An overview of arithmetic statistics

Peter Koymans
Utrecht University

Utrecht University

Bristol

20 April 2026

Arithmetic statistics

The aim of arithmetic statistics is to answer statistical questions of arithmetic objects (e.g. elliptic curves, number fields, class groups).

Arithmetic statistics

The aim of arithmetic statistics is to answer statistical questions of arithmetic objects (e.g. elliptic curves, number fields, class groups).

We will first discuss three recent results, and we will then give a high-level overview how such results are proven.

Arithmetic statistics

The aim of arithmetic statistics is to answer statistical questions of arithmetic objects (e.g. elliptic curves, number fields, class groups).

We will first discuss three recent results, and we will then give a high-level overview how such results are proven.

Techniques from arithmetic statistics can also be used to prove results that do not have a statistical nature.

Hilbert's tenth problem

At the 1900 mathematical conference in Paris, Hilbert introduced his famous list of 23 problems.

David Hilbert

Hilbert's tenth problem

At the 1900 mathematical conference in Paris, Hilbert introduced his famous list of 23 problems.

David Hilbert

Question (Hilbert's tenth problem)

Given a Diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: To devise a process according to which it can be determined in a finite number of operations whether the equation is solvable in rational integers.

Hilbert's tenth problem

At the 1900 mathematical conference in Paris, Hilbert introduced his famous list of 23 problems.

David Hilbert

Question (Hilbert's tenth problem)

Given a Diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: To devise a process according to which it can be determined in a finite number of operations whether the equation is solvable in rational integers.

In modern terms: does there exist an algorithm such that:
Input: a polynomial $p \in \mathbb{Z}[x_1, \ldots, x_n]$.
Output: "YES" if there is an integer solution $(a_1, \ldots, a_n) \in \mathbb{Z}^n$ with $p(a_1, \ldots, a_n) = 0$, "NO" otherwise.

Finitely generated rings

Theorem (MRDP, 1970)

Hilbert's tenth problem is undecidable, i.e. there is no algorithm that can decide whether a polynomial $p \in \mathbb{Z}[x_1, \ldots, x_n]$ has a zero or not.

Finitely generated rings

Theorem (MRDP, 1970)

Hilbert's tenth problem is undecidable, i.e. there is no algorithm that can decide whether a polynomial $p \in \mathbb{Z}[x_1, \ldots, x_n]$ has a zero or not.

Matiyasevich asks in the 1970s: what about other rings?

Finitely generated rings

Theorem (MRDP, 1970)

Hilbert's tenth problem is undecidable, i.e. there is no algorithm that can decide whether a polynomial $p \in \mathbb{Z}[x_1, \ldots, x_n]$ has a zero or not.

Matiyasevich asks in the 1970s: what about other rings?

Definition

For a finitely generated ring R, we have an analogue of "Hilbert's tenth problem" by replacing all occurrences of $\mathbb{Z}$ by R.

Finitely generated rings

Theorem (MRDP, 1970)

Hilbert's tenth problem is undecidable, i.e. there is no algorithm that can decide whether a polynomial $p \in \mathbb{Z}[x_1, \ldots, x_n]$ has a zero or not.

Matiyasevich asks in the 1970s: what about other rings?

Definition

For a finitely generated ring R, we have an analogue of "Hilbert's tenth problem" by replacing all occurrences of $\mathbb{Z}$ by R.

Theorem (K.–Pagano, 2024)

Let R be a finitely generated ring with $|R| = \infty$. Then Hilbert's tenth problem is undecidable over R.

Finitely generated rings

Theorem (MRDP, 1970)

Hilbert's tenth problem is undecidable, i.e. there is no algorithm that can decide whether a polynomial $p \in \mathbb{Z}[x_1, \ldots, x_n]$ has a zero or not.

Matiyasevich asks in the 1970s: what about other rings?

Definition

For a finitely generated ring R, we have an analogue of "Hilbert's tenth problem" by replacing all occurrences of $\mathbb{Z}$ by R.

Theorem (K.–Pagano, 2024)

Let R be a finitely generated ring with $|R| = \infty$. Then Hilbert's tenth problem is undecidable over R.

In the process, we also prove a conjecture of Denef–Lipshitz (1978).

Pell's equation

Pell's equation is

$$x^2 - dy^2 = \pm 1 \text{ to be solved in } x, y \in \mathbb{Z}.$$

Pell's equation

Pell's equation is

$$x^2 - dy^2 = \pm 1 \text{ to be solved in } x, y \in \mathbb{Z}.$$

Studied by Archimedes, Pythagoras, Bhaskara II, Brahmagupta, Fermat, Brouncker, Wallis, Euler, Lagrange, Legendre, Gauss, Dirichlet ...

Pell's equation

Pell's equation is

$$x^2 - dy^2 = \pm 1 \text{ to be solved in } x, y \in \mathbb{Z}.$$

Studied by Archimedes, Pythagoras, Bhaskara II, Brahmagupta, Fermat, Brouncker, Wallis, Euler, Lagrange, Legendre, Gauss, Dirichlet ...

Pythagoras proved that $\sqrt{2}$ is irrational, i.e. $x^2 - 2y^2 = 0$ has no solutions in $x, y \in \mathbb{Z}$ (except $x = y = 0$).

Pell's equation

Pell's equation is

$$x^2 - dy^2 = \pm 1 \text{ to be solved in } x, y \in \mathbb{Z}.$$

Studied by Archimedes, Pythagoras, Bhaskara II, Brahmagupta, Fermat, Brouncker, Wallis, Euler, Lagrange, Legendre, Gauss, Dirichlet ...

Pythagoras proved that $\sqrt{2}$ is irrational, i.e. $x^2 - 2y^2 = 0$ has no solutions in $x, y \in \mathbb{Z}$ (except $x = y = 0$).

The Pell equation is instead the "next best thing", namely $x^2 - 2y^2 = \pm 1$. It provides the best rational approximations to $\sqrt{2}$.

