The average size of 3-torsion in class groups of 2-extensions

Robert J. Lemke Oliver
Tufts University

(joint w/ Jiuya Wang & Melanie Matchett Wood)

Davenport–Heilbronn

Theorem (Davenport–Heilbronn; 1971)

The average size of the 3*-torsion subgroup* $\mathrm{Cl}_K[3]$ *for quadratic fields* $K/\mathbb{Q}$ *is exactly* $5/3$.

Davenport–Heilbronn

Theorem (Davenport–Heilbronn; 1971)

The average size of the 3-torsion subgroup $\mathrm{Cl}_K[3]$ for quadratic fields $K/\mathbb{Q}$ is exactly $5/3$.

That is, if $\mathcal{F}_2(X) := \{K/\mathbb{Q} \text{ quad.} : |\mathrm{Disc}(K)| \leq X\}$, then

$$\lim_{X\to\infty} \frac{1}{\#\mathcal{F}_2(X)} \sum_{K\in\mathcal{F}_2(X)} |\mathrm{Cl}_K[3]| = \frac{5}{3}.$$

Davenport–Heilbronn

Theorem (Davenport–Heilbronn; 1971)

The average size of the 3-torsion subgroup $\mathrm{Cl}_K[3]$ for quadratic fields $K/\mathbb{Q}$ is exactly $5/3$.

That is, if $\mathcal{F}_2(X) := \{K/\mathbb{Q} \text{ quad.} : |\mathrm{Disc}(K)| \leq X\}$, then

$$\lim_{X\to\infty} \frac{1}{\#\mathcal{F}_2(X)} \sum_{K\in\mathcal{F}_2(X)} |\mathrm{Cl}_K[3]| = \frac{5}{3}.$$

Davenport–Heilbronn: This is consistent with

- $\mathrm{Prob}(\mathrm{rk}_{\mathbb{F}_3}\mathrm{Cl}_K[3] \geq m) = 3^{1-2m}$ for imaginary quadratic K,

Davenport–Heilbronn

Theorem (Davenport–Heilbronn; 1971)

The average size of the 3-torsion subgroup $\mathrm{Cl}_K[3]$ *for quadratic fields* $K/\mathbb{Q}$ *is exactly* $5/3$.

That is, if $\mathcal{F}_2(X) := \{K/\mathbb{Q} \text{ quad.} : |\mathrm{Disc}(K)| \leq X\}$, *then*

$$\lim_{X\to\infty} \frac{1}{\#\mathcal{F}_2(X)} \sum_{K\in\mathcal{F}_2(X)} |\mathrm{Cl}_K[3]| = \frac{5}{3}.$$

Davenport–Heilbronn: This is consistent with

- $\mathrm{Prob}(\mathrm{rk}_{\mathbb{F}_3}\mathrm{Cl}_K[3] \geq m) = 3^{1-2m}$ for imaginary quadratic K, and
- $\mathrm{Prob}(\mathrm{rk}_{\mathbb{F}_3}\mathrm{Cl}_K[3] \geq m) = 3^{-2m}$ for real quadratic K.

Davenport–Heilbronn

Theorem (Davenport–Heilbronn; 1971)

The average size of the 3*-torsion subgroup* $\mathrm{Cl}_K[3]$ *for quadratic fields* $K/\mathbb{Q}$ *is exactly* $5/3$*.*

That is, if $\mathcal{F}_2(X) := \{K/\mathbb{Q} \text{ quad.} : |\mathrm{Disc}(K)| \leq X\}$*, then*

$$\lim_{X\to\infty} \frac{1}{\#\mathcal{F}_2(X)} \sum_{K\in\mathcal{F}_2(X)} |\mathrm{Cl}_K[3]| = \frac{5}{3}.$$

Davenport–Heilbronn: This is consistent with

- $\mathrm{Prob}(\mathrm{rk}_{\mathbb{F}_3}\mathrm{Cl}_K[3] \geq m) = 3^{1-2m}$ for imaginary quadratic K, and
- $\mathrm{Prob}(\mathrm{rk}_{\mathbb{F}_3}\mathrm{Cl}_K[3] \geq m) = 3^{-2m}$ for real quadratic K.

(Now believed to be wrong.)

The Cohen–Lenstra heuristics

Conjecture (Cohen–Lenstra; 1984)

If K is a quadratic field and ℓ is an odd prime, then $\mathrm{Cl}_K[\ell]$ should look like a "random" elementary abelian ℓ-group.

The Cohen–Lenstra heuristics

Conjecture (Cohen–Lenstra; 1984)

If K is a quadratic field and ℓ is an odd prime, then $\mathrm{Cl}_K[\ell]$ should look like a "random" elementary abelian ℓ-group.

More specifically, for any $k \geq 1$, the limit

$$\lim_{X\to\infty} \frac{1}{\#\mathcal{F}_2(X)} \sum_{K\in\mathcal{F}_2(X)} |\mathrm{Cl}_K[\ell]|^k =: \mathrm{Avg}_{\mathcal{F}_2}(|\mathrm{Cl}_K[\ell]|^k)$$

exists.

The Cohen–Lenstra heuristics

Conjecture (Cohen–Lenstra; 1984)

If K is a quadratic field and ℓ is an odd prime, then $\mathrm{Cl}_K[\ell]$ should look like a "random" elementary abelian ℓ-group.

More specifically, for any $k \geq 1$, the limit

$$\lim_{X \to \infty} \frac{1}{\#\mathcal{F}_2(X)} \sum_{K \in \mathcal{F}_2(X)} |\mathrm{Cl}_K[\ell]|^k =: \mathrm{Avg}_{\mathcal{F}_2}(|\mathrm{Cl}_K[\ell]|^k)$$

exists.

- Davenport–Heilbronn remains the only known case.

The Cohen–Lenstra heuristics

Conjecture (Cohen–Lenstra; 1984)

If K is a quadratic field and ℓ is an odd prime, then $\mathrm{Cl}_K[\ell]$ should look like a "random" elementary abelian ℓ-group.

More specifically, for any $k \geq 1$, the limit

$$\lim_{X\to\infty} \frac{1}{\#\mathcal{F}_2(X)} \sum_{K\in\mathcal{F}_2(X)} |\mathrm{Cl}_K[\ell]|^k =: \mathrm{Avg}_{\mathcal{F}_2}(|\mathrm{Cl}_K[\ell]|^k)$$

exists.

- Davenport–Heilbronn remains the only known case.
- Smith: Studies the distribution of $2\mathrm{Cl}_K[2^\infty]$.

The Cohen–Marinet heuristics

For $n \geq 2$, let $G \subseteq S_n$ be transitive.[1]

[1] N.B. In this talk, all Galois groups G are permutation groups.

The Cohen–Marinet heuristics

For $n \geq 2$, let $G \subseteq S_n$ be transitive.[1] Let

$$\mathcal{F}_G(X) := \{[K : \mathbb{Q}] = n : \mathrm{Gal}(\widetilde{K}/\mathbb{Q}) \simeq G, |\mathrm{Disc}(K)| \leq X\}.$$

[1] N.B. In this talk, all Galois groups G are permutation groups.

The Cohen–Marinet heuristics

For $n \geq 2$, let $G \subseteq S_n$ be transitive.[1] Let

$$\mathcal{F}_G(X) := \{[K : \mathbb{Q}] = n : \mathrm{Gal}(\widetilde{K}/\mathbb{Q}) \simeq G, |\mathrm{Disc}(K)| \leq X\}.$$

Conjecture (Cohen–Martinet; 1990)

For ℓ a "good" prime and $k \geq 1$, the limit

$$\lim_{X \to \infty} \frac{1}{\#\mathcal{F}_G(X)} \sum_{K \in \mathcal{F}_G(X)} |\mathrm{Cl}_K[\ell]|^k =: \mathrm{Avg}_{\mathcal{F}_G}(|\mathrm{Cl}_K[\ell]|^k)$$

exists.

[1] N.B. In this talk, all Galois groups G are permutation groups.

The Cohen–Marinet heuristics

For $n \geq 2$, let $G \subseteq S_n$ be transitive.[1] Let

$$\mathcal{F}_G(X) := \{[K : \mathbb{Q}] = n : \mathrm{Gal}(\widetilde{K}/\mathbb{Q}) \simeq G, |\mathrm{Disc}(K)| \leq X\}.$$

Conjecture (Cohen–Martinet; 1990)

For ℓ a "good" prime and $k \geq 1$, the limit

$$\lim_{X \to \infty} \frac{1}{\#\mathcal{F}_G(X)} \sum_{K \in \mathcal{F}_G(X)} |\mathrm{Cl}_K[\ell]|^k =: \mathrm{Avg}_{\mathcal{F}_G}(|\mathrm{Cl}_K[\ell]|^k)$$

exists.

Bhargava (2005): Determines the average of $|\mathrm{Cl}_K[2]|$ over S_3 cubics K.

[1] N.B. In this talk, all Galois groups G are permutation groups.

The Cohen–Marinet heuristics

For $n \geq 2$, let $G \subseteq S_n$ be transitive.[1] Let

$$\mathcal{F}_G(X) := \{[K : \mathbb{Q}] = n : \mathrm{Gal}(\widetilde{K}/\mathbb{Q}) \simeq G, |\mathrm{Disc}(K)| \leq X\}.$$

Conjecture (Cohen–Martinet; 1990)

For ℓ a "good" prime and $k \geq 1$, the limit

$$\lim_{X \to \infty} \frac{1}{\#\mathcal{F}_G(X)} \sum_{K \in \mathcal{F}_G(X)} |\mathrm{Cl}_K[\ell]|^k =: \mathrm{Avg}_{\mathcal{F}_G}(|\mathrm{Cl}_K[\ell]|^k)$$

exists.

Bhargava (2005): Determines the average of $|\mathrm{Cl}_K[2]|$ over S_3 cubics K. (i.e., $n = 3$, $G = S_3$, $\ell = 2$, and $k = 1$)

[1]N.B. In this talk, all Galois groups G are permutation groups.

The average size of 3-torsion in 2-extensions

Theorem (LO–Wang–Wood)

For $m \geq 1$, let $\mathcal{F}_{2^m}$ be the set of 2-extensions[1] *$K/\mathbb{Q}$ of degree 2^m.*

[1] $K/\mathbb{Q}$ is a 2-extension if it is built out of successive quadratic extensions.

