Local solubility in families of superelliptic curves

Christopher Keyes (Emory University)

joint work with Lea Beneish (UC Berkeley)

https://arxiv.org/abs/2111.04697

University of Georgia
November 2, 2022

Motivation

Let C be a curve defined over $\mathbb{Q}$.

Definition

C is **soluble** if $C(\mathbb{Q})$ is nonempty.

Question (hard)

How often is a curve over $\mathbb{Q}$ (in some family) soluble?

For place v of $\mathbb{Q}$, we have

$$C(\mathbb{Q}) \subset C(\mathbb{Q}_v).$$

Thus existence of a $\mathbb{Q}_v$-point for each v is necessary but not sufficient for C to have $\mathbb{Q}$-point!

Local solubility

Let $C/\mathbb{Q}$ be a curve and v a place of $\mathbb{Q}$ (i.e. $v = p$ or $v = \infty$).

Definition

C is **locally soluble at v** if $C(\mathbb{Q}_v)$ is nonempty.

C is **everywhere locally soluble (ELS)** if $C(\mathbb{Q}_v) \neq \emptyset$ for all v.

Question (revised)

How often is a curve over $\mathbb{Q}$ (in some family) ELS?

Known for genus 1 curves [BCF21], plane cubics [BCF16], some families of hypersurfaces e.g. [BBL16], [FHP21], [PV04], [Bro17].

Motivation: hyperelliptic curves

Consider *hyperelliptic curves* given by (weighted) homog. equation

$$C\colon y^2 = f(x,z) = c_{2g+2}x^{2g+2} + \cdots + c_0 z^{2g+2}.$$

Theorem (Poonen–Stoll, Bhargava–Cremona–Fisher)

A pos. prop. of hyperelliptics $C/\mathbb{Q}$ are ELS [PS99b].

75.96% of genus 1 curves of this form are ELS [BCF21].

Theorem (Bhargava–Gross–Wang [BGW17])

A positive proportion of everywhere locally soluble hyperelliptic curves $C/\mathbb{Q}$ have no points over any odd degree extension $k/\mathbb{Q}$.

Superelliptic curves

Fix a positive integer $m \geq 2$.

Definition

A **superelliptic curve** $C/\mathbb{Q}$ is a smooth projective curve with a cyclic Galois cover of $\mathbb{P}^1$ of degree m.

Such C has an equation in weighted projective space

$$C\colon y^m = f(x,z) = c_d x^d + \cdots + c_0 z^d$$

where f is a binary form of degree d.

Warning

Some authors assume $m \mid d$ (or not!), or that f is m-th power free.

Defining the proportion

Question

How often is a superelliptic curve over $\mathbb{Q}$ ELS?

For $\mathbf{c} = (c_i)_{i=0}^d \in \mathbb{Z}^{d+1}$, we associate a binary form and SEC

$$f(x,z) = \sum_{i=0}^{d} c_i x^i z^{d-i}, \quad C_f\colon y^m = f(x,z).$$

Definition

We define

$$\rho_{m,d} = \lim_{B\to\infty} \frac{\#\{\mathbf{c} \in ([-B,B]\cap\mathbb{Z})^{d+1} \mid C_f \text{ is ELS}\}}{\#\{\mathbf{c} \in ([-B,B]\cap\mathbb{Z})^{d+1}\}},$$

the proportion of ELS superelliptic curves of this form.

Main results

Fix $(m, d) \neq (2, 2)$ such that $m \mid d$.

Theorem (Beneish–K. [BK21b])

(A) *$0 < \rho_{m,d} < 1$, and $\rho_{m,d}$ is product of local densities,*

$$\rho_{m,d} = \rho_{m,d}(\infty) \prod_p \rho_{m,d}(p).$$

Main results

Fix $(m, d) \neq (2, 2)$ such that m is prime and $m \mid d$.

Theorem (Beneish–K. [BK21b], continued)

(B) *We can find explicit (and sometimes good) bounds for $\rho_{m,d}(p)$ and hence $\rho_{m,d}$. In particular,*

$$\liminf_{d\to\infty} \rho_{m,d} \geq \left(1 - \frac{1}{m^{m+1}}\right) \prod_{p\equiv 1(m)} \left(1 - \left(1 - \frac{p-1}{mp}\right)^{p+1}\right) \prod_{p\not\equiv 0,1(m)} \left(1 - \frac{1}{p^{2(p+1)}}\right).$$

When $m > 2$, we have

$$0.83511 \leq \liminf_{d\to\infty} \rho_{m,d} \quad \text{and} \quad \limsup_{d\to\infty} \rho_{m,d} \leq 0.99804.$$

Main results

Theorem (Beneish–K. [BK21b], continued)

(C) *In the case* $(m, d) = (3, 6)$, *we compute* $\rho_{3,6} \approx 96.94\%$. *Moreover,* $\exists$ *rational functions* $R_1(t)$ *and* $R_2(t)$ *such that*

$$\rho_{3,6}(p) = \begin{cases} R_1(p), & p \equiv 1 \pmod 3 \text{ and } p > 43 \\ R_2(p), & p \equiv 2 \pmod 3 \text{ and } p > 2. \end{cases}$$

