Directions in arithmetic statistics

Peter Koymans
University of Michigan

Seminar

Bonn, 16 November 2022

Part I
The negative Pell 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.

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

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

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

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

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

By the Hasse-Minkowski Theorem we have $\mathcal{D}^- \subseteq \mathcal{D}$.

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

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

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

By the Hasse-Minkowski Theorem we have $\mathcal{D}^- \subseteq \mathcal{D}$.

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

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

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

By the Hasse-Minkowski Theorem we have $\mathcal{D}^- \subseteq \mathcal{D}$.

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

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

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

Stevenhagen (1995) conjectured that

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

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

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

Chan–K.–Milovic–Pagano improved the lower bound to

$$\alpha \cdot \sum_{n=0}^{\infty} 2^{-n(n+3)/2} \approx \alpha \cdot 1.28325.$$

Progress towards Stevenhagen's conjecture

Fouvry–Klüners (2010) proved that

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

Chan–K.–Milovic–Pagano improved the lower bound to

$$\alpha \cdot \sum_{n=0}^{\infty} 2^{-n(n+3)/2} \approx \alpha \cdot 1.28325.$$

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

The negative Pell equation is soluble if and only if the natural surjective map $\mathrm{Cl}^+(\mathbb{Q}(\sqrt{d}))[2^\infty] \to \mathrm{Cl}(\mathbb{Q}(\sqrt{d}))[2^\infty]$ is an isomorphism.

Proof sketch

The negative Pell equation is soluble if and only if the natural surjective map $\mathrm{Cl}^+(\mathbb{Q}(\sqrt{d}))[2^\infty] \to \mathrm{Cl}(\mathbb{Q}(\sqrt{d}))[2^\infty]$ is an isomorphism.

Theorem (A. Smith (2017))

Let A be a finite, abelian 2-group. Then

$$\lim_{X\to\infty} \frac{\#\{K \text{ im. quadr.} : |D_K| < X, 2\mathrm{Cl}(K)[2^\infty] \cong A\}}{\#\{K \text{ im. quadr.} : |D_K| < X\}} = \frac{\prod_{i=1}^{\infty}\left(1-\frac{1}{2^i}\right)}{\#\mathrm{Aut}(A)}.$$

Proof sketch

The negative Pell equation is soluble if and only if the natural surjective map $\mathrm{Cl}^+(\mathbb{Q}(\sqrt{d}))[2^\infty] \to \mathrm{Cl}(\mathbb{Q}(\sqrt{d}))[2^\infty]$ is an isomorphism.

Theorem (A. Smith (2017))

Let A be a finite, abelian 2-group. Then

$$\lim_{X\to\infty} \frac{\#\{K \text{ im. quadr.} : |D_K| < X, 2\mathrm{Cl}(K)[2^\infty] \cong A\}}{\#\{K \text{ im. quadr.} : |D_K| < X\}} = \frac{\prod_{i=1}^{\infty}\left(1 - \frac{1}{2^i}\right)}{\#\mathrm{Aut}(A)}.$$

There are major obstructions to adapt Smith's work to the family $\mathcal{D}$

Proof sketch

The negative Pell equation is soluble if and only if the natural surjective map $\mathrm{Cl}^+(\mathbb{Q}(\sqrt{d}))[2^\infty] \to \mathrm{Cl}(\mathbb{Q}(\sqrt{d}))[2^\infty]$ is an isomorphism.

Theorem (A. Smith (2017))

Let A be a finite, abelian 2-group. Then

$$\lim_{X\to\infty} \frac{\#\{K \text{ im. quadr.} : |D_K| < X, 2\mathrm{Cl}(K)[2^\infty] \cong A\}}{\#\{K \text{ im. quadr.} : |D_K| < X\}} = \frac{\prod_{i=1}^\infty \left(1 - \frac{1}{2^i}\right)}{\#\mathrm{Aut}(A)}.$$

There are major obstructions to adapt Smith's work to the family $\mathcal{D}$

- we work with real quadratic fields instead of imaginary quadratic;

Proof sketch

The negative Pell equation is soluble if and only if the natural surjective map $\mathrm{Cl}^+(\mathbb{Q}(\sqrt{d}))[2^\infty] \to \mathrm{Cl}(\mathbb{Q}(\sqrt{d}))[2^\infty]$ is an isomorphism.

