KCL Postdoc Colloquium

Christopher Keyes

28 November 2023

Early life

University

Graduate school

Graduate school

PhD advisor: David Zureick-Brown (now at Amherst College)

Graduate school

PhD advisor: David Zureick-Brown (now at Amherst College)

Mentors, classmates, and collaborators

($L \to R$: Lea Beneish, Jackson Morrow, Santiago Arango-Piñeros, Daniel Keliher)

Overview

Broad: number theory, arithmetic geometry, arithmetic statistics

Overview

Broad: number theory, arithmetic geometry, arithmetic statistics

Specific: quantitative questions about arithmetic objects

Overview

Broad: number theory, arithmetic geometry, arithmetic statistics

Specific: quantitative questions about arithmetic objects

Example

E.g. how many ____ are there? Or, how often does ____?

Overview

Broad: number theory, arithmetic geometry, arithmetic statistics

Specific: quantitative questions about arithmetic objects

Example

E.g. how many ____ are there? Or, how often does ____?

- How many prime numbers are there?

Overview

Broad: number theory, arithmetic geometry, arithmetic statistics

Specific: quantitative questions about arithmetic objects

Example

E.g. how many ____ are there? Or, how often does ____?

- How many prime numbers are there?
- How many number fields are there (with certain properties)?

Overview

Broad: number theory, arithmetic geometry, arithmetic statistics

Specific: quantitative questions about arithmetic objects

Example

E.g. how many ____ are there? Or, how often does ____?

- How many prime numbers are there?
- How many number fields are there (with certain properties)?
- How many degree n points are there on a curve $C/\mathbb{Q}$?

Overview

Broad: number theory, arithmetic geometry, arithmetic statistics

Specific: quantitative questions about arithmetic objects

Example

E.g. how many ____ are there? Or, how often does ____?

- How many prime numbers are there?
- How many number fields are there (with certain properties)?
- How many degree n points are there on a curve $C/\mathbb{Q}$?
- How often does $y^3 = f(x, z)$ have a rational solution?

Motivation

Let $f(x,z)$ be an integral binary degree d form.

Let $m \geq 1$ an integer.

Question

How often does f represent an m-th power?

Motivation

Let $f(x, z)$ be an integral binary degree d form.

Let $m \geq 1$ an integer.

Question

How often does f represent an m-th power?

Theorem (Bhargava, 2013)

If d is even, many forms do not represent a square.

As $d \to \infty$, 100% of forms do not represent a square.

Translation to geometry

Idea

f represents an m-th power iff $C\colon y^m = f(x,z)$ has a rational point.

Translation to geometry

Idea

f represents an m-th power iff $C\colon y^m = f(x,z)$ has a rational point.

Number field K	**Curve C over $\mathbb{Q}$**
Degree $[K:\mathbb{Q}]$	Degree of $\mathbb{Q}(C)/\mathbb{Q}(t)$
Primes of $\mathcal{O}_K$	Rational points $C(\mathbb{Q})$
Splitting of $(p) = \prod \mathfrak{p}_i^{e_i}$	Fiber above $P \in \mathbb{P}^1(\mathbb{Q})$

Translation to geometry

Idea

f represents an m-th power iff $C\colon y^m = f(x,z)$ has a rational point.

Number field K	**Curve C over $\mathbb{Q}$**
Degree $[K:\mathbb{Q}]$	Degree of $\mathbb{Q}(C)/\mathbb{Q}(t)$
Primes of $\mathcal{O}_K$	Rational points $C(\mathbb{Q})$
Splitting of $(p) = \prod \mathfrak{p}_i^{e_i}$	Fiber above $P \in \mathbb{P}^1(\mathbb{Q})$
Quadratic field $\mathbb{Q}(\sqrt{d})$	Hyperelliptic curve $y^2 = f(t)$

Translation to geometry

Idea

f represents an m-th power iff $C\colon y^m = f(x,z)$ has a rational point.