Asymptotically,

$$1 - R_1(t) \sim \frac{2}{3} t^{-4},$$
$$1 - R_2(t) \sim \frac{53}{144} t^{-7}.$$

$$\rho = \begin{cases} \Big(1296p^{57} + 3888p^{56} + 9072p^{55} + 16848p^{54} + 27648p^{53} + 39744p^{52} + 53136p^{51} + 66483p^{50} + 80019p^{49} + 93141p^{48} \\ + 107469p^{47} + 120357p^{46} + 135567p^{45} + 148347p^{44} + 162918p^{43} + 176004p^{42} + 190278p^{41} + 203459p^{40} \\ + 218272p^{39} + 232083p^{38} + 243639p^{37} + 255267p^{36} + 261719p^{35} + 264925p^{34} + 265302p^{33} + 261540p^{32} \\ + 254790p^{31} + 250736p^{30} + 241384p^{29} + 226503p^{28} + 214137p^{27} + 195273p^{26} + 170793p^{25} + 151839p^{24} + 136215p^{23} \\ + 118998p^{22} + 105228p^{21} + 94860p^{20} + 80471p^{19} + 67048p^{18} + 52623p^{17} + 40617p^{16} + 28773p^{15} + 19247p^{14} & p \equiv 1 \pmod 3 \\ + 12109p^{13} + 7614p^{12} + 3420p^{11} + 756p^{10} - 2248p^{9} - 4943p^{8} - 6300p^{7} - 6894p^{6} - 5994p^{5} - 2448p^{4} - 648p^{3} \\ + 324p^{2} + 1296p + 1296\Big) \Big/ \Big(1296\left(p^{12} - p^{11} + p^{9} - p^{8} + p^{6} - p^{4} + p^{3} - p + 1\right)\left(p^{8} - p^{6} + p^{4} - p^{2} + 1\right) \\ \times \left(p^{6} + p^{5} + p^{4} + p^{3} + p^{2} + p + 1\right)\left(p^{4} + p^{3} + p^{2} + p + 1\right)^{3}\left(p^{4} - p^{3} + p^{2} - p + 1\right)\left(p^{2} + p + 1\right) \\ \times \left(p^{2} + 1\right)p^{11}\Big), \\ \\ \Big(144p^{57} + 432p^{56} + 1008p^{55} + 1872p^{54} + 3168p^{53} + 4608p^{52} + 6336p^{51} + 8011p^{50} + 9803p^{49} + 11357p^{48} \\ + 13061p^{47} + 14525p^{46} + 16295p^{45} + 17875p^{44} + 19654p^{43} + 21212p^{42} + 23030p^{41} + 24563p^{40} + 26320p^{39} \\ + 27771p^{38} + 29711p^{37} + 30859p^{36} + 31135p^{35} + 31525p^{34} + 31510p^{33} + 29436p^{32} + 28502p^{31} + 28616p^{30} \\ + 26856p^{29} + 25087p^{28} + 25057p^{27} + 23041p^{26} + 19921p^{25} + 18119p^{24} + 16287p^{23} + 13798p^{22} \\ + 12140p^{21} + 10844p^{20} + 9191p^{19} + 7480p^{18} + 5839p^{17} + 4265p^{16} + 2909p^{15} + 1943p^{14} + 1109p^{13} & p \equiv 2 \pmod 3 \\ + 590p^{12} + 604p^{11} + 372p^{10} - 144p^{9} - 87p^{8} - 84p^{7} - 678p^{6} - 618p^{5} - 144p^{4} - 168p^{3} - 156p^{2} \\ + 144p + 144\Big) \Big/ \Big(144\left(p^{12} - p^{11} + p^{9} - p^{8} + p^{6} - p^{4} + p^{3} - p + 1\right)\left(p^{8} - p^{6} + p^{4} - p^{2} + 1\right) \\ \times \left(p^{6} + p^{5} + p^{4} + p^{3} + p^{2} + p + 1\right)\left(p^{4} + p^{3} + p^{2} + p + 1\right)^{3}\left(p^{4} - p^{3} + p^{2} - p + 1\right)\left(p^{2} + p + 1\right) \\ \times \left(p^{2} + 1\right)p^{11}\Big), \end{cases}$$

Outline

- Set up and state main results,
- Local densities $\rho_{m,d}(p) \to$ global density $\rho_{m,d}$,
- Study local densities $\rho_{m,d}(p)$,
- Sketch exact computations of $\rho_{3,6}(p)$.

Local densities

Theorem (Beneish–K. [BK21b])

(A) $\rho_{m,d}$ *exists and is given by the product of local densities,*

$$\rho_{m,d} = \rho_{m,d}(\infty) \prod_p \rho_{m,d}(p) > 0.$$

$\rho_{m,d}(p)$ is (normalized) Haar measure of space of the $\mathbb{Q}_p$-soluble curves $C_f\colon y^m = f(x,z)$, with coefficients in $\mathbb{Z}_p$.

Idea

In *good situations*, imposing conditions at different primes looks independent...*even if there are infinitely many conditions*.

Local densities look independent

Idea

In *good situations*, imposing conditions at different primes looks independent...*even if there are infinitely many conditions*.

