

HASSE PRINCIPLE VIOLATIONS IN TWIST FAMILIES OF SUPERELLIPTIC CURVES

LORI D. WATSON

ABSTRACT. Conditionally on the *abc* conjecture, we generalize previous work of Clark and the author to show that a superelliptic curve $C : y^n = f(x)$ of sufficiently high genus has infinitely many twists violating the Hasse Principle if and only if $f(x)$ has no \mathbb{Q} -rational roots. We also show unconditionally that a curve defined by $C : y^{pN} = f(x)$ has infinitely many twists violating the Hasse Principle over any number field k such that k contains the p th roots of unity and $f(x)$ has no k -rational roots.

1. INTRODUCTION

Let k be a number field and C/k superelliptic curve¹ (see Definition 1). The main result of this work is that infinitely many twists² of a superelliptic curve will violate the Hasse Principle unless the existence of \mathbb{Q} -rational roots of f or the degree of f guarantees a \mathbb{Q} -rational point on every twist.

Definition 1. Let $n \geq 2$ be an integer and let k be a number field. A superelliptic curve C/k is a nice curve admitting an affine model of the form $y^n = f(x)$, where $f(x) \in k[x]$ factors over \bar{k} as

$$f(x) = A \prod_{j=1}^r (x - \alpha_j)^{n_j},$$

where $A \in \bar{k}^*$, the α_j are distinct, $1 \leq n_j < n$ for each j , and $\gcd(n, n_1, \dots, n_r) = 1$.

Remark 2. As shown in [Ko91, Lemma 1], the condition $\gcd(n, n_1, \dots, n_r) = 1$ guarantees that C is geometrically irreducible.

Remark 3. When $n = 2$, the curve is hyperelliptic.

Over an algebraic closure \bar{k} of k , such a curve is equipped with an automorphism τ of order n defined by $\tau(x, y) = (x, \zeta y)$, where ζ is a primitive n th root of unity. One especially interesting feature of these curves is that their automorphism groups give rise to families of twists. In this work, we consider twists $C_d : dy^n = f(x)$, where d is an n th power free integer. Though C and C_d define the same geometric object, their arithmetic can be very different.

Example 4. The elliptic curve $E : y^2 = x^3 + 7x$ has finitely many \mathbb{Q} -rational points while some of its quadratic twists have infinitely many, including $E_5 : 5y^2 = x^3 + 7x$ (see [Si97, P. 351]).

In Theorem 5 we show that if one assumes the *abc* conjecture, then a family of twists C_d of a superelliptic curve $C : y^n = f(x)$ exhibits one of two behaviors: either there are no Hasse Principle violations within the family of twists, or there are many. Following Mazur and Rubin ([MR]), for a given family of twists we say that “many” curves in the family exhibit property P if the number of twists C_d such that $|d| \leq X$ and C_d satisfies property P is $\gg X/(\log X)^\gamma$ for some $\gamma \in \mathbb{R}$. In order for the family of twists to have infinitely many Hasse Principle violations (or indeed any),

¹All curves are assumed to be *nice*: that is smooth, projective, and geometrically integral.

²Given a curve C defined over k , a twist of C is a curve C' also defined over k such that C and C' become isomorphic over \bar{k} .

it is necessary that the map $C \rightarrow C/\langle\tau\rangle \cong \mathbb{P}^1$ has no \mathbb{Q} -rational branch points; assuming the *abc* conjecture, we show that this condition is also sufficient. In particular, we show

Theorem 5. *Assume the abc conjecture. Let $C : y^n = f(x)$ where $n \geq 2$ is an integer and $f(x) \in \mathbb{Z}[x]$ has distinct roots in $\bar{\mathbb{Q}}$ and $\deg(f) \geq \frac{4n-2}{n-1}$. Then the following are equivalent:*

- (i) *The automorphism τ has no \mathbb{Q} -rational fixed points.*
- (ii) *There exists $0 \leq \gamma < 1$ such that as $X \rightarrow \infty$, the number of n th power free integers d with $|d| \leq X$ such that C_d violates the Hasse Principle is $\gg_C \frac{X}{\log(X)^\gamma}$.*
- (iii) *Some degree n twist C_d violates the Hasse Principle.*

That (ii) implies (iii) is immediate. For (iii) implies (i), a \mathbb{Q} -rational branch point of $\langle\tau\rangle$ will remain rational on every twist. Thus it remains to prove (i) implies (ii), which we do in Section 2. For this, we will require two results. The first is due to Granville ([Gr07]) and it provides an upper bound on the number of twists that have so-called “nontrivial” \mathbb{Q} -rational points. By nontrivial, Granville means a point that is *not* a fixed point of the ‘superelliptic automorphism. In the absence of any \mathbb{Q} -rational branch points, Granville’s results provides an upper bound on the number of twists which have any \mathbb{Q} -rational points at all. The second result is a strengthening of [CW18.2, Thm. 3]. It provides a lower bound on the number of twists of a curve that have points everywhere locally (and in fact shows that there are many such twists).

