Rational points on $y^2 = f(x)$

Christopher Keyes (King's College London)

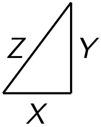
Norwich University

5 February 2026

Pythagorean triples

Find integers satisfying

$$X^2 + Y^2 = Z^2$$

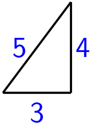


Pythagorean triples

Find integers satisfying

$$X^2 + Y^2 = Z^2$$

$(\pm 1, 0, 1)$, $(3, 4, 5)$, $(5, 12, 13)$,...

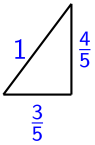


Pythagorean triples

Find integers satisfying

$$\frac{X^2}{Z^2} + \frac{Y^2}{Z^2} = 1$$

$(\pm 1, 0, 1)$, $(3, 4, 5)$, $(5, 12, 13)$,...

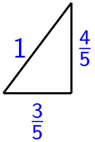


Pythagorean triples

Find rational numbers satisfying

$$x^2 + y^2 = 1$$

$(\pm 1, 0)$, $(\frac{3}{5}, \frac{4}{5})$, $(\frac{5}{13}, \frac{12}{13})$,...

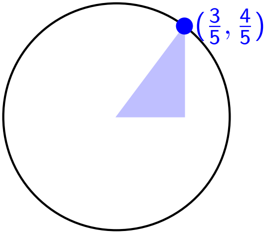


Pythagorean triples

Find rational numbers satisfying

$$x^2 + y^2 = 1$$

$(\pm 1, 0)$, $(\frac{3}{5}, \frac{4}{5})$, $(\frac{5}{13}, \frac{12}{13})$,...



Pythagorean triples

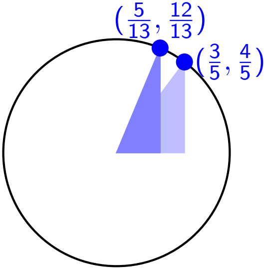
Find rational numbers satisfying

$$x^2 + y^2 = 1$$

$$(\pm 1, 0),\ (\tfrac{3}{5}, \tfrac{4}{5}),\ (\tfrac{5}{13}, \tfrac{12}{13}),\ldots$$

Each point on line

$$y = sx + s$$



Pythagorean triples

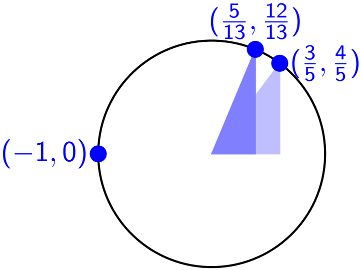
Find rational numbers satisfying

$$x^2 + y^2 = 1$$

$(\pm 1, 0)$, $(\frac{3}{5}, \frac{4}{5})$, $(\frac{5}{13}, \frac{12}{13})$,...

Each point on line

$$y = sx + s$$



Pythagorean triples

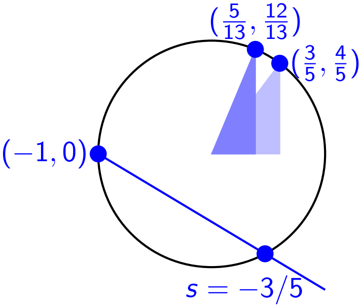
Find rational numbers satisfying

$$x^2 + y^2 = 1$$

$(\pm 1, 0)$, $(\frac{3}{5}, \frac{4}{5})$, $(\frac{5}{13}, \frac{12}{13})$,...

Each point on line

$$y = sx + s$$



Pythagorean triples

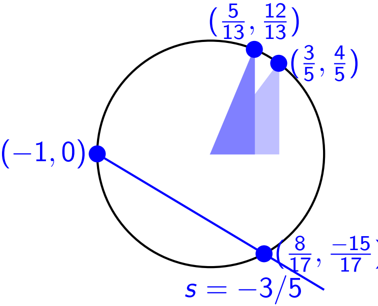
Find rational numbers satisfying

$$x^2 + y^2 = 1$$

$(\pm 1, 0)$, $(\frac{3}{5}, \frac{4}{5})$, $(\frac{5}{13}, \frac{12}{13})$,...