Think

Recall squarefree numbers.

$$n \text{ squarefree} \iff p^2 \nmid n \text{ for all } p.$$

If probabilities that $p^2 \mid n$ are independent, expect

$$\mathrm{Prob}(n \text{ squarefree}) = \prod_p \left(1 - \frac{1}{p^2}\right) = \frac{1}{\zeta(2)} = \frac{6}{\pi^2}.$$

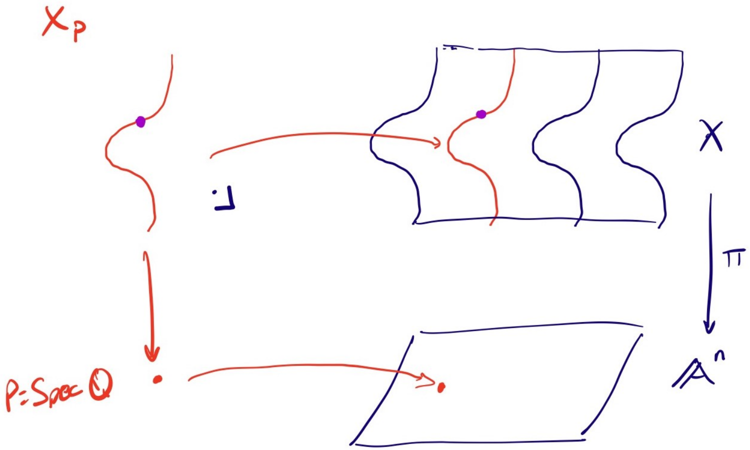
Local densities look independent

Idea

In *good situations*, imposing conditions at different primes looks independent...*even if there are infinitely many conditions*.

- Poonen–Stoll [PS99a] give criterion for when natural density is product of local densities.
- Apply to ELS in families of hyperelliptic curves [PS99b]; uses sieve of Ekedahl [Eke91].
- Bright–Browning–Loughran [BBL16] give *geometric criteria* when family comes from fibers of a morphism.

Geometric picture



A geometric criterion

Theorem (Bright–Browning–Loughran [BBL16])

Let $\pi\colon X \to \mathbb{A}^n$ *a dominant, quasiproj. morphism of* $\mathbb{Q}$*-varieties with geom. int. gen. fiber. Suppose*

(i) *fibers above each codim. 1 point of* $\mathbb{A}^n$ *are geom. integral,*

(ii) $X(\mathbf{A}_{\mathbb{Q}}) \neq \emptyset$,

(iii) *For all* $B \geq 1$ *we have* $B\pi(X(\mathbb{R})) \subseteq \pi(X(\mathbb{R}))$.

Let $\Psi' \subset \mathbb{R}^n$ *be a bounded subset of positive measure lying in* $\pi(X(\mathbb{R}))$ *whose boundary has measure zero. Then the limit*

$$\lim_{B\to\infty} \frac{\#\left\{P \in \mathbb{Z}^n \cap B\Psi' \mid X_P(\mathbf{A}_{\mathbb{Q}}) \neq \emptyset\right\}}{\#\left\{P \in \mathbb{Z}^n \cap B\Psi'\right\}}$$

exists, is nonzero, and is equal to a product of local densities,

$$\prod_{p\nmid\infty} \mu_p\left(\left\{P \in \mathbb{Z}_p^n \mid X_P(\mathbb{Q}_p) \neq \emptyset\right\}\right).$$

Geometric setup

We consider

$$\mathbb{A}_{\mathbb{Q}}^{d+1} = \operatorname{Spec} \mathbb{Q}[c_0, \ldots, c_d],$$
$$\mathcal{P}_{\mathbb{Q}} = \mathbb{P}_{\mathbb{Q}}(1, d, 1) \text{ with coordinates } [x : y : z].$$

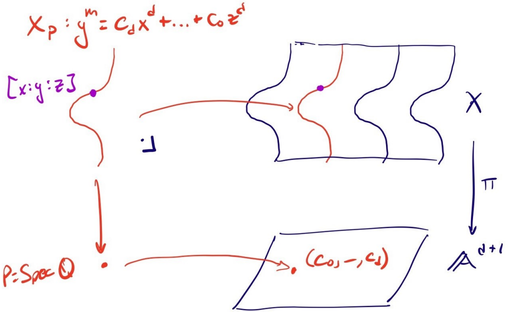
The variety

$$X \colon y^m = c_d x^d + \cdots + c_0 z^d \subset \mathbb{A}_{\mathbb{Q}}^{d+1} \times \mathcal{P}_{\mathbb{Q}}$$

comes with a projection map $\pi \colon X \to \mathbb{A}_{\mathbb{Q}}^{d+1}$.

Geometric picture

$$X\colon y^m = c_d x^d + \cdots + c_0 z^d \subset \mathbb{A}^{d+1}_{\mathbb{Q}} \times \mathcal{P}_{\mathbb{Q}}$$



Think

- A $\mathbb{Q}$-point $(\mathbf{c}, [x:y:z])$ of X is the data of superelliptic curve $C_f/\mathbb{Q}$ and a $\mathbb{Q}$-point $[x:y:z] \in C_f(\mathbb{Q})$.
- The fiber X_P of π over a point $P \in \mathbb{A}^{d+1}(\mathbb{Q})$ is a superelliptic curve $C_f/\mathbb{Q}$ whose coefficients are encoded in P.

Proof sketch of (A)

Check that π is dominant, projective, and has geom. int. gen. fiber.

(i) Codim. 1 points of $\mathbb{A}^{d+1}$ = single relation on coeffs c_i. Not enough to be reducible. (Unless $(m, d) = (2, 2)$!)

(ii) $X(\mathbb{Q}) \neq \emptyset$; e.g. $y^m = x^d + z^d$ has the point $[1:1:0]$.

(iii) $\pi(X(\mathbb{R}))$ closed under scaling by $B \geq 1$: C_f has a $\mathbb{R}$-point $\implies$ $C_{Bf}\colon y^m = Bf(x, z)$ has $\mathbb{R}$-point.

Finally, choose $\Psi' = [-1, 1]^{d+1} \cap \pi(X(\mathbb{R}))$ (verifying $\mu_\infty(\partial\Psi') = 0$), and see this agrees with original definition of $\rho_{m,d}$. $\square$

Outline

- Set up and state main results,
- Local densities $\rho_{m,d}(p) \to$ global density $\rho_{m,d}$,
- Bound local densities $\rho_{m,d}(p)$,
- Sketch exact computations of $\rho_{3,6}(p)$.

