Curves with prescribed rational points

Katerina Santicola

University of Warwick

Representation Theory XVIII Dubrovnik

23rd June 2023

Where it all began

Let

$$\mathcal{P}_{\mathbb{Z}} = \{\alpha^n \ : \ \alpha \in \mathbb{Z}, \quad n \geq 2\}$$

be the set of perfect powers in $\mathbb{Z}$.

What perfect powers can $f(X) = X^3 + 1$ hit?
Or: what is $f(\mathbb{Z}) \cap \mathcal{P}_{\mathbb{Z}}$?

- solutions to $X^3 + 1 = Y^n$
- Mihăilescu (2005): only

$$2^3 + 1 = 3^2, 0^3 + 1 = 1^2, (-1)^3 + 1 = 0^2$$

- so $f(\mathbb{Z}) \cap \mathcal{P}_{\mathbb{Z}} = \{0, 1, 3^2\}$

Where it all began

Let

$$\mathcal{P}_{\mathbb{Z}} = \{\alpha^n : \alpha \in \mathbb{Z}, \quad n \geq 2\}$$

be the set of perfect powers in $\mathbb{Z}$.

What perfect powers can $f(X) = X^3 + 1$ hit?
Or: what is $f(\mathbb{Z}) \cap \mathcal{P}_{\mathbb{Z}}$?

- solutions to $X^3 + 1 = Y^n$
- Mihăilescu (2005): only

$$2^3 + 1 = 3^2, 0^3 + 1 = 1^2, (-1)^3 + 1 = 0^2$$

- so $f(\mathbb{Z}) \cap \mathcal{P}_{\mathbb{Z}} = \{0, 1, 3^2\}$

Where it all began

Let

$$\mathcal{P}_{\mathbb{Z}} = \{\alpha^n : \alpha \in \mathbb{Z}, \quad n \geq 2\}$$

be the set of perfect powers in $\mathbb{Z}$.

What perfect powers can $f(X) = X^3 + 1$ hit?
Or: what is $f(\mathbb{Z}) \cap \mathcal{P}_{\mathbb{Z}}$?

- solutions to $X^3 + 1 = Y^n$
- Mihăilescu (2005): only

$$2^3 + 1 = 3^2, 0^3 + 1 = 1^2, (-1)^3 + 1 = 0^2$$

- so $f(\mathbb{Z}) \cap \mathcal{P}_{\mathbb{Z}} = \{0, 1, 3^2\}$

Where it all began

Let

$$\mathcal{P}_{\mathbb{Z}} = \{\alpha^n : \alpha \in \mathbb{Z}, \quad n \geq 2\}$$

be the set of perfect powers in $\mathbb{Z}$.

What perfect powers can $f(X) = X^3 + 1$ hit?
Or: what is $f(\mathbb{Z}) \cap \mathcal{P}_{\mathbb{Z}}$?

- solutions to $X^3 + 1 = Y^n$
- Mihăilescu (2005): only

$$2^3 + 1 = 3^2, 0^3 + 1 = 1^2, (-1)^3 + 1 = 0^2$$

- so $f(\mathbb{Z}) \cap \mathcal{P}_{\mathbb{Z}} = \{0, 1, 3^2\}$

Where it all began

Let

$$\mathcal{P}_{\mathbb{Z}} = \{\alpha^n : \alpha \in \mathbb{Z}, \quad n \geq 2\}$$

be the set of perfect powers in $\mathbb{Z}$.

What perfect powers can $f(X) = X^3 + 1$ hit?
Or: what is $f(\mathbb{Z}) \cap \mathcal{P}_{\mathbb{Z}}$?

