Cohen–Lenstra Heuristics: Distribution of Class Groups of Random Number Fields

Robin Ammon

University of Glasgow

Y-RANT 2022

The Ideal Class Group

- K number field with ring of integers $\mathcal{O}_K$
- The ideal class group of K is

$$\mathrm{Cl}_K := \frac{\{\text{fractional ideals of } K\}}{\{\text{principal fractional ideals of } K\}},$$

which is a finite abelian group

The Ideal Class Group

- K number field with ring of integers $\mathcal{O}_K$
- The ideal class group of K is

$$\mathrm{Cl}_K := \frac{\{\text{fractional ideals of } K\}}{\{\text{principal fractional ideals of } K\}},$$

  which is a finite abelian group
- Cl_K is fundamental object, measures how far $\mathcal{O}_K$ is from being a UFD
- Given K explicitly, there are algorithms to compute Cl_K
- Problem: Not much known about structure of Cl_K in general

How to Understand Class Groups Better?

How to Understand Class Groups Better?

- Arithmetic Statistics: Study statistical behaviour of class groups in families of number fields

How to Understand Class Groups Better?

- Arithmetic Statistics: Study statistical behaviour of class groups in families of number fields
- Idea: (unknown) structure of class groups causes patterns, so structural info on class groups is tied to their distribution
- Thus if we understand their distribution, then we understand class groups a lot better

How to Understand Class Groups Better?

- Arithmetic Statistics: Study statistical behaviour of class groups in families of number fields
- Idea: (unknown) structure of class groups causes patterns, so structural info on class groups is tied to their distribution
- Thus if we understand their distribution, then we understand class groups a lot better
- Goal: Given G finite abelian, what is $\mathbb{P}(\mathrm{Cl}_K \cong G)$ where K ranges over a certain family?

How to Understand Class Groups Better?

- Idea: (unknown) structure of class groups causes patterns, so structural info on class groups is tied to their distribution
- Goal: Given G finite abelian, what is $\mathbb{P}(\mathrm{Cl}_K \cong G)$ where K ranges over a certain family?

How to Understand Class Groups Better?

- Idea: (unknown) structure of class groups causes patterns, so structural info on class groups is tied to their distribution
- Goal: Given G finite abelian, what is $\mathbb{P}(\mathrm{Cl}_K \cong G)$ where K ranges over a certain family?

Computational Data for Imaginary Quadratic Fields

As $d < 0$ runs over squarefree integers...

- 3 divides $\# \mathrm{Cl}_{\mathbb{Q}(\sqrt{d})}$ about 44% of the time,
- the 3-Sylow subgroup $\mathrm{Cl}_{\mathbb{Q}(\sqrt{d})}[3^\infty]$ is cyclic about 98% of the time.

How to Understand Class Groups Better?

- Idea: (unknown) structure of class groups causes patterns, so structural info on class groups is tied to their distribution
- Goal: Given G finite abelian, what is $\mathbb{P}(\mathrm{Cl}_K \cong G)$ where K ranges over a certain family?

Computational Data for Imaginary Quadratic Fields

As $d < 0$ runs over squarefree integers...

- 3 divides $\# \mathrm{Cl}_{\mathbb{Q}(\sqrt{d})}$ about 44% of the time,
- the 3-Sylow subgroup $\mathrm{Cl}_{\mathbb{Q}(\sqrt{d})}[3^\infty]$ is cyclic about 98% of the time.

- Data seems strange and not random.

How to Understand Class Groups Better?

- Idea: (unknown) structure of class groups causes patterns, so structural info on class groups is tied to their distribution
- Goal: Given G finite abelian, what is $\mathbb{P}(\mathrm{Cl}_K \cong G)$ where K ranges over a certain family?

Computational Data for Imaginary Quadratic Fields

As $d < 0$ runs over squarefree integers...

- 3 divides $\#\,\mathrm{Cl}_{\mathbb{Q}(\sqrt{d})}$ about 44% of the time,
- the 3-Sylow subgroup $\mathrm{Cl}_{\mathbb{Q}(\sqrt{d})}[3^\infty]$ is cyclic about 98% of the time.

- Data seems strange and not random. But e.g. $\#\,\mathrm{Cl}_{\mathbb{Q}(\sqrt{d})}$ is not just a number, it is the size of a *group*!

How to Understand Class Groups Better?

- Idea: (unknown) structure of class groups causes patterns, so structural info on class groups is tied to their distribution
- Goal: Given G finite abelian, what is $\mathbb{P}(\mathrm{Cl}_K \cong G)$ where K ranges over a certain family?

Computational Data for Imaginary Quadratic Fields

As $d < 0$ runs over squarefree integers...