Each point on line

$$y = sx + s$$



Pythagorean triples

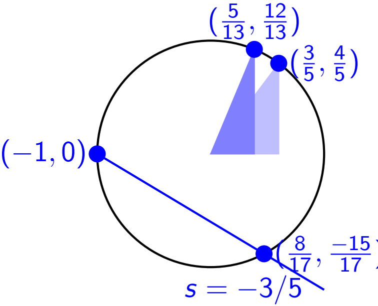
Find rational numbers satisfying

$$x^2 + y^2 = 1$$

$(\pm 1, 0)$, $(\frac{3}{5}, \frac{4}{5})$, $(\frac{5}{13}, \frac{12}{13})$,...

Each point on line

$$y = sx + s$$



Solving, we find all points

$$\left\{ \left(\frac{-s^2+1}{s^2+1}, \frac{2s}{s^2+1} \right) : \text{ rational } s \right\} \cup \{(-1, 0)\}$$

Rational points

Rational numbers: $\mathbb{Q} = \{\frac{a}{b} : a, b \text{ integers}\}$

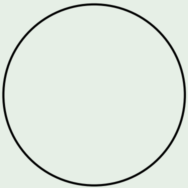
Rational points

Rational numbers: $\mathbb{Q} = \{\frac{a}{b} : a, b \text{ integers}\}$

If $f(x)$ is a polynomial, $y^2 = f(x)$ defines a curve

Example

$$y^2 = -x^2 + 1$$



Rational points

Rational numbers: $\mathbb{Q} = \{\frac{a}{b} : a, b \text{ integers}\}$

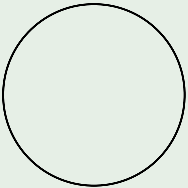
If $f(x)$ is a polynomial, $y^2 = f(x)$ defines a curve

Definition

A rational point on the curve is $(x, y) \in \mathbb{Q}^2$ satisfying $y^2 = f(x)$

Example

$$y^2 = -x^2 + 1$$



Rational points

Rational numbers: $\mathbb{Q} = \{\frac{a}{b} : a, b \text{ integers}\}$

If $f(x)$ is a polynomial, $y^2 = f(x)$ defines a curve

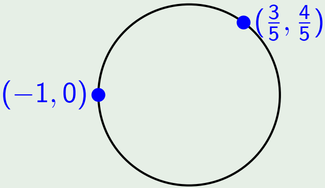
Definition

A rational point on the curve is $(x, y) \in \mathbb{Q}^2$ satisfying $y^2 = f(x)$

Example

$$y^2 = -x^2 + 1$$

Lots of rational points!



Rational points

Rational numbers: $\mathbb{Q} = \{\frac{a}{b} : a, b \text{ integers}\}$

If $f(x)$ is a polynomial, $y^2 = f(x)$ defines a curve

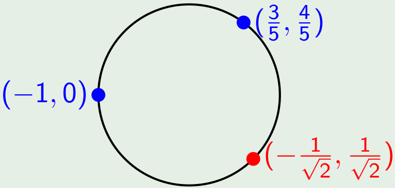
Definition

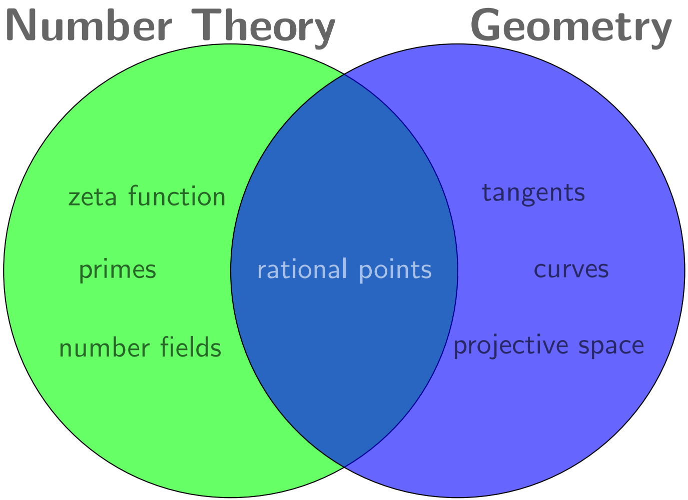
A rational point on the curve is $(x, y) \in \mathbb{Q}^2$ satisfying $y^2 = f(x)$

Example

$$y^2 = -x^2 + 1$$

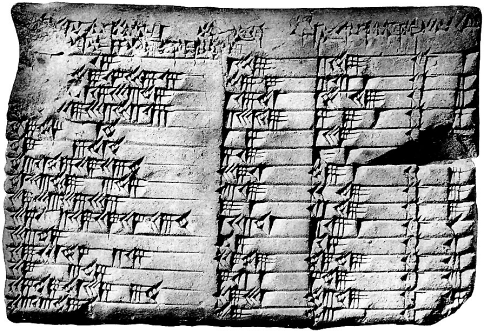
Lots of rational points!