Theorem (A. Smith (2017))

Let A be a finite, abelian 2-group. Then

$$\lim_{X\to\infty} \frac{\#\left\{K \text{ im. quadr.} : |D_K| < X, 2\mathrm{Cl}(K)[2^\infty] \cong A\right\}}{\#\left\{K \text{ im. quadr.} : |D_K| < X\right\}} = \frac{\prod_{i=1}^{\infty}\left(1-\frac{1}{2^i}\right)}{\#\mathrm{Aut}(A)}.$$

There are major obstructions to adapt Smith's work to the family $\mathcal{D}$

- we work with real quadratic fields instead of imaginary quadratic;
- $\mathcal{D}$ has density 0 in the squarefree integers;

Proof sketch

The negative Pell equation is soluble if and only if the natural surjective map $\mathrm{Cl}^+(\mathbb{Q}(\sqrt{d}))[2^\infty] \to \mathrm{Cl}(\mathbb{Q}(\sqrt{d}))[2^\infty]$ is an isomorphism.

Theorem (A. Smith (2017))

Let A be a finite, abelian 2-group. Then

$$\lim_{X\to\infty} \frac{\#\{K \text{ im. quadr.} : |D_K| < X, 2\mathrm{Cl}(K)[2^\infty] \cong A\}}{\#\{K \text{ im. quadr.} : |D_K| < X\}} = \frac{\prod_{i=1}^{\infty}\left(1 - \frac{1}{2^i}\right)}{\#\mathrm{Aut}(A)}.$$

There are major obstructions to adapt Smith's work to the family $\mathcal{D}$

- we work with real quadratic fields instead of imaginary quadratic;
- $\mathcal{D}$ has density 0 in the squarefree integers;
- $\mathcal{D}$ naturally ends up in the error term in Smith's proof!

Proof sketch

The negative Pell equation is soluble if and only if the natural surjective map $\mathrm{Cl}^+(\mathbb{Q}(\sqrt{d}))[2^\infty] \to \mathrm{Cl}(\mathbb{Q}(\sqrt{d}))[2^\infty]$ is an isomorphism.

Theorem (A. Smith (2017))

Let A be a finite, abelian 2-group. Then

$$\lim_{X\to\infty} \frac{\#\{K \text{ im. quadr.} : |D_K| < X, 2\mathrm{Cl}(K)[2^\infty] \cong A\}}{\#\{K \text{ im. quadr.} : |D_K| < X\}} = \frac{\prod_{i=1}^{\infty}\left(1 - \frac{1}{2^i}\right)}{\#\mathrm{Aut}(A)}.$$

There are major obstructions to adapt Smith's work to the family $\mathcal{D}$

- we work with real quadratic fields instead of imaginary quadratic;
- $\mathcal{D}$ has density 0 in the squarefree integers;
- $\mathcal{D}$ naturally ends up in the error term in Smith's proof!

Last part is due to some extra symmetry property in this family. This has prevented Smith's techniques from being applied in many other settings.

New tools

We prove a reciprocity law for $C_2 \wr C_2^n$-extensions of $\mathbb{Q}$.

New tools

We prove a reciprocity law for $C_2 \wr C_2^n$-extensions of $\mathbb{Q}$.
For $n = 0$: this is quadratic reciprocity.

New tools

We prove a reciprocity law for $C_2 \wr C_2^n$-extensions of $\mathbb{Q}$.
For $n = 0$: this is quadratic reciprocity.
For $n = 1$: this is Rédei reciprocity (splitting in D_4-extensions).

New tools

We prove a reciprocity law for $C_2 \wr C_2^n$-extensions of $\mathbb{Q}$.
For $n = 0$: this is quadratic reciprocity.
For $n = 1$: this is Rédei reciprocity (splitting in D_4-extensions).

Proof relies on our earlier description of $\mathrm{Cl}(K)[2]$ for K multiquadratic.

New tools

We prove a reciprocity law for $C_2 \wr C_2^n$-extensions of $\mathbb{Q}$.
For $n = 0$: this is quadratic reciprocity.
For $n = 1$: this is Rédei reciprocity (splitting in D_4-extensions).

Proof relies on our earlier description of $\mathrm{Cl}(K)[2]$ for K multiquadratic.

Another new aspect: appearance of *involution spins*

$$\left(\frac{\alpha}{\sigma(\alpha)}\right)_K,$$

where K is multiquadratic, $(\cdot/\cdot)_K$ is the Legendre symbol and σ is an element of $\mathrm{Gal}(K/\mathbb{Q})$.

New tools

We prove a reciprocity law for $C_2 \wr C_2^n$-extensions of $\mathbb{Q}$.
For $n = 0$: this is quadratic reciprocity.
For $n = 1$: this is Rédei reciprocity (splitting in D_4-extensions).

Proof relies on our earlier description of $\mathrm{Cl}(K)[2]$ for K multiquadratic.