This result generalizes Theorem 2 of [CW18.2], which proves the result when C is hyperelliptic. In [KL19], König and Legrand recover the hyperelliptic result. They then extend the result to Galois covers of \mathbb{P}^1/\mathbb{Q} , that is, when the Galois group of $\mathbb{Q}(C)/\mathbb{Q}(\mathbb{P}^1)$ contains in its center $\mathbb{Z}/n\mathbb{Z}$. We note that this result of König and Legrand is separate from Theorem 5 except in the hyperelliptic case: while the Galois group of $\bar{\mathbb{Q}}(C)/\bar{\mathbb{Q}}(\mathbb{P}^1)$ does contain $\langle\tau\rangle \cong \mathbb{Z}/n\mathbb{Z}$ for a superelliptic curve C , such a curve gives a Galois cover of \mathbb{P}^1/\mathbb{Q} only when $n = 2$. It gives a Galois cover of \mathbb{P}_k^1 if and only if k contains the n th roots of unity. In that sense, we may think of superelliptic curves as geometrically Galois covers of \mathbb{P}^1 .

In Section 2 we give the proof of Theorem 5. In Section 3 we provide asymptotic bounds for the number of Hasse Principle violations. In Section 4, we give unconditional results on Hasse Principle violations over a number field containing p th roots of unity (where p is prime) for curves of the form $y^{pN} = f(x)$.

2. PROOF OF THE MAIN RESULT

In this section we prove the main result.

We begin by providing criteria for the existence of Hasse Principle violations within a family of twists. A point P fixed under the action of the automorphism group $\langle\tau\rangle$ is either a point lying above ∞ or a point with y -coordinate 0. The quotient map $C \rightarrow C/\langle\tau\rangle \xrightarrow{\sim} \mathbb{P}^1$ has a \mathbb{Q} branch point above ∞ if and only if $n \nmid \deg(f)$ with the ramification index of the point at infinity being $e = n/\gcd(n, \deg(f))$ ([Ko91]). A point P with y -coordinate 0 necessarily has as its x -coordinate a root of the defining polynomial.

2.1. Bound on twists with nontrivial global points. The “global” step towards proving the main theorem is a result due to Granville. This results provides an upper bound on the number of twists with nontrivial \mathbb{Q} -rational points. It relies on the *abc* theorem to bound the height of the x -coordinate of a point that can appear on a twist C_d .

2.2. The *abc* conjecture. One of several equivalent statements of the *abc* conjecture over \mathbb{Q} is as follows ([Vo98, Conj. 2.4]):

Conjecture 6 (*abc* Conjecture, Masser-Oesterlé). *For each $\epsilon > 0$, there exists a constant K depending only on ϵ such that for all triples (a, b, c) of relatively prime integers with $a + b = c$,*

$$\max(|a|, |b|, |c|) \leq K \left(\prod_{\substack{p \text{ prime} \\ p|abc}} p \right)^{1+\epsilon},$$

The *abc* conjecture has numerous implications; most relevant to this work is that the *abc* conjecture, if true, allows one to count the number of n th power-free values achieved by a polynomial with integer coefficients.

Theorem 7 (Granville, [Gr07, §11]). *Assume that the *abc*-conjecture is true. Fix $\epsilon > 0$. Let $f(x) \in \mathbb{Z}[x]$ have no repeated roots in $\bar{\mathbb{Q}}$. Let $d \in \mathbb{Z}$ be an n th power free integer. Any rational point on $C_d : dy^n = f(x)$ with x -coordinate r/s where $\gcd(r, s) = 1$ satisfies*

$$|r|, |s| \ll_{f, \epsilon} |d|^{-\left(nk+i-1-\frac{\gcd(n, i)+1}{n-1}\right)+\epsilon},$$

where $\deg(f) = nk + i$, $1 \leq i \leq n$.