Computing local densities

Question

Once we know

$$\rho_{m,d} = \rho_{m,d}(\infty) \prod_p \rho_{m,d}(p),$$

how do we compute/estimate local densities $\rho_{m,d}(p)$?

$\rho_{m,d}(\infty)$: Euclidean measure of $\mathbb{R}$-soluble C_f with coeffs $\in [-1, 1]$.

- If m or d is odd, then $\rho_{m,d}(\infty) = 1$.
- If m, d even, no analytic solution known for $d > 2$, but rigorous estimates exist, e.g.

$$0.873914 \leq \rho_{2,4}(\infty) \leq 0.874196 \quad \text{[BCF21]}.$$

Computing local densities — finite places

$\rho_{m,d}(p)$ is (normalized) Haar measure of space of the $\mathbb{Q}_p$-soluble curves $C_f\colon y^m = f(x,z)$, *with coefficients in* $\mathbb{Z}_p$.

Think

Each possible reduction $\overline{f}(x,z)$ mod p occurs equally often.

Look mod p and check $\mathbb{Q}_p$-solubility with **Hensel's lemma**!

- Smooth $\mathbb{F}_p$-points on $\overline{C_f}$ lift to $\mathbb{Q}_p$-solutions (Hensel),
- $\overline{C_f}(\mathbb{F}_p) = \emptyset \implies$ no $\mathbb{Q}_p$-solutions,
- If $\overline{C_f}(\mathbb{F}_p)$ only non-smooth points, do more work.

An extended example

Example

Consider $(m, d) = (3, 6)$, family of genus 4 curves

$$C_f\colon y^3 = f(x,z) = c_6x^6 + c_5x^5z + \cdots + c_1xz^5 + c_0z^6.$$

When can we guarantee $\overline{C_f}$ has smooth $\mathbb{F}_p$-points?

Theorem (Hasse–Weil bound)

If $\overline{C_f}$ is irreducible and smooth of genus g, then

$$\#\overline{C_f}(\mathbb{F}_p) \geq p + 1 - g \cdot 2\sqrt{p}.$$

An extended example

Example

Consider $(m, d) = (3, 6)$, family of genus 4 curves

$$C_f \colon y^3 = f(x, z) = c_6 x^6 + c_5 x^5 z + \cdots + c_1 x z^5 + c_0 z^6.$$

When can we guarantee $\overline{C_f}$ has smooth $\mathbb{F}_p$-points?

Theorem (Hasse–Weil bound, refined)

If $\overline{C_f}$ is irreducible and smooth of genus g, then

$$\#\overline{C_f}(\mathbb{F}_p) \geq p + 1 - g \cdot \lfloor 2\sqrt{p} \rfloor.$$

An extended example

Whenever $p > 61$, we have

$$p + 1 - 8\sqrt{p} > 0,$$

so if $\overline{C_f}/\mathbb{F}_p$ is smooth for $p > 61$, C_f has $\mathbb{Q}_p$-point!

- $\overline{C_f}^{\mathrm{sm}}(\mathbb{F}_p) \neq \emptyset$ whenever $\overline{C_f}/\mathbb{F}_p$ geom. irr. and $p > 61$.
- Refinement of H–W $\implies$ $p \geq 61$ sufficient.
- Irreducibility over $\overline{\mathbb{F}_p}$ $\iff$ $\overline{f}(x, z) \neq ah(x, z)^3$.

$$\rho_{3,6}(p) \geq \frac{p^7 - p^3}{p^7} = 1 - \frac{1}{p^4} \text{ for all } p \geq 61.$$

An extended example — bounds for $p \equiv 2 \pmod 3$

Exploit fact that cubing map $\mathbb{F}_p^\times \xrightarrow{(\cdot)^3} \mathbb{F}_p^\times$ is an isomorphism.

Lemma

If $p > 2$ and $p \equiv 2 \pmod 3$ then C_f has a $\mathbb{Z}_p$-point whenever reduction $\overline{f}$ is nonzero.

What goes wrong? $\overline{f}(x, z)$ has multiple roots everywhere.

Example

If $p = 2$, could have $f(x, z) = x^2(x + z)^2 z^2$

An extended example

- $\rho_{3,6}(p) \geq 1 - \frac{1}{p^4}$ when $p \equiv 1 \pmod 3$ and $p > 43$
- $\rho_{3,6}(p) \geq 1 - \frac{1}{p^7}$ when $p \equiv 2 \pmod 3$ and $p > 2$
- Enumerate all $\overline{f}(x, z)$ and count Hensel-liftable $\mathbb{F}_p$-solutions:

p	$\rho_{3,6}(p) \geq$	p	$\rho_{3,6}(p) \geq$
2	$\frac{63}{64} \approx 0.98437$	19	$\frac{893660256}{893871739} \approx 0.99976$
3	$\frac{26}{27} \approx 0.96296$	31	$\frac{27512408250}{27512614111} \approx 0.99999$
7	$\frac{810658}{823543} \approx 0.98435$	37	$\frac{94931742132}{94931877133} \approx 0.999998$
13	$\frac{62655132}{62748517} \approx 0.99851$	43	$\frac{271818511748}{271818611107} \approx 0.9999996$

Put together with Theorem A:

$$\rho_{3,6} = \prod_p \rho_{3,6}(p) \geq 0.93134.$$

Bounds more generally for $m = 3$

Example (Lower bounds for general d)