Pell's equation

Pell's equation is

$$x^2 - dy^2 = \pm 1 \text{ to be solved in } x, y \in \mathbb{Z}.$$

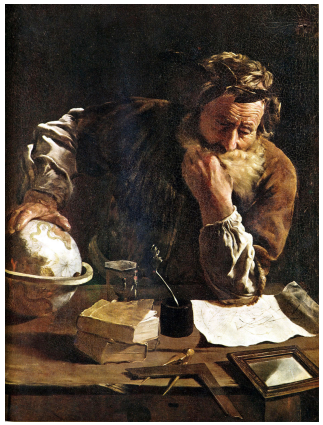
Studied by Archimedes, Pythagoras, Bhaskara II, Brahmagupta, Fermat, Brouncker, Wallis, Euler, Lagrange, Legendre, Gauss, Dirichlet ...

Pythagoras proved that $\sqrt{2}$ is irrational, i.e. $x^2 - 2y^2 = 0$ has no solutions in $x, y \in \mathbb{Z}$ (except $x = y = 0$).

The Pell equation is instead the "next best thing", namely $x^2 - 2y^2 = \pm 1$. It provides the best rational approximations to $\sqrt{2}$.

Solution x, y	Ratio x/y	Expansion of $\sqrt{2}$
$x = 1,\ y = 1$	1	1.4142135...
$x = 3,\ y = 2$	1.5	1.4142135...
$x = 7,\ y = 5$	1.4	1.4142135...
$x = 17,\ y = 12$	1.4166666...	1.4142135...
$x = 41,\ y = 29$	1.4137931...	1.4142135...
$x = 99,\ y = 70$	1.4142857...	1.4142135...

The positive Pell equation



Archimedes

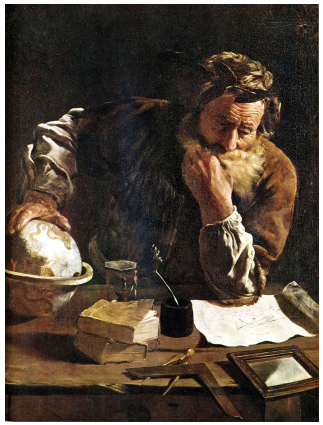
Dirichlet proved that one can always non-trivially solve

$$x^2 - dy^2 = 1$$

in integers x, y (i.e. $x^2 = 1$ and $y^2 = 0$ being the trivial solution).

Pierre de Fermat

The positive Pell equation



Archimedes

Dirichlet proved that one can always non-trivially solve

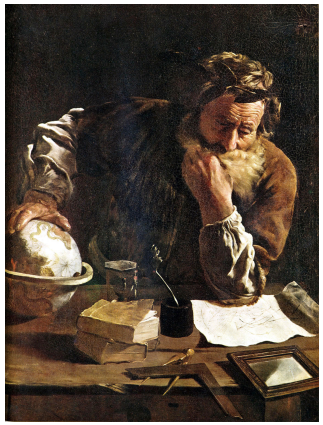
$$x^2 - dy^2 = 1$$

in integers x, y (i.e. $x^2 = 1$ and $y^2 = 0$ being the trivial solution).

Archimedes seems to have already been aware of this, and Brahmagupta and Bhaskara II even provided an algorithm for solving this equation.

Pierre de Fermat

The positive Pell equation



Archimedes

Dirichlet proved that one can always non-trivially solve

$$x^2 - dy^2 = 1$$

in integers x, y (i.e. $x^2 = 1$ and $y^2 = 0$ being the trivial solution).

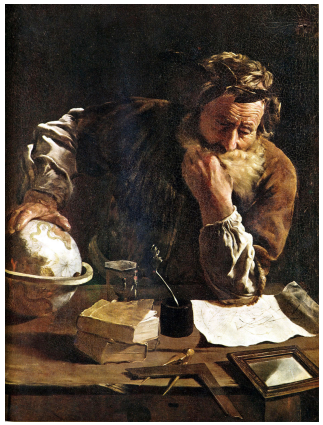
Archimedes seems to have already been aware of this, and Brahmagupta and Bhaskara II even provided an algorithm for solving this equation.

Pierre de Fermat

Example (Fermat's challenge to Brouncker and Wallis)

The smallest non-trivial solution to $x^2 - 61y^2 = 1$ *is*

The positive Pell equation



Archimedes

Dirichlet proved that one can always non-trivially solve

$$x^2 - dy^2 = 1$$

in integers x, y (i.e. $x^2 = 1$ and $y^2 = 0$ being the trivial solution).

Archimedes seems to have already been aware of this, and Brahmagupta and Bhaskara II even provided an algorithm for solving this equation.

Pierre de Fermat

Example (Fermat's challenge to Brouncker and Wallis)

The smallest non-trivial solution to $x^2 - 61y^2 = 1$ *is*

$$x = 1766319049, \quad y = 226153980.$$

The negative Pell equation

To solve the negative Pell equation $x^2 - dy^2 = -1$, one certainly needs to be able to solve it modulo p for all primes p. But if p divides d, we get

$$x^2 \equiv -1 \bmod p.$$

The negative Pell equation

To solve the negative Pell equation $x^2 - dy^2 = -1$, one certainly needs to be able to solve it modulo p for all primes p. But if p divides d, we get

$$x^2 \equiv -1 \bmod p.$$

This implies that $p \equiv 1 \bmod 4$ or $p = 2$. Define $\mathcal{D}$ to be the set of squarefree d for which $p \mid d$ implies $p \equiv 1 \bmod 4$ or $p = 2$.

The negative Pell equation

To solve the negative Pell equation $x^2 - dy^2 = -1$, one certainly needs to be able to solve it modulo p for all primes p. But if p divides d, we get

$$x^2 \equiv -1 \bmod p.$$

This implies that $p \equiv 1 \bmod 4$ or $p = 2$. Define $\mathcal{D}$ to be the set of squarefree d for which $p \mid d$ implies $p \equiv 1 \bmod 4$ or $p = 2$.