As a consequence, we conclude that as $X \rightarrow \infty$, the number of n th power free integers d with $|d| \leq X$ for which C_d has a nontrivial rational point is $\ll_f X^{2/\left(nk+i-1-\frac{\gcd(n, i)+1}{n-1}\right)+\epsilon}$

If $\frac{4n-2}{n-1} < \deg(f)$, then for sufficiently small $\epsilon > 0$, the number of n th power free $d \in \mathbb{Z}$ with $|d| \leq X$ such that C_d has a nontrivial rational point is X^a for some $a < 1$.

2.3. Bound on twists with points everywhere locally. With an eye towards eventually proving the main theorem for arbitrary number fields, in this section we prove that if a superelliptic curve C has points everywhere locally, then many of its twists has points everywhere locally as well.

Lemma 8. *Let $C : y^n = f(x)$ be a superelliptic curve of genus $g \geq 1$ defined over a number field k . Suppose C has points everywhere locally. For an element $d \in \mathcal{O}_k$, let $N(d) = |\mathcal{O}_k/(d)|$. As $X \rightarrow \infty$, the number of non-associate elements $\pi \in \mathcal{O}_k$ such that $N(\pi) \leq X$ and C_π has points everywhere locally is $\gg_{C, k} X/\log X$.*

Proof: Let $(\pi) = \mathfrak{p} \triangleleft \mathcal{O}_k$ denote a principal maximal ideal of \mathcal{O}_k with π satisfying $\sigma(\pi) > 0$ for every real embedding $\sigma : k \hookrightarrow \mathbb{R}$. (These ideals are precisely those which split in the narrow Hilbert Class Field of k , so by the finiteness of the class number they represent a positive density set of the prime ideals of \mathcal{O}_k , ([Ja96, §3])). For any place v of k , if $\pi \in k_v^{*n}$, then $C_\pi \cong C$ over k_v . Thus, if k_v is any archimedean completion of k then $C_\pi \cong C$ over k_v and $C_\pi(k_v) \neq \emptyset$. From now on, v will denote a finite place corresponding to a prime ideal \mathfrak{L}_v , \mathcal{O}_v will denote the ring of integers of k_v , and \mathbb{F}_ℓ the finite field with ℓ elements will denote the residue field of k_v .

Let $M_1 \in \mathbb{Z}^+$ be such that C extends to a smooth proper relative curve over \mathcal{O}_v for every v such that $\text{char}(\mathfrak{L}_v) > M_1$. Such an M_1 exists for any nice curve C/k by the openness of the smooth locus.

Suppose $\text{char}(\mathfrak{L}_v) > M := \max\{M_1, 4g^2 - 1, n\}$, $\mathfrak{L}_v \neq \mathfrak{p}$, and $\pi \notin k_v^{*n}$. Then the minimal regular model C/\mathcal{O}_v is smooth. Fix an extension $k_v(\sqrt[n]{\pi})/k_v$ which contains an n th root of π . Over $k_v(\sqrt[n]{\pi})$, $C \cong C_\pi$. Since $k_v(\sqrt[n]{\pi})/k_v$ is unramified for any choice of an n th root of π , and formation of the minimal regular model commutes with étale base change ([Liu02, Prop. 10.1.17]), it follows that the minimal regular model $(C_\pi)_{/\mathcal{O}_v}$ is smooth. By the Riemann hypothesis for curves over a finite field ([Si97, Thm. V.2.2]), since $\ell \geq 4g^2$, we have $C_\pi(\mathbb{F}_\ell) \neq \emptyset$, so by Hensel's Lemma ([Ca67]) we have $C_\pi(k_v) \neq \emptyset$.

Suppose now $\text{char}(\mathfrak{L}_v) \leq M$ and $\mathfrak{L}_v \neq \mathfrak{p}$. If the v -adic valuation of n is θ , then we require \mathfrak{p} to split completely in $\tilde{k} = k(\zeta_{\ell^{2\theta+1}})$, the compositum of k and $\mathbb{Q}(\zeta_{\ell^{2\theta+1}})$. In that case we have $\pi \equiv 1 \pmod{\ell^{2\theta+1}}$; letting $g(x) = x^n - \pi$, we then have $|g(1)|_v \leq \ell^{-(2\theta+1)} < \ell^{-2\theta} = |g'(1)|_v^2$, so by Hensel's lemma, there exists a unique $u \in \mathbb{Z}_v$ such that $g(u) = 0$. Thus π is an n th root in k_v , so $C/k_v \cong C_\pi/k_v$, and $C_\pi(k_v) \neq \emptyset$.