For $d > 6$ such that $3 \mid d$,

$$\rho_{3,d} \geq \left(1 - \frac{1}{3^4}\right) \prod_{\substack{p\equiv 2(3)\\ p\leq d/2-1}} \left(1 - \frac{1}{p^{2(p+1)}}\right) \prod_{\substack{p\equiv 2(3)\\ p> d/2-1}} \left(1 - \frac{1}{p^{d+1}}\right)$$

$$\times \prod_{\substack{p\equiv 1(3)\\ p<d}} \left(1 - \left(1 - \frac{p-1}{3p}\right)^{p+1}\right) \prod_{\substack{p\equiv 1(3)\\ d<p<4(d-2)^2}} \left(1 - \left(1 - \frac{p-1}{3p}\right)^{d+1}\right) \prod_{\substack{p\equiv 1(3)\\ p\geq 4(d-2)^2}} \left(1 - \frac{1}{p^{\frac{2d}{3}}}\right)$$

Example (Large genus limit)

Taking limit as $d \to \infty$

$$\liminf_{d\to\infty} \rho_{3,d} \geq \left(1 - \frac{1}{3^4}\right) \prod_{p\equiv 1(3)} \left(1 - \left(1 - \frac{p-1}{3p}\right)^{p+1}\right) \prod_{p\equiv 2(3)} \left(1 - \frac{1}{p^{2(p+1)}}\right)$$

$$\approx 0.90061.$$

Outline

- Set up and state main results,
- Local densities $\rho_{m,d}(p) \to$ global density $\rho_{m,d}$,
- Bound local densities $\rho_{m,d}(p)$,
- Sketch exact computations of $\rho_{3,6}(p)$.

Getting exact answer

Question

How do we go from bounds to exact values for $\rho_{3,6}(p)$?

Let $F(x, y, z) = y^3 - f(x, z)$ and look at reduction modulo p.

Recall $\overline{F}$ irreducible/$\overline{\mathbb{F}_p} \iff f(x, z) \neq h(x, z)^3$ over $\overline{\mathbb{F}_p}$.

Factorization type in y	$p = 3$	$p \equiv 1 \pmod 3$	$p \equiv 2 \pmod 3$
1. Abs. irr.	2160	$p^3(p^4 - 1)$	$p^3(p^4 - 1)$
2. 3 distinct linear over $\mathbb{F}_p$	0	$\frac{1}{3}(p^3 - 1)$	0
3. Linear + conj.	0	0	$p^3 - 1$
4. 3 conjugate factors	0	$\frac{2}{3}(p^3 - 1)$	0
5. $(y - h(x, z))^3$	27	1	1
Total	3^7	p^7	p^7

Getting exact answer

Let ξ_i be the proportion of $\overline{f}$ for which $\overline{F}$ has type i.

Let σ_i be the probability that $F(x, y, z) = 0$ has $\mathbb{Z}_p$-solution when $\overline{F}$ has type i. Then

$$\rho_{3,6}(p) = \sum_{i=1}^{5} \xi_i(p)\sigma_i(p).$$

Proposition

We have

$$\sigma_1 = \sigma_2 = \sigma_3 = 1$$

for all primes $p \geq 61$ *and* $p \equiv 2 \pmod 3$ *except* $p = 2$.

Getting exact answer

Proposition

We have

$$\sigma_1 = \sigma_2 = \sigma_3 = 1$$

for all primes $p \geq 61$ *and* $p \equiv 2 \pmod 3$ *except* $p = 2$.

Proof. We (essentially) already did this! Use Hasse–Weil bound on all components, possibly avoiding desingularized points. □

To improve on previous bounds, we

- carefully analyze σ_4, σ_5 and
- deal with more delicate primes $p = 2, 3, 7, 13, 19, 31, 37, 43$.

An example: computing σ_5

Suppose $f(x,z) \equiv 0 \pmod{p}$, but $f(x,z) \not\equiv 0 \pmod{p^2}$.

Set $f(x,z) \equiv pf_1(x,z)$ for nonzero $f_1(x,z) \in \mathbb{F}_p[x,z]$.

Observation

$\mathbb{Z}_p$-solution to $C_f \colon y^3 = f(x,z)$ must have $p \mid y$,

$$p^3 \mid f(x,z) \implies p^2 \mid f_1(x,z).$$

(0) If $\overline{f_1}(x,z)$ has no roots modulo p, then C_f has no $\mathbb{Z}_p$-points.

(1) If $\overline{f_1}(x,z)$ has a root of mult. 1, it lifts to $\mathbb{Z}_p$-point of C_f.

(2) Suppose $\overline{f_1}(x,z)$ has a double root (and no other roots).

Dealing with the double root

Assume $x^2 \mid \overline{f_1}$, giving p-adic valuations below (original coeffs of f):

Prob. lift	$v(c_6)$	$v(c_5)$	$v(c_4)$	$v(c_3)$	$v(c_2)$	$v(c_1)$	$v(c_0)$
$\tau_2 = \tau_{2a} = \frac{1}{p}\tau_{2b}$	≥ 1	≥ 1	≥ 1	≥ 1	$= 1$	≥ 2	≥ 2
$\tau_{2b} = \tau_{2c}$	≥ 1	≥ 1	≥ 1	≥ 1	$= 1$	≥ 2	≥ 3
$\tau_{2c} = 1$	≥ 4	≥ 3	≥ 2	≥ 1	$= 0$	≥ 0	≥ 0

Probability of lifting $[0:0:1]$ in this case is

$$\tau_2 = \frac{1}{p} = \text{Prob}\left(p^3 \mid c_0 : p^2 \mid c_0 \text{ and } p \mid\mid c_2\right).$$

Computing σ_5

$$\sigma_5 = \left(1 - \frac{1}{p^7}\right) \sum_{i=0}^{9} \eta_i \tau_i + \left(\frac{1}{p^7} - \frac{1}{p^{14}}\right) \sum_{i=0}^{9} \eta_i \theta_i + \frac{1}{p^{14}} \rho$$

- Index i indicates factorization type of $f_1(x,z)$ (or $f_2(x,z)$)
- η_i = proportion of sextic forms/$\mathbb{F}_p$ with i-th type
- τ_i (resp. θ_i) are proportion of f with f_1 (resp. f_2) of type i such that C_f has a $\mathbb{Z}_p$-point.