Nagell (1930s) conjectured

$$\lim_{X \to \infty} \frac{\#\{d \leq X : d \in \mathcal{D}, x^2 - dy^2 = -1 \text{ sol.}\}}{\#\{d \leq X : d \in \mathcal{D}\}}$$

exists and lies in $(0, 1)$.

The negative Pell equation

To solve the negative Pell equation $x^2 - dy^2 = -1$, one certainly needs to be able to solve it modulo p for all primes p. But if p divides d, we get

$$x^2 \equiv -1 \bmod p.$$

This implies that $p \equiv 1 \bmod 4$ or $p = 2$. Define $\mathcal{D}$ to be the set of squarefree d for which $p \mid d$ implies $p \equiv 1 \bmod 4$ or $p = 2$.

Nagell (1930s) conjectured

$$\lim_{X \to \infty} \frac{\#\{d \leq X : d \in \mathcal{D}, x^2 - dy^2 = -1 \text{ sol.}\}}{\#\{d \leq X : d \in \mathcal{D}\}}$$

exists and lies in $(0, 1)$. The smallest $d \in \mathcal{D}$ for which the negative Pell equation is not soluble is $d = 34$.

The negative Pell equation

To solve the negative Pell equation $x^2 - dy^2 = -1$, one certainly needs to be able to solve it modulo p for all primes p. But if p divides d, we get

$$x^2 \equiv -1 \bmod p.$$

This implies that $p \equiv 1 \bmod 4$ or $p = 2$. Define $\mathcal{D}$ to be the set of squarefree d for which $p \mid d$ implies $p \equiv 1 \bmod 4$ or $p = 2$.

Nagell (1930s) conjectured

$$\lim_{X \to \infty} \frac{\#\{d \leq X : d \in \mathcal{D}, x^2 - dy^2 = -1 \text{ sol.}\}}{\#\{d \leq X : d \in \mathcal{D}\}}$$

exists and lies in $(0, 1)$. The smallest $d \in \mathcal{D}$ for which the negative Pell equation is not soluble is $d = 34$. Stevenhagen (1995) predicted a precise value for the limit.

The negative Pell equation

To solve the negative Pell equation $x^2 - dy^2 = -1$, one certainly needs to be able to solve it modulo p for all primes p. But if p divides d, we get

$$x^2 \equiv -1 \bmod p.$$

This implies that $p \equiv 1 \bmod 4$ or $p = 2$. Define $\mathcal{D}$ to be the set of squarefree d for which $p \mid d$ implies $p \equiv 1 \bmod 4$ or $p = 2$.

Nagell (1930s) conjectured

$$\lim_{X \to \infty} \frac{\#\{d \leq X : d \in \mathcal{D}, x^2 - dy^2 = -1 \text{ sol.}\}}{\#\{d \leq X : d \in \mathcal{D}\}}$$

exists and lies in $(0, 1)$. The smallest $d \in \mathcal{D}$ for which the negative Pell equation is not soluble is $d = 34$. Stevenhagen (1995) predicted a precise value for the limit.

Theorem (K.–Pagano, 2022)

Nagell's and Stevenhagen's conjecture are true.

Sums of cubes

How many integers $1 \leq n \leq B$ are such that

$$x^3 + y^3 = n$$

has a solution in rational numbers $x, y \in \mathbb{Q}$?

Sums of cubes

How many integers $1 \leq n \leq B$ are such that

$$x^3 + y^3 = n$$

has a solution in rational numbers $x, y \in \mathbb{Q}$?

More formally, does the following limit exist

$$\lim_{B \to \infty} \frac{\#\{1 \leq n \leq B : \text{there exist } x, y \in \mathbb{Q} \text{ such that } x^3 + y^3 = n\}}{B}$$

and if so, what is its value?

Sums of cubes

How many integers $1 \leq n \leq B$ are such that

$$x^3 + y^3 = n$$

has a solution in rational numbers $x, y \in \mathbb{Q}$?

More formally, does the following limit exist

$$\lim_{B \to \infty} \frac{\#\{1 \leq n \leq B : \text{there exist } x, y \in \mathbb{Q} \text{ such that } x^3 + y^3 = n\}}{B}$$

and if so, what is its value?

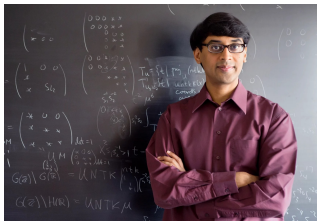
Example (Rational versus integer solutions)

For $n = 6$ one can use the factorization $x^3 + y^3 = (x + y)(x^2 - xy + y^2)$ to show that there are no integer solutions. However, we have

$$6 = \left(\frac{17}{21}\right)^3 + \left(\frac{37}{21}\right)^3.$$

Results

Levent Alpöge



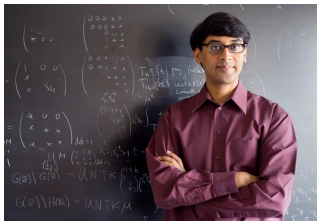
Manjul Bhargava

Ari Shnidman

Alpöge–Bhargava–Shnidman (2022) showed that at least 16.6% of the integers are not sums of two rational cubes, and 9.5% of the integers are sums of rational cubes.

Results

Levent Alpöge



Manjul Bhargava

Ari Shnidman

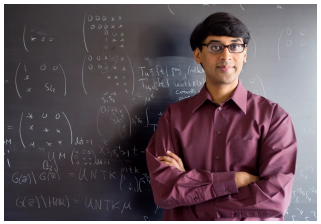
Alpöge–Bhargava–Shnidman (2022) showed that at least 16.6% of the integers are not sums of two rational cubes, and 9.5% of the integers are sums of rational cubes.

