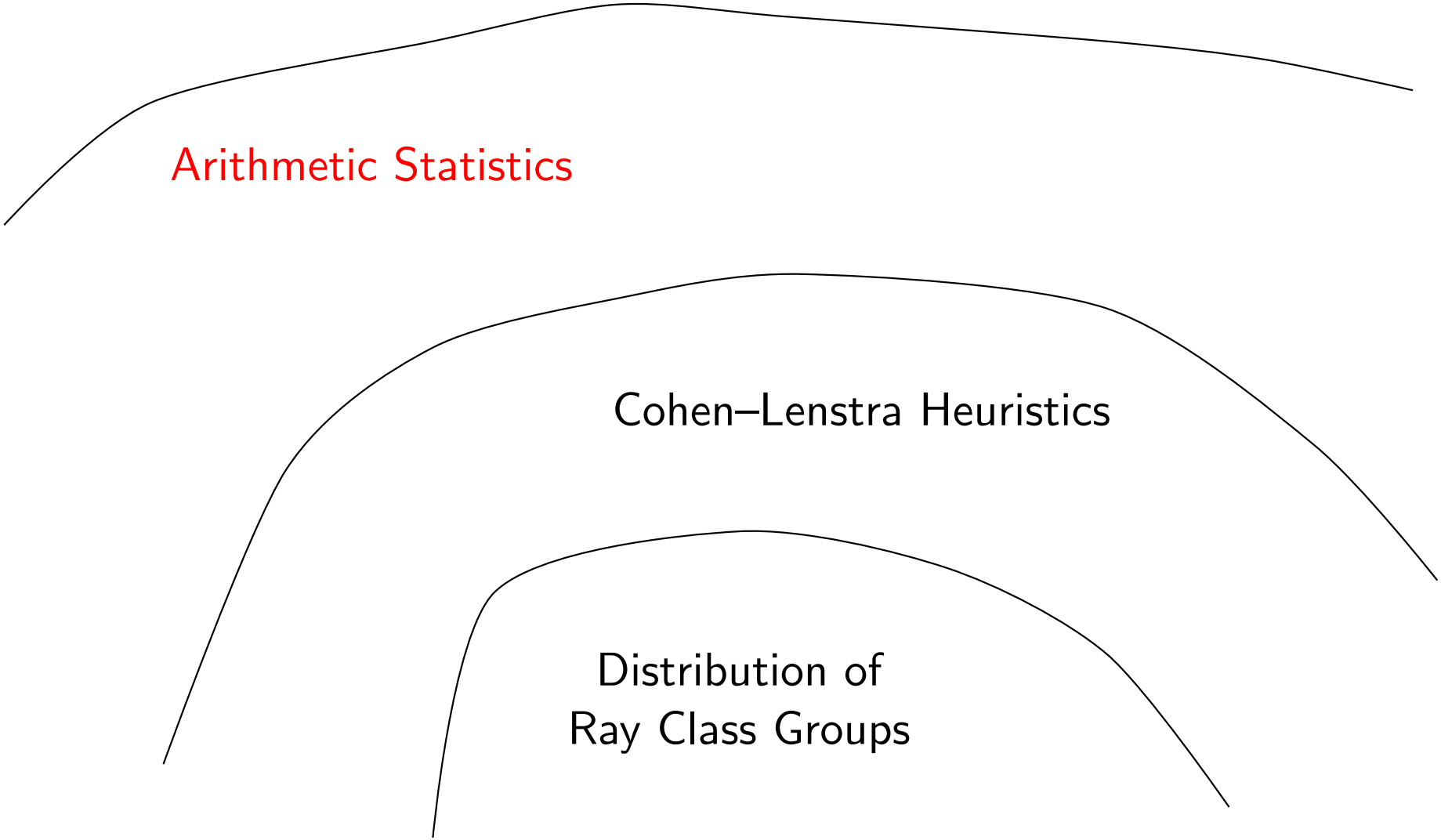
Distribution of Ray Class Groups of Random Number Fields

Robin Ammon

University of Glasgow

Y-RANT 2024

Landscape


Arithmetic Statistics
Cohen–Lenstra Heuristics
Distribution of
Ray Class Groups

What is Arithmetic Statistics?