Number field K	**Curve C over $\mathbb{Q}$**
Degree $[K:\mathbb{Q}]$	Degree of $\mathbb{Q}(C)/\mathbb{Q}(t)$
Primes of $\mathcal{O}_K$	Rational points $C(\mathbb{Q})$
Splitting of $(p) = \prod \mathfrak{p}_i^{e_i}$	Fiber above $P \in \mathbb{P}^1(\mathbb{Q})$
Quadratic field $\mathbb{Q}(\sqrt{d})$	Hyperelliptic curve $y^2 = f(t)$
Radical extension $\mathbb{Q}(\sqrt[m]{d})$	Superelliptic curve $y^m = f(t)$

Local solubility

Question

How often does $C_f\colon y^m = f(x,z)$ have a rational point?

$$C(\mathbb{Q}) \subset C(\mathbb{Q}_p) \text{ for all } p, \text{ and } C(\mathbb{Q}) \subset C(\mathbb{R})$$

Local solubility

Question

How often does $C_f\colon y^m = f(x,z)$ have a rational point?

$$C(\mathbb{Q}) \subset C(\mathbb{Q}_p) \text{ for all } p, \text{ and } C(\mathbb{Q}) \subset C(\mathbb{R})$$

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

Local solubility

Question

How often does $C_f \colon y^m = f(x,z)$ have a rational point?

$$C(\mathbb{Q}) \subset C(\mathbb{Q}_p) \text{ for all } p, \text{ and } C(\mathbb{Q}) \subset C(\mathbb{R})$$

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

$$C \text{ has } \mathbb{Q}\text{-point} \implies C \text{ ELS}.$$

Converse is Hasse principle (HP) — fails in general!

Local solubility

Question

How often does $C_f\colon y^m = f(x,z)$ have a rational point?

$$C(\mathbb{Q}) \subset C(\mathbb{Q}_p) \text{ for all } p, \text{ and } C(\mathbb{Q}) \subset C(\mathbb{R})$$

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

$$C \text{ has } \mathbb{Q}\text{-point} \implies C \text{ ELS.}$$

Converse is Hasse principle (HP) — fails in general!

Question

How often is C_f ELS? How often does it satisfy/fail HP?

Roadmap

Question

How often is C_f ELS?

1. Decide how to count curves

$$\rho_{m,d} = \lim_{B\to\infty} \frac{\#\{|f|\leq B,\ C_f \text{ ELS}\}}{\#\{|f|\leq B\}}$$

Roadmap

Question

How often is C_f ELS?

1. Decide how to count curves

$$\rho_{m,d} = \lim_{B\to\infty} \frac{\#\{|f|\le B,\ C_f \text{ ELS}\}}{\#\{|f|\le B\}}$$

2. Argue each place is independent

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

Roadmap

Question

How often is C_f ELS?

1. Decide how to count curves

$$\rho_{m,d} = \lim_{B\to\infty} \frac{\#\{|f|\le B,\ C_f \text{ ELS}\}}{\#\{|f|\le B\}}$$

2. Argue each place is independent

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

3. Explicitly compute locally soluble curves over $\mathbb{Z}_p$ (and $\mathbb{R}$)

A result

Theorem (Beneish–K., 2022)

For $\approx 97\%$ of integral deg. 6 $f(x,z)$, $y^3 = f(x,z)$ is ELS.

A result

Theorem (Beneish–K., 2022)

For $\approx 97\%$ of integral deg. 6 $f(x,z)$, $y^3 = f(x,z)$ is ELS.

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}$$

Advertisement

If you like to hear more, I'll be speaking again Thursday!

What?	KCL internal number theory seminar
When?	Thursday 30 November
	2:00pm – 3:00pm
Where?	K0.50 (King's Building)

Degrees of points

Another direction: higher degree points

$$\Gamma_n(C, \mathbb{Q}) = \bigcup_{[K/\mathbb{Q}]=n} C(K).$$

Degrees of points

Another direction: higher degree points

$$\Gamma_n(C, \mathbb{Q}) = \bigcup_{[K/\mathbb{Q}]=n} C(K).$$

Question

When is $\#\Gamma_n(C, \mathbb{Q}) = \infty$*?*

When is $\#\Gamma_n(C, \mathbb{Q}) = \emptyset$*?*

Degrees of points

Another direction: higher degree points

$$\Gamma_n(C,\mathbb{Q}) = \bigcup_{[K/\mathbb{Q}]=n} C(K).$$

Question

When is $\#\Gamma_n(C,\mathbb{Q}) = \infty$*?*

When is $\#\Gamma_n(C,\mathbb{Q}) = \emptyset$*?*

Idea

Points should be there for geometric reasons

Degrees of points

Idea

Points should be there for geometric reasons

E.g. maps:

$$\begin{tikzcd} \mathrm{Spec}(K) \arrow[r, hook] \arrow[d] & C \arrow[d, "n"] \\ \mathrm{Spec}(\mathbb{Q}) \arrow[r, hook] & \mathbb{P}^1 \end{tikzcd}$$

