Cohen–Lenstra Heuristics for Ray Class Groups

Robin Ammon

University of Glasgow

20 November 2023

Cohen–Lenstra Heuristics: Background

K number field. Write Id_K for group of fractional ideals

- Interested in class group $\mathrm{Cl}_K = \mathrm{Id}_K / \{ (a) \mid a \in K^\times \}$
- Cl_K is finite abelian group and fundamental object in number theory
- However, Cl_K not well understood, not much known about structure

Cohen and Lenstra:

- Instead of studying class groups individually, study their distribution
- Idea: Any structure of Cl_K causes patterns, so structural info on class groups is tied to their distribution

Cohen–Lenstra Heuristics: Setup

What do we mean by distribution? Setup:

- $\mathcal{K}$ family of number fields
- $h\colon \mathcal{K} \to \mathbb{R}_{>0}$ with $|\{\, K \in \mathcal{K} \mid h(K) \leq n \,\}| < \infty$ for all n

For a finite abelian group M want to study

$$\lim_{n\to\infty} \frac{|\{\, K \in \mathcal{K} \mid \mathrm{Cl}_K \cong M, h(K) \leq n \,\}|}{|\{K \in \mathcal{K} \mid h(K) \leq n\}|}$$

"probability that Cl_K of a random $K \in \mathcal{K}$ is isomorphic to M"

Here always:

- h: Similar to $|\mathrm{disc}(K)|$, write $\mathcal{K}_{\leq n} := \{\, K \in \mathcal{K} \mid h(K) \leq n \,\}$
- Study distribution of p-Sylow subgroup $\mathrm{Cl}_K[p^\infty]$ for fixed p

Cohen–Lenstra Heuristics: Setup

Setup:

- $\mathcal{K}$ family of number fields
- p prime

Goal: Determine the distribution of $\mathrm{Cl}_K[p^\infty]$ for $K \in \mathcal{K}$, i.e.

find a probability distribution $\mathbb{P}$ on finite abelian p-groups and prove

$$\lim_{n\to\infty} \frac{\left|\left\{K \in \mathcal{K}_{\leq n} \mid \mathrm{Cl}_K[p^\infty] \cong M\right\}\right|}{\left|\left\{K \in \mathcal{K}_{\leq n}\right\}\right|} = \mathbb{P}(M)$$

for all finite abelian p-groups M.

Imaginary Quadratic Fields

Write $\mathcal{K}^-$ for the family of imaginary quadratic fields.

Where to start to find $\mathbb{P}$?

Computational Data

Computing the class groups of $K \in \mathcal{K}^-_{\leq n}$ for big n indicates:

- the proportion of $K \in \mathcal{K}^-$ with $|\mathrm{Cl}_K|$ divisible by 3 is ≈ 0.44
- the proportion of $K \in \mathcal{K}^-$ for which $\mathrm{Cl}_K[3^\infty]$ is cyclic is ≈ 0.98

Looks surprising! (?)

How can this be explained?

Cohen and Lenstra's Idea

Cohen and Lenstra write:

> *The main idea [...] is that the scarcity of noncyclic groups can be attributed to the fact that they have many automorphisms. This naturally leads to the heuristic assumption that isomorphism classes M of abelian groups should be weighted with a weight proportional to $1/|\mathrm{Aut}\, M|$. This is a very natural and common weighting factor [...]*

Example: Groups of order 9

- $|\mathrm{Aut}(\mathbb{Z}/9)| = |(\mathbb{Z}/9)^\times| = 6$
- $|\mathrm{Aut}(\mathbb{Z}/3 \times \mathbb{Z}/3)| = |\mathrm{GL}_2(\mathbb{Z}/3)| = 48$

C–L Heuristics for Imaginary Quadratic Fields

Cohen and Lenstra's idea fits the data: It seems that

$$\lim_{n\to\infty} \frac{\left|\left\{K \in \mathcal{K}^-_{\leq n} \mid \mathrm{Cl}_K[p^\infty] \cong M\right\}\right|}{\left|\left\{K \in \mathcal{K}^-_{\leq n}\right\}\right|} \sim \frac{1}{|\mathrm{Aut}\, M|}.$$