Now suppose $\mathfrak{L}_v = \mathfrak{p}$. Let $P \in C(\bar{k})$ be a superelliptic branch point. We assume \mathfrak{p} splits completely in $K = k(P)$. Then, if \mathfrak{P} is a prime of K lying above \mathfrak{p} , since \mathfrak{p} splits completely, the completion $K_{\mathfrak{P}}$ has $[K_{\mathfrak{P}} : k_{\mathfrak{p}}] = 1$, thus K embeds into $k_{\mathfrak{p}}$, and $P \in C_{\pi}(k_{\mathfrak{p}})$, so $C_{\pi}(k_{\mathfrak{p}}) \neq \emptyset$. We have imposed finitely many conditions on \mathfrak{p} , each requiring that \mathfrak{p} splits completely in a certain number field. Letting L be the Galois closure of the compositum of these finitely many number fields, we have that C_{π} has points everywhere locally whenever $(\pi) = \mathfrak{p}$ splits completely in L . By the Chebotarev density theorem ([LS96, Appendix]), this set of primes (which we will denote by S and use in the next theorem) has positive density in the set of \mathcal{O}_k primes. By Landau's Prime Ideal Theorem, the number of prime ideals \mathfrak{p} of \mathcal{O}_k with $N\mathfrak{p} \leq X$ is asymptotic to $X/\log X$. \square

In the case $k = \mathbb{Q}$, having produced a positive density set of primes whose twists have points everywhere locally, we can construct a larger set of n th power free integers $d \in \mathbb{Z}$ such that the twists C_d have points everywhere locally.

Theorem 9. *Let $C : y^n = f(x)$ be a superelliptic curve of genus $g \geq 1$ defined over \mathbb{Q} . Suppose C has points everywhere locally. The number of n th power free integers d with $|d| \leq X$ such that C_d has points everywhere locally is $\gg_C X/\log(X)^{\gamma}$ for some $0 \leq \gamma < 1$.*

Proof: Denote the set of primes p constructed in Lemma 8 by S . By construction this set has density $0 < \delta(S) < 1$. Consider the set \mathcal{D} consisting of n th power free integers d , all of whose prime divisors are in S . If n is even we further require that all elements of \mathcal{D} be positive. We will show that for each $d \in \mathcal{D}$, the twist C_d has points everywhere locally.

If n is even then as $d > 0$ and $C(\mathbb{R}) \neq \emptyset$, we have $C_d(\mathbb{R}) \neq \emptyset$. If n is odd or if $f(x)$ has a real root then $C_d(\mathbb{R}) \neq \emptyset$ for every nonzero integer d .

Next, let M be as in Lemma 8, and let $\ell > M$, $\ell \nmid d$. If $d \in \mathbb{Q}_{\ell}^{*n}$, then C_d is isomorphic to C over \mathbb{Q}_{ℓ} , thus $C_d(\mathbb{Q}_{\ell}) \neq \emptyset$. So assume $d \notin \mathbb{Q}_{\ell}^{*n}$. Then $\mathbb{Q}_{\ell}(\sqrt[n]{d})/\mathbb{Q}_{\ell}$ is unramified, and as before we conclude that the minimal regular model $(C_d)_{/\mathbb{Z}_{\ell}}$ is smooth. Then by the Riemann Hypothesis for curves over a finite field, since $\ell \geq 4g^2$, $C_d(\mathbb{F}_{\ell}) \neq \emptyset$, so by Hensel's Lemma, we again have $C_d(\mathbb{Q}_{\ell}) \neq \emptyset$.

For $\ell < M$ and $\ell \nmid d$, as $d = p_1^{m_1} \cdots p_r^{m_r}$ with $p_j \in \mathbb{Q}_{\ell}^{*n}$ for all $1 \leq j \leq r$, $d \in \mathbb{Q}_{\ell}^{\times n}$, so C_d is isomorphic to C over \mathbb{Q}_{ℓ} , thus $C_d(\mathbb{Q}_{\ell}) \neq \emptyset$.

Finally, consider $C_d(\mathbb{Q}_p)$, where $p|d$. Then $p \in S$. By construction, for each $p \in S$, p splits completely in $K = \mathbb{Q}(P)$ where P is a fixed point of τ . As before, if \mathfrak{P} is a prime of K lying above p , since p splits completely, the completion $K_{\mathfrak{P}}$ has $[K_{\mathfrak{P}} : \mathbb{Q}_p] = 1$, thus K embeds into \mathbb{Q}_p . Since P is a fixed point of τ , it is of the form $P = (\alpha, 0)$, where α is a root of the defining polynomial $f(x)$. Thus $K = \mathbb{Q}(\alpha) \subset \mathbb{Q}_p$. Then $(\alpha, 0)$ is a \mathbb{Q}_p -rational point of every degree n twist of C , so in particular $C_d(\mathbb{Q}_p) \neq \emptyset$. Thus C_d has points everywhere locally for each $d \in \mathcal{D}$.