- solutions to $X^3 + 1 = Y^n$
- Mihăilescu (2005): only

$$2^3 + 1 = 3^2, 0^3 + 1 = 1^2, (-1)^3 + 1 = 0^2$$

- so $f(\mathbb{Z}) \cap \mathcal{P}_{\mathbb{Z}} = \{0, 1, 3^2\}$

The original question

- At the recent "Rational Points" conference (Schney, April 2022), Samir Siksek asked:

Question

Let S be a finite subset of $\mathcal{P}_{\mathbb{Z}}$. Is there a polynomial $f_S \in \mathbb{Z}[X]$ such that

$$f_S(\mathbb{Z}) \cap \mathcal{P}_{\mathbb{Z}} = S$$

- Gajović (2022): answered this affirmatively for $\mathbb{Z}$
- S. (2022): show his method can be extended to $\mathbb{Q}$

The original question

- At the recent "Rational Points" conference (Schney, April 2022), Samir Siksek asked:

Question

Let S be a finite subset of $\mathcal{P}_{\mathbb{Z}}$. Is there a polynomial $f_S \in \mathbb{Z}[X]$ such that

$$f_S(\mathbb{Z}) \cap \mathcal{P}_{\mathbb{Z}} = S$$

- Gajović (2022): answered this affirmatively for $\mathbb{Z}$
- S. (2022): show his method can be extended to $\mathbb{Q}$

A temporary deviation

Question

Let S be a finite subset of $\mathcal{O}_K$. Is there a polynomial $f_S \in \mathcal{O}_K[X]$ such that

$$f_S(\mathcal{O}_K) \cap \mathcal{P}_{\mathcal{O}_K} = S$$

- this question is much harder over number fields!
- assuming Serre's Uniformity Conjecture: can answer in the affirmative for totally real fields?

A temporary deviation

Question

Let S be a finite subset of $\mathcal{O}_K$. Is there a polynomial $f_S \in \mathcal{O}_K[X]$ such that

$$f_S(\mathcal{O}_K) \cap \mathcal{P}_{\mathcal{O}_K} = S$$

- this question is much harder over number fields!
- assuming Serre's Uniformity Conjecture: can answer in the affirmative for totally real fields?

Hmm, this looks a lot like...

- start with a set $S \subset \mathcal{P}_{\mathbb{Q}}$
- construct a polynomial $f_S(X)$ such that if $f_S(x) = y^m$, then $y^m \in S$
- the equation $y^n = f_S(X)$ looks like a superelliptic curve!

Hmm, this looks a lot like...

- start with a set $S \subset \mathcal{P}_{\mathbb{Q}}$
- construct a polynomial $f_S(X)$ such that if $f_S(x) = y^m$, then $y^m \in S$
- the equation $y^n = f_S(X)$ looks like a superelliptic curve!

Hmm, this looks a lot like...

- start with a set $S \subset \mathcal{P}_{\mathbb{Q}}$
- construct a polynomial $f_S(X)$ such that if $f_S(x) = y^m$, then $y^m \in S$
- the equation $y^n = f_S(X)$ looks like a superelliptic curve!

Falting's Theorem

- let $C/\mathbb{Q}$ be a nonsingular curve of genus $g \geq 2$
- $C(\mathbb{Q}) = C_{\text{aff}}(\mathbb{Q})$ + points at ∞
- **Falting's Theorem**: $C(\mathbb{Q})$ is finite
- no effective results for computing $C(\mathbb{Q})$, but possible sometimes (e.g. Chabauty)
- *converse of Falting's:*

given a finite set $S \subseteq \mathbb{P}^2(\mathbb{Q})$, does there exist $C/\mathbb{Q}$ such that $C(\mathbb{Q}) = S$?

Falting's Theorem

- let $C/\mathbb{Q}$ be a nonsingular curve of genus $g \geq 2$
- $C(\mathbb{Q}) = C_{\mathrm{aff}}(\mathbb{Q})$ + points at ∞
- **Falting's Theorem**: $C(\mathbb{Q})$ is finite
- no effective results for computing $C(\mathbb{Q})$, but possible sometimes (e.g. Chabauty)
- *converse of Falting's:*

  given a finite set $S \subseteq \mathbb{P}^2(\mathbb{Q})$, does there exist $C/\mathbb{Q}$ such that $C(\mathbb{Q}) = S$?

Falting's Theorem

- let $C/\mathbb{Q}$ be a nonsingular curve of genus $g \geq 2$
- $C(\mathbb{Q}) = C_{\text{aff}}(\mathbb{Q})$ + points at ∞
- **Falting's Theorem**: $C(\mathbb{Q})$ is finite
- no effective results for computing $C(\mathbb{Q})$, but possible sometimes (e.g. Chabauty)
- *converse of Falting's:*

  given a finite set $S \subseteq \mathbb{P}^2(\mathbb{Q})$, does there exist $C/\mathbb{Q}$ such that $C(\mathbb{Q}) = S$?