Want: Right hand side defines probability distribution. Indeed:

Theorem (Cohen, Lenstra, 1983)

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

C–L Heuristics for Imaginary Quadratic Fields

Theorem (Cohen, Lenstra, 1983)

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

Conjecture (Cohen, Lenstra, 1983)

p odd prime, M finite abelian p-group. Then

$$\lim_{n\to\infty} \frac{\left|\left\{K \in \mathcal{K}_{\leq n}^{-} \mid \mathrm{Cl}_K[p^\infty] \cong M\right\}\right|}{\left|\left\{K \in \mathcal{K}_{\leq n}^{-}\right\}\right|} = \frac{1}{c_p} \cdot \frac{1}{|\mathrm{Aut}\, M|}.$$

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

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

- Why is $1/|\mathrm{Aut}\, M|$ a "natural and common weighting factor"?
- What is a natural distribution for finite abelian p-groups?
- How does a random finite (abelian p-) group look like?

One approach:

- Generate random group R of order n by writing down a random $n \times n$ multiplication table (repeat if this is not a group structure)
- What is distribution? I.e. given group M of order n, what is

$$\mathbb{P}(R \cong M) = \frac{|\{\text{tables isomorphic to } M\}|}{|\{\text{tables that give group structure}\}|} \; ?$$

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

- Generate random group R of order n by writing down a random $n \times n$ multiplication table (repeat if this is not a group structure)
- What is distribution? I.e. given group M of order n, what is

$$\mathbb{P}(R \cong M) = \frac{|\{\text{tables isomorphic to } M\}|}{|\{\text{tables that give group structure}\}|} =: \frac{|T_M|}{|T|}?$$

- Note: S_n operates transitively on T_M and the stabiliser of $t \in T_M$ is $\mathrm{Aut}\, t \cong \mathrm{Aut}\, M$. Orbit-Stabiliser Theorem: $S_n/\mathrm{Aut}\, M \overset{1:1}{\longleftrightarrow} T_M$
- Conclude

$$\mathbb{P}(R \cong M) = \frac{|T_M|}{|T|} = \frac{n!}{|T|} \cdot \frac{1}{|\mathrm{Aut}\, M|}$$

- There are other ways to produce random groups that also give a distribution $\sim 1/|\mathrm{Aut}\, M|$!

The Cohen–Lenstra Principle

Principle

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

So Cohen and Lenstra conjecture that $\mathrm{Cl}_K[p^\infty]$ for $K \in \mathcal{K}^-$ behave like random finite abelian p-groups.

General philosophy in arithmetic statistics:
Suppose we are interested in objects X_i, $i \in I$.
Idea: statistical behaviour reflects properties of the X_i.

- If the X_i do not behave like random objects of some kind, they must have some extra structure
- If the X_i behave like random objects of some kind, we have "understood" their structure

The Cohen–Lenstra Principle

General philosophy in arithmetic statistics: When interested in X_i, $i \in I$:

- If the X_i do not behave like random objects of some kind, they must have some extra structure
- If the X_i behave like random objects of some kind, we have "understood" their structure

Example

- Have seen: for $K \in \mathcal{K}^-$, $|\mathrm{Cl}_K|$ does not behave like a random number. Reason: it is the size of a group.
- Cohen and Lenstra's conjecture asserts that the only structure on $\mathrm{Cl}_K[p^\infty]$ for $K \in \mathcal{K}^-$ is the abelian group structure

Real Quadratic Fields and Higher Degree Fields

What about real quadratic fields?