Theorem (K.–Smith, 2024)

At least 31.4% *of the integers are not sums of two rational cubes. Assuming a parity conjecture, at least* 47.4% *of integers are sums of two rational cubes.*

Results

Levent Alpöge



Manjul Bhargava

Ari Shnidman

Alpöge–Bhargava–Shnidman (2022) showed that at least 16.6% of the integers are not sums of two rational cubes, and 9.5% of the integers are sums of rational cubes.

Theorem (K.–Smith, 2024)

At least 31.4% *of the integers are not sums of two rational cubes. Assuming a parity conjecture, at least* 47.4% *of integers are sums of two rational cubes.*

Conjecturally, the limit should be $1/2$.

Elliptic curves

An elliptic curve E is an equation of the form

$$E : y^2 = x^3 + ax + b$$

with $a, b \in \mathbb{Q}$ fixed.

Elliptic curves

An elliptic curve E is an equation of the form

$$E : y^2 = x^3 + ax + b$$

with $a, b \in \mathbb{Q}$ fixed.

The rational points of an elliptic curve are

$$E(\mathbb{Q}) := \{(x, y) \in \mathbb{Q}^2 : y^2 = x^3 + ax + b\} \cup \{O\},$$

where O is an extra point (which one gets by taking the projective closure of E).

Elliptic curves

An elliptic curve E is an equation of the form

$$E : y^2 = x^3 + ax + b$$

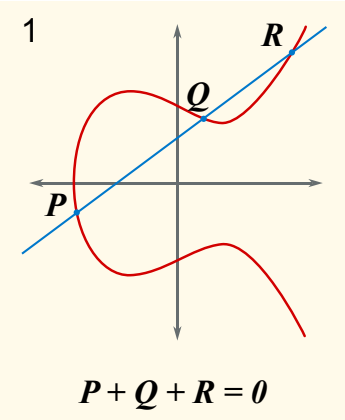
with $a, b \in \mathbb{Q}$ fixed.

The rational points of an elliptic curve are

$$E(\mathbb{Q}) := \{(x, y) \in \mathbb{Q}^2 : y^2 = x^3 + ax + b\} \cup \{O\},$$

where O is an extra point (which one gets by taking the projective closure of E).

An amazing fact is that $E(\mathbb{Q})$ is naturally a finitely generated abelian group.



The group law on $E(\mathbb{Q})$

Connecting elliptic curves to sums of rational cubes

Recall that we previously introduced the sums of rational cubes problem, namely how many $1 \leq n \leq B$ are such that

$$C_n : x^3 + y^3 = n$$

has a solution $x, y \in \mathbb{Q}$?

Connecting elliptic curves to sums of rational cubes

Recall that we previously introduced the sums of rational cubes problem, namely how many $1 \leq n \leq B$ are such that

$$C_n : x^3 + y^3 = n$$

has a solution $x, y \in \mathbb{Q}$?

It is not difficult to show that C_n can be brought into the following form using coordinate transformations

$$y^2 = x^3 - 432n^2,$$

so C_n is an elliptic curve, and our question is equivalent to $C_n \neq \{O\}$.

Connecting elliptic curves to sums of rational cubes

Recall that we previously introduced the sums of rational cubes problem, namely how many $1 \leq n \leq B$ are such that

$$C_n : x^3 + y^3 = n$$

has a solution $x, y \in \mathbb{Q}$?

It is not difficult to show that C_n can be brought into the following form using coordinate transformations

$$y^2 = x^3 - 432n^2,$$

so C_n is an elliptic curve, and our question is equivalent to $C_n \neq \{O\}$.

Now note that all the curves C_n are isomorphic to C_1 over $\overline{\mathbb{Q}}$. Indeed, we can divide x and y by $\sqrt[3]{n}$.

Connecting elliptic curves to sums of rational cubes

Recall that we previously introduced the sums of rational cubes problem, namely how many $1 \leq n \leq B$ are such that

$$C_n : x^3 + y^3 = n$$

has a solution $x, y \in \mathbb{Q}$?

It is not difficult to show that C_n can be brought into the following form using coordinate transformations

$$y^2 = x^3 - 432n^2,$$

so C_n is an elliptic curve, and our question is equivalent to $C_n \neq \{O\}$.

Now note that all the curves C_n are isomorphic to C_1 over $\overline{\mathbb{Q}}$. Indeed, we can divide x and y by $\sqrt[3]{n}$.

In fact, since $C_n \cong C_1$ over $\mathbb{Q}(\sqrt[3]{n})$, the family C_n is called a "cubic twist family".

Connecting elliptic curves to Hilbert's tenth problem

A key ingredient in Matiyasevich's resolution of Hilbert's tenth problem is the positive Pell equation.

Connecting elliptic curves to Hilbert's tenth problem

A key ingredient in Matiyasevich's resolution of Hilbert's tenth problem is the positive Pell equation.

Researchers attempted to generalize his arguments to arbitrary finitely generated rings, and were able to replace the role of Pell's equation in Matiyasevich's argument by *elliptic curves*.

Connecting elliptic curves to Hilbert's tenth problem

A key ingredient in Matiyasevich's resolution of Hilbert's tenth problem is the positive Pell equation.

Researchers attempted to generalize his arguments to arbitrary finitely generated rings, and were able to replace the role of Pell's equation in Matiyasevich's argument by *elliptic curves*.

However, the positive Pell equation always has a solution, and for this adaptation to work, one (roughly) needs to find for every number field K an elliptic curve E with $E(K) \cong \mathbb{Z}$.

Connecting elliptic curves to Hilbert's tenth problem

A key ingredient in Matiyasevich's resolution of Hilbert's tenth problem is the positive Pell equation.

Researchers attempted to generalize his arguments to arbitrary finitely generated rings, and were able to replace the role of Pell's equation in Matiyasevich's argument by *elliptic curves*.

However, the positive Pell equation always has a solution, and for this adaptation to work, one (roughly) needs to find for every number field K an elliptic curve E with $E(K) \cong \mathbb{Z}$.