The average size of 3-torsion in 2-extensions

Theorem (LO–Wang–Wood)

For $m \geq 1$, let $\mathcal{F}_{2^m}$ be the set of 2-extensions[1] *$K/\mathbb{Q}$ of degree 2^m. Then*

$$\lim_{X\to\infty} \frac{1}{\#\mathcal{F}_{2^m}(X)} \sum_{K\in\mathcal{F}_{2^m}(X)} |\mathrm{Cl}_K[3]|$$

exists, and is given by an explicit constant.

[1] $K/\mathbb{Q}$ is a 2-extension if it is built out of successive quadratic extensions.

The average size of 3-torsion in 2-extensions

Theorem (LO–Wang–Wood)

For $m \geq 1$, let $\mathcal{F}_{2^m}$ be the set of 2-extensions[1] $K/\mathbb{Q}$ of degree 2^m. Then

$$\lim_{X \to \infty} \frac{1}{\#\mathcal{F}_{2^m}(X)} \sum_{K \in \mathcal{F}_{2^m}(X)} |\mathrm{Cl}_K[3]|$$

exists, and is given by an explicit constant.

Theorem (LO–Wang–Wood)

Let $G \subseteq S_{2^m}$ be a transitive 2-group.

[1] $K/\mathbb{Q}$ is a 2-extension if it is built out of successive quadratic extensions.

The average size of 3-torsion in 2-extensions

Theorem (LO–Wang–Wood)

For $m \geq 1$, let $\mathcal{F}_{2^m}$ be the set of 2-extensions[1] *$K/\mathbb{Q}$ of degree 2^m. Then*

$$\lim_{X \to \infty} \frac{1}{\#\mathcal{F}_{2^m}(X)} \sum_{K \in \mathcal{F}_{2^m}(X)} |\mathrm{Cl}_K[3]|$$

exists, and is given by an explicit constant.

Theorem (LO–Wang–Wood)

Let $G \subseteq S_{2^m}$ be a transitive 2-group. If G has a transposition, then

$$\lim_{X \to \infty} \frac{1}{\#\mathcal{F}_G(X)} \sum_{K \in \mathcal{F}_G(X)} |\mathrm{Cl}_K[3]|$$

exists, and is given by an explicit constant.

---

[1] $K/\mathbb{Q}$ is a 2-extension if it is built out of successive quadratic extensions.

Important Aside: Malle's Conjecture for 2-extensions

Theorem

Let $G \subseteq S_{2^m}$ be a transitive 2-group. If G has a transposition, then

$$\#\mathcal{F}_G(X) \sim c_G X$$

for an explicit $c_G > 0$, and

$$\#\mathcal{F}_G(X) = O_{m,\epsilon}(X^{1/2+\epsilon})$$

if G does not have a transposition.

Important Aside: Malle's Conjecture for 2-extensions

Theorem

Let $G \subseteq S_{2^m}$ be a transitive 2-group. If G has a transposition, then

$$\#\mathcal{F}_G(X) \sim c_G X$$

for an explicit $c_G > 0$, and

$$\#\mathcal{F}_G(X) = O_{m,\epsilon}(X^{1/2+\epsilon})$$

if G does not have a transposition.

Proof.

Follows by combining work of Cohen–Diaz y Diaz–Olivier, Klüners–Malle, Klüners, and Shafarevich. □

The simplest new example: D_4 quartics

Corollary (LO–Wang–Wood)

Let $\mathcal{F}_{D_4}$ denote the family of D_4 quartic fields $K/\mathbb{Q}$.

The simplest new example: D_4 quartics

Corollary (LO–Wang–Wood)

Let $\mathcal{F}_{D_4}$ denote the family of D_4 quartic fields $K/\mathbb{Q}$. Then

$$\lim_{X\to\infty} \frac{1}{\#\mathcal{F}_{D_4}(X)} \sum_{K\in\mathcal{F}_{D_4}(X)} |\mathrm{Cl}_K[3]|$$

exists.

The simplest new example: D_4 quartics

Corollary (LO–Wang–Wood)

Let $\mathcal{F}_{D_4}$ denote the family of D_4 quartic fields $K/\mathbb{Q}$. Then

$$\lim_{X\to\infty} \frac{1}{\#\mathcal{F}_{D_4}(X)} \sum_{K\in\mathcal{F}_{D_4}(X)} |\mathrm{Cl}_K[3]|$$

exists.

Key Step: Show that C_4 and $C_2 \times C_2$ do not contribute to the overall average for $\mathcal{F}_4$.

The structure of D_4 quartics

- Each $K \in \mathcal{F}_{D_4}$ has a unique quadratic subfield F.

The structure of D_4 quartics

- Each $K \in \mathcal{F}_{D_4}$ has a unique quadratic subfield F.
- The number of $K \in \mathcal{F}_{D_4}(X)$ over a given F is $O_\epsilon(X/|\mathrm{Disc}(F)|^{2-\epsilon})$.

The structure of D_4 quartics

- Each $K \in \mathcal{F}_{D_4}$ has a unique quadratic subfield F.
- The number of $K \in \mathcal{F}_{D_4}(X)$ over a given F is $O_\epsilon(X/|\mathrm{Disc}(F)|^{2-\epsilon})$.
- $\Rightarrow$ The number of K with $|\mathrm{Disc}(F)| \geq Y$ is $O(X/Y^{1-\epsilon})$.

The structure of D_4 quartics

- Each $K \in \mathcal{F}_{D_4}$ has a unique quadratic subfield F.
- The number of $K \in \mathcal{F}_{D_4}(X)$ over a given F is $O_\epsilon(X/|\mathrm{Disc}(F)|^{2-\epsilon})$.
- $\Rightarrow$ The number of K with $|\mathrm{Disc}(F)| \geq Y$ is $O(X/Y^{1-\epsilon})$.
  - **Think:** 99% of $K \in \mathcal{F}_{D_4}$ have $|\mathrm{Disc}(F)| \leq 100$.

The structure of D_4 quartics

- Each $K \in \mathcal{F}_{D_4}$ has a unique quadratic subfield F.
- The number of $K \in \mathcal{F}_{D_4}(X)$ over a given F is $O_\epsilon(X/|\mathrm{Disc}(F)|^{2-\epsilon})$.
- $\Rightarrow$ The number of K with $|\mathrm{Disc}(F)| \geq Y$ is $O(X/Y^{1-\epsilon})$.
  - **Think:** 99% of $K \in \mathcal{F}_{D_4}$ have $|\mathrm{Disc}(F)| \leq 100$.
- **Goal:** Prove the same kind of thing for $|\mathrm{Cl}_K[3]|$.

The structure of D_4 quartics

- Each $K \in \mathcal{F}_{D_4}$ has a unique quadratic subfield F.
- The number of $K \in \mathcal{F}_{D_4}(X)$ over a given F is $O_\epsilon(X/|\mathrm{Disc}(F)|^{2-\epsilon})$.
- $\Rightarrow$ The number of K with $|\mathrm{Disc}(F)| \geq Y$ is $O(X/Y^{1-\epsilon})$.
  - **Think:** 99% of $K \in \mathcal{F}_{D_4}$ have $|\mathrm{Disc}(F)| \leq 100$.
- **Goal:** Prove the same kind of thing for $|\mathrm{Cl}_K[3]|$.

Theorem (LO–Wang–Wood; main technical result for D_4)

For any $X \geq 1$ and $Y \leq X^{1/2}$, we have

$$\sum_{\substack{K \in \mathcal{F}_4(X) \\ |\mathrm{Disc}(F)| \geq Y}} |\mathrm{Cl}_K[3]| = O_\epsilon(X/Y^{1-\epsilon}).$$

The strategy for D_4 quartics

For $K \in \mathcal{F}_{D_4}$, the 3-part factors: $|\mathrm{Cl}_K[3]| = |\mathrm{Cl}_F[3]| \cdot |\mathrm{Cl}_{K/F}[3]|$.

The strategy for D_4 quartics

For $K \in \mathcal{F}_{D_4}$, the 3-part factors: $|\mathrm{Cl}_K[3]| = |\mathrm{Cl}_F[3]| \cdot |\mathrm{Cl}_{K/F}[3]|$.
Thus,

$$\sum_{\substack{K \in \mathcal{F}_4(X) \\ |\mathrm{Disc}(F)| \geq Y}} |\mathrm{Cl}_K[3]|$$

The strategy for D_4 quartics

For $K \in \mathcal{F}_{D_4}$, the 3-part factors: $|\mathrm{Cl}_K[3]| = |\mathrm{Cl}_F[3]| \cdot |\mathrm{Cl}_{K/F}[3]|$.
Thus,

$$\sum_{\substack{K \in \mathcal{F}_4(X) \\ |\mathrm{Disc}(F)| \geq Y}} |\mathrm{Cl}_K[3]| \doteq \sum_{\substack{F \in \mathcal{F}_2(X^{1/2}) \\ |\mathrm{Disc}(F)| \geq Y}} |\mathrm{Cl}_F[3]| \sum_{\substack{[K:F]=2 \\ |\mathrm{Disc}(K)| \leq X}} |\mathrm{Cl}_{K/F}[3]|.$$

The strategy for D_4 quartics

For $K \in \mathcal{F}_{D_4}$, the 3-part factors: $|\mathrm{Cl}_K[3]| = |\mathrm{Cl}_F[3]| \cdot |\mathrm{Cl}_{K/F}[3]|$. Thus,

$$\sum_{\substack{K \in \mathcal{F}_4(X) \\ |\mathrm{Disc}(F)| \geq Y}} |\mathrm{Cl}_K[3]| \doteq \sum_{\substack{F \in \mathcal{F}_2(X^{1/2}) \\ |\mathrm{Disc}(F)| \geq Y}} |\mathrm{Cl}_F[3]| \sum_{\substack{[K:F]=2 \\ |\mathrm{Disc}(K)| \leq X}} |\mathrm{Cl}_{K/F}[3]|.$$

Davenport–Heilbronn handles first sum,

The strategy for D_4 quartics

For $K \in \mathcal{F}_{D_4}$, the 3-part factors: $|\mathrm{Cl}_K[3]| = |\mathrm{Cl}_F[3]| \cdot |\mathrm{Cl}_{K/F}[3]|$. Thus,

$$\sum_{\substack{K \in \mathcal{F}_4(X) \\ |\mathrm{Disc}(F)| \geq Y}} |\mathrm{Cl}_K[3]| \doteq \sum_{\substack{F \in \mathcal{F}_2(X^{1/2}) \\ |\mathrm{Disc}(F)| \geq Y}} |\mathrm{Cl}_F[3]| \sum_{\substack{[K:F]=2 \\ |\mathrm{Disc}(K)| \leq X}} |\mathrm{Cl}_{K/F}[3]|.$$

Davenport–Heilbronn handles first sum, if we bound the second.