Number Theory
Geometry
zeta function
primes
number fields
rational points
tangents
curves
projective space

Why rational points?

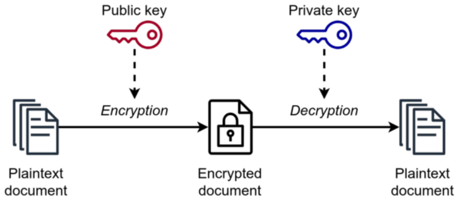
- Rich history
- Cryptography
- Moduli spaces



https://personal.math.ubc.ca/~cass/courses/m446-03/pl322/pl322.html

Why rational points?

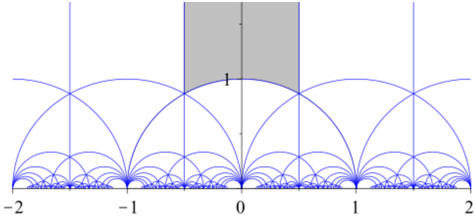
- Rich history
- Cryptography
- Moduli spaces



https://commons.wikimedia.org/wiki/File:Asymmetric_encryption_scheme.png

Why rational points?

- Rich history
- Cryptography
- Moduli spaces



https://commons.wikimedia.org/wiki/File:ModularGroup-FundamentalDomain.svg

Rational points

$y^2 = f(x)$ defines a curve

Definition

A rational point on the curve is $(x, y) \in \mathbb{Q}^2$ satisfying $y^2 = f(x)$

1. Do any rational points exist?
2. How many are there?
3. Can we find them explicitly?

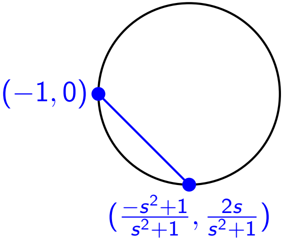
Rational points

$y^2 = f(x)$ defines a curve

Definition

A rational point on the curve is $(x, y) \in \mathbb{Q}^2$ satisfying $y^2 = f(x)$

1. Do any rational points exist?
2. How many are there?
3. Can we find them explicitly?



Changing the radius

Example

$$x^2 + y^2 = -1$$

Changing the radius

Example

$$x^2 + y^2 = -1$$

No real points $\implies$ no rational points

Changing the radius

Example

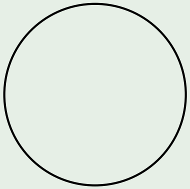
$$x^2 + y^2 = -1$$

No real points $\implies$ no rational points

Example

$$x^2 + y^2 = 3$$

Circle of radius $\sqrt{3}$



Changing the radius

Example

$$x^2 + y^2 = -1$$

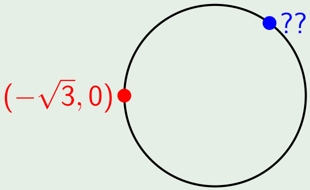
No real points $\implies$ no rational points

Example

$$x^2 + y^2 = 3$$

Circle of radius $\sqrt{3}$

Quick search: no points?