- 3 divides $\# \mathrm{Cl}_{\mathbb{Q}(\sqrt{d})}$ about 44% of the time,
- the 3-Sylow subgroup $\mathrm{Cl}_{\mathbb{Q}(\sqrt{d})}[3^\infty]$ is cyclic about 98% of the time.

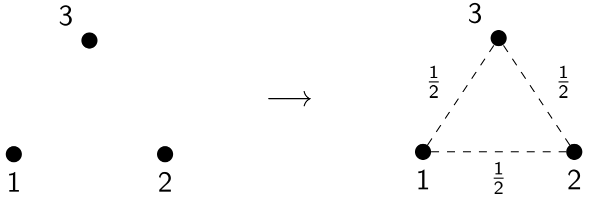
- Data seems strange and not random. But e.g. $\# \mathrm{Cl}_{\mathbb{Q}(\sqrt{d})}$ is not just a number, it is the size of a *group*!
- What distribution should we even expect from random groups?

Excursion:

Distribution of Random Algebraic Objects

Excursion: Distribution of Random Graphs

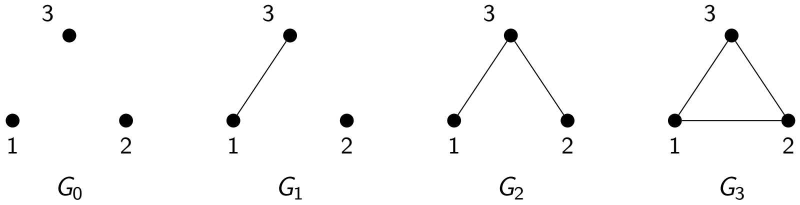
- Given 3 vertices, build a random graph R by independently inserting an edge between two vertices with probability $\frac{1}{2}$



- A graph isomorphism between two such graphs is $\sigma \in S_3$ such that vertices i and j are adjacent if and only if $\sigma(i)$ and $\sigma(j)$ are

Excursion: Distribution of Random Graphs

- Given 3 vertices, build a random graph R by independently inserting an edge between two vertices with probability $\frac{1}{2}$
- Possible outcomes up to isomorphism:



- Q: What are the probabilities $\mathbb{P}(R \cong G_i)$?

Excursion: Distribution of Random Graphs

- Each outcome has probability $\frac{1}{2} \cdot \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{8}$
- Let $\mathrm{Iso}(G_i)$ be the set of graphs isomorphic to G_i, then

$$\mathbb{P}(R \cong G_i) = \frac{\#\,\mathrm{Iso}(G_i)}{8}$$

Excursion: Distribution of Random Graphs

- Each outcome has probability $\frac{1}{2} \cdot \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{8}$
- Let $\mathrm{Iso}(G_i)$ be the set of graphs isomorphic to G_i, then

$$\mathbb{P}(R \cong G_i) = \frac{\# \mathrm{Iso}(G_i)}{8}$$

- Nicer: S_3 operates transitively on $\mathrm{Iso}(G_i)$ with stabiliser $\mathrm{Aut}(G_i)$,

Excursion: Distribution of Random Graphs

- Each outcome has probability $\frac{1}{2} \cdot \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{8}$
- Let $\operatorname{Iso}(G_i)$ be the set of graphs isomorphic to G_i, then

$$\mathbb{P}(R \cong G_i) = \frac{\# \operatorname{Iso}(G_i)}{8}$$

- Nicer: S_3 operates transitively on $\operatorname{Iso}(G_i)$ with stabiliser $\operatorname{Aut}(G_i)$, so by orbit-stabiliser theorem $S_3 / \operatorname{Aut}(G_i) \stackrel{1:1}{\longleftrightarrow} \operatorname{Iso}(G_i)$, thus

$$\mathbb{P}(R \cong G_i) = \frac{6}{8} \cdot \frac{1}{\# \operatorname{Aut}(G_i)}$$

Excursion: Distribution of Random Groups of Order n

- Generate a random group R of order n by writing down random $n \times n$ multiplication table (repeat if this is not a group structure)
- Q: If G is a group of order n, what is $\mathbb{P}(R \cong G)$?

Excursion: Distribution of Random Groups of Order n

- Generate a random group R of order n by writing down random $n \times n$ multiplication table (repeat if this is not a group structure)
- Q: If G is a group of order n, what is $\mathbb{P}(R \cong G)$?
- Exact same arguments as before yield

$$\mathbb{P}(R \cong G) = \frac{\#\{\text{tables isomorphic to } G\}}{\#\{\text{tables that give group structure}\}} \sim \frac{1}{\#\operatorname{Aut}(G)}$$

Principle

The probability that a randomly chosen algebraic object is isomorphic to a given object G is proportional to $\frac{1}{\#\operatorname{Aut}(G)}$.