Another new aspect: appearance of *involution spins*

$$\left(\frac{\alpha}{\sigma(\alpha)}\right)_K,$$

where K is multiquadratic, $(\cdot/\cdot)_K$ is the Legendre symbol and σ is an element of $\mathrm{Gal}(K/\mathbb{Q})$.

We prove that such an involution spin vanishes under suitable conditions.

New tools

We prove a reciprocity law for $C_2 \wr C_2^n$-extensions of $\mathbb{Q}$.
For $n = 0$: this is quadratic reciprocity.
For $n = 1$: this is Rédei reciprocity (splitting in D_4-extensions).

Proof relies on our earlier description of $\mathrm{Cl}(K)[2]$ for K multiquadratic.

Another new aspect: appearance of *involution spins*

$$\left(\frac{\alpha}{\sigma(\alpha)}\right)_K,$$

where K is multiquadratic, $(\cdot/\cdot)_K$ is the Legendre symbol and σ is an element of $\mathrm{Gal}(K/\mathbb{Q})$.

We prove that such an involution spin vanishes under suitable conditions.

Here we make essential use of the fact that all odd prime divisors of $\mathcal{D}$ are 1 modulo 4.

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), and many other families have also been studied.

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), and many other families have also been studied.

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 $y^2 = D$.

We now consider the Bloch–Kato Selmer groups $H^1(\mathbb{F}_q(t), M)$, where $M = \mathbb{Z}_2[x]/(x^2 - q)$.

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 $y^2 = D$.

We now consider the Bloch–Kato Selmer groups $H^1(\mathbb{F}_q(t), M)$, where $M = \mathbb{Z}_2[x]/(x^2 - q)$.

Bloch–Kato Selmer groups naturally come with a (sequence of) generalized Cassels–Tate pairings.

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 $y^2 = D$.

We now consider the Bloch–Kato Selmer groups $H^1(\mathbb{F}_q(t), M)$, where $M = \mathbb{Z}_2[x]/(x^2 - q)$.

Bloch–Kato Selmer groups naturally come with a (sequence of) generalized Cassels–Tate pairings.

We prove equidistribution of this pairing using the techniques from Stevenhagen's conjecture.

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 $y^2 = D$.

We now consider the Bloch–Kato Selmer groups $H^1(\mathbb{F}_q(t), M)$, where $M = \mathbb{Z}_2[x]/(x^2 - q)$.

Bloch–Kato Selmer groups naturally come with a (sequence of) generalized Cassels–Tate pairings.

We prove equidistribution of this pairing using the techniques from Stevenhagen's conjecture.

Critically, the first Bloch–Kato Selmer group satisfies some additional symmetry pairings.

Greenberg's conjecture

There is also a number field analogue, where one replaces Frob_q by a generator of the unique $\mathbb{Z}_2$-extension of $\mathbb{Q}$.

Greenberg's conjecture

There is also a number field analogue, where one replaces Frob_q by a generator of the unique $\mathbb{Z}_2$-extension of $\mathbb{Q}$.

In this way one obtains non-vanishing results for p-adic L-functions.

Greenberg's conjecture

There is also a number field analogue, where one replaces Frob_q by a generator of the unique $\mathbb{Z}_2$-extension of $\mathbb{Q}$.

In this way one obtains non-vanishing results for p-adic L-functions.

The next conjecture is one of the central conjectures in Iwasawa theory.

Conjecture (Greenberg's conjecture)

Let K be a real quadratic field. Then the p-part of the class group of KL is finite, where L is the cyclotomic $\mathbb{Z}_p$-extension.

Greenberg's conjecture

There is also a number field analogue, where one replaces Frob_q by a generator of the unique $\mathbb{Z}_2$-extension of $\mathbb{Q}$.

In this way one obtains non-vanishing results for p-adic L-functions.

The next conjecture is one of the central conjectures in Iwasawa theory.

Conjecture (Greenberg's conjecture)

Let K be a real quadratic field. Then the p-part of the class group of KL is finite, where L is the cyclotomic $\mathbb{Z}_p$-extension.

One may consider a statistical version of this conjecture for $p = 2$, i.e. a 100% result. In the first layer we have:

Theorem (K.–Morgan–Smit (2021))

We have $\mathrm{rk}_4 \mathrm{Cl}(\mathbb{Q}(\sqrt{n}, \sqrt{2})) = \omega_{3,5}(n) - 2$ *for 100% of the squarefree integers n.*

Part III
Malle's conjecture

The conjecture

Conjecture (Malle's conjecture)

Let G be a 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 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.

Known cases

Malle's conjecture is known in a limited number of cases.

- abelian G by Wright;

Known cases

Malle's conjecture is known in a limited number of cases.

- abelian G by Wright;
- S_3 by Davenport–Heilbronn;

Known cases

Malle's conjecture is known in a limited number of cases.