Falting's Theorem

- let $C/\mathbb{Q}$ be a nonsingular curve of genus $g \geq 2$
- $C(\mathbb{Q}) = C_{\text{aff}}(\mathbb{Q})$ + points at ∞
- **Falting's Theorem**: $C(\mathbb{Q})$ is finite
- no effective results for computing $C(\mathbb{Q})$, but possible sometimes (e.g. Chabauty)
- *converse of Falting's:*

  given a finite set $S \subseteq \mathbb{P}^2(\mathbb{Q})$, does there exist $C/\mathbb{Q}$ such that $C(\mathbb{Q}) = S$?

Superelliptic Curves

By a *superelliptic curve* we mean a smooth projective curve associated to

$$C:\ y^m = f(x)$$

where f is separable of degree $d \geq 3$ and $m \geq 2$ is an integer.

- $m = 2$ and $d = 3$: elliptic curves
- $m = 2$ and $d \geq 5$: hyperelliptic curves
- $m = d$ and $d \geq 4$: the genus g is

$$g = (d-1)(d-2)/2 \geq 2$$

and so $C(\mathbb{Q})$ is finite by Falting's

Superelliptic Curves

By a *superelliptic curve* we mean a smooth projective curve associated to

$$C: \; y^m = f(x)$$

where f is separable of degree $d \geq 3$ and $m \geq 2$ is an integer.

- $m = 2$ and $d = 3$: elliptic curves
- $m = 2$ and $d \geq 5$: hyperelliptic curves
- $m = d$ and $d \geq 4$: the genus g is

  $$g = (d-1)(d-2)/2 \geq 2$$

  and so $C(\mathbb{Q})$ is finite by Falting's

Main result

Let $S = \{(a_1, b_1), \ldots, (a_r, b_r)\} \subset \mathbb{Q}^2$ such that:

- if $(a_i, b_i), (a_j, b_j) \in S$ and $a_i = a_j$ then $b_i = b_j$
- $a_i \neq a_j$ if $i \neq j$.

We call such a set an *acceptable* set.

Theorem

Given an acceptable set $S \subseteq \mathbb{Q}^2$, there exists a separable polynomial $f_S(x) \in \mathbb{Q}[x]$ of degree d, such that $C_{aff}(\mathbb{Q}) = S$, where

$$C : y^d = f_S(x)$$

Moreover, C has no rational points at infinity.

Main result

Let $S = \{(a_1, b_1), \ldots, (a_r, b_r)\} \subset \mathbb{Q}^2$ such that:

- if $(a_i, b_i), (a_j, b_j) \in S$ and $a_i = a_j$ then $b_i = b_j$
- $a_i \neq a_j$ if $i \neq j$.

We call such a set an *acceptable* set.

Theorem

Given an acceptable set $S \subseteq \mathbb{Q}^2$, there exists a separable polynomial $f_S(x) \in \mathbb{Q}[x]$ of degree d, such that $C_{aff}(\mathbb{Q}) = S$, where

$$C : y^d = f_S(x)$$

Moreover, C has no rational points at infinity.

Separability

- want: a separable polynomial such that $h(a_i) = b_i^d$ for all $(a_i, b_i) \in S$
- Lagrange interpolation polynomial $L(X)$: not necessarily separable
- if $S = \{(0,0), (1,1), (2,4)\}$ then $L(X) = X^2$
- consider
$$h(X) = X^2 + X(X-1)(X-2)c(X)$$
can we construct $c(X)$ so that $h(X)$ is separable?

Separability

- want: a separable polynomial such that $h(a_i) = b_i^d$ for all $(a_i, b_i) \in S$
- Lagrange interpolation polynomial $L(X)$: not necessarily separable
- if $S = \{(0,0), (1,1), (2,4)\}$ then $L(X) = X^2$
- consider
$$h(X) = X^2 + X(X-1)(X-2)c(X)$$
can we construct $c(X)$ so that $h(X)$ is separable?