The strategy for D_4 quartics

For $K \in \mathcal{F}_{D_4}$, the 3-part factors: $|\mathrm{Cl}_K[3]| = |\mathrm{Cl}_F[3]| \cdot |\mathrm{Cl}_{K/F}[3]|$. Thus,

$$\sum_{\substack{K \in \mathcal{F}_4(X) \\ |\mathrm{Disc}(F)| \geq Y}} |\mathrm{Cl}_K[3]| \doteq \sum_{\substack{F \in \mathcal{F}_2(X^{1/2}) \\ |\mathrm{Disc}(F)| \geq Y}} |\mathrm{Cl}_F[3]| \sum_{\substack{[K:F]=2 \\ |\mathrm{Disc}(K)| \leq X}} |\mathrm{Cl}_{K/F}[3]|.$$

Davenport–Heilbronn handles first sum, if we bound the second.

For $x := X/|\mathrm{Disc}(F)|^2$, we have

$$\sum_{\substack{[K:F]=2 \\ |\mathrm{Disc}(K/F)| \leq x}} |\mathrm{Cl}_{K/F}[3]| \doteq N_3^{\mathrm{sf}}(x; F),$$

The strategy for D_4 quartics

For $K \in \mathcal{F}_{D_4}$, the 3-part factors: $|\mathrm{Cl}_K[3]| = |\mathrm{Cl}_F[3]| \cdot |\mathrm{Cl}_{K/F}[3]|$. Thus,

$$\sum_{\substack{K \in \mathcal{F}_4(X) \\ |\mathrm{Disc}(F)| \geq Y}} |\mathrm{Cl}_K[3]| \doteq \sum_{\substack{F \in \mathcal{F}_2(X^{1/2}) \\ |\mathrm{Disc}(F)| \geq Y}} |\mathrm{Cl}_F[3]| \sum_{\substack{[K:F]=2 \\ |\mathrm{Disc}(K)| \leq X}} |\mathrm{Cl}_{K/F}[3]|.$$

Davenport–Heilbronn handles first sum, if we bound the second.

For $x := X/|\mathrm{Disc}(F)|^2$, we have

$$\sum_{\substack{[K:F]=2 \\ |\mathrm{Disc}(K/F)| \leq x}} |\mathrm{Cl}_{K/F}[3]| \doteq N_3^{\mathrm{sf}}(x; F),$$

where $N_3^{\mathrm{sf}}(x; F)$ is the number of squarefree cubic extensions of F.

The strategy for D_4 quartics

For $K \in \mathcal{F}_{D_4}$, the 3-part factors: $|\mathrm{Cl}_K[3]| = |\mathrm{Cl}_F[3]| \cdot |\mathrm{Cl}_{K/F}[3]|$. Thus,

$$\sum_{\substack{K \in \mathcal{F}_4(X) \\ |\mathrm{Disc}(F)| \geq Y}} |\mathrm{Cl}_K[3]| \doteq \sum_{\substack{F \in \mathcal{F}_2(X^{1/2}) \\ |\mathrm{Disc}(F)| \geq Y}} |\mathrm{Cl}_F[3]| \sum_{\substack{[K:F]=2 \\ |\mathrm{Disc}(K)| \leq X}} |\mathrm{Cl}_{K/F}[3]|.$$

Davenport–Heilbronn handles first sum, if we bound the second.

For $x := X/|\mathrm{Disc}(F)|^2$, we have

$$\sum_{\substack{[K:F]=2 \\ |\mathrm{Disc}(K/F)| \leq x}} |\mathrm{Cl}_{K/F}[3]| \doteq N_3^{\mathrm{sf}}(x; F),$$

where $N_3^{\mathrm{sf}}(x; F)$ is the number of squarefree cubic extensions of F.

Key obstacle: The relative discriminant bound, x, may be small.

A shifted goalpost: Bounding small cubic extensions

Let $N_3(x; F) := \#\{L/F \text{ cubic} : |\mathrm{Disc}(L/F)| \leq x\}$.

A shifted goalpost: Bounding small cubic extensions

Let $N_3(x; F) := \#\{L/F \text{ cubic} : |\mathrm{Disc}(L/F)| \leq x\}$.

Datskovsky–Wright: $N_3(x; F) \sim c_F x$ as $x \to \infty$.

A shifted goalpost: Bounding small cubic extensions

Let $N_3(x; F) := \#\{L/F \text{ cubic} : |\mathrm{Disc}(L/F)| \le x\}$.

Datskovsky–Wright: $N_3(x; F) \sim c_F x$ as $x \to \infty$.

Question: What is the least α s.t. $N_3(x; F) = O(|\mathrm{Disc}(F)|^\alpha x)$ for all $x \geq 1$?

A shifted goalpost: Bounding small cubic extensions

Let $N_3(x; F) := \#\{L/F \text{ cubic} : |\mathrm{Disc}(L/F)| \leq x\}$.

Datskovsky–Wright: $N_3(x; F) \sim c_F x$ as $x \to \infty$.

Question: What is the least α s.t. $N_3(x; F) = O(|\mathrm{Disc}(F)|^\alpha x)$ for all $x \geq 1$?

- **Conjecture:** Any $\alpha > 0$ should work (i.e., $\alpha = \epsilon$).

A shifted goalpost: Bounding small cubic extensions

Let $N_3(x; F) := \#\{L/F \text{ cubic} : |\mathrm{Disc}(L/F)| \leq x\}$.

Datskovsky–Wright: $N_3(x; F) \sim c_F x$ as $x \to \infty$.

Question: What is the least α s.t. $N_3(x; F) = O(|\mathrm{Disc}(F)|^{\alpha} x)$ for all $x \geq 1$?

- **Conjecture:** Any $\alpha > 0$ should work (i.e., $\alpha = \epsilon$).
- **Goal:** Get some $\alpha < 1$.

A shifted goalpost: Bounding small cubic extensions

Let $N_3(x; F) := \#\{L/F \text{ cubic} : |\mathrm{Disc}(L/F)| \le x\}$.

Datskovsky–Wright: $N_3(x; F) \sim c_F x$ as $x \to \infty$.

Question: What is the least α s.t. $N_3(x; F) = O(|\mathrm{Disc}(F)|^\alpha x)$ for all $x \ge 1$?

- **Conjecture:** Any $\alpha > 0$ should work (i.e., $\alpha = \epsilon$).
- **Goal:** Get some $\alpha < 1$.
- **Trivial bound:** ?????

A shifted goalpost: Bounding small cubic extensions

Let $N_3(x; F) := \#\{L/F \text{ cubic} : |\mathrm{Disc}(L/F)| \leq x\}$.

Datskovsky–Wright: $N_3(x; F) \sim c_F x$ as $x \to \infty$.

Question: What is the least α s.t. $N_3(x; F) = O(|\mathrm{Disc}(F)|^\alpha x)$ for all $x \geq 1$?

- **Conjecture:** Any $\alpha > 0$ should work (i.e., $\alpha = \epsilon$).
- **Goal:** Get some $\alpha < 1$.
- **Trivial bound:** ?????

Spoiler: Get $\alpha = 1 + \epsilon$ pointwise,

A shifted goalpost: Bounding small cubic extensions

Let $N_3(x;F) := \#\{L/F \text{ cubic} : |\mathrm{Disc}(L/F)| \leq x\}$.

Datskovsky–Wright: $N_3(x;F) \sim c_F x$ as $x \to \infty$.

Question: What is the least α s.t. $N_3(x;F) = O(|\mathrm{Disc}(F)|^\alpha x)$ for all $x \geq 1$?

- **Conjecture:** Any $\alpha > 0$ should work (i.e., $\alpha = \epsilon$).
- **Goal:** Get some $\alpha < 1$.
- **Trivial bound:** ?????

Spoiler: Get $\alpha = 1 + \epsilon$ pointwise, only get $\alpha < 1$ on average.

Idea 1: Class field theory

Suppose $|\mathrm{Disc}(L/F)| = D$.

Idea 1: Class field theory

Suppose $|\mathrm{Disc}(L/F)| = D$.

- L/F cyclic: get at most $O(|\mathrm{Cl}_F[3]| \cdot D^{\epsilon})$ extensions.

Idea 1: Class field theory

Suppose $|\mathrm{Disc}(L/F)| = D$.

- L/F cyclic: get at most $O(|\mathrm{Cl}_F[3]| \cdot D^{\epsilon})$ extensions.
  - Trivial bound: $|\mathrm{Cl}_F[3]| \leq |\mathrm{Cl}_F| \ll |\mathrm{Disc}(F)|^{1/2+\epsilon}$.

Idea 1: Class field theory

Suppose $|\mathrm{Disc}(L/F)| = D$.

- L/F cyclic: get at most $O(|\mathrm{Cl}_F[3]| \cdot D^\epsilon)$ extensions.
    - Trivial bound: $|\mathrm{Cl}_F[3]| \leq |\mathrm{Cl}_F| \ll |\mathrm{Disc}(F)|^{1/2+\epsilon}$.
    - $\Rightarrow$ Get at most $O(|\mathrm{Disc}(F)|^{1/2+\epsilon} D^\epsilon)$ extensions.

Idea 1: Class field theory

Suppose $|\mathrm{Disc}(L/F)| = D$.

- L/F cyclic: get at most $O(|\mathrm{Cl}_F[3]| \cdot D^\epsilon)$ extensions.
  - Trivial bound: $|\mathrm{Cl}_F[3]| \leq |\mathrm{Cl}_F| \ll |\mathrm{Disc}(F)|^{1/2+\epsilon}$.
  - $\Rightarrow$ Get at most $O(|\mathrm{Disc}(F)|^{1/2+\epsilon} D^\epsilon)$ extensions.
- L/F noncyclic; parametrized by $\mathrm{Cl}_{K/F}[3]$ for K/F quad.

Idea 1: Class field theory

Suppose $|\mathrm{Disc}(L/F)| = D$.

- L/F cyclic: get at most $O(|\mathrm{Cl}_F[3]| \cdot D^\epsilon)$ extensions.
  - Trivial bound: $|\mathrm{Cl}_F[3]| \leq |\mathrm{Cl}_F| \ll |\mathrm{Disc}(F)|^{1/2+\epsilon}$.
  - $\Rightarrow$ Get at most $O(|\mathrm{Disc}(F)|^{1/2+\epsilon} D^\epsilon)$ extensions.
- L/F noncyclic; parametrized by $\mathrm{Cl}_{K/F}[3]$ for K/F quad.
  - $|\mathrm{Disc}(K/F)|$ divides $D \Rightarrow$ at most $O(D^\epsilon)$ different K.