Our construction fixes some $a_1, a_2, a_3 \in K$ and then considers the family

$$E^d : dy^2 = (x - a_1)(x - a_2)(x - a_3)$$

for varying d. Note that $E^d \cong E^1$ over $K(\sqrt{d})$ (in particular over $\overline{\mathbb{Q}}$) by changing y to $y/\sqrt{d}$. This is known as a *quadratic twist family*.

Connections with Pell's equation

There is no direct connection between elliptic curves and Pell's equation, but there is a close analogy between the two stories.

Connections with Pell's equation

There is no direct connection between elliptic curves and Pell's equation, but there is a close analogy between the two stories.

Elliptic curves have genus 1, while Pell's equation

$$C_d : x^2 - dy^2 = 1$$

defines a genus 0 curve.

Connections with Pell's equation

There is no direct connection between elliptic curves and Pell's equation, but there is a close analogy between the two stories.

Elliptic curves have genus 1, while Pell's equation

$$C_d : x^2 - dy^2 = 1$$

defines a genus 0 curve.

The solution sets have natural group structures in both cases; for Pell's equation this is classical, namely $C_d(\mathbb{Z}) \cong \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

Connections with Pell's equation

There is no direct connection between elliptic curves and Pell's equation, but there is a close analogy between the two stories.

Elliptic curves have genus 1, while Pell's equation

$$C_d : x^2 - dy^2 = 1$$

defines a genus 0 curve.

The solution sets have natural group structures in both cases; for Pell's equation this is classical, namely $C_d(\mathbb{Z}) \cong \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

Once more: all of the curves C_d are isomorphic over $\overline{\mathbb{Q}}$.

Generalized class groups

Class groups go back to Gauss: these measure how close rings such as $\mathbb{Z}[\zeta_n]$, $\mathbb{Z}[\sqrt{-3}]$, $\mathbb{Z}[\sqrt{-105}]$ and $\mathbb{Z}[\sqrt{d}]$ are to having "unique factorization".

Generalized class groups

Class groups go back to Gauss: these measure how close rings such as $\mathbb{Z}[\zeta_n]$, $\mathbb{Z}[\sqrt{-3}]$, $\mathbb{Z}[\sqrt{-105}]$ and $\mathbb{Z}[\sqrt{d}]$ are to having "unique factorization".

Conjecture (Gauss)

There are infinitely many squarefree d such that $\mathbb{Z}[\sqrt{d}]$ has unique factorization.

Generalized class groups

Class groups go back to Gauss: these measure how close rings such as $\mathbb{Z}[\zeta_n]$, $\mathbb{Z}[\sqrt{-3}]$, $\mathbb{Z}[\sqrt{-105}]$ and $\mathbb{Z}[\sqrt{d}]$ are to having "unique factorization".

Conjecture (Gauss)

There are infinitely many squarefree d such that $\mathbb{Z}[\sqrt{d}]$ has unique factorization.

These class groups took a prominent role in number theory from the 1850s, as the unique factorization theory of $\mathbb{Z}[\zeta_n]$ is closely connected to Fermat's last theorem.

Generalized class groups

Class groups go back to Gauss: these measure how close rings such as $\mathbb{Z}[\zeta_n]$, $\mathbb{Z}[\sqrt{-3}]$, $\mathbb{Z}[\sqrt{-105}]$ and $\mathbb{Z}[\sqrt{d}]$ are to having "unique factorization".

Conjecture (Gauss)

There are infinitely many squarefree d such that $\mathbb{Z}[\sqrt{d}]$ has unique factorization.

These class groups took a prominent role in number theory from the 1850s, as the unique factorization theory of $\mathbb{Z}[\zeta_n]$ is closely connected to Fermat's last theorem.

There is a "generalized class group" (known as Selmer group) that gives an upper bound on how many independent rational points an elliptic curve has.

The relevant class groups

The relevant class groups

The three relevant "generalized class groups" are:

The relevant class groups

The three relevant "generalized class groups" are:

- for Pell's equation it is $\mathrm{Cl}(\mathbb{Z}[\sqrt{d}])[2^\infty]$, which is closely connected to

$$H^1(G_{\mathbb{Q}}, \mathbb{Q}_2/\mathbb{Z}_2(\chi_d)),$$

The relevant class groups

The three relevant "generalized class groups" are:

- for Pell's equation it is $\mathrm{Cl}(\mathbb{Z}[\sqrt{d}])[2^\infty]$, which is closely connected to

$$H^1(G_{\mathbb{Q}}, \mathbb{Q}_2/\mathbb{Z}_2(\chi_d)),$$

- for sums of rational cubes it is $H^1(G_{\mathbb{Q}}, C_n[3^\infty])$,

The relevant class groups

The three relevant "generalized class groups" are:

- for Pell's equation it is $\mathrm{Cl}(\mathbb{Z}[\sqrt{d}])[2^\infty]$, which is closely connected to

$$H^1(G_{\mathbb{Q}}, \mathbb{Q}_2/\mathbb{Z}_2(\chi_d)),$$

- for sums of rational cubes it is $H^1(G_{\mathbb{Q}}, C_n[3^\infty])$,
- and for Hilbert's tenth problem it is $H^1(G_K, E^d[2^\infty])$.

The relevant class groups

The three relevant "generalized class groups" are:

- for Pell's equation it is $\mathrm{Cl}(\mathbb{Z}[\sqrt{d}])[2^\infty]$, which is closely connected to

$$H^1(G_{\mathbb{Q}}, \mathbb{Q}_2/\mathbb{Z}_2(\chi_d)),$$

- for sums of rational cubes it is $H^1(G_{\mathbb{Q}}, C_n[3^\infty])$,
- and for Hilbert's tenth problem it is $H^1(G_K, E^d[2^\infty])$.

Knowing the structure of the above groups allows one to decide if there is a solution to the relevant equation in each case (at least conjecturally).