Conjecture (Cohen, Lenstra, 1983)

p odd prime, M finite abelian p-group. Then

$$\lim_{n\to\infty} \frac{\left|\left\{K \in \mathcal{K}^+_{\leq n} \mid \mathrm{Cl}_K[p^\infty] \cong M\right\}\right|}{\left|\left\{K \in \mathcal{K}^+_{\leq n}\right\}\right|} = \frac{1}{c'_p} \cdot \frac{1}{|\mathrm{Aut}\, M| \cdot |M|}.$$

Cohen and Martinet (1990) made conjectures about $\mathrm{Cl}_K[p^\infty]$ for:

- $\mathcal{K}$: Galois extensions $K/\mathbb{Q}$ with fixed Galois group G and fixed structure of $\mathcal{O}_K^\times$,
- p prime with $p \nmid |K : \mathbb{Q}|$.

In general, $|M|$ is replaced by a term similar to $\left|\mathrm{Hom}(\mathcal{O}_K^\times, M)\right|$.

How can this be understood? Extra structure?

The Arakelov Class Group

Recall $\mathrm{Cl}_K = \mathrm{Id}_K / \{ (a) \mid a \in K^\times \}$ where $\mathrm{Id}_K \cong \bigoplus_{0 \neq \mathfrak{p} \trianglelefteq \mathcal{O}_K \text{ prime}} \mathbb{Z}$.

We "miss" the infinite primes. Instead consider the Arakelov class group which is a subgroup of

$$\mathrm{Id}_K \times \prod_{\mathfrak{p} \mid \infty} \mathbb{R}_{>0} \Big/ \{ \text{"principal ideals"} \}.$$

Key property: There is an exact sequence

$$0 \longrightarrow \mathcal{O}_K^\times \otimes_{\mathbb{Z}} \mathbb{R}/\mathbb{Z} \longrightarrow \mathrm{Ar}_K \longrightarrow \mathrm{Cl}_K \longrightarrow 0.$$

Example

- If $K \in \mathcal{K}^-$, then $\mathrm{Ar}_K = \mathrm{Cl}_K$.
- If $K \in \mathcal{K}^+$, then $\mathrm{Ar}_K \cong \mathrm{Cl}_K \oplus \mathbb{R}/\mathbb{Z}$. So $|\mathrm{Aut}\, \mathrm{Ar}_K| = 2\,|\mathrm{Aut}\, \mathrm{Cl}_K| \cdot |\mathrm{Cl}_K|$

Distribution of Arakelov Class Groups

Work in the general setup

- $\mathcal{K}$: Galois extensions $K/\mathbb{Q}$ with fixed Galois group G and fixed structure of $\mathcal{O}_K^\times$,
- p prime with $p \nmid |K : \mathbb{Q}|$.

There is a "p-Sylow subgroup" $\mathrm{Ar}_K[p^\infty]$, which is a finitely generated $\mathbb{Z}_{(p)}G$-module (previously: $\mathrm{Cl}_K[p^\infty]$ finite $\mathbb{Z}_{(p)}G$-module).

For $K \in \mathcal{K}$, $\mathrm{Ar}_K[p^\infty]$ can only be isomorphic to certain $\mathbb{Z}_{(p)}G$-modules, call them admissible $\mathbb{Z}_{(p)}G$-modules.

- What is the distribution of $\mathrm{Ar}_K[p^\infty]$?
- Want to conjecture: $\mathbb{P}(\mathrm{Ar}_K[p^\infty] \cong M) \sim 1/|\mathrm{Aut}\, M|$ for M admissible
- Problem: In general, $|\mathrm{Aut}\, M| = \infty$

Distribution of Arakelov Class Groups

For $K \in \mathcal{K}$, $\mathrm{Ar}_K[p^\infty]$ can only be isomorphic to certain $\mathbb{Z}_{(p)}G$-modules, call them admissible $\mathbb{Z}_{(p)}G$-modules.