Idea 1: Class field theory

Suppose $|\mathrm{Disc}(L/F)| = D$.

- L/F cyclic: get at most $O(|\mathrm{Cl}_F[3]| \cdot D^\epsilon)$ extensions.
  - Trivial bound: $|\mathrm{Cl}_F[3]| \leq |\mathrm{Cl}_F| \ll |\mathrm{Disc}(F)|^{1/2+\epsilon}$.
  - $\Rightarrow$ Get at most $O(|\mathrm{Disc}(F)|^{1/2+\epsilon} D^\epsilon)$ extensions.
- L/F noncyclic; parametrized by $\mathrm{Cl}_{K/F}[3]$ for K/F quad.
  - $|\mathrm{Disc}(K/F)|$ divides $D \Rightarrow$ at most $O(D^\epsilon)$ different K.
  - Given K, get $O(|\mathrm{Cl}_{K/F}[3]| \cdot D^\epsilon)$ extensions.

Idea 1: Class field theory

Suppose $|\mathrm{Disc}(L/F)| = D$.

- L/F cyclic: get at most $O(|\mathrm{Cl}_F[3]| \cdot D^\epsilon)$ extensions.
  - Trivial bound: $|\mathrm{Cl}_F[3]| \leq |\mathrm{Cl}_F| \ll |\mathrm{Disc}(F)|^{1/2+\epsilon}$.
  - $\Rightarrow$ Get at most $O(|\mathrm{Disc}(F)|^{1/2+\epsilon} D^\epsilon)$ extensions.
- L/F noncyclic; parametrized by $\mathrm{Cl}_{K/F}[3]$ for K/F quad.
  - $|\mathrm{Disc}(K/F)|$ divides $D \Rightarrow$ at most $O(D^\epsilon)$ different K.
  - Given K, get $O(|\mathrm{Cl}_{K/F}[3]| \cdot D^\epsilon)$ extensions.
  - Trivial bound: $|\mathrm{Cl}_{K/F}| \ll |\mathrm{Disc}(F)|^{1/2+\epsilon} |\mathrm{Disc}(K/F)|^{1/2+\epsilon}$.

Idea 1: Class field theory

Suppose $|\mathrm{Disc}(L/F)| = D$.

- L/F cyclic: get at most $O(|\mathrm{Cl}_F[3]| \cdot D^{\epsilon})$ extensions.
  - Trivial bound: $|\mathrm{Cl}_F[3]| \leq |\mathrm{Cl}_F| \ll |\mathrm{Disc}(F)|^{1/2+\epsilon}$.
  - $\Rightarrow$ Get at most $O(|\mathrm{Disc}(F)|^{1/2+\epsilon} D^{\epsilon})$ extensions.
- L/F noncyclic; parametrized by $\mathrm{Cl}_{K/F}[3]$ for K/F quad.
  - $|\mathrm{Disc}(K/F)|$ divides $D \Rightarrow$ at most $O(D^{\epsilon})$ different K.
  - Given K, get $O(|\mathrm{Cl}_{K/F}[3]| \cdot D^{\epsilon})$ extensions.
  - Trivial bound: $|\mathrm{Cl}_{K/F}| \ll |\mathrm{Disc}(F)|^{1/2+\epsilon} |\mathrm{Disc}(K/F)|^{1/2+\epsilon}$.
  - $\Rightarrow$ Get at most $O(|\mathrm{Disc}(F)|^{1/2+\epsilon} D^{1/2+\epsilon})$ extensions.

Idea 1: Class field theory

Suppose $|\mathrm{Disc}(L/F)| = D$.

- L/F cyclic: get at most $O(|\mathrm{Cl}_F[3]| \cdot D^{\epsilon})$ extensions.
  - Trivial bound: $|\mathrm{Cl}_F[3]| \leq |\mathrm{Cl}_F| \ll |\mathrm{Disc}(F)|^{1/2+\epsilon}$.
  - $\Rightarrow$ Get at most $O(|\mathrm{Disc}(F)|^{1/2+\epsilon} D^{\epsilon})$ extensions.
- L/F noncyclic; parametrized by $\mathrm{Cl}_{K/F}[3]$ for K/F quad.
  - $|\mathrm{Disc}(K/F)|$ divides $D \Rightarrow$ at most $O(D^{\epsilon})$ different K.
  - Given K, get $O(|\mathrm{Cl}_{K/F}[3]| \cdot D^{\epsilon})$ extensions.
  - Trivial bound: $|\mathrm{Cl}_{K/F}| \ll |\mathrm{Disc}(F)|^{1/2+\epsilon} |\mathrm{Disc}(K/F)|^{1/2+\epsilon}$.
  - $\Rightarrow$ Get at most $O(|\mathrm{Disc}(F)|^{1/2+\epsilon} D^{1/2+\epsilon})$ extensions.

Adding across $D \leq x$, get:

$\boxed{\textbf{First bound: } N_3(x; F) = O_{\epsilon}(|\mathrm{Disc}(F)|^{1/2+\epsilon} x^{3/2+\epsilon}) \text{ for all } x \geq 1.}$

Idea 1: Class field theory

Suppose $|\mathrm{Disc}(L/F)| = D$.

- L/F cyclic: get at most $O(|\mathrm{Cl}_F[3]| \cdot D^{\epsilon})$ extensions.
  - Trivial bound: $|\mathrm{Cl}_F[3]| \leq |\mathrm{Cl}_F| \ll |\mathrm{Disc}(F)|^{1/2+\epsilon}$.
  - $\Rightarrow$ Get at most $O(|\mathrm{Disc}(F)|^{1/2+\epsilon} D^{\epsilon})$ extensions.
- L/F noncyclic; parametrized by $\mathrm{Cl}_{K/F}[3]$ for K/F quad.
  - $|\mathrm{Disc}(K/F)|$ divides $D \Rightarrow$ at most $O(D^{\epsilon})$ different K.
  - Given K, get $O(|\mathrm{Cl}_{K/F}[3]| \cdot D^{\epsilon})$ extensions.
  - Trivial bound: $|\mathrm{Cl}_{K/F}| \ll |\mathrm{Disc}(F)|^{1/2+\epsilon} |\mathrm{Disc}(K/F)|^{1/2+\epsilon}$.
  - $\Rightarrow$ Get at most $O(|\mathrm{Disc}(F)|^{1/2+\epsilon} D^{1/2+\epsilon})$ extensions.

Adding across $D \leq x$, get:

First bound: $N_3(x; F) = O_{\epsilon}(|\mathrm{Disc}(F)|^{1/2+\epsilon} x^{3/2+\epsilon})$ for all $x \geq 1$.

(Only usable for us if x is very small, $\leq |\mathrm{Disc}(F)|^{1-\delta}$.)

Idea 2: Shintani zeta functions

Idea 2: Shintani zeta functions

The **Shintani zeta function** $\xi_F(s)$ is the Dirichlet series

$$\xi_F(s) = \sum_{\substack{R/F: \\ \mathrm{Disc}(R/F) \neq 0}} \frac{|\mathrm{Aut}(R)|^{-1}}{|\mathrm{Disc}(R/F)|^s}$$

for cubic rings R/F. (Developed by Datskovsky–Wright)

Idea 2: Shintani zeta functions

The **Shintani zeta function** $\xi_F(s)$ is the Dirichlet series

$$\xi_F(s) = \sum_{\substack{R/F: \\ \mathrm{Disc}(R/F)\neq 0}} \frac{|\mathrm{Aut}(R)|^{-1}}{|\mathrm{Disc}(R/F)|^s}$$

for cubic rings R/F. (Developed by Datskovsky–Wright)

- Abs. conv. for $\Re(s) > 1$; has analytic continuation, functional equation like a degree 4 L-function over F

Idea 2: Shintani zeta functions

The **Shintani zeta function** $\xi_F(s)$ is the Dirichlet series

$$\xi_F(s) = \sum_{\substack{R/F: \\ \mathrm{Disc}(R/F) \neq 0}} \frac{|\mathrm{Aut}(R)|^{-1}}{|\mathrm{Disc}(R/F)|^s}$$

for cubic rings R/F. (Developed by Datskovsky–Wright)

- Abs. conv. for $\Re(s) > 1$; has analytic continuation, functional equation like a degree 4 L-function over F
- Poles at $s = 1, 5/6$; no Euler product, no Ramanujan bound

Idea 2: Shintani zeta functions

The **Shintani zeta function** $\xi_F(s)$ is the Dirichlet series

$$\xi_F(s) = \sum_{\substack{R/F: \\ \mathrm{Disc}(R/F) \neq 0}} \frac{|\mathrm{Aut}(R)|^{-1}}{|\mathrm{Disc}(R/F)|^s}$$

for cubic rings R/F. (Developed by Datskovsky–Wright)

- Abs. conv. for $\Re(s) > 1$; has analytic continuation, functional equation like a degree 4 L-function over F
- Poles at $s = 1, 5/6$; no Euler product, no Ramanujan bound

First bound $+$ "convexity principle" gives:

Second bound: $N_3(x; F) = O_\epsilon(|\mathrm{Disc}(F)|^\epsilon x)$ for all $x \geq |\mathrm{Disc}(F)|^3$.

Idea 3: Propagation of orders; exploiting a ~~bug~~ feature

The Shintani zeta function counts cubic rings, not just cubic fields.

Idea 3: Propagation of orders; exploiting a ~~bug~~ feature

The Shintani zeta function counts cubic rings, not just cubic fields.

- Suppose $|\mathrm{Disc}(L/F)| = D$ for some $D \leq |\mathrm{Disc}(F)|^3$.

Idea 3: Propagation of orders; exploiting a ~~bug~~ feature

The Shintani zeta function counts cubic rings, not just cubic fields.

- Suppose $|\mathrm{Disc}(L/F)| = D$ for some $D \leq |\mathrm{Disc}(F)|^3$.
  - Expect $\approx |\mathrm{Disc}(F)|^{3/2}/D^{1/2}$ rings $R \subseteq L$ with $|\mathrm{Disc}(R/F)| \leq |\mathrm{Disc}(F)|^3$.

Idea 3: Propagation of orders; exploiting a ~~bug~~ feature

The Shintani zeta function counts cubic rings, not just cubic fields.

