

ABC AND THE HASSE PRINCIPLE FOR QUADRATIC TWISTS OF HYPERELLIPTIC CURVES

PETE L. CLARK AND LORI D. WATSON

ABSTRACT. Conditionally on the ABC conjecture, we 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.

1. INTRODUCTION

Let C/\mathbb{Q} be an algebraic curve. (All our curves will be 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 $\text{Aut}(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) = \langle \sigma_d \rangle$ action on $C(\mathbb{Q}(\sqrt{d}))$ is “twisted by ι ”: $\sigma : P \in C(\mathbb{Q}(\sqrt{d})) \mapsto \iota(\sigma_d(P))$, and thus

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

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

Let $q : C \rightarrow C/\iota$ 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 $\bar{P} \in C/\iota(\mathbb{Q})$. If \bar{P} a branch point of ι , then the unique point $P \in C(\mathbb{Q})$ such that $q(P) = \bar{P}$ is also rational on every quadratic twist. If \bar{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 $q : \mathcal{T}_d(C, \iota) \rightarrow C/\iota$ consists of two \mathbb{Q} -rational points.

Previous work of Clark and Clark-Stankewicz [Cl08], [ClXX], [CS18] gave 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 adèle ring over \mathbb{Q} , we have $\mathcal{T}_d(C, \iota)(\mathbf{A}_{\mathbb{Q}}) \neq \emptyset$ but $\mathcal{T}_d(C, \iota)(\mathbb{Q}) = \emptyset$. Here is one version.

Theorem 1. [CS18, 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: $\{P \in C(\overline{\mathbb{Q}}) \mid \iota(P) = P\} \neq \emptyset$.*
- (T3) *For some $d \in \mathbb{Q}^{\times}/\mathbb{Q}^{\times 2}$ we have $\mathcal{T}_d(C, \iota)(\mathbf{A}_{\mathbb{Q}}) \neq \emptyset$.*
- (T4) *The set $(C/\iota)(\mathbb{Q})$ is finite.*

Then, as $X \rightarrow \infty$, 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.

¹We 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.

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 $X \rightarrow \infty$, 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) \implies (iii). As for (iii) \implies (i): if ι has a \mathbb{Q} -rational branch point then this point stays rational on every quadratic twist. The matter of it is to show that (i) \implies (ii), which we will do in §2. Some final remarks are given in §3.

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 $C(\mathbf{A}_{\mathbb{Q}}) \neq \emptyset$, then the set of primes $p \equiv 1 \pmod{8}$ for which $\mathcal{T}_p(C, \iota)(\mathbf{A}_{\mathbb{Q}}) \neq \emptyset$ 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 $\mathcal{T}_p(C, \iota)(\mathbb{Q}_{\ell}) \neq \emptyset$. 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}_{ℓ} 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 [L, 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 $\mathcal{T}_p(C, \iota)(\mathbb{F}_{\ell}) \neq \emptyset$, so by Hensel's Lemma we have $\mathcal{T}_p(C, \iota)(\mathbb{Q}_{\ell}) \neq \emptyset$.

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 assume that p is a quadratic residue modulo ℓ , so again $p \in \mathbb{Q}_{\ell}^{\times 2}$. Either way, $\mathcal{T}_p(C, \iota)(\mathbb{Q}_{\ell}) = C(\mathbb{Q}_{\ell}) \neq \emptyset$.

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 $\mathcal{T}_p(C, \iota)(\mathbf{A}_{\mathbb{Q}}) \neq \emptyset$. By (e.g.) the Chebotarev density theorem, this set of primes has positive density. \square

2.2. Global.

Theorem 4. *(Granville [Gr07, Cor. 1.2]) Assume the ABC conjecture. Let $(C, \iota)_{/\mathbb{Q}}$ be a hyperelliptic curve of genus $g \geq 3$. The number of squarefree integers d with $|d| \leq X$ such that $\mathcal{T}_d(C, \iota)(\mathbb{Q})$ has a point that is not a hyperelliptic branch point is $\ll_C X^{\frac{1}{g-1} + o(1)} \ll_C X^{2/3}$.*

2.3. Local-global. We now complete the proof of Theorem 2. Let (C, ι) be a hyperelliptic curve of genus $g \geq 3$ without \mathbb{Q} -rational hyperelliptic branch points, so C has an affine model of the form $y^2 = f(x)$ with $f(x) \in \mathbb{Z}[x]$ of degree $2g + 2$, with distinct roots in $\overline{\mathbb{Q}}$ and no roots in \mathbb{Q} . Put $d_0 := f(1)$. Then $(1, 1)$ is a \mathbb{Q} -point on $d_0 y^2 = f(x)$ and thus on $\mathcal{T}_{d_0}(C, \iota)$. The involution ι remains \mathbb{Q} -rational on $\mathcal{T}_{d_0}(C, \iota)$ (cf. [CS18, §2.1]). We may thus apply Theorem 3 to the hyperelliptic curve $(\mathcal{T}_{d_0}(C, \iota), \iota)$, getting a set of primes $p \equiv 1 \pmod{8}$ of density $\delta > 0$ such that

