May 20th, 4:00 PM - 5:00 PM

An effective Chebotarev density theorem for families of fields, with an application to class groups

Caroline Turnage-Butterbaugh
Carleton College, cturnageb@carleton.edu

A Chebotarev density theorem for families of fields, with an application to class groups

Caroline Turnage-Butterbaugh
Carleton College

(Joint work with Lillian Pierce and Melanie Matchett Wood)

NSF-CBMS Conference
L-functions and Multiplicative Number Theory
University of Mississippi
May 20, 2019

Binary Quadratic Forms

$$(a, b, c) := ax^2 + bxy + cy^2, \qquad a, b, c \text{ integers.}$$

Binary Quadratic Forms

$$(a, b, c) := ax^2 + bxy + cy^2, \qquad a, b, c \text{ integers.}$$

Gauss

- classified the binary quadratic forms with a given discriminant $D := b^2 - 4ac$;

Binary Quadratic Forms

$$(a, b, c) := ax^2 + bxy + cy^2, \qquad a, b, c \text{ integers.}$$

Gauss

- classified the binary quadratic forms with a given discriminant $D := b^2 - 4ac$;
- formed the *class group*, the group of equivalence classes of binary quadratic forms of a given D with group action Gauss composition;

Binary Quadratic Forms

$$(a, b, c) := ax^2 + bxy + cy^2, \qquad a, b, c \text{ integers.}$$

Gauss

- classified the binary quadratic forms with a given discriminant $D := b^2 - 4ac$;
- formed the *class group*, the group of equivalence classes of binary quadratic forms of a given D with group action Gauss composition;
- showed that, for any given discriminant D, there exist *only finitely* many equivalence classes of binary quadratic forms.

Quadratic forms and quadratic number fields

Let $K = \mathbb{Q}(\sqrt{D})$ be a quadratic number field. To each form

$$(a, b, c) := ax^2 + bxy + cy^2$$

with discriminant $D = b^2 - 4ac$, we may associate an ideal I of $\mathcal{O}_K$, where

$$I = \left\langle a, \frac{-b + \sqrt{D}}{2} \right\rangle.$$

Binary quadratic forms	$\longleftrightarrow$	**Nonzero ideals of** $\mathcal{O}_{\mathbb{Q}[\sqrt{D}]}$
$(a,b,c) := ax^2 + bxy + cy^2$		$I = \left\langle a, \frac{-b+\sqrt{D}}{2} \right\rangle$

Binary quadratic forms	$\longleftrightarrow$	**Nonzero ideals of** $\mathcal{O}_{\mathbb{Q}[\sqrt{D}]}$
$(a, b, c) := ax^2 + bxy + cy^2$		$I = \left\langle a, \frac{-b+\sqrt{D}}{2} \right\rangle$
equivalent binary quadratic forms	$\longleftrightarrow$	equivalent ideals
composition of equivalence classes of forms	$\longleftrightarrow$	multiplication of equivalence classes of ideals

Binary quadratic forms	$\longleftrightarrow$	**Nonzero ideals of** $\mathcal{O}_{\mathbb{Q}[\sqrt{D}]}$
$(a, b, c) := ax^2 + bxy + cy^2$		$I = \left\langle a, \frac{-b+\sqrt{D}}{2} \right\rangle$
equivalent binary quadratic forms	$\longleftrightarrow$	equivalent ideals
composition of equivalence classes of forms	$\longleftrightarrow$	multiplication of equivalence classes of ideals

$$\mathrm{Cl}_K := \text{ the ideal class group of } K = \mathbb{Q}(\sqrt{D})$$

$$h(K) = |\mathrm{Cl}_K| := \text{ the class number of } K = \mathbb{Q}(\sqrt{D})$$

Note: $h(K)$ is finite via the correspondence.

Class group of K, $[K : \mathbb{Q}] \geq 2$

The ideal class group of K is defined by

$$\mathrm{Cl}_K := J_K / P_K$$

- $J_K :=$ the group of fractional ideals of K
- $P_K :=$ the subgroup of principal ideals of K.

