$. Thus, we have:

$$\mathcal{T}_d(C,\iota)(\mathbb{Q}) = \{P \in C(\mathbb{Q}(\sqrt{d})) \mid \iota(P) = \sigma_d(P)\}.$$

If $d \in \mathbb{Q}^{\times 2}$, we put $\mathcal{T}_d(C,\iota) = C$, the "trivial quadratic twist."

Let $q : C \to C/\iota$ be the quotient map. Every $\mathbb{Q}$-rational point on $\mathcal{T}_d(C,\iota)$ maps via q to a $\mathbb{Q}$-rational point on C/ι. Let $\overline{P} \in (C/\iota)(\mathbb{Q})$. If $\overline{P}$ a branch point of ι, the unique point $P \in C(\mathbb{Q})$ such that $q(P) = \overline{P}$ is also rational on every quadratic twist. If $\overline{P}$ is not a branch point of ι, there is a unique $d \in \mathbb{Q}^{\times}/\mathbb{Q}^{\times 2}$ such that the fiber of $q : \mathcal{T}_d(C,\iota) \to C/\iota$ consists of two $\mathbb{Q}$-rational points.

E-mail addresses: plclark@gmail.com (P.L. Clark), watson@math.uga.edu (L.D. Watson).

https://doi.org/10.1016/j.crma.2018.07.007
1631-073X/

Work of Clark and Clark–Stankewicz [2], [3], [4] gives criteria on C and ι for there to be infinitely many $d \in \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ such that $\mathcal{T}_d(C,\iota)_{/\mathbb{Q}}$ violates the Hasse Principle: letting $\mathbf{A}_\mathbb{Q}$ be the adele ring over $\mathbb{Q}$, this means $\mathcal{T}_d(C,\iota)(\mathbf{A}_\mathbb{Q}) \neq \varnothing$ but $\mathcal{T}_d(C,\iota)(\mathbb{Q}) = \varnothing$. Here is one version.

Theorem 1. *[4, Thm. 2] Let $C_{/\mathbb{Q}}$ be a nice curve, and let ι be an involution on C. Suppose:*
(T1) the involution ι has no $\mathbb{Q}$-rational branch points;
(T2) the involution ι has at least one geometric branch point: $\{P \in C(\overline{\mathbb{Q}}) \mid \iota(P) = P\} \neq \varnothing$;
(T3) For some $d \in \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ we have $\mathcal{T}_d(C,\iota)(\mathbf{A}_\mathbb{Q}) \neq \varnothing$;
(T4) The set $(C/\iota)(\mathbb{Q})$ is finite.
Then, as $X \to \infty$, the number of squarefree d with $|d| \leq X$ such that $\mathcal{T}_d(C,\iota)_{/\mathbb{Q}}$ violates the Hasse Principle is $\gg_C \frac{X}{\log X}$.

An involution ι on a curve $C_{/\mathbb{Q}}$ is hyperelliptic if $C/\iota \cong \mathbb{P}^1$. A hyperelliptic curve is a pair (C,ι) with ι a hyperelliptic involution on C. (A curve of genus at least two admits at most one hyperelliptic involution.) A hyperelliptic curve (C,ι) of genus g has an affine model $y^2 = f(x)$ with $f(x) \in \mathbb{Q}[x]$ squarefree of degree $2g+2$ and $\iota : (x,y) \mapsto (x,-y)$. The twist $\mathcal{T}_d(C,\iota)$ has affine model $dy^2 = f(x)$. The branch points of ι are the roots of f in $\overline{\mathbb{Q}}$.[1]

If ι is a hyperelliptic involution then $(C/\iota)(\mathbb{Q}) = \mathbb{P}^1(\mathbb{Q})$ is infinite, so (T4) is *not* satisfied. In this note, we give a conditional complement to Theorem 1 that applies to hyperelliptic curves.

Theorem 2. *Assume the ABC conjecture. For a hyperelliptic curve (C,ι) of genus $g \geq 3$, the following are equivalent:*
(i) the hyperelliptic involution ι has no $\mathbb{Q}$-rational branch points;
(ii) as $X \to \infty$, the number of squarefree integers d with $|d| \leq X$ such that $\mathcal{T}_d(C,\iota)_{/\mathbb{Q}}$ violates the Hasse Principle is $\gg_C \frac{X}{\log X}$;
(iii) some quadratic twist $\mathcal{T}_d(C,\iota)_{/\mathbb{Q}}$ violates the Hasse Principle.