Deals with statistical questions about number-theoretic objects, e.g.

- When $d > 0$ varies, how often is $x^2 - dy^2 = 4$ soluble over $\mathbb{Z}$?
- How often is the ideal class group of a number field cyclic?
- What is the distribution of (ray) class groups?

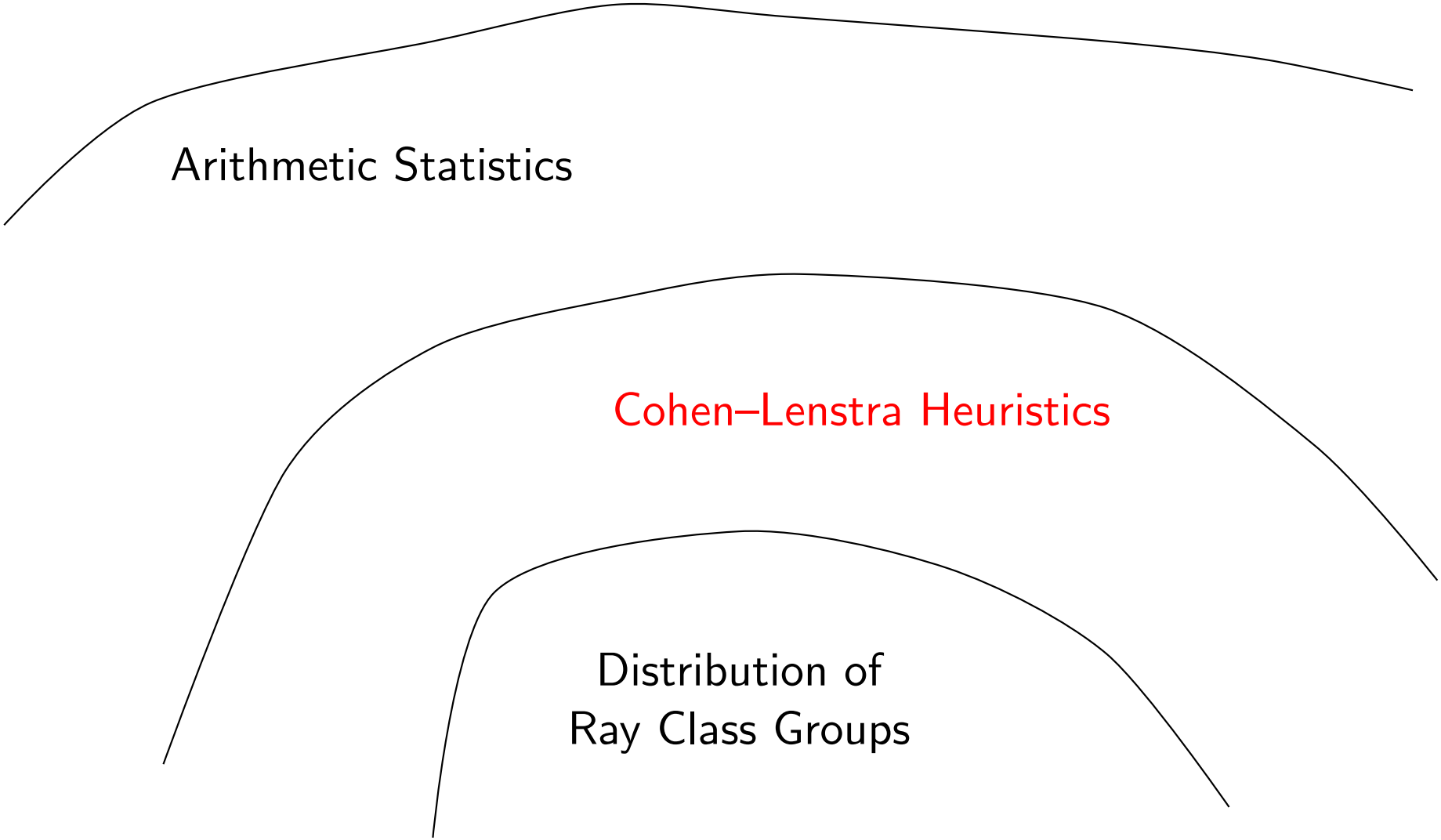
Motivation:

- Statistical behaviour reflects properties of the objects
- So: Understand statistics $\Longrightarrow$ understand objects

Note: deal with deterministic objects, so can prove statements

- Theorems are powerful as they contain a lot of info about the objects
- Findind good conjecture is often hard

Landscape


Arithmetic Statistics
Cohen–Lenstra Heuristics
Distribution of
Ray Class Groups

Ideal Class Groups

K number field, Cl_K ideal class group

- Cl_K is finite abelian, measures failure of unique factorisation in $\mathcal{O}_K$
- Central object yet structure is poorly understood

Cohen, Lenstra: Study distribution of Cl_K!

- Here: Distribution of Sylow subgroup $\mathrm{Cl}_K[p^\infty]$ for $p \nmid |K : \mathbb{Q}|$

What do we mean by Distribution?

- $\mathcal{K}$ family of number fields, e.g. $\mathcal{K}^-$ imaginary quadratic fields
- $h\colon \mathcal{K} \to \mathbb{R}_{>0}$ height

For a finite abelian p-group G want to study

$$\lim_{n\to\infty} \frac{|\{\, K \in \mathcal{K} \,|\, \mathrm{Cl}_K[p^\infty] \cong G, h(K) \leq n \,\}|}{|\{K \in \mathcal{K}, h(K) \leq n\}|} =: \mathbb{P}_{\mathcal{K}}(\mathrm{Cl}_K[p^\infty] \cong G)$$

"probability that $\mathrm{Cl}_K[p^\infty]$ of a random $K \in \mathcal{K}$ is isomorphic to G"

Goal: Find probability distribution μ on finite abelian p-groups and prove

$$\mathbb{P}_{\mathcal{K}}(\mathrm{Cl}_K[p^\infty] \cong G) = \mu(G) \qquad \text{for all } G$$

nature

model

Imaginary Quadratic Fields $\mathcal{K}^-$

- Computations show: $\mathbb{P}_{\mathcal{K}^-}(\mathrm{Cl}_K[3^\infty] \text{ cyclic}) \approx 0.98$
- C–L: noncyclic groups scarce as they have many automorphisms, group G should appear with a weight $\sim 1/|\mathrm{Aut}\, G|$

Theorem (Cohen–Lenstra 1983)

$\sum_{G \text{ fin. ab. } p\text{-gp.}/\cong} 1/|\mathrm{Aut}\, G| =: c_p < \infty$

Conjecture (Cohen–Lenstra 1983)

p odd, G finite abelian p-group. Then

$$\mathbb{P}_{\mathcal{K}^-}(\mathrm{Cl}_K[p^\infty] \cong G) = \frac{1}{c_p} \cdot \frac{1}{|\mathrm{Aut}\, G|}.$$

Open except for one small partial result for $p = 3$!

Why $1/|\mathrm{Aut}|$?

Various methods to generate random group R (e.g. random mult. table) give distribution $\mathbb{P}(R \cong G) \sim 1/|\mathrm{Aut}\, G|$

Cohen–Lenstra Principle

The probability that a random algebraic object is isomorphic to a given object X of the same kind is $\sim 1/|\mathrm{Aut}\, X|$.

Key philosophy:

- If objects of interest don't behave like certain random objects, they must have extra structure!
- Conversely, if objects behave randomly, have understood structure