Squares mod n

Let n be an integer

Do arithmetic in $\{0, 1, 2, \dots, n-1\}$ by taking remainder

Example ($n = 3$)

$$2^2 = 4$$

Squares mod n

Let n be an integer

Do arithmetic in $\{0, 1, 2, \ldots, n-1\}$ by taking remainder

Example ($n = 3$)

$$2^2 = 3 + 1$$

Squares mod n

Let n be an integer

Do arithmetic in $\{0, 1, 2, \ldots, n-1\}$ by taking remainder

Example ($n = 3$)

$$2^2 \equiv 1 \pmod 3$$

Squares mod n

Let n be an integer

Do arithmetic in $\{0, 1, 2, \ldots, n-1\}$ by taking remainder

Example ($n = 3$)

$$0^2 \equiv 0,\; 1^2 \equiv 1,\; 2^2 \equiv 1 \pmod 3$$

Squares mod n

Let n be an integer

Do arithmetic in $\{0, 1, 2, \ldots, n-1\}$ by taking remainder

Example ($n = 3$)

$$0^2 \equiv 0,\ 1^2 \equiv 1,\ 2^2 \equiv 1 \pmod 3$$

Can we solve

$$x^2 + y^2 \equiv 0 \pmod 3$$

Only solution is $x \equiv y \equiv 0 \pmod 3$

Squares mod n

Let n be an integer

Do arithmetic in $\{0, 1, 2, \ldots, n-1\}$ by taking remainder

Example ($n = 3$)

$$0^2 \equiv 0,\ 1^2 \equiv 1,\ 2^2 \equiv 1 \pmod 3$$

Can we solve

$$x^2 + y^2 \equiv 0 \pmod 3$$

Only solution is $x \equiv y \equiv 0 \pmod 3$

Example ($n = 5$)

$$x^2 + y^2 \equiv 0 \pmod 5$$

Squares mod n

Let n be an integer

Do arithmetic in $\{0, 1, 2, \ldots, n-1\}$ by taking remainder

Example ($n = 3$)

$$0^2 \equiv 0,\ 1^2 \equiv 1,\ 2^2 \equiv 1 \pmod 3$$

Can we solve

$$x^2 + y^2 \equiv 0 \pmod 3$$

Only solution is $x \equiv y \equiv 0 \pmod 3$

Example ($n = 5$)

$$1^2 + 2^2 \equiv 0 \pmod 5$$

Back to the example

Example ($x^2 + y^2 = 3$)

Assume a solution exists.

Write $x = \frac{X}{Z}$ and $y = \frac{Y}{Z}$ with no common divisors.

Back to the example

Example ($x^2 + y^2 = 3$)

Assume a solution exists.

Write $x = \frac{X}{Z}$ and $y = \frac{Y}{Z}$ with no common divisors.

$$X^2 + Y^2 = 3Z^2$$

Back to the example

Example ($x^2 + y^2 = 3$)

Assume a solution exists.

Write $x = \frac{X}{Z}$ and $y = \frac{Y}{Z}$ with no common divisors.

$$X^2 + Y^2 = 3Z^2$$

$$X^2 + Y^2 \equiv 0 \pmod 3$$

Look mod 3:

$$X \equiv Y \equiv 0 \pmod 3 \implies Z \equiv 0 \pmod 3$$

Back to the example

Example ($x^2 + y^2 = 3$)

Assume a solution exists.

Write $x = \frac{X}{Z}$ and $y = \frac{Y}{Z}$ with no common divisors.

$$X^2 + Y^2 = 3Z^2$$

$$X^2 + Y^2 \equiv 0 \pmod 3$$

Look mod 3:

$$X \equiv Y \equiv 0 \pmod 3 \implies Z \equiv 0 \pmod 3$$

Obstruction to rational points at $p = 3$!

Local obstructions in general

p-adic numbers

"Obstruction at p" $\approx$ no p-adic solutions to $y^2 = f(x)$

Local obstructions in general

p-adic numbers

"Obstruction at p" $\approx$ no p-adic solutions to $y^2 = f(x)$

$$\mathbb{Q} \subset \mathbb{R}$$

$$\{(x,y) \in \mathbb{Q}^2 : y^2 = f(x)\} \subset \{(x,y) \in \mathbb{R}^2 : y^2 = f(x)\}$$

Local obstructions in general

p-adic numbers

"Obstruction at p" $\approx$ no p-adic solutions to $y^2 = f(x)$

$$\mathbb{Q} \subset \mathbb{Q}_p$$

$$\{(x,y) \in \mathbb{Q}^2 : y^2 = f(x)\} \subset \{(x,y) \in \mathbb{Q}_p^2 : y^2 = f(x)\}$$