AUG 16-17 2021
1st annual?
theta & tau
PALOOZA
When life give you sigmas and rhos,
make etas, thetas, and taus, with
subscripts that just can't be contained!
θ
τ

Factorization types

Fact. type	η_i	η_i' (monic forms only)
0. No roots	$\dfrac{\left(53p^4+26p^3+19p^2-2p+24\right)(p-1)p}{144\left(p^6+p^5+p^4+p^3+p^2+p+1\right)}$	$\dfrac{\left(53p^4+26p^3+19p^2-2p+24\right)(p-1)}{144p^5}$
1. $(1*)$	$\dfrac{\left(91p^4+26p^3+23p^2+16p-12\right)(p+1)p}{144\left(p^6+p^5+p^4+p^3+p^2+p+1\right)}$	$\dfrac{\left(91p^3-27p^2+50p-48\right)(p+1)(p-1)}{144p^5}$
2. (1^24) or (1^222)	$\dfrac{\left(3p^2+p+2\right)(p+1)(p-1)p}{8\left(p^6+p^5+p^4+p^3+p^2+p+1\right)}$	$\dfrac{\left(3p^2+p+2\right)(p-1)}{8p^4}$
3. (1^21^22)	$\dfrac{(p+1)(p-1)p^2}{4\left(p^6+p^5+p^4+p^3+p^2+p+1\right)}$	$\dfrac{(p-1)^2}{4p^4}$
4. $(1^21^21^2)$	$\dfrac{(p+1)(p-1)p}{6\left(p^6+p^5+p^4+p^3+p^2+p+1\right)}$	$\dfrac{(p-1)(p-2)}{6p^5}$
5. (1^33)	$\dfrac{(p+1)^2(p-1)p}{3\left(p^6+p^5+p^4+p^3+p^2+p+1\right)}$	$\dfrac{(p+1)(p-1)}{3p^4}$
6. (1^31^3)	$\dfrac{(p+1)p}{2\left(p^6+p^5+p^4+p^3+p^2+p+1\right)}$	$\dfrac{p-1}{2p^5}$
7. (1^42)	$\dfrac{(p+1)(p-1)p}{2\left(p^6+p^5+p^4+p^3+p^2+p+1\right)}$	$\dfrac{p-1}{2p^4}$
8. (1^21^4)	$\dfrac{(p+1)p}{p^6+p^5+p^4+p^3+p^2+p+1}$	$\dfrac{p-1}{p^5}$
9. (1^6)	$\dfrac{p+1}{p^6+p^5+p^4+p^3+p^2+p+1}$	$\dfrac{1}{p^5}$

Type 9: yikes!

Type 9, e.g. $f(x,z) \equiv px^6 \pmod{p^2}$.

τ_9 is a degree 44 rational function in p.

$$
\begin{aligned}
\tau_9 = \quad \tau_{9a} &= \tfrac{1}{p}\tau_{9b} \\
\tau_{9b} &= \left(1-\tfrac{1}{p}\right) + \tfrac{1}{p}\tau_{9c} \\
\tau_{9c} &= \Phi(p) + \tfrac{1}{p}\tau_{9d} \\
\tau_{9d} &= \left(1-\tfrac{1}{p}\right)\left(\tfrac{p-1}{2p} + \tfrac{1}{p^2}\right) + \tfrac{1}{p}\tau_{9e} \\
\tau_{9e} &= \left(1-\tfrac{1}{p}\right) + \tfrac{1}{p}\tau_{9f} \\
\tau_{9f} &= \tfrac{1}{p}\tau_{9g} \\
\tau_{9g} &= \left(1-\tfrac{1}{p}\right)\alpha'' + \tfrac{1}{p}\tau_{9h} \\
\tau_{9h} &= \left(1-\tfrac{1}{p}\right)\left(\tfrac{p-1}{2p} + \tfrac{\theta_2}{p}\right) + \tfrac{1}{p}\tau_{9i} \\
\tau_{9i} &= \left(1-\tfrac{1}{p}\right) + \tfrac{1}{p}\tau_{9j} \\
\tau_{9j} &= \tfrac{1}{p}\tau_{9k} \\
\tau_{9k} &= \left(1-\tfrac{1}{p}\right) + \tfrac{1}{p}\tau_{9\ell} \\
\tau_{9\ell} &= \Phi(p) + \left(1-\Phi(p)-\tfrac{1}{p}\right)\beta + \tfrac{1}{p}\tau_{9m} \\
\tau_{9m} &= \left(1-\tfrac{1}{p}\right) + \tfrac{1}{p}\tau_{9n} \\
\tau_{9n} &= \left(1-\tfrac{1}{p}\right) + \tfrac{1}{p}\tau_{9o} \\
\tau_{9o} &= \Phi(p) + \tfrac{1}{p}\tau_{9p} \\
\tau_{9p} &= \sigma_5'
\end{aligned}
$$