- Suppose $|\mathrm{Disc}(L/F)| = D$ for some $D \leq |\mathrm{Disc}(F)|^3$.
  - Expect $\approx |\mathrm{Disc}(F)|^{3/2}/D^{1/2}$ rings $R \subseteq L$ with $|\mathrm{Disc}(R/F)| \leq |\mathrm{Disc}(F)|^3$.
- $\Rightarrow$ Inside all L/F with $D \leq x$, expect $\approx N_3(x; F) \cdot \frac{|\mathrm{Disc}(F)|^{3/2}}{x^{1/2}}$ rings with $|\mathrm{Disc}(R/F)| \leq |\mathrm{Disc}(F)|^3$.

Idea 3: Propagation of orders; exploiting a ~~bug~~ feature

The Shintani zeta function counts cubic rings, not just cubic fields.

- Suppose $|\mathrm{Disc}(L/F)| = D$ for some $D \leq |\mathrm{Disc}(F)|^3$.
  - Expect $\approx |\mathrm{Disc}(F)|^{3/2}/D^{1/2}$ rings $R \subseteq L$ with $|\mathrm{Disc}(R/F)| \leq |\mathrm{Disc}(F)|^3$.
- $\Rightarrow$ Inside all L/F with $D \leq x$, expect $\approx N_3(x; F) \cdot \frac{|\mathrm{Disc}(F)|^{3/2}}{x^{1/2}}$ rings with $|\mathrm{Disc}(R/F)| \leq |\mathrm{Disc}(F)|^3$.
- Can't be more than total number of rings, $O(|\mathrm{Disc}(F)|^{3+\epsilon})$, from **second bound**.

Idea 3: Propagation of orders; exploiting a ~~bug~~ feature

The Shintani zeta function counts cubic rings, not just cubic fields.

- Suppose $|\mathrm{Disc}(L/F)| = D$ for some $D \leq |\mathrm{Disc}(F)|^3$.
  - Expect $\approx |\mathrm{Disc}(F)|^{3/2}/D^{1/2}$ rings $R \subseteq L$ with $|\mathrm{Disc}(R/F)| \leq |\mathrm{Disc}(F)|^3$.
- $\Rightarrow$ Inside all L/F with $D \leq x$, expect $\approx N_3(x; F) \cdot \frac{|\mathrm{Disc}(F)|^{3/2}}{x^{1/2}}$ rings with $|\mathrm{Disc}(R/F)| \leq |\mathrm{Disc}(F)|^3$.
- Can't be more than total number of rings, $O(|\mathrm{Disc}(F)|^{3+\epsilon})$, from **second bound**.
  - $\Rightarrow N_3(x; F) \ll x^{1/2}|\mathrm{Disc}(F)|^{3/2+\epsilon}$.

Idea 3: Propagation of orders; exploiting a ~~bug~~ feature

The Shintani zeta function counts cubic rings, not just cubic fields.

- Suppose $|\mathrm{Disc}(L/F)| = D$ for some $D \leq |\mathrm{Disc}(F)|^3$.
  - Expect $\approx |\mathrm{Disc}(F)|^{3/2}/D^{1/2}$ rings $R \subseteq L$ with $|\mathrm{Disc}(R/F)| \leq |\mathrm{Disc}(F)|^3$.
- $\Rightarrow$ Inside all L/F with $D \leq x$, expect $\approx N_3(x; F) \cdot \frac{|\mathrm{Disc}(F)|^{3/2}}{x^{1/2}}$ rings with $|\mathrm{Disc}(R/F)| \leq |\mathrm{Disc}(F)|^3$.
- Can't be more than total number of rings, $O(|\mathrm{Disc}(F)|^{3+\epsilon})$, from **second bound**.
  - $\Rightarrow N_3(x; F) \ll x^{1/2}|\mathrm{Disc}(F)|^{3/2+\epsilon}$.
- Exploit average over L to realize this expectation.

Idea 3: Propagation of orders; exploiting a ~~bug~~ feature

The Shintani zeta function counts cubic rings, not just cubic fields.

- Suppose $|\mathrm{Disc}(L/F)| = D$ for some $D \leq |\mathrm{Disc}(F)|^3$.
  - Expect $\approx |\mathrm{Disc}(F)|^{3/2}/D^{1/2}$ rings $R \subseteq L$ with $|\mathrm{Disc}(R/F)| \leq |\mathrm{Disc}(F)|^3$.
- $\Rightarrow$ Inside all L/F with $D \leq x$, expect $\approx N_3(x; F) \cdot \frac{|\mathrm{Disc}(F)|^{3/2}}{x^{1/2}}$ rings with $|\mathrm{Disc}(R/F)| \leq |\mathrm{Disc}(F)|^3$.
- Can't be more than total number of rings, $O(|\mathrm{Disc}(F)|^{3+\epsilon})$, from **second bound**.
  - $\Rightarrow N_3(x; F) \ll x^{1/2}|\mathrm{Disc}(F)|^{3/2+\epsilon}$.
- Exploit average over L to realize this expectation.

Altogether, we find:

Third bound:

$$N_3(x; F) \ll \begin{cases} |\mathrm{Disc}(F)|^{3/2+\epsilon}x^{1/2}, & \text{if } x \leq |\mathrm{Disc}(F)|^2 \\ |\mathrm{Disc}(F)|^{1/2+\epsilon}x, & \text{if } |\mathrm{Disc}(F)|^2 \leq x \leq |\mathrm{Disc}(F)|^3. \end{cases}$$

Summarizing our progress

Summarizing our progress

Combining the three bounds, we find:

Theorem (LO–Wang–Wood)

If F is quadratic, then $N_3(x; F) = O(|\mathrm{Disc}(F)|^{1+\epsilon} x)$ for all $x \geq 1$.

Summarizing our progress

Combining the three bounds, we find:

Theorem (LO–Wang–Wood)

If F is quadratic, then $N_3(x; F) = O(|\mathrm{Disc}(F)|^{1+\epsilon} x)$ for all $x \geq 1$.

- Holds also when F is a 2-extension; variant for general F

Summarizing our progress

Combining the three bounds, we find:

Theorem (LO–Wang–Wood)

If F is quadratic, then $N_3(x; F) = O(|\mathrm{Disc}(F)|^{1+\epsilon} x)$ for all $x \geq 1$.

- Holds also when F is a 2-extension; variant for general F
- Barely not enough for our purposes

Summarizing our progress

Combining the three bounds, we find:

Theorem (LO–Wang–Wood)

If F is quadratic, then $N_3(x; F) = O(|\mathrm{Disc}(F)|^{1+\epsilon} x)$ for all $x \geq 1$.

- Holds also when F is a 2-extension; variant for general F
- Barely not enough for our purposes
  - Recall: Needed $N_3(x; F) = O(|\mathrm{Disc}(F)|^{\alpha} x)$ for some $\alpha < 1$.

Summarizing our progress

Combining the three bounds, we find:

Theorem (LO–Wang–Wood)

If F is quadratic, then $N_3(x; F) = O(|\mathrm{Disc}(F)|^{1+\epsilon} x)$ for all $x \geq 1$.

- Holds also when F is a 2-extension; variant for general F
- Barely not enough for our purposes
  - Recall: Needed $N_3(x; F) = O(|\mathrm{Disc}(F)|^{\alpha} x)$ for some $\alpha < 1$.
- Tension point is $x \approx |\mathrm{Disc}(F)|$

Summarizing our progress

Combining the three bounds, we find:

Theorem (LO–Wang–Wood)

If F is quadratic, then $N_3(x; F) = O(|\mathrm{Disc}(F)|^{1+\epsilon} x)$ for all $x \geq 1$.

- Holds also when F is a 2-extension; variant for general F
- Barely not enough for our purposes
  - Recall: Needed $N_3(x; F) = O(|\mathrm{Disc}(F)|^{\alpha} x)$ for some $\alpha < 1$.
- Tension point is $x \approx |\mathrm{Disc}(F)|$
  - Handoff from class field theory to propagation of orders

Summarizing our progress

Combining the three bounds, we find:

Theorem (LO–Wang–Wood)

If F is quadratic, then $N_3(x;F) = O(|\mathrm{Disc}(F)|^{1+\epsilon}x)$ for all $x \geq 1$.

- Holds also when F is a 2-extension; variant for general F
- Barely not enough for our purposes
  - Recall: Needed $N_3(x;F) = O(|\mathrm{Disc}(F)|^{\alpha}x)$ for some $\alpha < 1$.
- Tension point is $x \approx |\mathrm{Disc}(F)|$
  - Handoff from class field theory to propagation of orders
- Class field theory relied on trivial bound $|\mathrm{Cl}_{K/F}[3]| \leq |\mathrm{Cl}_{K/F}|$.

Summarizing our progress

Combining the three bounds, we find:

Theorem (LO–Wang–Wood)

If F is quadratic, then $N_3(x; F) = O(|\mathrm{Disc}(F)|^{1+\epsilon} x)$ for all $x \geq 1$.

- Holds also when F is a 2-extension; variant for general F
- Barely not enough for our purposes
  - Recall: Needed $N_3(x; F) = O(|\mathrm{Disc}(F)|^{\alpha} x)$ for some $\alpha < 1$.
- Tension point is $x \approx |\mathrm{Disc}(F)|$
  - Handoff from class field theory to propagation of orders
- Class field theory relied on trivial bound $|\mathrm{Cl}_{K/F}[3]| \leq |\mathrm{Cl}_{K/F}|$.
- **Idea 4:** Do better than trivial bound “on average.”