Separability

- want: a separable polynomial such that $h(a_i) = b_i^d$ for all $(a_i, b_i) \in S$
- Lagrange interpolation polynomial $L(X)$: not necessarily separable
- if $S = \{(0,0),(1,1),(2,4)\}$ then $L(X) = X^2$
- consider
$$h(X) = X^2 + X(X-1)(X-2)c(X)$$
can we construct $c(X)$ so that $h(X)$ is separable?

Separability

- want: a separable polynomial such that $h(a_i) = b_i^d$ for all $(a_i, b_i) \in S$
- Lagrange interpolation polynomial $L(X)$: not necessarily separable
- if $S = \{(0,0),(1,1),(2,4)\}$ then $L(X) = X^2$
- consider
$$h(X) = X^2 + X(X-1)(X-2)c(X)$$
can we construct $c(X)$ so that $h(X)$ is separable?

Dirichlet's theorem for polynomial rings

Theorem (Bary-Soroker)

Let $a(X), b(X) \in \mathbb{Q}[X]$ be relatively prime. For every

$$n > 2\max\{\deg a(X), \deg b(X) + 2\} + 4$$

there exists $c(X) \in \mathbb{Q}[X]$ for which

$$f(X, Y) = a(X) + b(X)c(X)Y$$

is irreducible in $\mathbb{Q}(Y)[X]$ of degree n in X and $Gal(f(X,Y), \mathbb{Q}(Y)) \cong S_n$.

With this theorem we construct $h(X)$ such that:

- $h(a_i) = b_i^d$
- $h(X)$ is separable modulo a prime ℓ

Dirichlet's theorem for polynomial rings

Theorem (Bary-Soroker)

Let $a(X), b(X) \in \mathbb{Q}[X]$ be relatively prime. For every

$$n > 2\max\{\deg a(X), \deg b(X) + 2\} + 4$$

there exists $c(X) \in \mathbb{Q}[X]$ for which

$$f(X,Y) = a(X) + b(X)c(X)Y$$

is irreducible in $\mathbb{Q}(Y)[X]$ of degree n in X and $Gal(f(X,Y), \mathbb{Q}(Y)) \cong S_n$.

With this theorem we construct $h(X)$ such that:

- $h(a_i) = b_i^d$
- $h(X)$ is separable modulo a prime ℓ

Main construction

Now define the polynomial

$$g(X) = \ell q^k \prod (X - a_i)^k + 1$$

Then our curve is given by

$$C : y^d = f_S(X)$$

where

$$f_S(X) = g(X)((h(X) - 1)g(X) + 1)$$

Main construction

Now define the polynomial

$$g(X) = \ell q^k \prod (X - a_i)^k + 1$$

Then our curve is given by

$$C : y^d = f_S(X)$$

where

$$f_S(X) = g(X)((h(X) - 1)g(X) + 1)$$

Main construction

We have

$$f_S(a_i) = h(a_i) = b_i^d$$

and $f_S(X)$ is separable (by separability of $h(X)$ and Eisenstein's criterion)

We prove:

if $f_S(x) = y^d$ for some rational $y \in \mathbb{Q} \Rightarrow (x, y) \in S$

which proves that $C(\mathbb{Q}) = S$ (no rational points at infinity: leading coefficient is not a d^{th} power)

Main construction

We have

$$f_S(a_i) = h(a_i) = b_i^d$$

and $f_S(X)$ is separable (by separability of $h(X)$ and Eisenstein's criterion)

We prove:

$$\text{if } f_S(x) = y^d \text{ for some rational } y \in \mathbb{Q} \Rightarrow (x, y) \in S$$

which proves that $C(\mathbb{Q}) = S$ (no rational points at infinity: leading coefficient is not a d^{th} power)

Where does Falting's come in?

Theorem (Darmon and Granville)

If A, B, C, p, q, r are fixed positive integers with

$$\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1$$

then the equation

$$Ax^p + By^q = Cz^r$$

has at most finitely many solutions in coprime non-zero integers x, y, z.

Proof: application of Falting's theorem

Where does Falting's come in?