The class number of K is defined by

$$h(K) = |\mathrm{Cl}_K|.$$

Class group of K, $[K : \mathbb{Q}] \geq 2$

The ideal class group of K is defined by

$$\mathrm{Cl}_K := J_K / P_K$$

- $J_K :=$ the group of fractional ideals of K
- $P_K :=$ the subgroup of principal ideals of K.

The class number of K is defined by

$$h(K) = |\mathrm{Cl}_K|.$$

$$h(K) = 1 \iff \mathrm{Cl}_K = \{\mathrm{id}\}$$

Class group of K, $[K:\mathbb{Q}] \geq 2$

The ideal class group of K is defined by

$$\mathrm{Cl}_K := J_K / P_K$$

- $J_K :=$ the group of fractional ideals of K
- $P_K :=$ the subgroup of principal ideals of K.

The class number of K is defined by

$$h(K) = |\mathrm{Cl}_K|.$$

$$h(K) = 1 \iff \mathrm{Cl}_K = \{\mathrm{id}\} \iff \mathcal{O}_K \text{ is a PID}$$

CLASS GROUP OF K, $[K:\mathbb{Q}] \geq 2$

The ideal class group of K is defined by

$$\mathrm{Cl}_K := J_K/P_K$$

- $J_K :=$ the group of fractional ideals of K
- $P_K :=$ the subgroup of principal ideals of K.

The class number of K is defined by

$$h(K) = |\mathrm{Cl}_K|.$$

$$h(K) = 1 \iff \mathrm{Cl}_K = \{\mathrm{id}\} \iff \mathcal{O}_K \text{ is a PID } \iff \mathcal{O}_K \text{ is a UFD}$$

Class group of K, $[K:\mathbb{Q}] \geq 2$

The ideal class group of K is defined by

$$\mathrm{Cl}_K := J_K / P_K$$

- $J_K :=$ the group of fractional ideals of K
- $P_K :=$ the subgroup of principal ideals of K.

The class number of K is defined by

$$h(K) = |\mathrm{Cl}_K|.$$

$$h(K) = 1 \iff \mathrm{Cl}_K = \{\mathrm{id}\} \iff \mathcal{O}_K \text{ is a PID } \iff \mathcal{O}_K \text{ is a UFD}$$

Question: How big is $|\mathrm{Cl}_K|$ in general?

Landau observed that if $[K : \mathbb{Q}] = n$, then

$$|\mathrm{Cl}_K| \ll_n D_K^{1/2+\varepsilon}$$

We may conclude that Cl_K is a finite abelian group.

Landau observed that if $[K:\mathbb{Q}] = n$, then

$$|\mathrm{Cl}_K| \ll_n D_K^{1/2+\varepsilon}$$

We may conclude that Cl_K is a finite abelian group.

For any integer $\ell > 1$, the ℓ-**torsion subgroup** of Cl_K is given by

$$\mathrm{Cl}_K[\ell] := \left\{[\mathfrak{a}] \in \mathrm{Cl}_K : [\mathfrak{a}]^\ell = \mathrm{Id}\right\}$$

Landau observed that if $[K : \mathbb{Q}] = n$, then

$$|\mathrm{Cl}_K| \ll_n D_K^{1/2+\varepsilon}$$

We may conclude that Cl_K is a finite abelian group.

For any integer $\ell > 1$, the ℓ**-torsion subgroup** of Cl_K is given by

$$\mathrm{Cl}_K[\ell] := \left\{ [\mathfrak{a}] \in \mathrm{Cl}_K : [\mathfrak{a}]^\ell = \mathrm{Id} \right\}$$

Natural Question: What is the size of $\mathrm{Cl}_K[\ell]$ as K varies within a family of fields of fixed degree?

How big is $|\mathrm{Cl}_K[\ell]|$?