Arakelov class groups and prime ideals

Lemma (Ellenberg–Venkatesh)

Suppose K/F is degree d, $\ell \geq 2$ is an integer, and $\theta < 1/2\ell(d-1)$. If there are M primes $\mathfrak{p}$ of K, not extended from any subextension, with $\mathrm{Nm}\mathfrak{p} \leq |\mathrm{Disc}(K/F)|^{\theta}$, then

$$|\mathrm{Cl}_K[\ell]| = O_\epsilon(|\mathrm{Disc}(K)|^{1/2+\epsilon}/M).$$

Arakelov class groups and prime ideals

Lemma (Ellenberg–Venkatesh)

Suppose K/F is degree d, $\ell \geq 2$ is an integer, and $\theta < 1/2\ell(d-1)$. If there are M primes $\mathfrak{p}$ of K, not extended from any subextension, with $\mathrm{Nm}\mathfrak{p} \leq |\mathrm{Disc}(K/F)|^{\theta}$, then

$$|\mathrm{Cl}_K[\ell]| = O_\epsilon(|\mathrm{Disc}(K)|^{1/2+\epsilon}/M).$$

- Uses the Arakelov class group, $\widetilde{\mathrm{Cl}_K}$

Arakelov class groups and prime ideals

Lemma (Ellenberg–Venkatesh)

Suppose K/F is degree d, $\ell \geq 2$ is an integer, and $\theta < 1/2\ell(d-1)$. If there are M primes $\mathfrak{p}$ of K, not extended from any subextension, with $\mathrm{Nm}\mathfrak{p} \leq |\mathrm{Disc}(K/F)|^{\theta}$, then

$$|\mathrm{Cl}_K[\ell]| = O_\epsilon(|\mathrm{Disc}(K)|^{1/2+\epsilon}/M).$$

- Uses the Arakelov class group, $\widetilde{\mathrm{Cl}_K}$
  - **Think:** $\widetilde{\mathrm{Cl}_K} \simeq \mathrm{Cl}_K \times K^1_\infty/\mathcal{O}_K^\times$

Arakelov class groups and prime ideals

Lemma (Ellenberg–Venkatesh)

Suppose K/F is degree d, $\ell \geq 2$ is an integer, and $\theta < 1/2\ell(d-1)$. If there are M primes $\mathfrak{p}$ of K, not extended from any subextension, with $\mathrm{Nm}\mathfrak{p} \leq |\mathrm{Disc}(K/F)|^\theta$, then

$$|\mathrm{Cl}_K[\ell]| = O_\epsilon(|\mathrm{Disc}(K)|^{1/2+\epsilon}/M).$$

- Uses the Arakelov class group, $\widetilde{\mathrm{Cl}_K}$
  - **Think:** $\widetilde{\mathrm{Cl}_K} \simeq \mathrm{Cl}_K \times K_\infty^1/\mathcal{O}_K^\times$
  - $\Rightarrow \mathrm{Vol}(\widetilde{\mathrm{Cl}_K}) = |\mathrm{Cl}_K| \cdot \mathrm{Reg}(K) \ll |\mathrm{Disc}(K)|^{1/2+\epsilon}$

Arakelov class groups and prime ideals

Lemma (Ellenberg–Venkatesh)

Suppose K/F is degree d, $\ell \geq 2$ is an integer, and $\theta < 1/2\ell(d-1)$. If there are M primes $\mathfrak{p}$ of K, not extended from any subextension, with $\mathrm{Nm}\mathfrak{p} \leq |\mathrm{Disc}(K/F)|^{\theta}$, then

$$|\mathrm{Cl}_K[\ell]| = O_\epsilon(|\mathrm{Disc}(K)|^{1/2+\epsilon}/M).$$

- Uses the Arakelov class group, $\widetilde{\mathrm{Cl}_K}$
  - **Think:** $\widetilde{\mathrm{Cl}_K} \simeq \mathrm{Cl}_K \times K_\infty^1/\mathcal{O}_K^\times$
  - $\Rightarrow \mathrm{Vol}(\widetilde{\mathrm{Cl}_K}) = |\mathrm{Cl}_K| \cdot \mathrm{Reg}(K) \ll |\mathrm{Disc}(K)|^{1/2+\epsilon}$
- Create discs $D_\mathfrak{p} \subseteq \widetilde{\mathrm{Cl}_K}$

Arakelov class groups and prime ideals

Lemma (Ellenberg–Venkatesh)

Suppose K/F is degree d, $\ell \geq 2$ is an integer, and $\theta < 1/2\ell(d-1)$. If there are M primes $\mathfrak{p}$ of K, not extended from any subextension, with $\mathrm{Nm}\mathfrak{p} \leq |\mathrm{Disc}(K/F)|^{\theta}$, then

$$|\mathrm{Cl}_K[\ell]| = O_\epsilon(|\mathrm{Disc}(K)|^{1/2+\epsilon}/M).$$

- Uses the Arakelov class group, $\widetilde{\mathrm{Cl}_K}$
  - **Think:** $\widetilde{\mathrm{Cl}_K} \simeq \mathrm{Cl}_K \times K_\infty^1/\mathcal{O}_K^\times$
  - $\Rightarrow \mathrm{Vol}(\widetilde{\mathrm{Cl}_K}) = |\mathrm{Cl}_K| \cdot \mathrm{Reg}(K) \ll |\mathrm{Disc}(K)|^{1/2+\epsilon}$
- Create discs $D_\mathfrak{p} \subseteq \widetilde{\mathrm{Cl}_K}$
  - Conditions on $\mathfrak{p} \Rightarrow$ discs $\ell D_\mathfrak{p}$ don't intersect

Arakelov class groups and prime ideals

Lemma (Ellenberg–Venkatesh)

Suppose K/F is degree d, $\ell \geq 2$ is an integer, and $\theta < 1/2\ell(d-1)$. If there are M primes $\mathfrak{p}$ of K, not extended from any subextension, with $\mathrm{Nm}\mathfrak{p} \leq |\mathrm{Disc}(K/F)|^{\theta}$, then

$$|\mathrm{Cl}_K[\ell]| = O_\epsilon(|\mathrm{Disc}(K)|^{1/2+\epsilon}/M).$$

- Uses the Arakelov class group, $\widetilde{\mathrm{Cl}_K}$
  - **Think:** $\widetilde{\mathrm{Cl}_K} \simeq \mathrm{Cl}_K \times K_\infty^1/\mathcal{O}_K^\times$
  - $\Rightarrow \mathrm{Vol}(\widetilde{\mathrm{Cl}_K}) = |\mathrm{Cl}_K| \cdot \mathrm{Reg}(K) \ll |\mathrm{Disc}(K)|^{1/2+\epsilon}$
- Create discs $D_\mathfrak{p} \subseteq \widetilde{\mathrm{Cl}_K}$
  - Conditions on $\mathfrak{p} \Rightarrow$ discs $\ell D_\mathfrak{p}$ don't intersect
  - $\Rightarrow \mathrm{Vol}(\ell\widetilde{\mathrm{Cl}_K}) \gg M$,

Arakelov class groups and prime ideals

Lemma (Ellenberg–Venkatesh)

Suppose K/F is degree d, $\ell \geq 2$ is an integer, and $\theta < 1/2\ell(d-1)$. If there are M primes $\mathfrak{p}$ of K, not extended from any subextension, with $\mathrm{Nm}\mathfrak{p} \leq |\mathrm{Disc}(K/F)|^{\theta}$, then

$$|\mathrm{Cl}_K[\ell]| = O_\epsilon(|\mathrm{Disc}(K)|^{1/2+\epsilon}/M).$$

- Uses the Arakelov class group, $\widetilde{\mathrm{Cl}_K}$
  - **Think:** $\widetilde{\mathrm{Cl}_K} \simeq \mathrm{Cl}_K \times K_\infty^1/\mathcal{O}_K^\times$
  - $\Rightarrow \mathrm{Vol}(\widetilde{\mathrm{Cl}_K}) = |\mathrm{Cl}_K| \cdot \mathrm{Reg}(K) \ll |\mathrm{Disc}(K)|^{1/2+\epsilon}$
- Create discs $D_\mathfrak{p} \subseteq \widetilde{\mathrm{Cl}_K}$
  - Conditions on $\mathfrak{p} \Rightarrow$ discs $\ell D_\mathfrak{p}$ don't intersect
  - $\Rightarrow \mathrm{Vol}(\ell\widetilde{\mathrm{Cl}_K}) \gg M$,
  - $\Rightarrow |\mathrm{Cl}_K/\ell\mathrm{Cl}_K| \ll \mathrm{Vol}(\widetilde{\mathrm{Cl}_K}/\ell\widetilde{\mathrm{Cl}_K}) \ll |\mathrm{Disc}(K)|^{1/2+\epsilon}/M$.

Arakelov class groups and prime ideals

Lemma (Ellenberg–Venkatesh)

Suppose K/F is degree d, $\ell \geq 2$ is an integer, and $\theta < 1/2\ell(d-1)$. If there are M primes $\mathfrak{p}$ of K, not extended from any subextension, with $\mathrm{Nm}\mathfrak{p} \leq |\mathrm{Disc}(K/F)|^{\theta}$, then

$$|\mathrm{Cl}_K[\ell]| = O_\epsilon(|\mathrm{Disc}(K)|^{1/2+\epsilon}/M).$$

- Uses the Arakelov class group, $\widetilde{\mathrm{Cl}_K}$
  - **Think:** $\widetilde{\mathrm{Cl}_K} \simeq \mathrm{Cl}_K \times K_\infty^1/\mathcal{O}_K^\times$
  - $\Rightarrow \mathrm{Vol}(\widetilde{\mathrm{Cl}_K}) = |\mathrm{Cl}_K| \cdot \mathrm{Reg}(K) \ll |\mathrm{Disc}(K)|^{1/2+\epsilon}$
- Create discs $D_\mathfrak{p} \subseteq \widetilde{\mathrm{Cl}_K}$
  - Conditions on $\mathfrak{p} \Rightarrow$ discs $\ell D_\mathfrak{p}$ don't intersect
  - $\Rightarrow \mathrm{Vol}(\ell\widetilde{\mathrm{Cl}_K}) \gg M$,
  - $\Rightarrow |\mathrm{Cl}_K/\ell\mathrm{Cl}_K| \ll \mathrm{Vol}(\widetilde{\mathrm{Cl}_K}/\ell\widetilde{\mathrm{Cl}_K}) \ll |\mathrm{Disc}(K)|^{1/2+\epsilon}/M$.
- **Problem:** Doesn't realize savings in $\mathrm{Cl}_{K/F}[\ell]$, only $\mathrm{Cl}_K[\ell]$.

Relative Arakelov class groups and prime ideals

Lemma (LO–Wang–Wood)

Suppose K/F is degree d, $\ell \geq 2$ is an integer, and $\theta < 1/4\ell(d-1)$.