Recall we define

$$g(X) = \ell q^k \prod (X - a_i)^k + 1$$

Where does this "q" come from? We consider the four equations

$$\ell x^6 + y^6 = 2^i \ell^j z^3, \qquad i, j \in \{0, 1\}$$

and we choose $q \neq xyz$ for all solutions (x, y, z), finitely many by Darmon and Granville

Where does Falting's come in?

Recall we define

$$g(X) = \ell q^k \prod (X - a_i)^k + 1$$

Where does this "q" come from? We consider the four equations

$$\ell x^6 + y^6 = 2^i \ell^j z^3, \qquad i, j \in \{0, 1\}$$

and we choose $q \neq xyz$ for all solutions (x, y, z), finitely many by Darmon and Granville

Example

Let S be the set of points

$$S = \{(0,2),(1,3),(2,6),(-1,1)\}$$

Example

Let S be the set of points

$$S = \{(0,2),(1,3),(2,6),(-1,1)\}$$

we compute $r = 4$, $d = 3 \cdot 17$ and $k = 6$,

Example

Let S be the set of points

$$S = \{(0,2),(1,3),(2,6),(-1,1)\}$$

we compute $r = 4$, $d = 3 \cdot 17$ and $k = 6$, and Lagrange interpolation polynomial is:

$$h(x) = \frac{1}{3}x^3 + \frac{2}{3}x + 2$$

Example

Let S be the set of points

$$S = \{(0,2),(1,3),(2,6),(-1,1)\}$$

we compute $r = 4$, $d = 3 \cdot 17$ and $k = 6$, and Lagrange interpolation polynomial is:

$$h(x) = \frac{1}{3}x^3 + \frac{2}{3}x + 2$$

irreducible modulo $\ell = 5$, so consider

$$5x^6 + y^6 = 2^i 5^j z^3, \qquad i,j \in \{0,1\}$$

Example

Let S be the set of points

$$S = \{(0,2),(1,3),(2,6),(-1,1)\}$$

we compute $r = 4$, $d = 3 \cdot 17$ and $k = 6$, and Lagrange interpolation polynomial is:

$$h(x) = \frac{1}{3}x^3 + \frac{2}{3}x + 2$$

irreducible modulo $\ell = 5$, so consider

$$5x^6 + y^6 = 2^i 5^j z^3, \qquad i,j \in \{0,1\}$$

which have no integer solutions, by examining relevant elliptic curves, say

$$E_1 : y^2 = x^3 - 5$$

so can take $q = 1$.

Let S be the set of points

$$S = \{(0,2),(1,3),(2,6),(-1,1)\}$$

we compute $r = 4$, $d = 3 \cdot 17$ and $k = 6$, and Lagrange interpolation polynomial is:

$$h(x) = \frac{1}{3}x^3 + \frac{2}{3}x + 2$$

Let S be the set of points

$$S = \{(0,2),(1,3),(2,6),(-1,1)\}$$

we compute $r = 4$, $d = 3 \cdot 17$ and $k = 6$, and Lagrange interpolation polynomial is:

$$h(x) = \frac{1}{3}x^3 + \frac{2}{3}x + 2$$

and now we have

$$g(X) = 5\left(X(X-1)(X-2)(X+1)\right)^6 + 1$$

Let S be the set of points

$$S = \{(0,2),(1,3),(2,6),(-1,1)\}$$

we compute $r = 4$, $d = 3 \cdot 17$ and $k = 6$, and Lagrange interpolation polynomial is:

$$h(x) = \frac{1}{3}x^3 + \frac{2}{3}x + 2$$

and now we have

$$g(X) = 5\left(X(X-1)(X-2)(X+1)\right)^6 + 1$$

and

$$C : y^{51} = f_S(X) = g(X)((h(X)-1)g(X)-1)$$

this gives us a curve of genus 1225!

Thank you for listening!

L.B. Soroker.
Dirichlet's theorem for polynomial rings
Proceedings of the American Mathematical Society. 137, 2006.

S. Gajović.
Reverse engineered Diophantine equations, 2022.
https://arxiv.org/abs/2205.09684

K. Santicola.
Reverse engineered Diophantine equations over $\mathbb{Q}$, 2022.
https://arxiv.org/abs/2208.05145