Trivial Bound – For $[K:\mathbb{Q}] = n$, any integer $\ell \geq 1$, and $\varepsilon > 0$

$$|\mathrm{Cl}_K[\ell]| \leq |\mathrm{Cl}_K| \ll_{n,\varepsilon} D_K^{1/2+\varepsilon}$$

How big is $|\mathrm{Cl}_K[\ell]|$?

Trivial Bound – For $[K:\mathbb{Q}] = n$, any integer $\ell \geq 1$, and $\varepsilon > 0$

$$|\mathrm{Cl}_K[\ell]| \leq |\mathrm{Cl}_K| \ll_{n,\varepsilon} D_K^{1/2+\varepsilon}$$

Conjecture – For $[K:\mathbb{Q}] = n$, any integer $\ell \geq 1$, and $\varepsilon > 0$

$$|\mathrm{Cl}_K[\ell]| \ll_{n,\ell,\varepsilon} D_K^{\varepsilon}.$$

How big is $|\mathrm{Cl}_K[\ell]|$?

Trivial Bound – For $[K:\mathbb{Q}] = n$, any integer $\ell \geq 1$, and $\varepsilon > 0$

$$|\mathrm{Cl}_K[\ell]| \leq |\mathrm{Cl}_K| \ll_{n,\varepsilon} D_K^{1/2+\varepsilon}$$

Conjecture – For $[K:\mathbb{Q}] = n$, any integer $\ell \geq 1$, and $\varepsilon > 0$

$$|\mathrm{Cl}_K[\ell]| \ll_{n,\ell,\varepsilon} D_K^{\varepsilon}.$$

Recorded by

- Brumer-Silverman, ’96
- Duke, ’98
- Zhang, ’05
- Ellenberg-Venkatesh, ’07

HOW BIG IS $|\mathrm{Cl}_K[\ell]|$?

Trivial Bound – For $[K:\mathbb{Q}] = n$, any integer $\ell \geq 1$, and $\varepsilon > 0$

$$|\mathrm{Cl}_K[\ell]| \leq |\mathrm{Cl}_K| \ll_{n,\varepsilon} D_K^{1/2+\varepsilon}$$

Conjecture – For $[K:\mathbb{Q}] = n$, any integer $\ell \geq 1$, and $\varepsilon > 0$

$$|\mathrm{Cl}_K[\ell]| \ll_{n,\ell,\varepsilon} D_K^{\varepsilon}.$$

Recorded by

- Brumer-Silverman, '96
- Duke, '98
- Zhang, '05
- Ellenberg-Venkatesh, '07

Implied by

- Cohen-Lenstra-Martinet heuristics on the distribution of class groups and ℓ-torsion subgroups within families

What do we know is true?

Conjecture – For $[K:\mathbb{Q}] = n$, any integer $\ell \geq 1$, and $\varepsilon > 0$

$$|\mathrm{Cl}_K[\ell]| \ll_{n,\ell,\varepsilon} D_K^{\varepsilon}.$$

What do we know is true?

Conjecture – For $[K:\mathbb{Q}] = n$, any integer $\ell \geq 1$, and $\varepsilon > 0$

$$|\mathrm{Cl}_K[\ell]| \ll_{n,\ell,\varepsilon} D_K^{\varepsilon}.$$

Theorem (Gauss)

For all quadratic fields K, we have $|\mathrm{Cl}_K[2]| \ll_{\varepsilon} D_K^{\varepsilon}$.

What do we know is true?

Conjecture – For $[K:\mathbb{Q}] = n$, any integer $\ell \geq 1$, and $\varepsilon > 0$

$$|\mathrm{Cl}_K[\ell]| \ll_{n,\ell,\varepsilon} D_K^{\varepsilon}.$$

Theorem (Gauss)

For all quadratic fields K, we have $|\mathrm{Cl}_K[2]| \ll_{\varepsilon} D_K^{\varepsilon}$.