$$\mathcal{T}_{pd_0}(C, \iota)_{/\mathbb{Q}} = \mathcal{T}_p(\mathcal{T}_{d_0}(C, \iota), \iota)_{/\mathbb{Q}}$$

has points everywhere locally. By the Prime Number Theorem, for at least $(\frac{\delta}{d_0} + o(1))\frac{X}{\log X}$ squarefree d with $|d| \leq X$, we have $\mathcal{T}_d(C, \iota)(\mathbf{A}_{\mathbb{Q}}) \neq \emptyset$. By Theorem 4, we have $\mathcal{T}_d(C, \iota)(\mathbb{Q}) \neq \emptyset$ for $\ll X^{2/3}$ squarefree d with $|d| \leq X$. So the number of squarefree d with $|d| \leq X$ such that $\mathcal{T}_d(C, \iota)_{/\mathbb{Q}}$ violates the Hasse Principle is $\gg_C \frac{X}{\log X}$.

3. SOME REMARKS

In [Gr07, Conj. 1.3], Granville conjectures that for all $g \geq 2$, if $f \in \mathbb{Z}[x]$ with distinct roots in $\overline{\mathbb{Q}}$ of degree $2g+1$ or $2g+2$, then there is a constant $\kappa'_f > 0$ such that the number of squarefree d with $|d| \leq X$ such that $dy^2 = f(x)$ has a \mathbb{Q} -point that is not a hyperelliptic branch point is $\sim \kappa'_f X^{\frac{1}{g+1}}$. The above arguments apply verbatim to show that conditionally on Granville's conjecture, for all $g \geq 2$, a hyperelliptic curve $C_{/\mathbb{Q}}$ has $\gg_C \frac{X}{\log X}$ twists that violate the Hasse principle iff C has no \mathbb{Q} -rational branch points. This addresses the case $g = 2$. On the other hand, Vatsal has exhibited a genus one hyperelliptic curve $(C, \iota)_{/\mathbb{Q}}$ for which a positive proportion of the quadratic twists have infinitely many rational points [Va98]. Still, it may be true that every hyperelliptic curve of genus 1 without \mathbb{Q} -rational branch points has infinitely many twists that violate the Hasse Principle.

Work in progress of the second author aims to quantitatively sharpen Theorem 2. The recent work [CS18] considered quadratic twists of (X^D, w_D) – here X^D is a Shimura curve, w_D is the main Atkin-Lehner involution, and D is chosen such that X^D/w_D has genus at least 2 – violating the Hasse Principle and showed that the number $T(X)$ of such twists up to X satisfies

$$\frac{X}{\log^\alpha X} \ll T(X) \ll \frac{X}{\log^\beta X}$$

for $0 < \beta < \alpha < 1$. Since we assumed that X^D/w_D has genus at least 2, the pair (X^D, w_D) cannot be hyperelliptic. However, [CS18, Thm. 7b)] shows that, for any $D > 1$, the number of quadratic twists up to X with points everywhere locally is $O(\frac{X}{\log^{5/8} X})$. This applies to the genus 3 hyperelliptic pair (X^{35}, w_{35}) , and thus the set of quadratic twists with points everywhere locally has density zero.

Recent work of Bhargava-Gross-Wang [BGW17] shows that for each fixed $g \geq 1$, when genus g hyperelliptic curves $(C, \iota)_{/\mathbb{Q}}$ are ordered by height, a positive proportion violate the Hasse Principle. Apart from being unconditional, their result is quantitatively stronger, yielding a positive proportion rather than proportion zero. On the other hand, since all quadratic twists of a hyperelliptic curve induce the same point of the moduli space \mathcal{H}_g of hyperelliptic curves of genus g , our result gives (conditionally on ABC) precisely located Hasse Principle violations as \mathbb{Q} -points of \mathcal{H}_g .

REFERENCES

- [BGW17] M. Bhargava, B.H. Gross and X. Wang, *A positive proportion of locally soluble hyperelliptic curves over \mathbb{Q} have no point over any odd degree extension*. With an appendix by Tim Dokchitser and Vladimir Dokchitser. J. Amer. Math. Soc. 30 (2017), 451-493.
- [Cl08] P.L. Clark, *An “Anti-Hasse Principle” for prime twists*. Int. J. of Number Theory 4 (2008), 627–637.
- [ClXX] P.L. Clark, *Curves over global fields violating the Hasse Principle*. <https://arxiv.org/abs/0905.3459>
- [CS18] P.L. Clark and J.H. Stankewicz, *Hasse Principle Violations for Atkin-Lehner Twists of Shimura Curves*. To appear in Proc. Amer. Math. Soc.
- [Gr07] A. Granville, *Rational and integral points on quadratic twists of a given hyperelliptic curve*. Int. Math. Res. Not. IMRN 2007, no. 8, Art. ID 027, 24 pp.
- [L] Q. Liu, *Algebraic geometry and arithmetic curves* Translated from the French by Reinie Ern e. Oxford Graduate Texts in Mathematics, 6. Oxford Science Publications. Oxford University Press, Oxford, 2002.
- [Va98] V. Vatsal, *Rank-one twists of a certain elliptic curve*. Math. Ann. 311 (1998), 791-794.