Certainly (ii) $\Longrightarrow$ (iii). As for (iii) $\Longrightarrow$ (i): if ι has a $\mathbb{Q}$-rational branch point, then this point stays rational on every quadratic twist. So the crux is to show (i) $\Longrightarrow$ (ii), which we will do in §2. The global part and the dependence on ABC both come from work of Granville [5]. In §3 we give upper and, in a special case, lower bounds on the number of quadratic twists having adelic points. We use these results to show that when hyperelliptic curves of genus $g \geq 3$ are ordered by height, for 100% of such curves the number of twists up to X violating the Hasse Principle is $o(X)$, but conditionally on ABC, there are hyperelliptic curves for which the number of twists up to X violating the Hasse Principle is $\gg X$. Some final remarks are given in §4.

2. Proof of Theorem 2

2.1. Local

Theorem 3. *Let $(C,\iota)_{/\mathbb{Q}}$ be a hyperelliptic curve of genus $g \geq 1$. If $C(\mathbf{A}_\mathbb{Q}) \neq \varnothing$, then the set of primes $p \equiv 1 \pmod 8$ for which $\mathcal{T}_p(C,\iota)(\mathbf{A}_\mathbb{Q}) \neq \varnothing$ has positive density.*

Proof. For any place $\ell \leq \infty$ of $\mathbb{Q}$, if $p \in \mathbb{Q}_\ell^{\times 2}$ then $\mathcal{T}_p(C,\iota)_{/\mathbb{Q}_\ell} \cong C_{/\mathbb{Q}_\ell}$ and thus $\mathcal{T}_p(C,\iota)(\mathbb{Q}_\ell) \neq \varnothing$. In particular, this holds for $\ell = \infty$. Henceforth ℓ denotes a prime number.

Let $M_1 \in \mathbb{Z}^+$ be such that C extends to a smooth relative curve over $\mathbb{Z}_\ell$ for all $\ell > M_1$. Such an M_1 exists for any nice curve $C_{/\mathbb{Q}}$ by openness of the smooth locus. Since C is hyperelliptic, we can take M_1 to be the largest prime dividing its minimal discriminant.

Suppose $\ell > M := \max(M_1, 4g^2 - 1)$, $\ell \neq p$ and $p \notin \mathbb{Q}_\ell^{\times 2}$. Then the minimal regular model $C_{/\mathbb{Z}_\ell}$ is smooth. We have $\mathcal{T}_p(C,\iota)_{/\mathbb{Q}_\ell(\sqrt{p})} \cong C_{/\mathbb{Q}_\ell(\sqrt{p})}$. Since $\mathbb{Q}_\ell(\sqrt{p})/\mathbb{Q}_\ell$ is unramified and formation of the minimal regular model commutes with étale base change [6, Prop. 10.1.17], it follows that the minimal regular model $\mathcal{T}_p(C,\iota)_{/\mathbb{Z}_\ell}$ is smooth. By the Riemann hypothesis for curves over a finite field, since $\ell \geq 4g^2$, we have $\mathcal{T}_p(C,\iota)(\mathbb{F}_\ell) \neq \varnothing$, and then by Hensel's Lemma we have $\mathcal{T}_p(C,\iota)(\mathbb{Q}_\ell) \neq \varnothing$.

Suppose $\ell \leq M$ and $\ell \neq p$. If $\ell = 2$, then $p \in \mathbb{Q}_\ell^{\times 2}$ because $p \equiv 1 \pmod 8$. If ℓ is odd, we require that p is a quadratic residue modulo ℓ, so again $p \in \mathbb{Q}_\ell^{\times 2}$. Either way, $\mathcal{T}_p(C,\iota)(\mathbb{Q}_\ell) = C(\mathbb{Q}_\ell) \neq \varnothing$.

Suppose $\ell = p$. Let $P \in C(\overline{\mathbb{Q}})$ be a hyperelliptic branch point. We assume that p splits completely in $\mathbb{Q}(P)$. Then $P \in C(\mathbb{Q}_p) \cap \mathcal{T}_p(C,\iota)(\mathbb{Q}_p)$.

All in all, we have finitely many conditions on p, each of the form that p splits completely in a certain number field. Taking the compositum of these finitely many number fields and its Galois closure, say L, we see that if p splits completely in L then $\mathcal{T}_p(C,\iota)(\mathbf{A}_\mathbb{Q}) \neq \varnothing$. By (e.g.) the Chebotarev density theorem, this set of primes has positive density. □

[1] We have chosen a model in which the point at ∞ is not a branch point; this is always possible. There is a model in which the point at ∞ is a branch point iff there is a $\mathbb{Q}$-rational branch point.