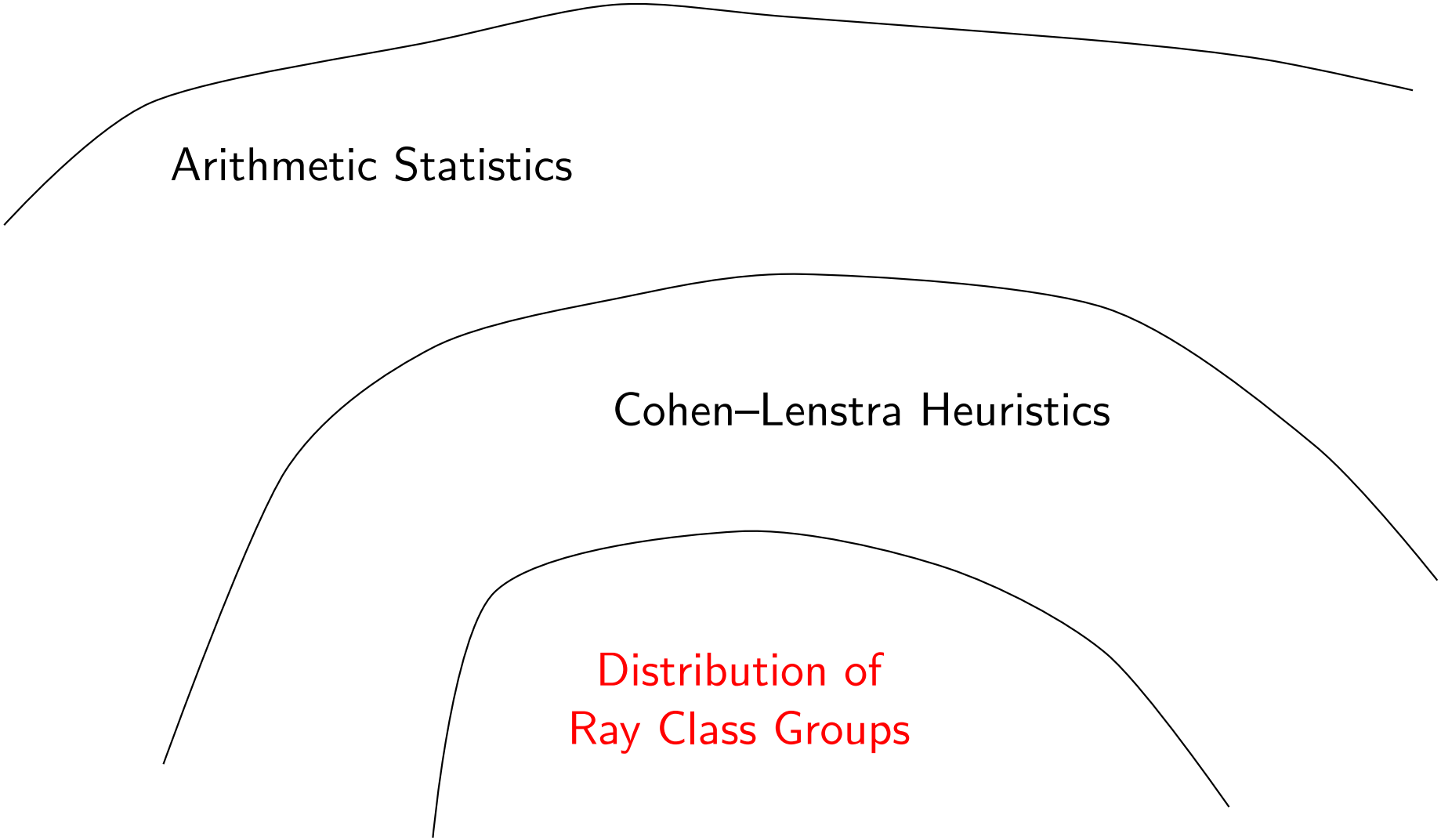
Other Families of Number Fields

In general, $\mathrm{Cl}_K[p^\infty]$ not a random finite abelian p-group $\rightsquigarrow$ extra structure

Bartel–Lenstra (2015, 2018):

- Consider bigger group $\overline{\mathrm{Cl}_K}$ with extra structure "added"
- Problem: $\left|\mathrm{Aut}(\overline{\mathrm{Cl}_K}[p^\infty])\right| = \infty$
- Developed theory to make sense of $1/\left|\mathrm{Aut}\, X\right|$ even if $\left|\mathrm{Aut}\, X\right| = \infty$
- Conjecture: $\mathbb{P}_{\mathcal{K}}(\overline{\mathrm{Cl}_K}[p^\infty] \cong X) \sim 1/\left|\mathrm{Aut}\, X\right|$

Landscape


Arithmetic Statistics
Cohen–Lenstra Heuristics
Distribution of
Ray Class Groups

Ray Class Groups

K number field. For $\mathfrak{m}_0 \trianglelefteq \mathcal{O}_K$ and $\mathfrak{m}_\infty$ a set of real embeddings of K, have ray class group $\mathrm{Cl}_K(\mathfrak{m}_0, \mathfrak{m}_\infty)$