Let $\gamma = 1 - \delta(S)$. By [Ser76, Thm 2.4], we have that the number of $d \in \mathcal{D}$ with $|d| \leq X$ such that C_d has points everywhere locally is $\gg X/\log(X)^{\gamma}$. \square

2.4. Proof of the Main Theorem.

We now complete the proof of the main theorem.

Proof of 5: Let $C : y^n = f(x)$ be a superelliptic curve, where $f(x)$ has coefficients in \mathbb{Z} , distinct roots in $\bar{\mathbb{Q}}$, no roots in \mathbb{Q} , and $\deg(f) > (4n - 2)/(n - 1)$. If C does not have points everywhere locally, write $f(1) = d_1 d_2^n$ where $d_1, d_2 \in \mathbb{Z}$ and d_1 is n th power free. Then the curve $C' := C_{d_1}$ (with model $d_1 y^n = f(x)$) has the \mathbb{Q} -rational point $(1, d_2)$ and hence has points everywhere locally. Applying Theorem 9 to C' , we have that the number of n th power free integers d with $|d| \leq X$ such that the twist C'_d of C' with points everywhere locally is $\gg X/\log(X)^{\gamma}$. As the twist C'_d is a twist of the original curve C , we have that the number of n th power free integers d with $|d| \leq X$ such that C_d has points everywhere locally is still $\gg_C X/\log(X)^{\gamma}$.

By 7, we have that the number of n th power free $d \in \mathbb{Z}$ with $|d| \leq X$ such that $C_d(\mathbb{Q}) \neq \emptyset$ is $\ll X^{2/3}$. Thus the number of n th power free d with $|d| \leq X$ such that C_d violates the Hasse Principle is $\gg_C X/\log(X)^\gamma$. \square

3. ASYMPTOTIC BOUNDS

Assuming the *abc* conjecture, Theorem 5 shows that the existence of any (equivalently infinitely many) Hasse Principle violations within a family of twists of a curve $C : y^n = f(x)$ depends on the degree of f and whether f possesses any \mathbb{Q} -rational roots. By more closely examining the local behavior of f , we can provide more precise bounds on the number of twists violating the Hasse Principle.

Let $\mathfrak{D}_C := \{n\text{th power free } d \in \mathbb{Z} : C_d \text{ has points everywhere locally}\}$. For $X \geq 1$, put $\mathfrak{D}_C(X) = \#\mathfrak{D}_C \cap [-X, X]$. We saw in Thm 9, that $\mathfrak{D}_C(X) \gg \frac{X}{\log(X)^\gamma}$ for some $\gamma \in (0, 1)$. We will soon see that $\mathfrak{D}_C(X)$ (and hence the number of Hasse Principle violations for C with no \mathbb{Q} -rational branch points) depends on the density (within the set of all primes) of the set $\mathcal{S} = \{\ell \text{ prime} : f(x) \text{ has a root modulo } \ell\}$. For the hyperelliptic case $n = 2$, we can provide an unconditional upper bound on the number of twists having points everywhere locally in terms of the density δ of \mathcal{S} . For $n \geq 2$, when the density of \mathcal{S} equals 1, we will show that, conditional on the *abc* conjecture, a positive density set of twists have points everywhere locally. Before proceeding we introduce some new terminology:

Definition 10. We say a polynomial $f \in \mathbb{Z}[x]$ is weakly intersective if $\delta = 1$.

Theorem 11. Let $C : y^n = f(x)$ be a superelliptic curve with $f(x) \in \mathbb{Z}[x]$ squarefree and weakly intersective. Then $\mathfrak{D}_C(X) \gg_C X$.

As an immediate consequence of Theorem 11 we have the following corollary:

Corollary 12. Let $C : y^n = f(x)$ be a superelliptic curve with $f(x) \in \mathbb{Z}[x]$ squarefree. If C has no \mathbb{Q} -rational superelliptic branch points and $\deg(f) > 5$, then conditionally on the *abc* conjecture, as $X \rightarrow \infty$, the number of degree n twists of C/\mathbb{Q} that violate the Hasse Principle is $\gg_C X$.