Local obstructions in general

p-adic numbers

"Obstruction at p" $\approx$ no p-adic solutions to $y^2 = f(x)$

$$\mathbb{Q} \subset \mathbb{Q}_p$$

$$\{(x, y) \in \mathbb{Q}^2 : y^2 = f(x)\} \subset \{(x, y) \in \mathbb{Q}_p^2 : y^2 = f(x)\}$$

Think

Right hand side easier to determine if (non)empty

Local obstructions in general

p-adic numbers

"Obstruction at p" $\approx$ no p-adic solutions to $y^2 = f(x)$

$$\mathbb{Q} \subset \mathbb{Q}_p$$

$$\{(x, y) \in \mathbb{Q}^2 : y^2 = f(x)\} \subset \{(x, y) \in \mathbb{Q}_p^2 : y^2 = f(x)\}$$

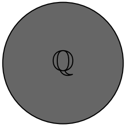
Think

Right hand side easier to determine if (non)empty

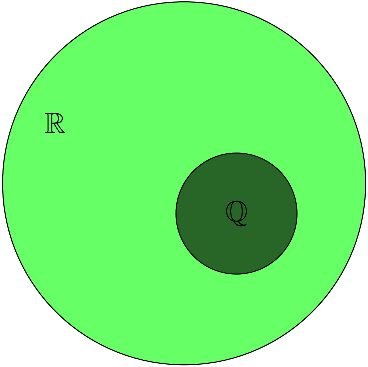
Definition (ELS)