Relative Arakelov class groups and prime ideals

Lemma (LO–Wang–Wood)

Suppose K/F is degree d, $\ell \geq 2$ is an integer, and $\theta < 1/4\ell(d-1)$. If there are M pairs $(\mathfrak{p}, \overline{\mathfrak{p}})$ of conjugate primes, not extended from the same subextension, such that $\max\{\mathrm{Nm}\mathfrak{p}, \mathrm{Nm}\overline{\mathfrak{p}}\} \leq |\mathrm{Disc}(K/F)|^{\theta}$,

Relative Arakelov class groups and prime ideals

Lemma (LO–Wang–Wood)

Suppose K/F is degree d, $\ell \geq 2$ is an integer, and $\theta < 1/4\ell(d-1)$. If there are M pairs $(\mathfrak{p}, \overline{\mathfrak{p}})$ of conjugate primes, not extended from the same subextension, such that $\max\{\mathrm{Nm}\mathfrak{p}, \mathrm{Nm}\overline{\mathfrak{p}}\} \leq |\mathrm{Disc}(K/F)|^{\theta}$, then

$$|\mathrm{Cl}_{K/F}[\ell]| \ll \frac{|\mathrm{Disc}(K/F)|^{1/2+\epsilon}|\mathrm{Disc}(F)|^{(d-1)/2+\epsilon}}{M}.$$

Relative Arakelov class groups and prime ideals

Lemma (LO–Wang–Wood)

Suppose K/F is degree d, $\ell \geq 2$ is an integer, and $\theta < 1/4\ell(d-1)$. If there are M pairs $(\mathfrak{p}, \overline{\mathfrak{p}})$ of conjugate primes, not extended from the same subextension, such that $\max\{\mathrm{Nm}\mathfrak{p}, \mathrm{Nm}\overline{\mathfrak{p}}\} \leq |\mathrm{Disc}(K/F)|^{\theta}$, then

$$|\mathrm{Cl}_{K/F}[\ell]| \ll \frac{|\mathrm{Disc}(K/F)|^{1/2+\epsilon}|\mathrm{Disc}(F)|^{(d-1)/2+\epsilon}}{M}.$$

- Define $\widetilde{\mathrm{Cl}_{K/F}} := \ker(\mathrm{Nm}\colon \widetilde{\mathrm{Cl}_K} \to \widetilde{\mathrm{Cl}_F})$.

Relative Arakelov class groups and prime ideals

Lemma (LO–Wang–Wood)

Suppose K/F is degree d, $\ell \geq 2$ is an integer, and $\theta < 1/4\ell(d-1)$. If there are M pairs $(\mathfrak{p}, \overline{\mathfrak{p}})$ of conjugate primes, not extended from the same subextension, such that $\max\{\mathrm{Nm}\mathfrak{p}, \mathrm{Nm}\overline{\mathfrak{p}}\} \leq |\mathrm{Disc}(K/F)|^{\theta}$, *then*

$$|\mathrm{Cl}_{K/F}[\ell]| \ll \frac{|\mathrm{Disc}(K/F)|^{1/2+\epsilon}|\mathrm{Disc}(F)|^{(d-1)/2+\epsilon}}{M}.$$

- Define $\widetilde{\mathrm{Cl}_{K/F}} := \ker(\mathrm{Nm}\colon \widetilde{\mathrm{Cl}_K} \to \widetilde{\mathrm{Cl}_F})$.
  - Lemma: $\mathrm{Vol}(\widetilde{\mathrm{Cl}_{K/F}}) \ll |\mathrm{Disc}(K/F)|^{1/2+\epsilon}|\mathrm{Disc}(F)|^{(d-1)/2+\epsilon}$.

Relative Arakelov class groups and prime ideals

Lemma (LO–Wang–Wood)

Suppose K/F is degree d, $\ell \geq 2$ is an integer, and $\theta < 1/4\ell(d-1)$. If there are M pairs $(\mathfrak{p}, \overline{\mathfrak{p}})$ of conjugate primes, not extended from the same subextension, such that $\max\{\mathrm{Nm}\mathfrak{p}, \mathrm{Nm}\overline{\mathfrak{p}}\} \leq |\mathrm{Disc}(K/F)|^{\theta}$, *then*

$$|\mathrm{Cl}_{K/F}[\ell]| \ll \frac{|\mathrm{Disc}(K/F)|^{1/2+\epsilon}|\mathrm{Disc}(F)|^{(d-1)/2+\epsilon}}{M}.$$

- Define $\widetilde{\mathrm{Cl}_{K/F}} := \ker(\mathrm{Nm}\colon \widetilde{\mathrm{Cl}_K} \to \widetilde{\mathrm{Cl}_F})$.
    - Lemma: $\mathrm{Vol}(\widetilde{\mathrm{Cl}_{K/F}}) \ll |\mathrm{Disc}(K/F)|^{1/2+\epsilon}|\mathrm{Disc}(F)|^{(d-1)/2+\epsilon}$.
- Create discs $D_{\mathfrak{p},\overline{\mathfrak{p}}} \subseteq \widetilde{\mathrm{Cl}_{K/F}}$.

Relative Arakelov class groups and prime ideals

Lemma (LO–Wang–Wood)

Suppose K/F is degree d, $\ell \geq 2$ is an integer, and $\theta < 1/4\ell(d-1)$. If there are M pairs $(\mathfrak{p}, \overline{\mathfrak{p}})$ of conjugate primes, not extended from the same subextension, such that $\max\{\mathrm{Nm}\mathfrak{p}, \mathrm{Nm}\overline{\mathfrak{p}}\} \leq |\mathrm{Disc}(K/F)|^\theta$, *then*

$$|\mathrm{Cl}_{K/F}[\ell]| \ll \frac{|\mathrm{Disc}(K/F)|^{1/2+\epsilon}|\mathrm{Disc}(F)|^{(d-1)/2+\epsilon}}{M}.$$

- Define $\widetilde{\mathrm{Cl}_{K/F}} := \ker(\mathrm{Nm}\colon \widetilde{\mathrm{Cl}_K} \to \widetilde{\mathrm{Cl}_F})$.
  - Lemma: $\mathrm{Vol}(\widetilde{\mathrm{Cl}_{K/F}}) \ll |\mathrm{Disc}(K/F)|^{1/2+\epsilon}|\mathrm{Disc}(F)|^{(d-1)/2+\epsilon}$.
- Create discs $D_{\mathfrak{p},\overline{\mathfrak{p}}} \subseteq \widetilde{\mathrm{Cl}_{K/F}}$.
  - Conditions on $\mathfrak{p}, \overline{\mathfrak{p}} \Rightarrow$ discs $\ell D_{\mathfrak{p},\overline{\mathfrak{p}}}$ don't intersect.

Relative Arakelov class groups and prime ideals

Lemma (LO–Wang–Wood)

Suppose K/F is degree d, $\ell \geq 2$ is an integer, and $\theta < 1/4\ell(d-1)$. If there are M pairs $(\mathfrak{p}, \overline{\mathfrak{p}})$ of conjugate primes, not extended from the same subextension, such that $\max\{\mathrm{Nm}\mathfrak{p}, \mathrm{Nm}\overline{\mathfrak{p}}\} \leq |\mathrm{Disc}(K/F)|^{\theta}$, *then*

$$|\mathrm{Cl}_{K/F}[\ell]| \ll \frac{|\mathrm{Disc}(K/F)|^{1/2+\epsilon}|\mathrm{Disc}(F)|^{(d-1)/2+\epsilon}}{M}.$$

- Define $\widetilde{\mathrm{Cl}}_{K/F} := \ker(\mathrm{Nm}\colon \widetilde{\mathrm{Cl}}_K \to \widetilde{\mathrm{Cl}}_F)$.
  - Lemma: $\mathrm{Vol}(\widetilde{\mathrm{Cl}}_{K/F}) \ll |\mathrm{Disc}(K/F)|^{1/2+\epsilon}|\mathrm{Disc}(F)|^{(d-1)/2+\epsilon}$.
- Create discs $D_{\mathfrak{p},\overline{\mathfrak{p}}} \subseteq \widetilde{\mathrm{Cl}}_{K/F}$.
  - Conditions on $\mathfrak{p}, \overline{\mathfrak{p}} \Rightarrow$ discs $\ell D_{\mathfrak{p},\overline{\mathfrak{p}}}$ don't intersect.
  - $\Rightarrow \mathrm{Vol}(\ell\widetilde{\mathrm{Cl}}_{K/F}) \gg M$.

Idea 4: Exploiting prime ideals

When K/F is quadratic, the previous lemma reduces to:

Lemma

Suppose K/F is quadratic, $\ell \geq 2$ is an integer, and $\theta < 1/4\ell$. If there are M split primes $\mathfrak{p}$ in K with $\mathrm{Nm}\mathfrak{p} \leq |\mathrm{Disc}(K/F)|^{\theta}$, then

$$|\mathrm{Cl}_{K/F}[\ell]| \ll \frac{|\mathrm{Disc}(K/F)|^{1/2+\epsilon}|\mathrm{Disc}(F)|^{1/2+\epsilon}}{M}.$$

Idea 4: Exploiting prime ideals

When K/F is quadratic, the previous lemma reduces to:

Lemma

Suppose K/F is quadratic, $\ell \geq 2$ is an integer, and $\theta < 1/4\ell$. If there are M split primes $\mathfrak{p}$ in K with $\mathrm{Nm}\mathfrak{p} \leq |\mathrm{Disc}(K/F)|^{\theta}$, then

$$|\mathrm{Cl}_{K/F}[\ell]| \ll \frac{|\mathrm{Disc}(K/F)|^{1/2+\epsilon}|\mathrm{Disc}(F)|^{1/2+\epsilon}}{M}.$$

- **Problem:** Need "lots" of small split primes in K

Idea 4: Exploiting prime ideals

When K/F is quadratic, the previous lemma reduces to:

Lemma

Suppose K/F is quadratic, $\ell \geq 2$ is an integer, and $\theta < 1/4\ell$. If there are M split primes $\mathfrak{p}$ in K with $\mathrm{Nm}\mathfrak{p} \leq |\mathrm{Disc}(K/F)|^{\theta}$, then

$$|\mathrm{Cl}_{K/F}[\ell]| \ll \frac{|\mathrm{Disc}(K/F)|^{1/2+\epsilon}|\mathrm{Disc}(F)|^{1/2+\epsilon}}{M}.$$

- **Problem:** Need "lots" of small split primes in K $\Rightarrow$ need lots of primes in F

Idea 4: Exploiting prime ideals

When K/F is quadratic, the previous lemma reduces to:

Lemma

Suppose K/F is quadratic, $\ell \geq 2$ is an integer, and $\theta < 1/4\ell$. If there are M split primes $\mathfrak{p}$ in K with $\mathrm{Nm}\mathfrak{p} \leq |\mathrm{Disc}(K/F)|^{\theta}$, then

$$|\mathrm{Cl}_{K/F}[\ell]| \ll \frac{|\mathrm{Disc}(K/F)|^{1/2+\epsilon}|\mathrm{Disc}(F)|^{1/2+\epsilon}}{M}.$$

