Hasse Principle Violations of Quadratic Twists of Hyperelliptic Curves

Lori Watson
Joint work with Pete Clark

University of Georgia

June 1, 2018

Given a nice curve defined over $\mathbb{Q}$, does the existence of points over every completion of $\mathbb{Q}$ imply the existence of a point over $\mathbb{Q}$ itself?

Given a nice curve defined over $\mathbb{Q}$, does the existence of points over every completion of $\mathbb{Q}$ imply the existence of a point over $\mathbb{Q}$ itself?

Theorem (Hasse-Minkowski)

For a genus 0 curve C, $C(\mathbb{Q}) \neq \emptyset \iff C(\mathbb{R}) \neq \emptyset$ and $C(\mathbb{Q}_p) \neq \emptyset$ for all primes p

In general, this does not hold:

In general, this does not hold:

Example (Selmer)

The genus 1 *curve* $3x^3 + 4y^3 + 5z^3 = 0$ *has only the solution* $(0, 0, 0)$ *over* $\mathbb{Q}$*, but a nontrivial solution over* $\mathbb{R}$ *and over* $\mathbb{Q}_p$ *for every prime* p*.*

Definition

A curve $C_{/\mathbb{Q}}$ *violates the Hasse Principle* if $C(\mathbb{R}) \neq \emptyset$ and $C(\mathbb{Q}_p) \neq \emptyset$ for all primes p, but $C(\mathbb{Q}) = \emptyset$

That is, a curve C violates the Hasse Principle if it has points everywhere locally, but does not have a global point.

Recall that a hyperelliptic curve is a pair (C, ι), with $C_{/\mathbb{Q}}$ a nice curve and ι (the *hyperelliptic involution*) an order 2 automorphism of $C_{/\mathbb{Q}}$ such that $(C/\iota) \cong \mathbb{P}^1$.

Denote the quadratic twist of C by ι and $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ by C_d.

Our goal is to understand how many Hasse Principle violations occur in the family of quadratic twists of C. In other words, for how many squarefree integers d do we have $C_d(\mathbb{Q}) = \emptyset$ despite the existence of points everywhere locally?

Theorem

Assume the ABC conjecture. For a hyperelliptic curve C 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 C_d violates the Hasse Principle is $\gg_C \frac{X}{\log X}$

(iii) Some quadratic twist C_d violates the Hasse Principle.

The theorem follows from two results:

Lemma

Let C be a hyperelliptic curve of genus $g \geq 1$. If C has points everywhere locally, then there is a positive density set of primes $p \equiv 1 \pmod 8$ such that C_p has points everywhere locally.

The theorem follows from two results:

Lemma

Let C be a hyperelliptic curve of genus $g \geq 1$. If C has points everywhere locally, then there is a positive density set of primes $p \equiv 1 \pmod 8$ such that C_p has points everywhere locally.

Theorem (Granville)

Assume the ABC conjecture. Let C be a hyperelliptic curve of genus $g \geq 3$. The number of squarefree integers d with $|d| \leq X$ such that $C_d(\mathbb{Q})$ has a point that is not a hyperelliptic branch point is $\ll_C X^{2/3}$

To complete the proof of the main theorem, take C to be a hyperelliptic curve of genus ≥ 3 with no $\mathbb{Q}$-rational hyperelliptic branch points. If C does not have points everywhere locally, we can twist by $d_0 = f(1)$ to obtain a hyperelliptic curve C_{d_0} that does.

Applying the lemma to the curve C_{d_0}, we have a positive density set of primes p such that the twists C_{pd_0} all have points everyhwere locally, and thus $\gg \frac{X}{\log X}$ squarefree d with $|d| \leq X$ such that C_d has points everywhere locally. Combining this with Granville's theorem gives the desired result.

A curve C satisfying (i) in the main theorem has an affine model of the form $y^2 = f(x)$, where $f(x) \in \mathbb{Z}[x]$ is of degree $2g + 2$ with distinct roots in $\overline{\mathbb{Q}}$ and no roots in $\mathbb{Q}$.

We can determine how many Hasse Principle violations occur (asymptotically) in the family of quadratic twists of C in terms of the density of primes p for which f has a root modulo p.

Definition (Weakly Intersective)

A polynomial $f \in \mathbb{Z}[x]$ is *weakly intersective* if the set of primes p such that f has a root modulo p has density 1.

We will call a hyperelliptic curve C weakly intersective if it has a weakly intersective, squarefree, even degree defining polynomial.

Theorem

Let C be a hyperelliptic curve with an affine equation $y^2 = f(x)$, with $f \in \mathbb{Z}[x]$ squarefree of even degree. Let $\mathfrak{D}_C(X)$ be the number of squarefree integers d with $|d| \leq X$ such that C_d has points everywhere locally.

(a) If f is weakly intersective, then $\mathfrak{D}_C(X) \gg X$.

(b) If f is not weakly intersective, let β be the density of the set of primes p such that f has no root modulo p. Then $\mathfrak{D}_C(X) \ll \frac{X}{\log^{\beta} X}$

Sketch of Proof

(a) If the polynomial f is weakly intersective, then it has a root in $\mathbb{Z}_p$ for all but finitely many p, so the set $\mathcal{P}$ of primes p such that $C(\mathbb{Q}_p) = \emptyset$ is finite.

For each $p \in \mathcal{P}$, $C_d(\mathbb{Q}_p) \neq \emptyset$ whenever d is in the same $\mathbb{Q}_p$-adic square class as $f(1)$; this holds for d lying in appropriate congruence classes modulo p^2 (p is odd) or modulo 16 ($p = 2$). By the Chinese Remainder Theorem, a positive density set of d satisfy the necessary conditions.

If f has a real root, then C_d has points everywhere locally for all d in that positive density set; otherwise, C_d has points everywhere locally for half of all d in the set.

Sketch of Proof (cont.)

(b) By an argument of Sadek, if p is an odd prime of good reduction such that f has no root modulo p, then $C_d(\mathbb{Q}_p) = \emptyset$ for any squarefree d which is an integer multiple of p. A result of Serre then gives the upper bound on $\mathfrak{D}_C(X)$.

Corollary

Let C be a hyperelliptic curve of genus g without $\mathbb{Q}$-rational hyperelliptic branch points.

(a) If C is weakly intersective and $g \geq 3$ then, conditionally on ABC, as $X \to \infty$, the number of quadratic twists of C that violate the Hasse Principle is $\gg X$.

(b) If C is not weakly intersective, then as $X \to \infty$, the number of quadratic twists of C that violate the Hasse Principle is $o(X)$.

Thank You

References:

- 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.
- M. Sadek, *On quadratic twists of hypereliptic curves*. Rocky Mountain J. Math 44 (2014), 1015-1026
- J.-P. Serre *Divisibilité de certained fonctions arithmétiques*. Enseignement Math. (2) 22 (1976), 227–260.