Everywhere locally soluble: real points and no obstructions at p

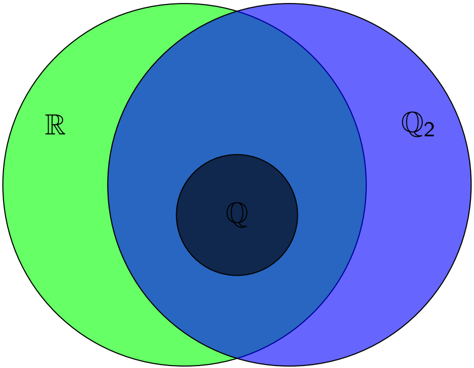
Local obstructions



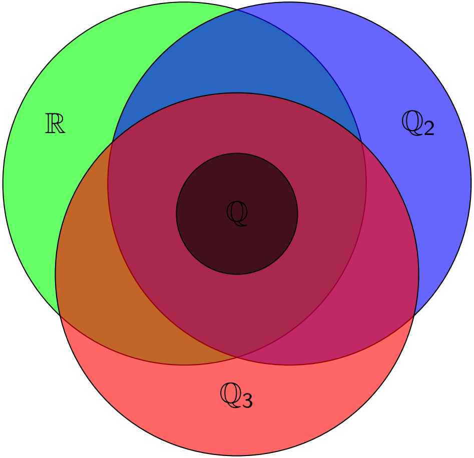
Local obstructions



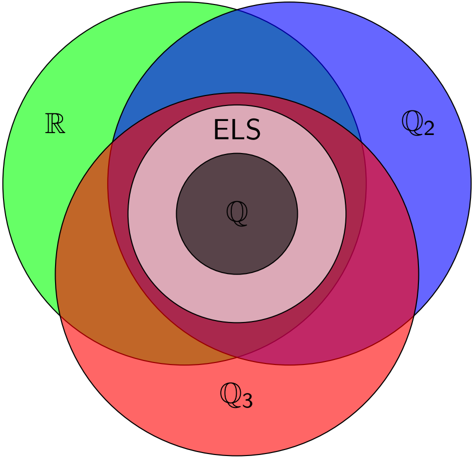
Local obstructions



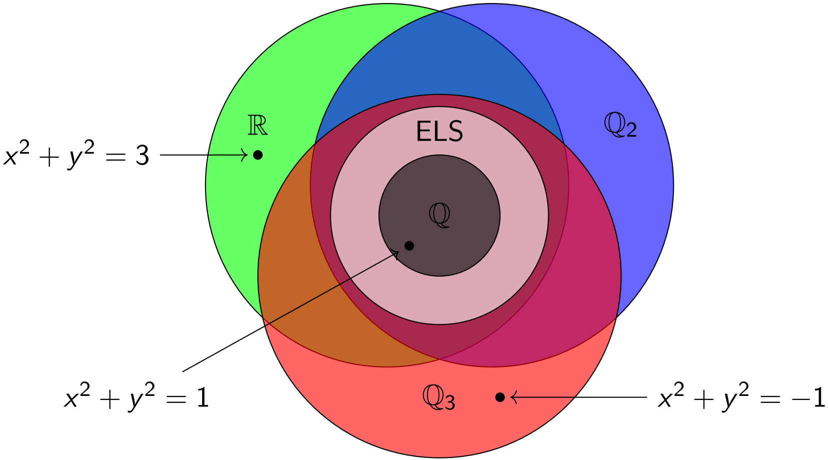
Local obstructions



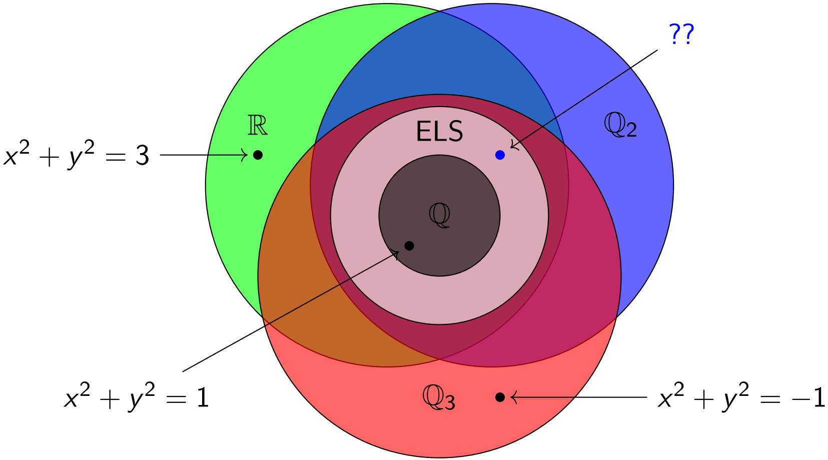
Local obstructions



Local obstructions



Local obstructions



Local to global principles

Definition (ELS)

Everywhere locally soluble: real points and no obstructions at p

Necessary for rational points. Is it sufficient?

Local to global principles

Definition (ELS)

Everywhere locally soluble: real points and no obstructions at p

Necessary for rational points. Is it sufficient?

Theorem (Hasse–Minkowski)

If $\deg f = 2$, *then yes! ELS* $\implies$ *rational points exist.*

This is a local to global principle for rational points

Local to global principles

Definition (ELS)

Everywhere locally soluble: real points and no obstructions at p

Necessary for rational points. Is it sufficient?

Theorem (Hasse–Minkowski)

If $\deg f = 2$, *then yes! ELS* $\implies$ *rational points exist.*

This is a local to global principle for rational points

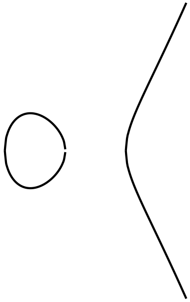
Question

What happens if $\deg f > 2$*? Is there local to global principle?*

$d = 3$: Elliptic curves

For $A, B \in \mathbb{Q}$, study rational points on

$$E\colon y^2 = x^3 + Ax + B$$

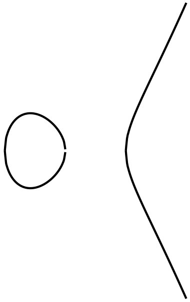


$d = 3$: Elliptic curves

For $A, B \in \mathbb{Q}$, study rational points on

$$E\colon y^2 = x^3 + Ax + B$$

- Existence: point "at infinity"

