Directions in arithmetic statistics

Peter Koymans
University of Michigan

Seminar

Zurich, 21 November 2022

Introduction

The aim of arithmetic statistics is to answer statistical questions of arithmetic objects (e.g. zeta functions, number fields, class groups) with many applications to other areas of mathematics and cryptography.

Introduction

The aim of arithmetic statistics is to answer statistical questions of arithmetic objects (e.g. zeta functions, number fields, class groups) with many applications to other areas of mathematics and cryptography.

We will discuss three leading conjectures in arithmetic statistics in this talk and my recent work on them.

Part I
Stevenhagen's conjecture

History of Pell's equation

For a fixed squarefree integer $d > 0$, the equation

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

has been studied since at least the ancient Greeks.

History of Pell's equation

For a fixed squarefree integer $d > 0$, the equation

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

has been studied since at least the ancient Greeks.

Bhaskara II (12th century) gave an algorithm to find non-trivial solutions of this equation.

History of Pell's equation

For a fixed squarefree integer $d > 0$, the equation

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

has been studied since at least the ancient Greeks.

Bhaskara II (12th century) gave an algorithm to find non-trivial solutions of this equation.

Fermat challenged Brouncker and Wallis to solve it for $d = 61$. The smallest non-trivial solution is

$$1766319049^2 - 61 \cdot 226153980^2 = 1.$$

History of Pell's equation

For a fixed squarefree integer $d > 0$, the equation

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

has been studied since at least the ancient Greeks.

Bhaskara II (12th century) gave an algorithm to find non-trivial solutions of this equation.

Fermat challenged Brouncker and Wallis to solve it for $d = 61$. The smallest non-trivial solution is

$$1766319049^2 - 61 \cdot 226153980^2 = 1.$$

Pell's equation plays a prominent role in modern number theory.

The negative Pell equation

The equation

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

is known as the negative Pell equation and is not always soluble.

The negative Pell equation

The equation

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

is known as the negative Pell equation and is not always soluble.

Define

$$\mathcal{D} := \{d > 0 : d \text{ squarefree}, p \mid d \Rightarrow p \not\equiv 3 \bmod 4\}$$

$$\mathcal{D}^- := \{d > 0 : d \text{ squarefree}, \text{negative Pell is soluble}\}.$$

The negative Pell equation

The equation

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

is known as the negative Pell equation and is not always soluble.

Define

$$\mathcal{D} := \{d > 0 : d \text{ squarefree}, p \mid d \Rightarrow p \not\equiv 3 \bmod 4\}$$

$$\mathcal{D}^- := \{d > 0 : d \text{ squarefree}, \text{negative Pell is soluble}\}.$$

We have $\mathcal{D}^- \subseteq \mathcal{D}$ by checking whether the equation is soluble modulo p.

The negative Pell equation

The equation

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

is known as the negative Pell equation and is not always soluble.

Define

$$\mathcal{D} := \{d > 0 : d \text{ squarefree}, p \mid d \Rightarrow p \not\equiv 3 \bmod 4\}$$

$$\mathcal{D}^- := \{d > 0 : d \text{ squarefree}, \text{negative Pell is soluble}\}.$$

We have $\mathcal{D}^- \subseteq \mathcal{D}$ by checking whether the equation is soluble modulo p.

Classical techniques in analytic number theory give a constant $C > 0$ such that

$$\#\{d \leq X : d \in \mathcal{D}\} \sim C \cdot \frac{X}{\sqrt{\log X}}.$$

The negative Pell equation

The equation

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

is known as the negative Pell equation and is not always soluble.

Define

$$\mathcal{D} := \{d > 0 : d \text{ squarefree}, p \mid d \Rightarrow p \not\equiv 3 \bmod 4\}$$

$$\mathcal{D}^- := \{d > 0 : d \text{ squarefree}, \text{negative Pell is soluble}\}.$$

We have $\mathcal{D}^- \subseteq \mathcal{D}$ by checking whether the equation is soluble modulo p.

Classical techniques in analytic number theory give a constant $C > 0$ such that

$$\#\{d \leq X : d \in \mathcal{D}\} \sim C \cdot \frac{X}{\sqrt{\log X}}.$$

Question: what is the density of $\mathcal{D}^-$ inside $\mathcal{D}$?