- What is the distribution of $\mathrm{Ar}_K[p^\infty]$?
- Want to conjecture: $\mathbb{P}(\mathrm{Ar}_K[p^\infty] \cong M) \sim 1/|\mathrm{Aut}\, M|$ for M admissible
- Problem: In general, $|\mathrm{Aut}\, M| = \infty$

For M, N admissible $\mathbb{Z}_{(p)}G$-modules, there is a way of comparing the infinite quantities $|\mathrm{Aut}\, M|$ and $|\mathrm{Aut}\, N|$. Key notion:

Definition

An isogeny of groups A, B is a homomorphism $f : A \to B$ with $|\ker f| < \infty$ and $|B : \mathrm{im}\, f| < \infty$. Its index is $\mathrm{i}(f) := |B : \mathrm{im}\, f| \,/\, |\ker f|$.

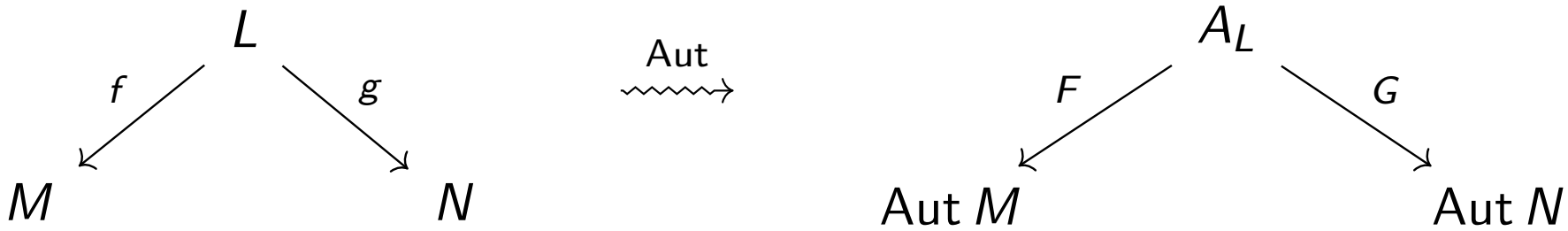
Comparing Infinite Automorphism Groups

Theorem (Bartel, Lenstra, 2016)

Let L, M, N be admissible $\mathbb{Z}_{(p)}G$-modules. Then there are isogenies $f\colon L \to M$, $g\colon L \to N$ and any such pair induces a pair of isogenies $F\colon A_L \to \operatorname{Aut} M$, $G\colon A_L \to \operatorname{Aut} N$. Moreover, the ratio

$$|\operatorname{Aut} N : \operatorname{Aut} M| := \mathrm{i}(G)/\mathrm{i}(F) \in \mathbb{Q}_{>0}$$

is independent of L, f, g.



Distribution of Arakelov Class Groups

Idea: instead of $1/|\mathrm{Aut}\, M|$ use $|\mathrm{Aut}\, N : \mathrm{Aut}\, M|$ for some N

Theorem (Bartel, Lenstra, 2020)

Let M and N be admissible. Then $\sum_{L \text{ adm.}} |\mathrm{Aut}\, N : \mathrm{Aut}\, L| < \infty$ and

$$\mathbb{P}^{\mathrm{mod}}(M) := \frac{|\mathrm{Aut}\, N : \mathrm{Aut}\, M|}{\sum_{L \text{ adm.}} |\mathrm{Aut}\, N : \mathrm{Aut}\, L|}$$

is independent of N and defines a prob. distribution on admissible modules.

Conjecture (Bartel, Lenstra, 2020)

Let M be an admissible $\mathbb{Z}_{(p)}G$-module. Then

$$\lim_{n\to\infty} \frac{\left|\left\{K \in \mathcal{K}_{\leq n} \mid \mathrm{Ar}_K[p^\infty] \cong M\right\}\right|}{\left|\left\{K \in \mathcal{K}_{\leq n}\right\}\right|} = \mathbb{P}^{\mathrm{mod}}(M).$$

This implies the previous conjectures on $\mathrm{Cl}_K[p^\infty]$!

Ray Class Groups

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

$$\mathrm{Cl}_K(\mathfrak{m}) = \frac{\{I \in \mathrm{Id}_K \text{ coprime to } \mathfrak{m}_0\}}{\{\text{suitable principal ideals}\}}.$$

Have $\mathrm{Cl}_K(\mathcal{O}_K, \varnothing) = \mathrm{Cl}_K$, so $\mathrm{Cl}_K(\mathfrak{m})$ generalises Cl_K.