Remark 13. Before proving Theorem 11, we will first show that if $f(x)$ is weakly intersective, then the set of primes ℓ for which $f(x)$ does not have a root $(\bmod \ell)$ is finite. (This argument appears in [CW18.2]). Let $f(x) = \sum_{j=1}^n a_j x^j \in \mathbb{Z}[x]$ have degree $n \geq 2$ and let Δ be the discriminant of f . Suppose $f(x)$ has distinct roots in $\bar{\mathbb{Q}}$ and let G denote the Galois group of f .

For each prime $\ell \nmid a_n \Delta$, the partition of n given by the cycle type of a Frobenius element σ_ℓ at ℓ coincides with a partition of n given by the degrees of the irreducible factors of the image of f in $(\mathbb{Z}/\ell\mathbb{Z})[x]$. Since $f(x)$ is weakly intersective, by the Frobenius Density Theorem ([LS96, §3]), every $\sigma \in G$ has a fixed point, and thus f has a root $(\bmod \ell)$ for every $\ell \nmid a_n \Delta$. By Hensel's Lemma, $f(x)$ has a root in \mathbb{Z}_ℓ for all but finitely many ℓ .

Proof of 11: By the remark above, if f is weakly intersective, then f has a root modulo ℓ for all but finitely many ℓ and hence has a root in \mathbb{Z}_ℓ for all but finitely many primes ℓ . Therefore, the set \mathcal{P} of primes ℓ such that $C(\mathbb{Q}_\ell) = \emptyset$ is finite. For each $\ell \in \mathcal{P}$, we have $C_d(\mathbb{Q}_\ell) \neq \emptyset$ for any d lying in the same \mathbb{Q}_ℓ -adic n th power class as $f(1)$. The set of integers lying in any given \mathbb{Q}_ℓ -adic n th power class is a nonempty union of congruence classes modulo $\ell^{2v_\ell(n)}$ if ℓ is odd and modulo $2^{4v_\ell(n)}$ if $\ell = 2$. By the Chinese Remainder Theorem there are $a, N \in \mathbb{Z}^+$ such that if $d \equiv a \pmod{N}$, then $C_d(\mathbb{Q}_\ell) \neq \emptyset$ for all primes ℓ . A result of Prachar ([Pr58]) guarantees that there is a positive density set of $d \equiv a \pmod{N}$ which are squarefree (and thus n th power free), so long as $a \in (\mathbb{Z}/N\mathbb{Z})^*$. If f has a real root, then $C_d(\mathbb{R}) \neq \emptyset$ for all n th power free $d \in \mathbb{Z}$. Otherwise, $C_d(\mathbb{R}) \neq \emptyset \iff df(1) > 0$. In either case, $\mathfrak{D}_C(X) \gg_f X$. (The implied constant depends on the discriminant of f .) \square

4. UNCONDITIONAL RESULTS

In this section, we provide an unconditional result on Hasse Principle violations in families of twists of certain superelliptic curves which map to curves of sufficiently large genus and few points. We prove a theorem, first stated in ([C108, Thm. 2]), to produce many twists which fail to have k -rational points and thus, combined with Lemma 8 yield many Hasse Principle violations within some families of twists.

Theorem 14. *Let k be a number field containing the p th roots of unity where p is prime. Let C/k be a smooth, projective, geometrically integral curve, and let $\psi : C \rightarrow C$ be a k -rational automorphism of order p . Assume the following hold:*

- (i) $\{P \in C(k) : \psi(P) = P\} = \emptyset$.
- (ii) $\{P \in C(\bar{k}) : \psi(P) = P\} \neq \emptyset$.
- (iii) For some extension $L = k(d^{1/p})$, the twist C_d has points everywhere locally.
- (iv) The set $(C/\langle\psi\rangle)(k)$ is finite.

Then for all but finitely many d , the twisted curve C_d has no k -rational points.

Proof: Let L/k be a cyclic degree p extension. As k contains the p th roots of unity, by Kummer Theory, $L = k(d^{1/p})$, for some p th power free $d \in k$. Let $Y := Y_L$ be the twist of C by ψ with respect to L/k . Then ψ defines a k -rational automorphism on Y . Let $\theta : G_k \rightarrow \text{Aut}(C)$ be the 1-cocycle corresponding to the twist Y . For a generator σ of the Galois group of L/k , we have $\theta(\sigma) = \psi^j$ for some $j = j_\sigma \in (\mathbb{Z}/p\mathbb{Z})^*$. We have that $Y/L \cong C/L$, and σ acts on $Y(L)$ by $\sigma^*(P) = \psi^j \sigma(P)$. Thus, for all $P \in Y(A)$ (for any k -algebra A) we have

$$\sigma^* \psi(\sigma^*)^{-1} = (\psi^j \sigma) \psi(\psi^j \sigma)^{-1} = (\psi^j \sigma) \psi(\sigma^{-1} \psi^{-j}) = \psi^j (\sigma \psi \sigma^{-1}) \psi^{-j} = \psi^j \psi \psi^{-j} = \psi$$