The relevant class groups

The three relevant "generalized class groups" are:

- for Pell's equation it is $\mathrm{Cl}(\mathbb{Z}[\sqrt{d}])[2^\infty]$, which is closely connected to

$$H^1(G_{\mathbb{Q}}, \mathbb{Q}_2/\mathbb{Z}_2(\chi_d)),$$

- for sums of rational cubes it is $H^1(G_{\mathbb{Q}}, C_n[3^\infty])$,
- and for Hilbert's tenth problem it is $H^1(G_K, E^d[2^\infty])$.

Knowing the structure of the above groups allows one to decide if there is a solution to the relevant equation in each case (at least conjecturally).

Since the relevant curves are isomorphic over $\overline{\mathbb{Q}}$, this gives the extra structure:

$$\mathbb{F}_2(\chi_d) \cong \mathbb{F}_2(\chi_{d'}) = \mathbb{F}_2, \qquad C_n[3] \cong C_{n'}[3], \qquad E^d[2] \cong E^{d'}[2].$$

Exploiting this isomorphism

These isomorphisms ensure that the above Galois cohomology groups can intersect non-trivially.

Exploiting this isomorphism

These isomorphisms ensure that the above Galois cohomology groups can intersect non-trivially. For example, for Pell's equation, the bottom layer is just

$$H^1(G_{\mathbb{Q}}, \mathbb{F}_2) \leftrightarrow \{\text{sqf. integers}\}.$$

The same squarefree integer can appear for different curves C_d.

Exploiting this isomorphism

These isomorphisms ensure that the above Galois cohomology groups can intersect non-trivially. For example, for Pell's equation, the bottom layer is just

$$H^1(G_{\mathbb{Q}}, \mathbb{F}_2) \leftrightarrow \{\text{sqf. integers}\}.$$

The same squarefree integer can appear for different curves C_d.

Alex Smith was the first to realize that these isomorphisms have higher order analogues; namely, it is still possible to compare 2^k elements of order 2^k to get a reasonable object. Using this, he proved:

Exploiting this isomorphism

These isomorphisms ensure that the above Galois cohomology groups can intersect non-trivially. For example, for Pell's equation, the bottom layer is just

$$H^1(G_{\mathbb{Q}}, \mathbb{F}_2) \leftrightarrow \{\text{sqf. integers}\}.$$

The same squarefree integer can appear for different curves C_d.

Alex Smith was the first to realize that these isomorphisms have higher order analogues; namely, it is still possible to compare 2^k elements of order 2^k to get a reasonable object. Using this, he proved:

Theorem (Smith, 2017)

Assume BSD and let $E^d : dy^2 = x^3 - x$ be the "congruent number curve". The density of squarefree integers $|d| \leq B$ such that $E^d(\mathbb{Q})/E^d(\mathbb{Q})^{\text{tors}} \cong \mathbb{Z}^r$ is:

Exploiting this isomorphism

These isomorphisms ensure that the above Galois cohomology groups can intersect non-trivially. For example, for Pell's equation, the bottom layer is just

$$H^1(G_{\mathbb{Q}}, \mathbb{F}_2) \leftrightarrow \{\text{sqf. integers}\}.$$

The same squarefree integer can appear for different curves C_d.

Alex Smith was the first to realize that these isomorphisms have higher order analogues; namely, it is still possible to compare 2^k elements of order 2^k to get a reasonable object. Using this, he proved:

Theorem (Smith, 2017)

Assume BSD and let $E^d : dy^2 = x^3 - x$ be the "congruent number curve". The density of squarefree integers $|d| \leq B$ such that $E^d(\mathbb{Q})/E^d(\mathbb{Q})^{\text{tors}} \cong \mathbb{Z}^r$ is:

$$\begin{cases} 0.5 & \text{if } r = 0 \\ 0.5 & \text{if } r = 1 \\ 0 & \text{if } r \geq 2. \end{cases}$$

High-level proof overview

Smith's proof works in three high-level steps:

High-level proof overview

Smith's proof works in three high-level steps:

Step 1:

Algebra: Compare Galois cohomology classes

High-level proof overview

Smith's proof works in three high-level steps:

Step 1:

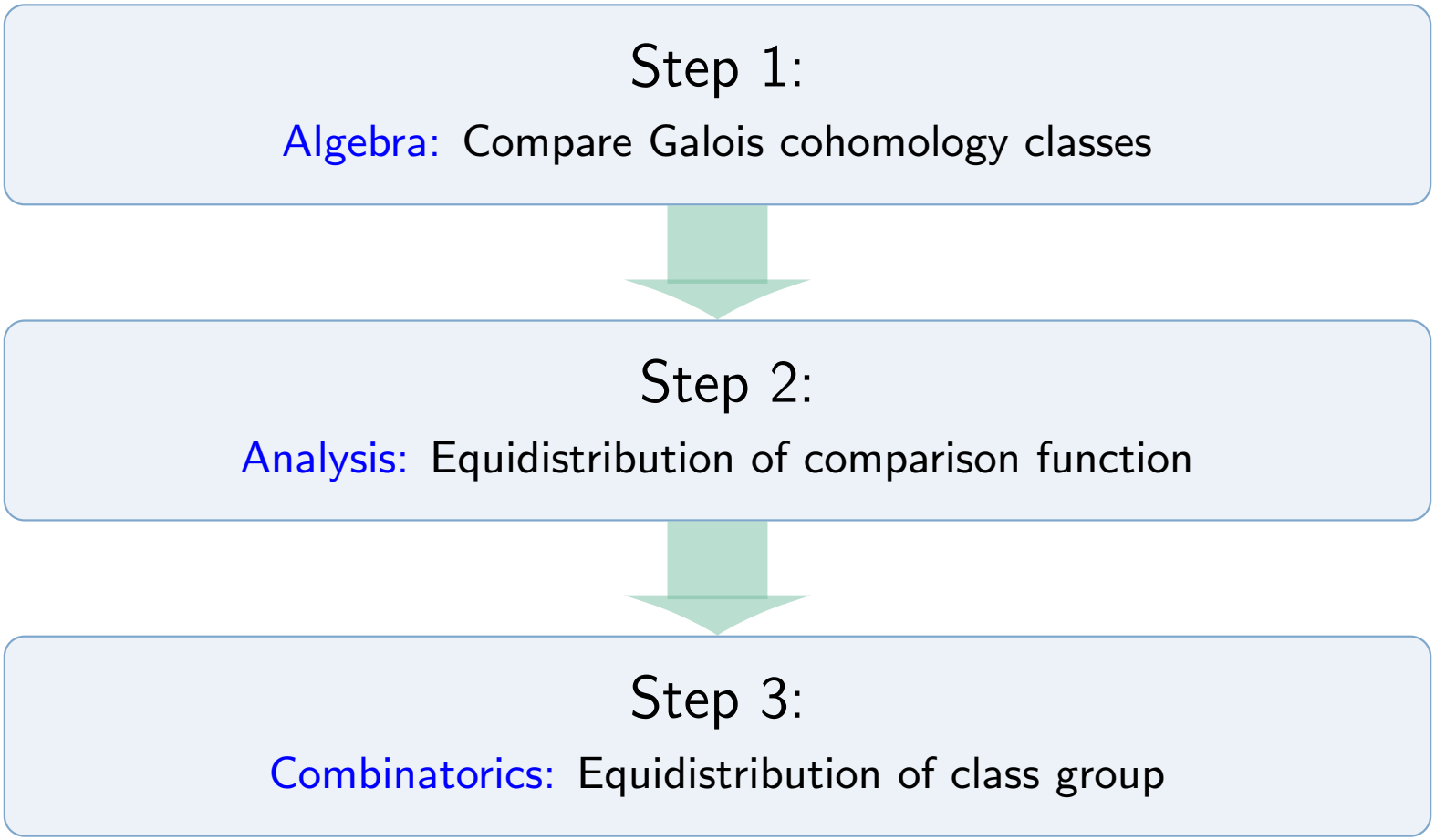
Algebra: Compare Galois cohomology classes

Step 2:

Analysis: Equidistribution of comparison function

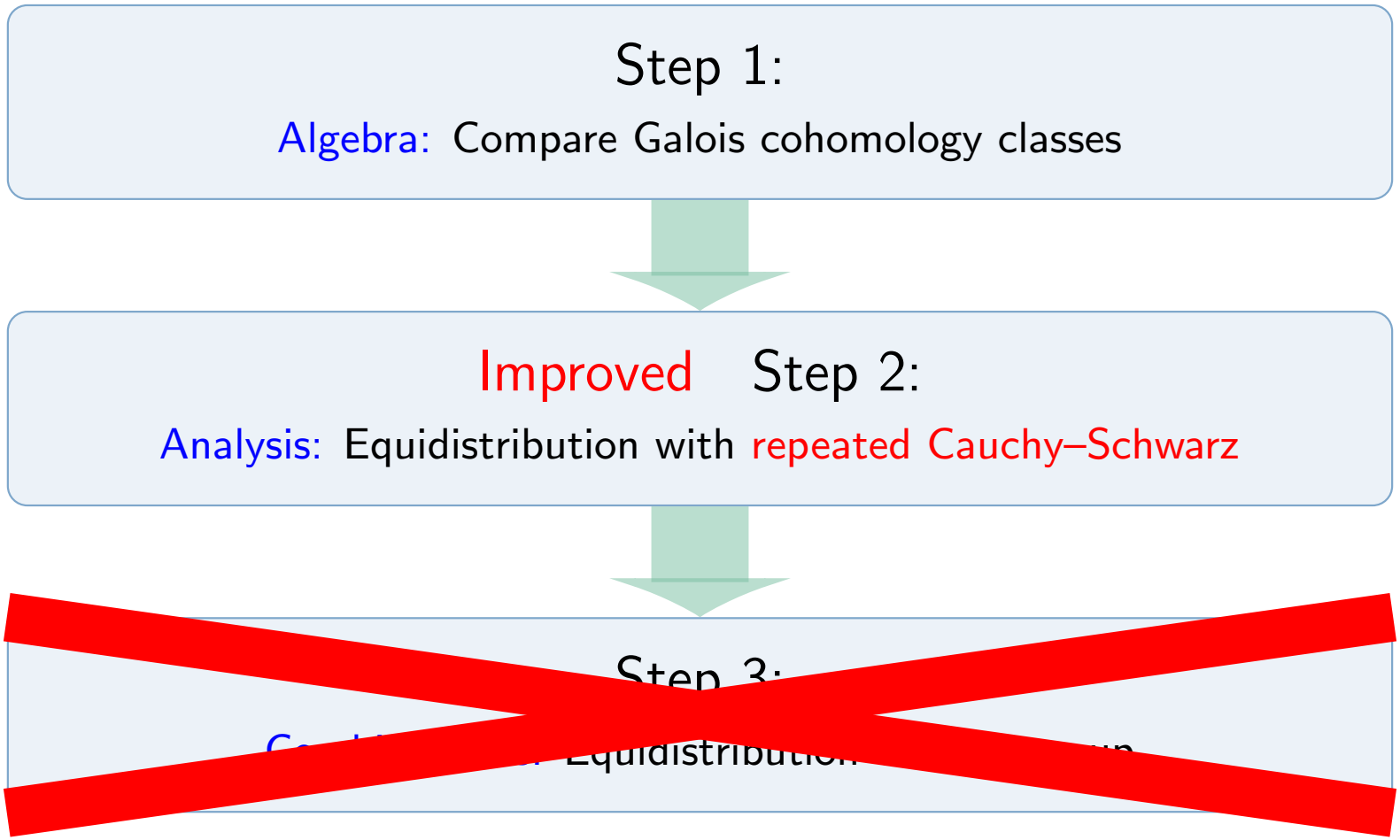
High-level proof overview

Smith's proof works in three high-level steps:



High-level proof overview

Lecture series:



Repeated Cauchy–Schwarz

Rough idea: given a product space, say $X := X_1 \times X_2 \times X_3$ with each X_i a subset of the prime numbers, we want to prove that

$$\sum_{(p,q,r)\in X} g(pqr)$$

is small, where $g(x)$ is some ± 1 function on X (namely the Cassels–Tate pairing).