In fact, have exact sequence

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

where $|\ker\varphi| < \infty$.

Question: What is the distribution of $\mathrm{Cl}_K(\mathfrak{m})[p^\infty]$ for fixed $\mathfrak{m}$?

To make sense: Take $\mathfrak{m} = (m, \varnothing)$ with $m \in \mathbb{Z}$.

Imaginary Quadratic Fields

Varma (2021) proved a result that shows $\mathrm{Cl}_K(m)[p^\infty]$ for $K \in \mathcal{K}^-$ does not behave like a random finite abelian p-group

How can this be explained? Extra structure?

Yes! Given by the exact sequence

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

Idea: Instead of $\mathrm{Cl}_K(m)[p^\infty]$ consider the whole sequence $\Phi_K[p^\infty]$!

- A homomorphism of sequences is a homomorphism in the category of chain complexes
- Again only certain admissible sequences are attained by $\Phi_K[p^\infty]$ for $K \in \mathcal{K}^-$

Imaginary Quadratic Fields

Idea: Instead of $\mathrm{Cl}_K(m)[p^\infty]$ consider the whole sequence $\Phi_K[p^\infty]$!

Theorem

$$\sum_{X \text{ admissible seq.}} \frac{1}{|\mathrm{Aut}\, X|} =: c_{p,m} < \infty$$

Conjecture (Pagano–Sofos 2017, Bartel–Pagano 2021)

p odd prime, X admissible sequence. Then

$$\lim_{n\to\infty} \frac{\left|\left\{K \in \mathcal{K}^-_{\leq n} \mid \Phi_K[p^\infty] \cong X\right\}\right|}{\left|\left\{K \in \mathcal{K}^-_{\leq n}\right\}\right|} = \frac{1}{c_{p,m}} \cdot \frac{1}{|\mathrm{Aut}\, X|}.$$

This implies Varma's results!

Real Quadratic Fields and Higher Degree Fields

For other families, again problems arise because of the unit group $\mathcal{O}_K^\times$.

Solution: Introduce Arakelov ray class group $\mathrm{Ar}_K(m)$, which again adds infinite primes to $\mathrm{Cl}_K(m)$. Have exact sequence

$$0 \longrightarrow \ker\theta \longrightarrow \mathrm{Ar}_K(m) \xrightarrow{\theta} \mathrm{Ar}_K \longrightarrow 0.$$

In the general setup

- $\mathcal{K}$: Galois extensions $K/\mathbb{Q}$ with fixed Galois group G and fixed structure of $\mathcal{O}_K^\times$,
- p prime with $p \nmid |K:\mathbb{Q}|$,

want to model distribution of

$$\Theta_K[p^\infty]\colon \quad 0 \longrightarrow (\ker\theta)[p^\infty] \longrightarrow \mathrm{Ar}_K(m)[p^\infty] \xrightarrow{\theta} \mathrm{Ar}_K[p^\infty] \longrightarrow 0.$$

Real Quadratic Fields and Higher Degree Fields

In the general setup want to model distribution of

$$\Theta_K[p^\infty]\colon \quad 0 \longrightarrow (\ker\theta)[p^\infty] \longrightarrow \mathrm{Ar}_K(m)[p^\infty] \xrightarrow{\theta} \mathrm{Ar}_K[p^\infty] \longrightarrow 0.$$

- Again only certain admissible sequences of $\mathbb{Z}_{(p)}G$-modules are attained by $\Theta_K[p^\infty]$ for $K \in \mathcal{K}$
- Problem: admissible sequences have infinitely many automorphisms
- Solution: extend theory to compare infinite Aut groups

Definition

Let $X\colon 0 \to X_1 \to X_2 \to X_3 \to 0$, $Y\colon 0 \to Y_1 \to Y_2 \to Y_3 \to 0$ be SES of modules. An isogeny from X to Y is a homomorphism $f = (f_1, f_2, f_3)\colon X \to Y$ such that f_1, f_2, f_3 are isogenies of modules.