c_6	c_5	c_4	c_3	c_2	c_1	c_0
$=1$	≥ 2	≥ 2	≥ 2	≥ 2	≥ 2	≥ 2
$=4$	≥ 4	≥ 3	≥ 2	≥ 1	≥ 0	≥ 0
$=4$	≥ 4	≥ 3	≥ 2	≥ 1	≥ 1	≥ 0
$=4$	≥ 4	≥ 3	≥ 2	≥ 1	≥ 1	≥ 1
$=4$	≥ 4	≥ 3	≥ 2	≥ 2	≥ 1	≥ 1
$=4$	≥ 4	≥ 3	≥ 2	≥ 2	≥ 2	≥ 1
$=4$	≥ 4	≥ 3	≥ 2	≥ 2	≥ 2	≥ 2
$=4$	≥ 4	≥ 3	≥ 3	≥ 2	≥ 2	≥ 2
$=4$	≥ 4	≥ 3	≥ 3	≥ 3	≥ 2	≥ 2
$=4$	≥ 4	≥ 3	≥ 3	≥ 3	≥ 3	≥ 2
$=1$	≥ 1	≥ 0	≥ 0	≥ 0	≥ 0	≥ 0
$=1$	≥ 1	≥ 1	≥ 0	≥ 0	≥ 0	≥ 0
$=1$	≥ 1	≥ 1	≥ 1	≥ 0	≥ 0	≥ 0
$=1$	≥ 1	≥ 1	≥ 1	≥ 1	≥ 0	≥ 0
$=1$	≥ 1	≥ 1	≥ 1	≥ 1	≥ 1	≥ 0
$=1$	≥ 1	≥ 1	≥ 1	≥ 1	≥ 1	≥ 1

What is $\rho_{3,6}(p)$?

$$\rho = \begin{cases} \Big(1296p^{57} + 3888p^{56} + 9072p^{55} + 16848p^{54} + 27648p^{53} + 39744p^{52} + 53136p^{51} + 66483p^{50} + 80019p^{49} + 93141p^{48} \\ + 107469p^{47} + 120357p^{46} + 135567p^{45} + 148347p^{44} + 162918p^{43} + 176004p^{42} + 190278p^{41} + 203459p^{40} \\ + 218272p^{39} + 232083p^{38} + 243639p^{37} + 255267p^{36} + 261719p^{35} + 264925p^{34} + 265302p^{33} + 261540p^{32} \\ + 254790p^{31} + 250736p^{30} + 241384p^{29} + 226503p^{28} + 214137p^{27} + 195273p^{26} + 170793p^{25} + 151839p^{24} + 136215p^{23} \\ + 118998p^{22} + 105228p^{21} + 94860p^{20} + 80471p^{19} + 67048p^{18} + 52623p^{17} + 40617p^{16} + 28773p^{15} + 19247p^{14} & p \equiv 1 \pmod 3 \\ + 12109p^{13} + 7614p^{12} + 3420p^{11} + 756p^{10} - 2248p^{9} - 4943p^{8} - 6300p^{7} - 6894p^{6} - 5994p^{5} - 2448p^{4} - 648p^{3} \\ + 324p^{2} + 1296p + 1296\Big) \Big/ \Big(1296\left(p^{12} - p^{11} + p^{9} - p^{8} + p^{6} - p^{4} + p^{3} - p + 1\right)\left(p^{8} - p^{6} + p^{4} - p^{2} + 1\right) \\ \times \left(p^{6} + p^{5} + p^{4} + p^{3} + p^{2} + p + 1\right)\left(p^{4} + p^{3} + p^{2} + p + 1\right)^{3}\left(p^{4} - p^{3} + p^{2} - p + 1\right)\left(p^{2} + p + 1\right) \\ \times \left(p^{2} + 1\right)p^{11}\Big), \\ \\ \Big(144p^{57} + 432p^{56} + 1008p^{55} + 1872p^{54} + 3168p^{53} + 4608p^{52} + 6336p^{51} + 8011p^{50} + 9803p^{49} + 11357p^{48} \\ + 13061p^{47} + 14525p^{46} + 16295p^{45} + 17875p^{44} + 19654p^{43} + 21212p^{42} + 23030p^{41} + 24563p^{40} + 26320p^{39} \\ + 27771p^{38} + 29711p^{37} + 30859p^{36} + 31135p^{35} + 31525p^{34} + 31510p^{33} + 29436p^{32} + 28502p^{31} + 28616p^{30} \\ + 26856p^{29} + 25087p^{28} + 25057p^{27} + 23041p^{26} + 19921p^{25} + 18119p^{24} + 16287p^{23} + 13798p^{22} \\ + 12140p^{21} + 10844p^{20} + 9191p^{19} + 7480p^{18} + 5839p^{17} + 4265p^{16} + 2909p^{15} + 1943p^{14} + 1109p^{13} & p \equiv 2 \pmod 3 \\ + 590p^{12} + 604p^{11} + 372p^{10} - 144p^{9} - 87p^{8} - 84p^{7} - 678p^{6} - 618p^{5} - 144p^{4} - 168p^{3} - 156p^{2} \\ + 144p + 144\Big) \Big/ \Big(144\left(p^{12} - p^{11} + p^{9} - p^{8} + p^{6} - p^{4} + p^{3} - p + 1\right)\left(p^{8} - p^{6} + p^{4} - p^{2} + 1\right) \\ \times \left(p^{6} + p^{5} + p^{4} + p^{3} + p^{2} + p + 1\right)\left(p^{4} + p^{3} + p^{2} + p + 1\right)^{3}\left(p^{4} - p^{3} + p^{2} - p + 1\right)\left(p^{2} + p + 1\right) \\ \times \left(p^{2} + 1\right)p^{11}\Big), \end{cases}$$