We have natural maps

$$\kappa : Y_L(k) \hookrightarrow C(L)$$

and

$$\lambda : C(L) \rightarrow (C/\langle\psi\rangle)(L)$$

so that

$$S_L := (\lambda \circ \kappa)(Y_L(k)) \subseteq (C/\langle\psi\rangle)(k) \text{ and } (C/\langle\psi\rangle)(k) = \psi(C(k)) \cup \bigcup_{L=k(d^{1/p})} S_L.$$

For distinct degree p extensions of k , L_1 and L_2 , $P \in S_{L_1} \cap S_{L_2} \implies P \in C(L_1) \cap C(L_2) = C(k)$ (since $[L_i : k]$ is prime and the extensions are distinct, $L_1 \cap L_2 = k$). If $P \in S_L \cap C(k)$, then $P = \lambda(\kappa(Q))$ for some $Q \in Y_L(k)$. As $\lambda(\kappa(Q)) \in (C/\langle\psi\rangle)(L)$, P is a fixed point of ψ , but by hypothesis, no such points are k -rational. Thus $S_{L_1} \cap S_{L_2} = \emptyset$ and $(C/\langle\psi\rangle)(k)$ is a disjoint union of the S_L . Since $(C/\langle\psi\rangle)(k)$ is finite, we conclude that there are only finitely many twists Y_L which have k -rational points. \square

Corollary 15. *Let $C : y^n = f(x)$ be a superelliptic curve defined over a number field k with no k -rational superelliptic fixed points. Suppose $n = pN$ with $1 < N < n$ and p prime, and that k contains the p th roots of unity. Let $N(d) := |\mathcal{O}_k/(d)|$ denote the norm of d . Suppose that $\text{Aut}(C/\bar{k}) \cong \mu_n$ and that the curve $C^{(N)} : y^N = f(x)$ has finitely many k -rational points. Then as $X \rightarrow \infty$ the number of N th power free $d \in \mathcal{O}_k$ such that C_d violates the Hasse Principle is $\gg_C \frac{X}{\log(X)}$. In particular, if the genus $g(C^{(N)}) \geq 2$ or if $C^{(N)}$ is an elliptic curve with finite Mordell-Weil rank over k , then C has many twists violating the Hasse Principle.*

Proof: We assume without loss of generality that C has points everywhere locally over k . From Lemma 8, there is a set of non-associate, totally positive prime elements $\pi \in \mathcal{O}_k$ such that C_π has points everywhere locally. We consider now the twists C_d where $d = \pi^p$. As before, there is $M \in \mathbb{Z}^+$ (depending on n and the genus and discriminant of C) such that for every prime ideal $\mathfrak{L}_v \neq (\pi)$, with $N_{\mathfrak{L}_v} > M$, $C_d(k_v) \neq \emptyset$ (where v is the finite place corresponding to \mathfrak{L}_v , and k_v the completion of k at v). For $\mathfrak{L}_v \neq (\pi)$ with $N_{\mathfrak{L}_v} \leq M$, π , and hence d is an n th power in k_v , thus

$C/k_v \cong (C_d)/k_v$, so $(C_d)/k_v \neq \emptyset$. Finally, for $\mathcal{L}_v = (\pi)$, by construction k_v contains a root of $f(x)$, and so $(C_d)/k_v \neq \emptyset$ for every twist of C .

We take for $\langle \psi \rangle$ in Theorem 14 the unique subgroup of order p in $\text{Aut}(C/\bar{k})$. Then $(C/\langle \psi \rangle) \cong C^{(N)}$. By Theorem 14, only finitely many of the degree p -twists C_d , $d = \pi^p$ have k -rational points. \square

4.1. Examples of the unconditional result. Examples satisfying the hypotheses of Cor 15 include hyperelliptic curves of the form $y^2 = x^{2\ell} - A$, where $\ell \geq 5$ (or $\ell = 3, 4$ and the genus 1 curve $y^2 = x^\ell - A$ has finitely many k -rational points) and A is not an 2ℓ th power in k . In such cases, $y^2 = x^\ell - A$ has finitely many points, so by Thm. 14, only finitely many quadratic twists of $y^2 = x^{2\ell} - A$ (with respect to the automorphism $\tau(x, y) = (x, \zeta_\ell y)$) have k -rational points.