Conjectures on the negative Pell equation

Nagell (1930s) conjectured that

$$\lim_{X \to \infty} \frac{\#\{d \leq X : d \in \mathcal{D}^-\}}{\#\{d \leq X : d \in \mathcal{D}\}}$$

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

Conjectures on the negative Pell equation

Nagell (1930s) conjectured that

$$\lim_{X\to\infty} \frac{\#\{d \le X : d \in \mathcal{D}^-\}}{\#\{d \le X : d \in \mathcal{D}\}}$$

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

Stevenhagen (1995) conjectured that

$$\lim_{X\to\infty} \frac{\#\{d \le X : d \in \mathcal{D}^-\}}{\#\{d \le X : d \in \mathcal{D}\}} = 1-\alpha,$$

where

$$\alpha = \prod_{j=1}^{\infty}(1+2^{-j})^{-1} \approx 0.41942.$$

Progress towards Stevenhagen's conjecture

Fouvry–Klüners (2010) proved that

$$\frac{5\alpha}{4} \leq \liminf_{X\to\infty} \frac{\#\{d \leq X : d \in \mathcal{D}^-\}}{\#\{d \leq X : d \in \mathcal{D}\}} \leq \limsup_{X\to\infty} \frac{\#\{d \leq X : d \in \mathcal{D}^-\}}{\#\{d \leq X : d \in \mathcal{D}\}} \leq \frac{2}{3}.$$

Progress towards Stevenhagen's conjecture

Fouvry–Klüners (2010) proved that

$$\frac{5\alpha}{4} \leq \liminf_{X\to\infty} \frac{\#\{d \leq X : d \in \mathcal{D}^-\}}{\#\{d \leq X : d \in \mathcal{D}\}} \leq \limsup_{X\to\infty} \frac{\#\{d \leq X : d \in \mathcal{D}^-\}}{\#\{d \leq X : d \in \mathcal{D}\}} \leq \frac{2}{3}.$$

Theorem (K.–Pagano (2022))

We have

$$\lim_{X\to\infty} \frac{\#\{d \leq X : d \in \mathcal{D}^-\}}{\#\{d \leq X : d \in \mathcal{D}\}} = 1 - \alpha$$

in accordance with Nagell's and Stevenhagen's conjecture.

Progress towards Stevenhagen's conjecture

Fouvry–Klüners (2010) proved that

$$\frac{5\alpha}{4} \leq \liminf_{X\to\infty} \frac{\#\{d \leq X : d \in \mathcal{D}^-\}}{\#\{d \leq X : d \in \mathcal{D}\}} \leq \limsup_{X\to\infty} \frac{\#\{d \leq X : d \in \mathcal{D}^-\}}{\#\{d \leq X : d \in \mathcal{D}\}} \leq \frac{2}{3}.$$

Theorem (K.–Pagano (2022))

We have

$$\lim_{X\to\infty} \frac{\#\{d \leq X : d \in \mathcal{D}^-\}}{\#\{d \leq X : d \in \mathcal{D}\}} = 1 - \alpha$$

in accordance with Nagell's and Stevenhagen's conjecture.

Proof sketch: turn problem into question about $\mathrm{Cl}(\mathbb{Q}(\sqrt{d}))[2^\infty]$, the class group of $\mathbb{Q}(\sqrt{d})$, and obtain the distribution of the class group.

Part II
Applications of new techniques

Chowla's conjecture

Conjecture (Generalized Riemann hypothesis)

All non-trivial zeroes of $L(s, \chi)$ lie on $s = 1/2 + it$.

Chowla's conjecture

Conjecture (Generalized Riemann hypothesis)

All non-trivial zeroes of $L(s, \chi)$ lie on $s = 1/2 + it$.

Conjecture (Chowla's conjecture)

We have $L(\frac{1}{2}, \chi) \neq 0$ for all primitive Dirichlet characters χ.

Chowla's conjecture

Conjecture (Generalized Riemann hypothesis)

All non-trivial zeroes of $L(s, \chi)$ lie on $s = 1/2 + it$.

Conjecture (Chowla's conjecture)

We have $L(\frac{1}{2}, \chi) \neq 0$ for all primitive Dirichlet characters χ.

Important results towards Chowla's conjecture are due to Soundararajan (unconditionally) and Özlük–Snyder (conditionally).

Chowla's conjecture

Conjecture (Generalized Riemann hypothesis)

All non-trivial zeroes of $L(s, \chi)$ lie on $s = 1/2 + it$.

Conjecture (Chowla's conjecture)

We have $L(\frac{1}{2}, \chi) \neq 0$ for all primitive Dirichlet characters χ.

Important results towards Chowla's conjecture are due to Soundararajan (unconditionally) and Özlük–Snyder (conditionally).

There has also been great interest in the function field case of this conjecture.

Function fields

Theorem (W. Li (2018))

Let q be an odd prime power. There are infinitely many monic, squarefree polynomials $D \in \mathbb{F}_q[t]$ such that $L(\frac{1}{2}, \chi_D) = 0$.