- **Problem:** Need "lots" of small split primes in $K \Rightarrow$ need lots of primes in F
- Zero densisty estimates (LO–Thorner; Thorner–Zaman) imply:

Idea 4: Exploiting prime ideals

When K/F is quadratic, the previous lemma reduces to:

Lemma

Suppose K/F is quadratic, $\ell \geq 2$ is an integer, and $\theta < 1/4\ell$. If there are M split primes $\mathfrak{p}$ in K with $\mathrm{Nm}\mathfrak{p} \leq |\mathrm{Disc}(K/F)|^{\theta}$, then

$$|\mathrm{Cl}_{K/F}[\ell]| \ll \frac{|\mathrm{Disc}(K/F)|^{1/2+\epsilon}|\mathrm{Disc}(F)|^{1/2+\epsilon}}{M}.$$

- **Problem:** Need "lots" of small split primes in $K \Rightarrow$ need lots of primes in F
- Zero densisty estimates (LO–Thorner; Thorner–Zaman) imply:
  - Almost all F have "lots" of small primes;

Idea 4: Exploiting prime ideals

When K/F is quadratic, the previous lemma reduces to:

Lemma

Suppose K/F is quadratic, $\ell \geq 2$ is an integer, and $\theta < 1/4\ell$. If there are M split primes $\mathfrak{p}$ in K with $\mathrm{Nm}\mathfrak{p} \leq |\mathrm{Disc}(K/F)|^{\theta}$, then

$$|\mathrm{Cl}_{K/F}[\ell]| \ll \frac{|\mathrm{Disc}(K/F)|^{1/2+\epsilon}|\mathrm{Disc}(F)|^{1/2+\epsilon}}{M}.$$

- **Problem:** Need "lots" of small split primes in $K \Rightarrow$ need lots of primes in F
- Zero densisty estimates (LO–Thorner; Thorner–Zaman) imply:
  - Almost all F have "lots" of small primes; and
  - Given "good" F, almost all K/F have "lots" of split primes.

Idea 4: Exploiting prime ideals

When K/F is quadratic, the previous lemma reduces to:

Lemma

Suppose K/F is quadratic, $\ell \geq 2$ is an integer, and $\theta < 1/4\ell$. If there are M split primes $\mathfrak{p}$ in K with $\mathrm{Nm}\mathfrak{p} \leq |\mathrm{Disc}(K/F)|^{\theta}$, then

$$|\mathrm{Cl}_{K/F}[\ell]| \ll \frac{|\mathrm{Disc}(K/F)|^{1/2+\epsilon}|\mathrm{Disc}(F)|^{1/2+\epsilon}}{M}.$$

- **Problem:** Need "lots" of small split primes in $K \Rightarrow$ need lots of primes in F
- Zero densisty estimates (LO–Thorner; Thorner–Zaman) imply:
  - Almost all F have "lots" of small primes; and
  - Given "good" F, almost all K/F have "lots" of split primes.
- $\Rightarrow$ Get better than trivial for almost all K/F.

Nearing final assembly

This finally yields:

Theorem (LO–Wang–Wood; main technical result for D_4)

For any $X \geq 1$ and $Y \leq X^{1/2}$, we have

$$\sum_{\substack{K \in \mathcal{F}_4(X) \\ |\mathrm{Disc}(F)| \geq Y}} |\mathrm{Cl}_K[3]| = O_\epsilon(X/Y^{1-\epsilon}).$$

Nearing final assembly

This finally yields:

Theorem (LO–Wang–Wood; main technical result for D_4)

For any $X \geq 1$ and $Y \leq X^{1/2}$, we have

$$\sum_{\substack{K \in \mathcal{F}_4(X) \\ |\mathrm{Disc}(F)| \geq Y}} |\mathrm{Cl}_K[3]| = O_\epsilon(X/Y^{1-\epsilon}).$$

To get the average for $\mathcal{F}_{D_4}$, it remains to:

- Handle the "sparse" groups $G = C_2 \times C_2$ and $G = C_4$;

Nearing final assembly

This finally yields:

Theorem (LO–Wang–Wood; main technical result for D_4)

For any $X \geq 1$ and $Y \leq X^{1/2}$, we have

$$\sum_{\substack{K \in \mathcal{F}_4(X) \\ |\mathrm{Disc}(F)| \geq Y}} |\mathrm{Cl}_K[3]| = O_\epsilon(X/Y^{1-\epsilon}).$$

To get the average for $\mathcal{F}_{D_4}$, it remains to:

- Handle the "sparse" groups $G = C_2 \times C_2$ and $G = C_4$; and
- Piece together the contributions from F with $|\mathrm{Disc}(F)| \leq Y$.

Handling sparse groups

Theorem (LO–Wang–Wood)

If $G = C_2 \times C_2$ *or* C_4,

Handling sparse groups

Theorem (LO–Wang–Wood)

If $G = C_2 \times C_2$ or C_4, then there is a $\delta > 0$ s.t.

$$\sum_{K \in \mathcal{F}_G(X)} |\mathrm{Cl}_K[3]| = O(X^{1-\delta}).$$

Handling sparse groups

Theorem (LO–Wang–Wood)

If $G = C_2 \times C_2$ or C_4, then there is a $\delta > 0$ s.t.

$$\sum_{K \in \mathcal{F}_G(X)} |\mathrm{Cl}_K[3]| = O(X^{1-\delta}).$$

Idea:

- Technical result $\Rightarrow$ assume quadratic subfield F is very small

Handling sparse groups

Theorem (LO–Wang–Wood)

If $G = C_2 \times C_2$ or C_4, then there is a $\delta > 0$ s.t.

$$\sum_{K \in \mathcal{F}_G(X)} |\mathrm{Cl}_K[3]| = O(X^{1-\delta}).$$

Idea:

- Technical result $\Rightarrow$ assume quadratic subfield F is very small
- $\Rightarrow$ F has many small primes

Handling sparse groups

Theorem (LO–Wang–Wood)

If $G = C_2 \times C_2$ or C_4, then there is a $\delta > 0$ s.t.

$$\sum_{K \in \mathcal{F}_G(X)} |\mathrm{Cl}_K[3]| = O(X^{1-\delta}).$$

Idea:

- Technical result $\Rightarrow$ assume quadratic subfield F is very small
- $\Rightarrow$ F has many small primes
- $\Rightarrow$ almost all K/F beat trivial $|\mathrm{Cl}_K[3]| \ll |\mathrm{Disc}(K)|^{1/2+\epsilon}$

Handling sparse groups

Theorem (LO–Wang–Wood)

If $G = C_2 \times C_2$ or C_4, then there is a $\delta > 0$ s.t.

$$\sum_{K \in \mathcal{F}_G(X)} |\mathrm{Cl}_K[3]| = O(X^{1-\delta}).$$

Idea:

- Technical result $\Rightarrow$ assume quadratic subfield F is very small
- $\Rightarrow$ F has many small primes
- $\Rightarrow$ almost all K/F beat trivial $|\mathrm{Cl}_K[3]| \ll |\mathrm{Disc}(K)|^{1/2+\epsilon}$
- Then, combine with sparsity: $\#\mathcal{F}_G(X) \ll X^{1/2+\epsilon}$.

Piecing together quadratic subfields

Piecing together quadratic subfields

Theorem (Datskovsky–Wright)

If F is a number field, then

$$\sum_{\substack{[K:F]=2\\ |\mathrm{Disc}(K/F)|\leq x}} |\mathrm{Cl}_{K/F}[3]| \sim C_F x.$$

Piecing together quadratic subfields

Theorem (Datskovsky–Wright)

If F is a number field, then

$$\sum_{\substack{[K:F]=2 \\ |\mathrm{Disc}(K/F)| \leq x}} |\mathrm{Cl}_{K/F}[3]| \sim C_F x.$$

Finally, for $K \in \mathcal{F}_{D_4}(X)$:

- May assume $|\mathrm{Disc}(F)| \leq Y$ for any Y

Piecing together quadratic subfields

Theorem (Datskovsky–Wright)

If F is a number field, then

$$\sum_{\substack{[K:F]=2 \\ |\mathrm{Disc}(K/F)|\leq x}} |\mathrm{Cl}_{K/F}[3]| \sim C_F x.$$

Finally, for $K \in \mathcal{F}_{D_4}(X)$:

- May assume $|\mathrm{Disc}(F)| \leq Y$ for any Y
- Datskovsky–Wright handles $\mathrm{Cl}_{K/F}$ for any finite set of F

Piecing together quadratic subfields

Theorem (Datskovsky–Wright)

If F is a number field, then

$$\sum_{\substack{[K:F]=2 \\ |\mathrm{Disc}(K/F)|\leq x}} |\mathrm{Cl}_{K/F}[3]| \sim C_F x.$$

Finally, for $K \in \mathcal{F}_{D_4}(X)$:

- May assume $|\mathrm{Disc}(F)| \leq Y$ for any Y
- Datskovsky–Wright handles $\mathrm{Cl}_{K/F}$ for any finite set of F
- Letting $Y \to \infty$ sufficiently slowly $\Rightarrow \mathrm{Avg}_{\mathcal{F}_{D_4}}(|\mathrm{Cl}_K[3]|)$ exists.

The general case

Induction yields:

The general case

Induction yields:

Theorem (LO–Wang–Wood)

Let $G \subseteq S_{2^m}$ be a transitive 2-group.

- *If G has a transposition, then $\mathrm{Avg}_{\mathcal{F}_G}(|\mathrm{Cl}_K[3]|)$ exists.*

The general case

Induction yields:

Theorem (LO–Wang–Wood)

Let $G \subseteq S_{2^m}$ be a transitive 2-group.

- *If G has a transposition, then $\mathrm{Avg}_{\mathcal{F}_G}(|\mathrm{Cl}_K[3]|)$ exists.*
- *If G does not have a transposition, then*

$$\sum_{K \in \mathcal{F}_G(X)} |\mathrm{Cl}_K[3]| = O(X^{1-\delta_G})$$

  for a positive constant δ_G.

The general case

Induction yields:

Theorem (LO–Wang–Wood)

Let $G \subseteq S_{2^m}$ be a transitive 2-group.

- *If G has a transposition, then $\mathrm{Avg}_{\mathcal{F}_G}(|\mathrm{Cl}_K[3]|)$ exists.*
- *If G does not have a transposition, then*

$$\sum_{K \in \mathcal{F}_G(X)} |\mathrm{Cl}_K[3]| = O(X^{1-\delta_G})$$

for a positive constant δ_G.

Thank you!