Repeated Cauchy–Schwarz

Rough idea: given a product space, say $X := X_1 \times X_2 \times X_3$ with each X_i a subset of the prime numbers, we want to prove that

$$\sum_{(p,q,r)\in X} g(pqr)$$

is small, where $g(x)$ is some ± 1 function on X (namely the Cassels–Tate pairing).

In Step 1, one is able to prove a comparison result for 2^3 elements (a "cube")

$$C := \{p_1, p_2\} \times \{q_1, q_2\} \times \{r_1, r_2\},$$

Repeated Cauchy–Schwarz

Rough idea: given a product space, say $X := X_1 \times X_2 \times X_3$ with each X_i a subset of the prime numbers, we want to prove that

$$\sum_{(p,q,r)\in X} g(pqr)$$

is small, where $g(x)$ is some ± 1 function on X (namely the Cassels–Tate pairing).

In Step 1, one is able to prove a comparison result for 2^3 elements (a "cube")

$$C := \{p_1, p_2\} \times \{q_1, q_2\} \times \{r_1, r_2\},$$

namely we can show that the following product "along the cube C"

$$f(C) := \prod_{i,j,k\in\{1,2\}} g(p_i q_j r_k)$$

equals a "Chebotarev symbol".

Repeated Cauchy–Schwarz

Rough idea: given a product space, say $X := X_1 \times X_2 \times X_3$ with each X_i a subset of the prime numbers, we want to prove that

$$\sum_{(p,q,r)\in X} g(pqr)$$

is small, where $g(x)$ is some ± 1 function on X (namely the Cassels–Tate pairing).

In Step 1, one is able to prove a comparison result for 2^3 elements (a "cube")

$$C := \{p_1, p_2\} \times \{q_1, q_2\} \times \{r_1, r_2\},$$

namely we can show that the following product "along the cube C"

$$f(C) := \prod_{i,j,k\in\{1,2\}} g(p_i q_j r_k)$$

equals a "Chebotarev symbol". Moreover, we can prove equidistribution of $f(C)$ when summig over all $p_1, p_2 \in X_1, q_2, q_2 \in X_2, r_1, r_2 \in X_3$.

Repeated Cauchy–Schwarz II

There is a very natural abstract way to arrive at the correlation $\prod_{i,j,k\in\{1,2\}} g(p_i q_j r_k)$.

Repeated Cauchy–Schwarz II

There is a very natural abstract way to arrive at the correlation $\prod_{i,j,k\in\{1,2\}} g(p_i q_j r_k)$. The Cauchy–Schwarz inequality gives

$$\sum_{(p,q,r)\in X} g(pqr) \leq \sum_{(q,r)\in X_2\times X_3} 1 \cdot \left| \sum_{p\in X_1} g(pqr) \right|$$

$$\leq |X_2 \times X_3|^{1/2} \left(\sum_{p_1,p_2\in X_1} \sum_{(q,r)\in X_2\times X_3} g(p_1 qr) g(p_2 qr) \right)^{1/2}.$$

Repeated Cauchy–Schwarz II

There is a very natural abstract way to arrive at the correlation $\prod_{i,j,k\in\{1,2\}} g(p_i q_j r_k)$. The Cauchy–Schwarz inequality gives

$$\sum_{(p,q,r)\in X} g(pqr) \leq \sum_{(q,r)\in X_2\times X_3} 1 \cdot \left| \sum_{p\in X_1} g(pqr) \right|$$

$$\leq |X_2 \times X_3|^{1/2} \left(\sum_{p_1,p_2\in X_1} \sum_{(q,r)\in X_2\times X_3} g(p_1 qr) g(p_2 qr) \right)^{1/2}.$$

Doing this once over every interval X_i, one gets exactly the sum

$$\leq (|X_1||X_2||X_3|)^{3/4} \left(\sum_{p_1,p_2\in X_1} \sum_{q_1,q_2\in X_2} \sum_{r_1,r_2\in X_3} \prod_{i,j,k\in\{1,2\}} g(p_i q_j r_k) \right)^{1/8}.$$

Repeated Cauchy–Schwarz II

There is a very natural abstract way to arrive at the correlation $\prod_{i,j,k\in\{1,2\}} g(p_i q_j r_k)$. The Cauchy–Schwarz inequality gives

$$\sum_{(p,q,r)\in X} g(pqr) \leq \sum_{(q,r)\in X_2\times X_3} 1 \cdot \left| \sum_{p\in X_1} g(pqr) \right|$$

$$\leq |X_2 \times X_3|^{1/2} \left(\sum_{p_1,p_2\in X_1} \sum_{(q,r)\in X_2\times X_3} g(p_1 qr) g(p_2 qr) \right)^{1/2}.$$

Doing this once over every interval X_i, one gets exactly the sum

$$\leq (|X_1||X_2||X_3|)^{3/4} \left(\sum_{p_1,p_2\in X_1} \sum_{q_1,q_2\in X_2} \sum_{r_1,r_2\in X_3} \prod_{i,j,k\in\{1,2\}} g(p_i q_j r_k) \right)^{1/8}.$$

Now one can directly use our Step 1 to replace $\prod_{i,j,k\in\{1,2\}} g(p_i q_j r_k)$ by a symbol for which we can prove equidistribution, thus giving equidistribution of $g(x)$ on X.

Questions?

Thank you for your attention! Quick recap:

1. Introduction
2. Hilbert's tenth problem
3. The negative Pell equation
4. Sums of rational cubes
5. The common theme
6. High-level proof overview