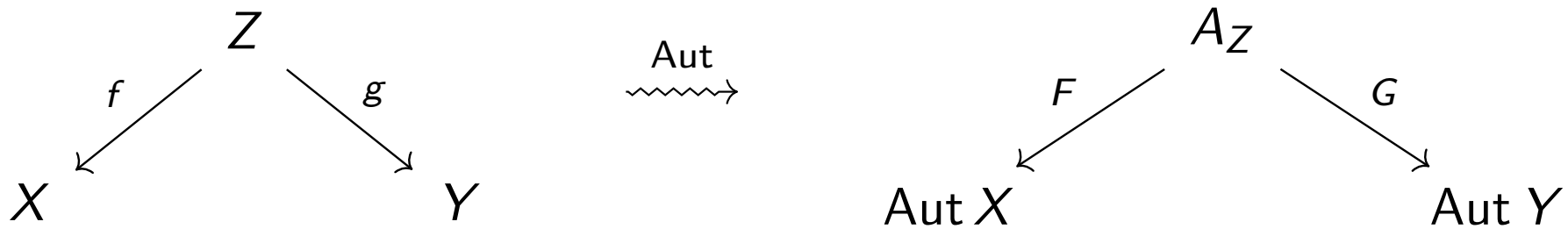
Comparing Infinite Automorphism Groups of SES

Theorem (A.)

Let X, Y, Z be admissible SES of $\mathbb{Z}_{(p)}G$-modules. Then there are isogenies $f\colon Z \to X$, $g\colon Z \to Y$ and any such pair induces a pair of isogenies $F\colon A_Z \to \operatorname{Aut} X$, $G\colon A_Z \to \operatorname{Aut} Y$. Moreover, the ratio

$$|\operatorname{Aut} Y : \operatorname{Aut} X| := \mathrm{i}(G)/\mathrm{i}(F) \in \mathbb{Q}_{>0}$$

is independent of Z, f, g.



Distribution of Arakelov Ray Class Groups

Theorem (A.)

Let X and Y be admissible SES. Then $\sum_{Z \text{ adm.}} |\mathrm{Aut}\, Y : \mathrm{Aut}\, Z| < \infty$ and

$$\mathbb{P}^{\mathrm{seq}}(X) := \frac{|\mathrm{Aut}\, Y : \mathrm{Aut}\, X|}{\sum_{Z \text{ adm.}} |\mathrm{Aut}\, Y : \mathrm{Aut}\, Z|}$$

is independent of Y and defines a prob. distribution on admissible SES.

Conjecture

Let X be an admissible SES of $\mathbb{Z}_{(p)}G$-modules. Then

$$\lim_{n\to\infty} \frac{\left|\left\{K \in \mathcal{K}_{\leq n} \mid \Theta_K[p^\infty] \cong X\right\}\right|}{\left|\left\{K \in \mathcal{K}_{\leq n}\right\}\right|} = \mathbb{P}^{\mathrm{seq}}(X).$$

This implies all previous conjectures!

A Corollary on Fundamental Units

Write $\mathcal{K}^+(2;-1)$ for the set of real quadratic number fields in which 2 is inert. If $K \in \mathcal{K}^+(2;-1)$ write $\varepsilon_K \in \mathcal{O}_K^\times$ for a fundamental unit and write

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

Corollary

Assume the previous conjecture holds. Then

$$\lim_{n\to\infty} \frac{\left|\left\{K \in \mathcal{K}^+_{\leq n}(2;-1) \mid \rho_K(\varepsilon_K) = 0\right\}\right|}{\left|\left\{K \in \mathcal{K}^+_{\leq n}(2;-1)\right\}\right|} = \frac{1}{3}.$$

This is an old conjecture by Stevenhagen.

More generally, obtain conjectures about distribution of ε_K in $(\mathcal{O}_K/m)^\times$.

A Corollary on Fundamental Units