Function fields

Theorem (W. Li (2018))

Let q be an odd prime power. There are infinitely many monic, squarefree polynomials $D \in \mathbb{F}_q[t]$ such that $L(\frac{1}{2}, \chi_D) = 0$.

However, 100% non-vanishing is still expected. This is currently not known for any single family of L-functions.

Function fields

Theorem (W. Li (2018))

Let q be an odd prime power. There are infinitely many monic, squarefree polynomials $D \in \mathbb{F}_q[t]$ such that $L(\frac{1}{2}, \chi_D) = 0$.

However, 100% non-vanishing is still expected. This is currently not known for any single family of L-functions.

The Özlük–Snyder result is known unconditionally over function fields (Bui–Florea).

Function fields

Theorem (W. Li (2018))

Let q be an odd prime power. There are infinitely many monic, squarefree polynomials $D \in \mathbb{F}_q[t]$ such that $L(\frac{1}{2}, \chi_D) = 0$.

However, 100% non-vanishing is still expected. This is currently not known for any single family of L-functions.

The Özlük–Snyder result is known unconditionally over function fields (Bui–Florea).

Many other families have also been studied but no 100% non-vanishing result is known.

Function fields

Theorem (W. Li (2018))

Let q be an odd prime power. There are infinitely many monic, squarefree polynomials $D \in \mathbb{F}_q[t]$ such that $L(\frac{1}{2}, \chi_D) = 0$.

However, 100% non-vanishing is still expected. This is currently not known for any single family of L-functions.

The Özlük–Snyder result is known unconditionally over function fields (Bui–Florea).

Many other families have also been studied but no 100% non-vanishing result is known.

Theorem (K.–Pagano–Shusterman (in progress))

We have $L(\frac{1}{2}, \chi_D) \neq 0$ for 100% of the monic squarefree polynomials D.

Proof sketch

By a result of Groethendieck we have $L(\frac{1}{2}, \chi_D) \neq 0$ if and only if there exists an embedding

$$\mathbb{Q}_2/\mathbb{Z}_2 \hookrightarrow \mathrm{Jac}(C_D)(\overline{\mathbb{F}_q})[2^\infty][\mathrm{Frob}_q^2 - q],$$

where C_D is the curve $y^2 = D$.

Proof sketch

By a result of Groethendieck we have $L(\frac{1}{2}, \chi_D) \neq 0$ if and only if there exists an embedding

$$\mathbb{Q}_2/\mathbb{Z}_2 \hookrightarrow \mathrm{Jac}(C_D)(\overline{\mathbb{F}_q})[2^\infty][\mathrm{Frob}_q^2 - q],$$

where C_D is the curve $y^2 = D$.

The Jacobian can be viewed as a function field analogue of the class group.

Proof sketch

By a result of Groethendieck we have $L(\frac{1}{2}, \chi_D) \neq 0$ if and only if there exists an embedding

$$\mathbb{Q}_2/\mathbb{Z}_2 \hookrightarrow \mathrm{Jac}(C_D)(\overline{\mathbb{F}_q})[2^\infty][\mathrm{Frob}_q^2 - q],$$

where C_D is the curve $y^2 = D$.

The Jacobian can be viewed as a function field analogue of the class group.

A suitable adaptation of our methods for Stevenhagen's conjecture allow one to obtain the distribution of this Jacobian, from which the theorem follows.

Part III
Malle's conjecture

Number fields

Definition

A number field is a field extension K of $\mathbb{Q}$ such that K is finite dimensional as a vector space over $\mathbb{Q}$.

Number fields

Definition

A number field is a field extension K of $\mathbb{Q}$ such that K is finite dimensional as a vector space over $\mathbb{Q}$.

Number fields provide an incredibly rich source of lattices.

Number fields

Definition

A number field is a field extension K of $\mathbb{Q}$ such that K is finite dimensional as a vector space over $\mathbb{Q}$.

Number fields provide an incredibly rich source of lattices.

Number fields also play a key role in the currently fastest (general purpose) algorithm for factoring integers, the number field sieve.

Number fields

Definition

A number field is a field extension K of $\mathbb{Q}$ such that K is finite dimensional as a vector space over $\mathbb{Q}$.

Number fields provide an incredibly rich source of lattices.

Number fields also play a key role in the currently fastest (general purpose) algorithm for factoring integers, the number field sieve.

Arithmetic statistics is interested in counting number fields with given properties, which goes back to Gauss counting squarefree integers.