Degrees of points

Idea

Points should be there for geometric reasons

E.g. maps:

$$\begin{tikzcd} \mathrm{Spec}(K) \arrow[r, hook] \arrow[d] & C \arrow[d, "n"] \\ \mathrm{Spec}(\mathbb{Q}) \arrow[r, hook] & \mathbb{P}^1 \end{tikzcd}$$

or

$$\begin{tikzcd} \mathrm{Spec}(K) \arrow[r, hook] \arrow[d] & C \arrow[d, "n"] \\ \mathrm{Spec}(\mathbb{Q}) \arrow[r, hook] & E \end{tikzcd}$$

Degrees of points

Idea

Points should be there for geometric reasons

E.g. maps:

$$\begin{tikzcd} \mathrm{Spec}(K) \arrow[r, hook] \arrow[d] & C \arrow[d, "n"] \\ \mathrm{Spec}(\mathbb{Q}) \arrow[r, hook] & \mathbb{P}^1 \end{tikzcd} \quad \text{or} \quad \begin{tikzcd} \mathrm{Spec}(K) \arrow[r, hook] \arrow[d] & C \arrow[d, "n"] \\ \mathrm{Spec}(\mathbb{Q}) \arrow[r, hook] & E \end{tikzcd}$$

Remarks

If $n = 2, 3$, maps are only way to have ∞-ly many deg. n points.

Degrees of points

Idea

Points should be there for geometric reasons

E.g. maps:

$$\begin{tikzcd} \mathrm{Spec}(K) \arrow[r, hook] \arrow[d] & C \arrow[d, "n"] \\ \mathrm{Spec}(\mathbb{Q}) \arrow[r, hook] & \mathbb{P}^1 \end{tikzcd}$$

or

$$\begin{tikzcd} \mathrm{Spec}(K) \arrow[r, hook] \arrow[d] & C \arrow[d, "n"] \\ \mathrm{Spec}(\mathbb{Q}) \arrow[r, hook] & E \end{tikzcd}$$

Remarks

If $n = 2, 3$, maps are only way to have ∞-ly many deg. n points.

General n: look for abelian subarieties in Jacobian $\mathrm{Jac}(C)$.

Degrees of points

Idea

Points should be there for geometric reasons

E.g. maps:

$$\begin{array}{ccc} \mathrm{Spec}(K) & \hookrightarrow & C \\ \downarrow & & \downarrow n \\ \mathrm{Spec}(\mathbb{Q}) & \longrightarrow & \mathbb{P}^1 \end{array} \quad \text{or} \quad \begin{array}{ccc} \mathrm{Spec}(K) & \hookrightarrow & C \\ \downarrow & & \downarrow n \\ \mathrm{Spec}(\mathbb{Q}) & \hookrightarrow & E \end{array}$$

Remarks

If $n = 2, 3$, maps are only way to have ∞-ly many deg. n points.

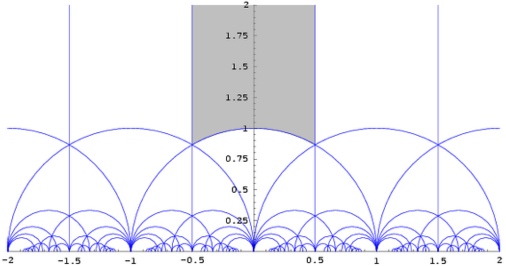
General n: look for abelian subarieties in Jacobian $\mathrm{Jac}(C)$.

Or, look for obstructions to $\mathrm{Pic}^1(C)$ having points.

Other interests

I also like to think about

- Modular curves



Other interests

I also like to think about

- Modular curves
- Integral points on stacky curves

Other interests

I also like to think about

- Modular curves
- Integral points on stacky curves
- Baseball statistics

Other interests

I also like to think about

- Modular curves
- Integral points on stacky curves
- Baseball statistics
- Math circles and math for kids

Present day!