Additional examples include superelliptic curves defined by $y^4 = f(x)$ where $\deg(f) = 2m > 4$ (or $\deg(f) = 4$ and $y^2 = f(x)$ is of genus 1 and has only finitely many k -rational points) and $f(x) \in k[x]$ has no k -rational roots. As the hyperelliptic curve $y^2 = f(x)$ has only finitely many rational points, there are only finitely many quadratic twists corresponding to the automorphism $(x, y^2) \mapsto (x, -y^2)$ which have k -rational points.

REFERENCES

- [Bi67] Birch, B.J. "Cyclotomic fields and Kummer extensions," in Cassels, J.W.S and Fröhlich, *Algebraic number theory; proceedings of an instructional conference*. Thompson Book Co., Washington, 1967.
- [Ca67] Cassels, J.W.S., "Global fields, Appendix C," in Cassels, J.W.S and Fröhlich, *Algebraic number theory; proceedings of an instructional conference*. Thompson Book Co., Washington, 1967.
- [Cl08] Clark, P.L. *An "anti-Hasse principle" for prime twists*. Int. J. Number Theory 4, no. 4, 627–637, 2008.
- [CW18.2] Clark, P.L and Watson, L.D., *ABC and the Hasse principle for quadratic twists of hyperelliptic curves*. C. R. Math. Acad. Sci. Paris 356, 911-915, 2018.
- [Gr07] Granville, A., *Rational and integral points on quadratic twists of a given hyperelliptic curve*. Int. Math. Res. Not. IMRN, no. 8, Art. ID 027, 24 pp, 2007.
- [Ja96] Janusz, G. *Algebraic number fields (2nd ed.)* American Mathematical Society, Providence, RI, Graduate Studies in Mathematics, Vol 7, 1996.
- [KL19] König, J. and Legrand, F. *Density results for specialization sets of Galois covers*. J. Inst. Math. Jussieu, 1-42, 2019.
- [Ko91] Koo, J. K., *On holomorphic differentials of some algebraic function field of one variable over \mathbb{C}* . Bull. Austral. Math. Soc. 43, 399-405. MR 92e:14019, 1991.
- [LS96] Lenstra Jr., H.W. and Stevenhagen, P., *Chebotarev and his density theorem*. Math. Intell. 18, 26-37, 1996.
- [Liu02] Liu, Q., *Algebraic geometry and arithmetic curves*. Oxford University Press, Oxford, Oxford Graduate Texts in Mathematics 6, 2002.
- [Lo90] Lorenzini, D., *Dual graphs of degenerating curves*. Math. Ann., 287:135-150, 1990.
- [Lo13] Lorenzini, D., *Wild quotient singularities of surfaces*. Math. Zeit. 275 Issue 1, 211-232, 2013.
- [MR] Mazur, B. and Rubin, K., *Ranks of twists of elliptic curves and Hilbert's tenth problem*. Invent. math., Vol. 181, Issue 3, 541–575, 2010.
- [PS97] Poonen, B. and Schaefer, E.F., *Explicit descent for Jacobians of cyclic covers of the projective line*. J. Reine Angew. Math., 488, 141–188, 1997.
- [Pr58] Prachar, K., *Über die kleinste quadratfreie Zahl einer arithmetischen Reihe*. Monatsh. Math., 62, 173-176, 1958.
- [Re42] Reichardt, H., *Einige im Kleinen überall lösbare, im Grossen unlösbare diophantische Gleichungen*. J. Reine Angew. Math. 184, 12-18, 1942.
- [Ri08] Rivin, I., *Walks on groups, counting reducible matrices, polynomials, and surface and free group automorphisms*. Duke Math. J. Vol.142,, no. 2, 353-379, 2008.
- [Sa14] Sadek, M., *On quadratic twists of hyperelliptic curves*. Rocky Mountain J. Math. 44, 1015-1026, 2014.
- [Ser76] Serre, J.P., *Divisibilité de certaines fonctions arithmétiques*. Enseignement Math. (2) 22, 227–260, 1976.
- [Si97] Silverman, J., *The arithmetic of elliptic curves (2nd. ed.)*. Springer-Verlag, New York, Graduate Texts in Mathematics, No. 106, 2009.
- [Sk10] Skorobogatov, A. N., *Torsors and rational points*. Cambridge University Press, Cambridge, Cambridge Tracts in Mathematics, Vol. 144, 2001.
- [Vo98] Vojta, P., *A More General ABC Conjecture*. Int. Math. Res. Not. IMRN, no. 21, 1103-1116, 1998.