- $\mathrm{Cl}_K(\mathfrak{m}_0, \mathfrak{m}_\infty)$ finite abelian and $\mathrm{Cl}_K(\mathcal{O}_K, \varnothing) = \mathrm{Cl}_K$, so generalises Cl_K
- Have exact sequence

$$0 \longrightarrow \ker \varphi \longrightarrow \mathrm{Cl}_K(\mathfrak{m}_0, \mathfrak{m}_\infty) \xrightarrow{\varphi} \mathrm{Cl}_K \longrightarrow 0$$

Bhargava (2016): What is distribution of $\mathrm{Cl}_K(m, \varnothing)[p^\infty]$ for fixed $m \in \mathbb{Z}$?

Imaginary Quadratic Fields $\mathcal{K}^-$

Varma (2016) proved: $\mathrm{Cl}_K(m,\varnothing)[p^\infty]$ for $K \in \mathcal{K}^-$ does not behave like random finite abelian p-group

Pagano–Sofos (2017): Have extra structure given by exact sequence

$$R_K(m)[p^\infty]: \quad 0 \longrightarrow (\ker\varphi)[p^\infty] \longrightarrow \mathrm{Cl}_K(m,\varnothing)[p^\infty] \xrightarrow{\varphi} \mathrm{Cl}_K[p^\infty] \longrightarrow 0$$

- Instead of $\mathrm{Cl}_K(m,\varnothing)[p^\infty]$ consider whole sequence $R_K(m)[p^\infty]$!
- P–S conjecture: $R_K(m)[p^\infty]$ for $K \in \mathcal{K}^-$ has distribution $\sim 1/|\mathrm{Aut}|$
- Conjecture implies Varma's results

In other families, $R_K(m)[p^\infty]$ not a random sequence $\rightsquigarrow$ extra structure

Other Families of Number Fields

Bartel–Pagano (2021): Can "add" extra structure to $R_K(m)$ to obtain bigger sequence $\overline{R_K(m)}$, but it has ∞ many automorphisms

Theorem (A.) (vague version)

$\mathcal{K}$ family of Galois number fields, $\Omega_{\mathcal{K}}$ the set of outcomes for $\overline{R_K(m)}[p^\infty]$. Then for $X \in \Omega_{\mathcal{K}}$, can make sense of $1/|\mathrm{Aut}\, X|$ even if $|\mathrm{Aut}\, X| = \infty$. Moreover, $\sum_{X \in \Omega_{\mathcal{K}}} 1/|\mathrm{Aut}\, X| =: c_{\mathcal{K}} < \infty$

Conjecture (A.) (vague version)

$\mathcal{K}$ family of Galois number fields, X an outcome for $\overline{R_K(m)}[p^\infty]$. Then

$$\mathbb{P}_{\mathcal{K}}(\overline{R_K(m)}[p^\infty] \cong X) = \frac{1}{c_{\mathcal{K}}} \cdot \frac{1}{|\mathrm{Aut}\, X|}$$

Distribution of Ray Class Sequences

Conjecture (A.) (vague version)

$\mathcal{K}$ family of Galois number fields, X an outcome for $\overline{R_K(m)}[p^\infty]$. Then

$$\mathbb{P}_{\mathcal{K}}(\overline{R_K(m)}[p^\infty] \cong X) = \frac{1}{c_{\mathcal{K}}} \cdot \frac{1}{|\mathrm{Aut}\, X|}$$

Consider sequences $\rightarrow$ a lot of info! Implies conjectures on Cl_K and more:

Eisenstein (1844): Among the $d \in \mathbb{Z}_{>0}$ squarefree with $d \equiv 5 \bmod 8$, for how many can you solve

$$x^2 - dy^2 = 4$$

in *odd* integers x, y?

Corollary

Assume the above conjecture holds. Then the proportion of such d is $\frac{1}{3}$.

A Corollary on a Pell Equation

Eisenstein (1844): Among the $d \in \mathbb{Z}_{>0}$ squarefree with $d \equiv 5 \bmod 8$, for how many can you solve $x^2 - dy^2 = 4$ in *odd* integers x, y?