The conjecture

Conjecture (Malle's conjecture)

Let G be a finite, non-trivial group. Then there exist numbers $c(G) > 0$, $b(G) \in \mathbb{Z}_{\geq 0}$ and $a(G) \in \mathbb{Q}_{>0}$ such that

$$\#\{K/\mathbb{Q} : D_K \leq X, \mathrm{Gal}(K/\mathbb{Q}) \cong G\} \sim c(G) X^{a(G)} (\log X)^{b(G)}.$$

The conjecture

Conjecture (Malle's conjecture)

Let G be a finite, non-trivial group. Then there exist numbers $c(G) > 0$, $b(G) \in \mathbb{Z}_{\geq 0}$ and $a(G) \in \mathbb{Q}_{>0}$ such that

$$\#\{K/\mathbb{Q} : D_K \leq X, \mathrm{Gal}(K/\mathbb{Q}) \cong G\} \sim c(G) X^{a(G)} (\log X)^{b(G)}.$$

This is a generalization of the inverse Galois problem.

The conjecture

Conjecture (Malle's conjecture)

Let G be a finite, non-trivial group. Then there exist numbers $c(G) > 0$, $b(G) \in \mathbb{Z}_{\geq 0}$ and $a(G) \in \mathbb{Q}_{>0}$ such that

$$\#\{K/\mathbb{Q} : D_K \leq X, \mathrm{Gal}(K/\mathbb{Q}) \cong G\} \sim c(G) X^{a(G)} (\log X)^{b(G)}.$$

This is a generalization of the inverse Galois problem.

Important known cases: abelian G by Wright (1989), S_4, S_5 by Bhargava, Heisenberg extensions by Fouvry–K. (2021).

Malle's conjecture by product of ramified primes

Ordering by discriminant has some undesirable features: leading constant need not be an Euler product and subfields may occur a positive proportion of the time.

Malle's conjecture by product of ramified primes

Ordering by discriminant has some undesirable features: leading constant need not be an Euler product and subfields may occur a positive proportion of the time.

Wood (2010) introduced a class of "fair counting functions".

Malle's conjecture by product of ramified primes

Ordering by discriminant has some undesirable features: leading constant need not be an Euler product and subfields may occur a positive proportion of the time.

Wood (2010) introduced a class of "fair counting functions".

Important examples of fair counting functions are the conductor and the product of ramified primes.

Malle's conjecture by product of ramified primes

Ordering by discriminant has some undesirable features: leading constant need not be an Euler product and subfields may occur a positive proportion of the time.

Wood (2010) introduced a class of "fair counting functions".

Important examples of fair counting functions are the conductor and the product of ramified primes.

Mäki (1993): Malle's conjecture for abelian extensions ordered by conductor.

Malle's conjecture by product of ramified primes

Ordering by discriminant has some undesirable features: leading constant need not be an Euler product and subfields may occur a positive proportion of the time.

Wood (2010) introduced a class of "fair counting functions".

Important examples of fair counting functions are the conductor and the product of ramified primes.

Mäki (1993): Malle's conjecture for abelian extensions ordered by conductor.

Wood (2010): Malle's conjecture for abelian extensions ordered by any fair counting function.

Nilpotent groups

Theorem (K.–Pagano (in progress))

Assume GRH. Let G be a nilpotent group with $\#G$ odd. Then

$$\#\left\{K/\mathbb{Q} : \prod_{p : I_p \neq \{\mathrm{id}\}} p \leq X, \mathrm{Gal}(K/\mathbb{Q}) \cong G\right\} \sim c'(G) X (\log X)^{b'(G)}.$$

Nilpotent groups

Theorem (K.–Pagano (in progress))

Assume GRH. Let G be a nilpotent group with $\#G$ odd. Then

$$\#\left\{K/\mathbb{Q} : \prod_{p : I_p \neq \{\mathrm{id}\}} p \leq X, \mathrm{Gal}(K/\mathbb{Q}) \cong G\right\} \sim c'(G) X (\log X)^{b'(G)}.$$

Remark: any group G with $|G| = p^n$ is nilpotent. Also all abelian groups are nilpotent.

Nilpotent groups

Theorem (K.–Pagano (in progress))

Assume GRH. Let G be a nilpotent group with $\#G$ odd. Then

$$\#\left\{K/\mathbb{Q} : \prod_{p : I_p \neq \{\mathrm{id}\}} p \leq X, \mathrm{Gal}(K/\mathbb{Q}) \cong G\right\} \sim c'(G) X (\log X)^{b'(G)}.$$

Remark: any group G with $|G| = p^n$ is nilpotent. Also all abelian groups are nilpotent.

Here $c'(G)$ is the expected Euler product and $b'(G)$ is the naïve analogue of Malle's $b(G)$ in this situation.

Questions?

Thank you for your attention!