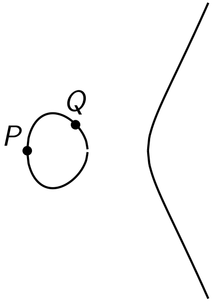


$d = 3$: Elliptic curves

For $A, B \in \mathbb{Q}$, study rational points on

$$E\colon y^2 = x^3 + Ax + B$$

- Existence: point "at infinity"
- Group structure: can add points

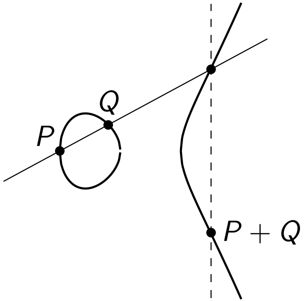


$d = 3$: Elliptic curves

For $A, B \in \mathbb{Q}$, study rational points on

$$E\colon y^2 = x^3 + Ax + B$$

- Existence: point "at infinity"
- Group structure: can add points

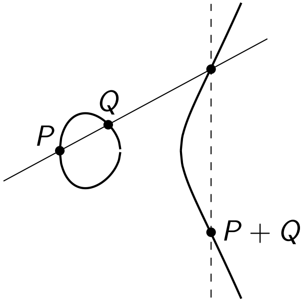


$d = 3$: Elliptic curves

For $A, B \in \mathbb{Q}$, study rational points on

$$E\colon y^2 = x^3 + Ax + B$$

- Existence: point "at infinity"
- Group structure: can add points
- Finding all points is hard!



An extended example

Example

$$C\colon y^2 = (x^2 + x - 1)(2x^2 + 3)$$

Computer search: no (x, y) with numerator/denominator ≤ 1000.

An extended example

Example

$$C\colon y^2 = (x^2 + x - 1)(2x^2 + 3)$$

Computer search: no (x, y) with numerator/denominator ≤ 1000.

It is ELS! Does local to global principle fail?

An extended example

Example

$$C\colon y^2 = (x^2 + x - 1)(2x^2 + 3)$$

Computer search: no (x, y) with numerator/denominator ≤ 1000.

It is ELS! Does local to global principle fail?

If (x, y) is a point, then

$$x^2 + x - 1 = u_1 v_1^2 \qquad 2x^2 + 3 = u_2 v_2^2$$

where u_1, u_2 are squarefree integers.

An extended example

Example

$$C\colon y^2 = (x^2 + x - 1)(2x^2 + 3)$$

Computer search: no (x, y) with numerator/denominator ≤ 1000.

It is ELS! Does local to global principle fail?

If (x, y) is a point, then

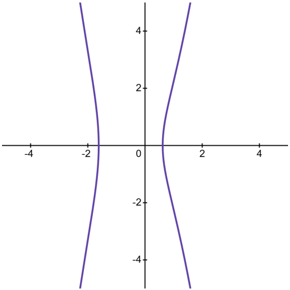
$$x^2 + x - 1 = u_1 v_1^2 \qquad 2x^2 + 3 = u_2 v_2^2$$

where u_1, u_2 are squarefree integers.

$$y^2 = u_1 u_2 v_1^2 v_2^2 \implies u_1 = u_2 = d$$

In pictures

$$C\colon y^2 = f_1(x) f_2(x)$$

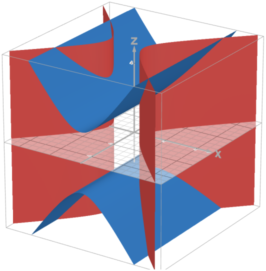


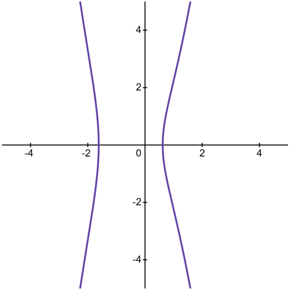
In pictures

$$C'_d\colon \begin{cases} dy_1^2 = f_1(x) \\ dy_2^2 = f_2(x) \end{cases} \qquad (x, y_1, y_2)$$

$$\downarrow \qquad\qquad \downarrow$$

$$C\colon y^2 = f_1(x)f_2(x) \qquad (x, dy_1y_2)$$





Back to example

$$C'_d\colon \begin{cases} dv_1^2 = x^2 + x - 1 \\ dv_2^2 = 2x^2 + 3 \end{cases}$$

Back to example

$$C'_d \colon \begin{cases} dv_1^2 = x^2 + x - 1 \\ dv_2^2 = 2x^2 + 3 \end{cases}$$

- Obstruction at p unless $d \in \{\pm 1, \pm 31\}$
- $d \equiv 1 \pmod 3$: no $\mathbb{Q}_3$ points
- $d < 0$: No real points

Back to example

$$C'_d\colon \begin{cases} dv_1^2 = x^2 + x - 1 \\ dv_2^2 = 2x^2 + 3 \end{cases}$$

- Obstruction at p unless $d \in \{\pm 1, \pm 31\}$
- $d \equiv 1 \pmod 3$: no $\mathbb{Q}_3$ points
- $d < 0$: No real points

Example

$$C\colon y^2 = (x^2 + x - 1)(2x^2 + 3)$$

No rational points! Failure of local to global principle.