What is $\rho_{3,6}(p)$? Small primes edition

$$\rho(2) = \frac{4594897725819217081}{4616483254090301440\!0} \approx 0.99532$$

$$\rho(3) = \frac{900175334869743731875930997281}{908381960435133191895132960000} \approx 0.99096$$

$$\rho(7) = \frac{631044947551786228516032926231872770547437301836456778939 72}{640831747872066968824299456558012815388441498964001598153 75} \approx 0.98472$$

$$\rho(13) = \frac{787772835724457741402590193129674740968207625566652698451527352682285 3}{789064357062010674777673729279278062351072702642077953989377239970147 5} \approx 0.99836$$

$$\rho(19) = \frac{3122673715489206150449285868243361150392235799365815266879438393279346795671}{3123410013311365155035964479837966797560851333614271490136481337080636454180} \approx 0.99976$$

$$\rho(31) = \frac{919679645767831886913908993678646214653521003983285045429787748202063507385715975829 9}{919686506158784354483098904147380879891312858742599564585782857261091843603583390725 0} \approx 0.999992$$

$$\rho(37) = \frac{1711286479008201947844581017879529201699244648865190554538446471541848050364474766403457351 19}{1711288896361570605368944741870170884642712365099771994912089394497381276586797237155889445 00} \approx 0.999998$$

$$\rho(43) = \frac{8400012134328309038865335643180410070733136477929066449054710576886784486271213444783272050875028 1}{8400015167151355519164771256759610171080084620911683056801372937740499115090197310509303993923750 0} \approx 0.9999996$$

Use `Magma` to help when Hasse–Weil doesn't apply, modify calculations accordingly.

What is $\rho_{3,6}$?

Theorem (Beneish-K.)

(C) *We have determined $\rho_{3,6}(p)$ exactly for all p.*

Taking product over $p \leq 10000$ gives

$$\rho_{3,6} \approx \prod_{p \leq 10000} \rho_{3,6}(p) = 0.96943,$$

with error of $O(10^{-14})$.

97% of superelliptic curves $y^3 = c_6x^6 + \ldots + c_0z^6$ are ELS.

Further questions

Question

What proportion of superelliptic curves $C_f\colon y^m = f(x,z)$

- *are globally soluble?*
- *satisfy/fail the Hasse principle?*
- *satisfy/fail weak approximation?*
- *have some/no points of certain higher degrees?*

Preliminary results [BK21a, Prop. 7.2] give conditions for which pos. prop. of SECs have finitely many points of certain degrees.

Study these/other solubility questions for more families. Can methods be adapted to integral pts. on stacky curves (see [BP20])?

Thank you I

Thank you for the invitation and for your attention!

M. J. Bright, T. D. Browning, and D. Loughran, Failures of weak approximation in families, Compos. Math. **152** (2016), no. 7, 1435–1475. MR 3530447

Manjul Bhargava, John Cremona, and Tom Fisher, The proportion of plane cubic curves over $\mathbb{Q}$ that everywhere locally have a point, Int. J. Number Theory **12** (2016), no. 4, 1077–1092. MR 3484299

______, The proportion of genus one curves over $\mathbb{Q}$ defined by a binary quartic that everywhere locally have a point, Int. J. Number Theory **17** (2021), no. 4, 903–923. MR 4262272

Manjul Bhargava, Benedict H. Gross, and Xiaoheng Wang, A positive proportion of locally soluble hyperelliptic curves over $\mathbb{Q}$ have no point over any odd degree extension, J. Amer. Math. Soc. **30** (2017), no. 2, 451–493, With an appendix by Tim Dokchitser and Vladimir Dokchitser. MR 3600041

Lea Beneish and Christopher Keyes, Fields generated by points on superelliptic curves, 2021.

______, On the proportion of locally soluble superelliptic curves, Accepted for publication in *Finite Fields and Their Applications*. Preprint available at: https://arxiv.org/abs/2111.04697, 2021.

Manjul Bhargava and Bjorn Poonen, The local-global principle for integral points on stacky curves, https://arxiv.org/abs/2006.00167, 2020.

T. D. Browning, Many cubic surfaces contain rational points, Mathematika **63** (2017), no. 3, 818–839. MR 3731306

Thank you II

Torsten Ekedahl, An infinite version of the Chinese remainder theorem, Comment. Math. Univ. St. Paul. **40** (1991), no. 1, 53–59. MR 1104780

Tom Fisher, Wei Ho, and Jennifer Park, Everywhere local solubility for hypersurfaces in products of projective spaces, Res. Number Theory **7** (2021), no. 1, Paper No. 6, 27. MR 4199457

Bjorn Poonen and Michael Stoll, The Cassels-Tate pairing on polarized abelian varieties, Ann. of Math. (2) **150** (1999), no. 3, 1109–1149. MR 1740984

______, A local-global principle for densities, Topics in number theory (University Park, PA, 1997), Math. Appl., vol. 467, Kluwer Acad. Publ., Dordrecht, 1999, pp. 241–244. MR 1691323

Bjorn Poonen and José Felipe Voloch, Random Diophantine equations, Arithmetic of higher-dimensional algebraic varieties (Palo Alto, CA, 2002), Progr. Math., vol. 226, Birkhäuser Boston, Boston, MA, 2004, With appendices by Jean-Louis Colliot-Thélène and Nicholas M. Katz, pp. 175–184. MR 2029869