Back to Class Groups

Cohen–Lenstra Heuristics for Imaginary Quadratic Fields

- Recall: Want to find distribution of Cl_K for K imaginary quadratic
- Look at distribution of p-Sylow subgroups $\mathrm{Cl}_K[p^\infty]$ individually

Cohen–Lenstra Heuristics for Imaginary Quadratic Fields

- Recall: Want to find distribution of Cl_K for K imaginary quadratic
- Look at distribution of p-Sylow subgroups $\mathrm{Cl}_K[p^\infty]$ individually
- Computational data for $\mathrm{Cl}_K[p^\infty]$ for odd p agrees with behaviour of random abelian p-groups!

Cohen–Lenstra Heuristics for Imaginary Quadratic Fields

- Recall: Want to find distribution of Cl_K for K imaginary quadratic
- Look at distribution of p-Sylow subgroups $\mathrm{Cl}_K[p^\infty]$ individually
- Computational data for $\mathrm{Cl}_K[p^\infty]$ for odd p agrees with behaviour of random abelian p-groups!

Conjecture (Cohen–Lenstra, '83)

p odd prime, G finite abelian p-group. Then as K ranges over imaginary quadratic fields,

$$\mathbb{P}(\mathrm{Cl}_K[p^\infty] \cong G) = \frac{c}{\#\,\mathrm{Aut}(G)}$$

for a constant c depending only on p.

- Suggests that $\mathrm{Cl}_K[p^\infty]$ does not carry additional structure!

Cohen–Lenstra Heuristics for Real Quadratic Fields

- For K real quadratic, $\mathrm{Cl}_K[p^\infty]$ behaves differently; data suggests:

Conjecture (Cohen–Lenstra, '83)

p odd prime, G finite abelian p-group. Then as K ranges over real quadratic fields,

$$\mathbb{P}(\mathrm{Cl}_K[p^\infty] \cong G) = \frac{c}{\#\,\mathrm{Aut}(G) \cdot \#G}$$

for a constant c depending only on p.

Cohen–Lenstra Heuristics for Real Quadratic Fields

- For K real quadratic, $\mathrm{Cl}_K[p^\infty]$ behaves differently; data suggests:

Conjecture (Cohen–Lenstra, '83)

p odd prime, G finite abelian p-group. Then as K ranges over real quadratic fields,

$$\mathbb{P}(\mathrm{Cl}_K[p^\infty] \cong G) = \frac{c}{\#\,\mathrm{Aut}(G) \cdot \#G}$$

for a constant c depending only on p.

Cohen–Lenstra Heuristics for Real Quadratic Fields

- For K real quadratic, $\mathrm{Cl}_K[p^\infty]$ behaves differently; data suggests:

Conjecture (Cohen–Lenstra, '83)

p odd prime, G finite abelian p-group. Then as K ranges over real quadratic fields,

$$\mathbb{P}(\mathrm{Cl}_K[p^\infty] \cong G) = \frac{c}{\#\operatorname{Aut}(G) \cdot \#G}$$

for a constant c depending only on p.

- Non-random behaviour is related to $\mathcal{O}_K^\times$ which now has rank 1

Cohen–Lenstra Heuristics for Real Quadratic Fields

- For K real quadratic, $\mathrm{Cl}_K[p^\infty]$ behaves differently; data suggests:

Conjecture (Cohen–Lenstra, '83)

p odd prime, G finite abelian p-group. Then as K ranges over real quadratic fields,

$$\mathbb{P}(\mathrm{Cl}_K[p^\infty] \cong G) = \frac{c}{\#\,\mathrm{Aut}(G) \cdot \#G}$$

for a constant c depending only on p.

- Non-random behaviour is related to $\mathcal{O}_K^\times$ which now has rank 1
- Bartel–Lenstra (2020) conjecture that Arakelov class group, which knows about Cl_K and $\mathcal{O}_K^\times$, is random object as in our principle
- Principle guides us to a better behaved object

Bad Primes and Higher Degrees

- Conjectures have been extended to Galois extensions K/F for "good primes"
- There are "bad primes" for which distribution is not understood in many cases, including:
  - p that divide $|K : F|$
  - p for which $\mu_p \subseteq K$

Bad Primes and Higher Degrees

- Conjectures have been extended to Galois extensions K/F for "good primes"
- There are "bad primes" for which distribution is not understood in many cases, including:
  - p that divide $|K : F|$
  - p for which $\mu_p \subseteq K$
- Overall: Cohen–Lenstra heuristics are very strong conjectures that would imply good understanding of class groups
- Many open questions, existing conjectures vastly open!

Thank you!