Corollary

Assume the above conjecture holds. Then the proportion of such d is $\frac{1}{3}$.

$$\text{solubility} \quad \longleftrightarrow \quad \begin{array}{c}\text{behaviour of fdmtl. unit} \\ \text{of } K = \mathbb{Q}(\sqrt{d}) \text{ under} \\ \mathcal{O}_K^\times \to (\mathcal{O}_K/2)^\times\end{array} \quad \longleftarrow \quad \begin{array}{c}\text{distribution of} \\ \text{ray class groups}\end{array}$$

This works because the ray class sequence is

$$0 \longrightarrow \operatorname{cok}(\mathcal{O}_K^\times \to (\mathcal{O}_K/m)^\times) \longrightarrow \mathrm{Cl}_K(m, \varnothing) \xrightarrow{\varphi} \mathrm{Cl}_K \longrightarrow 0$$

More generally: Implications about distr. of ε_K in $(\mathcal{O}_K/m)^\times$ for any m

Why Sylow Subgroups?

Why consider $\mathrm{Cl}_K[p^\infty]$ and not Cl_K?

Theorem (Cohen–Lenstra, 1983)

$$\sum_{G \text{ fin. ab. } p\text{-gp.}/\cong} \frac{1}{|\mathrm{Aut}\, G|} =: c_p < \infty$$

In contrast:

$$\sum_{G \text{ fin. ab. gp.}/\cong} \frac{1}{|\mathrm{Aut}\, G|} \geq \sum_{p \text{ prime}} \frac{1}{|\mathrm{Aut}(\mathbb{Z}/p)|} = \sum_{p \text{ prime}} \frac{1}{p-1} \geq \sum_{p \text{ prime}} \frac{1}{p} = \infty$$

Bad Prime Case $p \mid |K : \mathbb{Q}|$

In general, behaviour of $\mathrm{Cl}_K[p^\infty]$ for $p \mid |K : \mathbb{Q}|$ is open question.

Imaginary quadratic fields: For $K \in \mathcal{K}^-$, $\mathrm{Cl}_K[2^\infty]$ does not behave like random finite abelian 2-group $\rightsquigarrow$ extra structure

Genus theory says

$$\mathrm{Cl}_K[2] \cong (\mathbb{Z}/2)^r, \qquad r = |\{p \mid \mathrm{disc}(K)\}| - 1.$$

Instead:

Theorem (Smith, 2022)

G finite abelian 2-group. Then

$$\mathbb{P}_{\mathcal{K}^-}((2\,\mathrm{Cl}_K)[2^\infty] \cong G) = \frac{1}{c_2} \cdot \frac{1}{|\mathrm{Aut}\, G|}.$$

Generating Random Groups

Generate random group R by writing down random $n \times n$ mult. table. Given group G of order n, then

$$\mathbb{P}(R \cong G) = \frac{|\{\text{tables isomorphic to } G\}|}{|\{\text{all mult. tables}\}|} \sim 1/|\operatorname{Aut} G|$$

Different method:

Theorem (Friedman–Washington 1989)

Pick $R_n \in \operatorname{Mat}_{n\times n}(\mathbb{Z}_p)$ random wrt. Haar measure. Given G finite abelian p-group, then

$$\lim_{n\to\infty} \mathbb{P}(\operatorname{cok} R_n \cong G) \sim 1/|\operatorname{Aut} G|$$

A Corollary on Fundamental Units

Let $\mathcal{K}^+(2;-1)$ set of real quadratic number fields in which 2 is inert.
For $K \in \mathcal{K}^+(2;-1)$ let $\varepsilon_K \in \mathcal{O}_K^\times$ fundamental unit and

$$\rho_K : \mathcal{O}_K^\times \to (\mathcal{O}_K/2)^\times \cong \mathbb{Z}/3.$$

Corollary

Assume the conjecture on the distribution of ray class sequences holds.
Then

$$\mathbb{P}_{\mathcal{K}^+(2;-1)}(\rho_K(\varepsilon_K) = 0) = \frac{1}{3}.$$

More generally: Implications about distr. of ε_K in $(\mathcal{O}_K/m)^\times$ for any m