Arithmetic statistics

Question

1. *How often does* $y^2 = f(x)$ *have a rational point?*
2. *How often is* $y^2 = f(x)$ *ELS?*

Arithmetic statistics

Question

1. *How often does $y^2 = f(x)$ have a rational point?*
2. *How often is $y^2 = f(x)$ ELS?*

$$\lim_{T \to \infty} \frac{\#\{f(x) : \text{coeffs} \leq T, \ \text{rat. pt.}\}}{\#\{f(x) : \text{coeffs} \leq T\}}$$

Arithmetic statistics

Question

1. *How often does $y^2 = f(x)$ have a rational point?*
2. *How often is $y^2 = f(x)$ ELS?*

$$\lim_{T\to\infty} \frac{\#\{f(x) : \text{coeffs} \leq T,\ \text{rat. pt.}\}}{\#\{f(x) : \text{coeffs} \leq T\}}$$

$\deg f = 2$: 0% are ELS/have rational point [FI10]

Arithmetic statistics

Question

1. *How often does $y^2 = f(x)$ have a rational point?*
2. *How often is $y^2 = f(x)$ ELS?*

$$\lim_{T\to\infty} \frac{\#\{f(x) : \text{coeffs} \leq T, \text{ rat. pt.}\}}{\#\{f(x) : \text{coeffs} \leq T\}}$$

$\deg f = 2$: 0% are ELS/have rational point [FI10]

As (even) $\deg f$ grows

- Most are ELS [PS99]
- 100% have no rational points [Bha13]

More families

- $y^3 = c_6x^6 + \dots c_1x + c_0$: 97% ELS [BK23]

More families

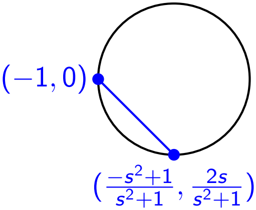
- $y^3 = c_6x^6 + \dots c_1x + c_0$: 97% ELS [BK23]
- Conj: 0.999927% of cubic surfaces have rational point [BK25]

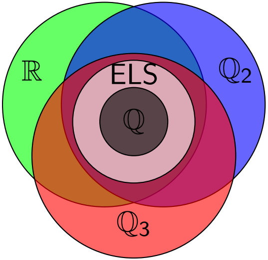
More families

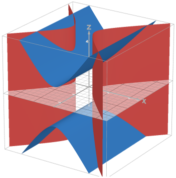
- $y^3 = c_6x^6 + \dots c_1x + c_0$: 97% ELS [BK23]
- Conj: 0.999927% of cubic surfaces have rational point [BK25]
- $\geq 1\%$ of $x^2 + By^2 = Cz^3$ satisfy *integral* LGP [DRKK$^+$]

More families

- $y^3 = c_6 x^6 + \ldots c_1 x + c_0$: 97% ELS [BK23]
- Conj: 0.999927% of cubic surfaces have rational point [BK25]
- $\geq 1\%$ of $x^2 + By^2 = Cz^3$ satisfy *integral* LGP [DRKK$^+$]







Thank you for your attention!

Manjul Bhargava, Most hyperelliptic curves over q have no rational points, 2013.

Lea Beneish and Christopher Keyes, On the proportion of locally soluble superelliptic curves, Finite Fields and Their Applications **85** (2023), 102128.

______, How often does a cubic hypersurface have a rational point?, Selecta Mathematica **31** (2025), no. 92, Available at https://doi.org/10.1007/s00029-025-01079-w.

Juanita Duque-Rosero, Christopher Keyes, Andrew Kobin, Manami Roy, Soumya Sankar, and Yidi Wang, The integral Hasse principle for stacky curves associated to a family of generalized Fermat equations, Submitted, Available at https://arxiv.org/pdf/2509.13248.

John Friedlander and Henryk Iwaniec, Ternary quadratic forms with rational zeros, J. Théor. Nombres Bordeaux **22** (2010), no. 1, 97–113. MR 2675875

Bjorn Poonen and Michael Stoll, 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