- abelian G by Wright;
- S_3 by Davenport–Heilbronn;
- S_4, S_5 by Bhargava;

Known cases

Malle's conjecture is known in a limited number of cases.

- abelian G by Wright;
- S_3 by Davenport–Heilbronn;
- S_4, S_5 by Bhargava;
- sextic S_3 by Bhargava–Wood;

Known cases

Malle's conjecture is known in a limited number of cases.

- abelian G by Wright;
- S_3 by Davenport–Heilbronn;
- S_4, S_5 by Bhargava;
- sextic S_3 by Bhargava–Wood;
- quartic D_4 by Cohen–Diaz y Diaz–Olivier;

Known cases

Malle's conjecture is known in a limited number of cases.

- abelian G by Wright;
- S_3 by Davenport–Heilbronn;
- S_4, S_5 by Bhargava;
- sextic S_3 by Bhargava–Wood;
- quartic D_4 by Cohen–Diaz y Diaz–Olivier;
- generalized quaternion groups by Klüners;

Known cases

Malle's conjecture is known in a limited number of cases.

- abelian G by Wright;
- S_3 by Davenport–Heilbronn;
- S_4, S_5 by Bhargava;
- sextic S_3 by Bhargava–Wood;
- quartic D_4 by Cohen–Diaz y Diaz–Olivier;
- generalized quaternion groups by Klüners;
- any nilpotent group G such that all elements of order p are central, where p is the smallest prime dividing $\#G$, by K.–Pagano;

Known cases

Malle's conjecture is known in a limited number of cases.

- abelian G by Wright;
- S_3 by Davenport–Heilbronn;
- S_4, S_5 by Bhargava;
- sextic S_3 by Bhargava–Wood;
- quartic D_4 by Cohen–Diaz y Diaz–Olivier;
- generalized quaternion groups by Klüners;
- any nilpotent group G such that all elements of order p are central, where p is the smallest prime dividing $\#G$, by K.–Pagano;
- direct products $S_n \times A$ for $n \in \{3, 4, 5\}$ and A abelian by Wang (with $\#A$ coprime to some values) and later by Masri–Thorne–Tsai–Wang;

Known cases

Malle's conjecture is known in a limited number of cases.

- abelian G by Wright;
- S_3 by Davenport–Heilbronn;
- S_4, S_5 by Bhargava;
- sextic S_3 by Bhargava–Wood;
- quartic D_4 by Cohen–Diaz y Diaz–Olivier;
- generalized quaternion groups by Klüners;
- any nilpotent group G such that all elements of order p are central, where p is the smallest prime dividing $\#G$, by K.–Pagano;
- direct products $S_n \times A$ for $n \in \{3, 4, 5\}$ and A abelian by Wang (with $\#A$ coprime to some values) and later by Masri–Thorne–Tsai–Wang;
- nonic Heisenberg extensions by K.–Fouvry.

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 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 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 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 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.

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 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.

Altug–Shankar–Varma–Wilson count D_4-extensions by (Artin) conductor.

Nilpotent groups

Theorem (K.–Pagano (in progress))

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

$$\#\left\{K/\mathbb{Q} : \prod_{p: I_p \neq \{\mathrm{id}\}} p \leq X, \mathrm{Gal}(K/\mathbb{Q}) \cong G, K \cap \mathbb{Q}(\zeta_{|G|^\infty}) = \mathbb{Q}\right\}$$

is asymptotic to $c'(G)X(\log X)^{b'(G)}$.

Nilpotent groups

Theorem (K.–Pagano (in progress))

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

$$\#\left\{K/\mathbb{Q} : \prod_{p : I_p \neq \{\mathrm{id}\}} p \leq X, \mathrm{Gal}(K/\mathbb{Q}) \cong G, K \cap \mathbb{Q}(\zeta_{|G|^\infty}) = \mathbb{Q}\right\}$$

is asymptotic to $c'(G)X(\log X)^{b'(G)}$.

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

Nilpotent groups

Theorem (K.–Pagano (in progress))

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

$$\#\left\{K/\mathbb{Q} : \prod_{p : I_p \neq \{\mathrm{id}\}} p \leq X, \mathrm{Gal}(K/\mathbb{Q}) \cong G, K \cap \mathbb{Q}(\zeta_{|G|^\infty}) = \mathbb{Q}\right\}$$

is asymptotic to $c'(G)X(\log X)^{b'(G)}$.

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

Surprisingly, the exponent $b'(G)$ need no longer be correct if the condition $K \cap \mathbb{Q}(\zeta_{|G|^\infty}) = \mathbb{Q}$ is dropped.

Questions?

Thank you for your attention!