- This is the only case (for ℓ prime) in which the conjecture has been proved.

What do we know is true?

Conjecture – For $[K:\mathbb{Q}] = n$, any integer $\ell \geq 1$, and $\varepsilon > 0$

$$|\mathrm{Cl}_K[\ell]| \ll_{n,\ell,\varepsilon} D_K^{\varepsilon}.$$

Theorem (Gauss)

For all quadratic fields K, we have $|\mathrm{Cl}_K[2]| \ll_{\varepsilon} D_K^{\varepsilon}$.

- This is the only case (for ℓ prime) in which the conjecture has been proved.
- **Question:** Are there cases for which nontrivial bounds known?

Nontrivial bounds on $|\mathrm{Cl}_K[\ell]|$

Theorem (Ellenberg & Venkatesh, 2007)

Let $K/\mathbb{Q}$ be a number field of degree 2 or 3. We have

$$|\mathrm{Cl}_K[3]| \ll_{n,\varepsilon} D_K^{\frac{1}{3}+\varepsilon}.$$

Nontrivial bounds on $|\mathrm{Cl}_K[\ell]|$

Theorem (Ellenberg & Venkatesh, 2007)

Let $K/\mathbb{Q}$ be a number field of degree 2 or 3. We have

$$|\mathrm{Cl}_K[3]| \ll_{n,\varepsilon} D_K^{\frac{1}{3}+\varepsilon}.$$

Let $K/\mathbb{Q}$ be a non-D_4 number field of degree 4. We have

$$|\mathrm{Cl}_K[3]| \ll_{\varepsilon} D_K^{\frac{1}{2}-\frac{1}{168}+\varepsilon}.$$

Nontrivial bounds on $|\mathrm{Cl}_K[\ell]|$

Theorem (Ellenberg & Venkatesh, 2007)

Let $K/\mathbb{Q}$ be a number field of degree 2 or 3. We have

$$|\mathrm{Cl}_K[3]| \ll_{n,\varepsilon} D_K^{\frac{1}{3}+\varepsilon}.$$

Let $K/\mathbb{Q}$ be a non-D_4 number field of degree 4. We have

$$|\mathrm{Cl}_K[3]| \ll_{\varepsilon} D_K^{\frac{1}{2}-\frac{1}{168}+\varepsilon}.$$

Theorem (Bhargava, Shankar, Taniguchi, Thorne, Tsimerman & Zhao, 2017)

Let $K/\mathbb{Q}$ be a number field of degree $n > 2$. For some $\delta_n > 0$ we have

$$|\mathrm{Cl}_K[2]| \ll_{n,\varepsilon} D_K^{\frac{1}{2}-\delta_n+\varepsilon}.$$

NONTRIVIAL BOUNDS ON $|\mathrm{Cl}_K[\ell]|$ ... UNDER GRH

Theorem (Ellenberg & Venkatesh, 2007)

Let $K/\mathbb{Q}$ be a number field of degree n and ℓ a positive integer. Assuming GRH, we have

$$|\mathrm{Cl}_K[\ell]| \ll_{n,\ell,\varepsilon} D_K^{\frac{1}{2}-\frac{1}{2\ell(n-1)}+\varepsilon}.$$

NONTRIVIAL BOUNDS ON $|\mathrm{Cl}_K[\ell]|$ . . . UNDER GRH

Theorem (Ellenberg & Venkatesh, 2007)

Let $K/\mathbb{Q}$ be a number field of degree n and ℓ a positive integer. Assuming GRH, we have

$$|\mathrm{Cl}_K[\ell]| \ll_{n,\ell,\varepsilon} D_K^{\frac{1}{2}-\frac{1}{2\ell(n-1)}+\varepsilon}.$$

- **Question:** What can we say unconditionally for all but a possible exceptional set of fields K within a family?

Nontrivial bounds on $|\mathrm{Cl}_K[\ell]|$ ... in families

Theorem (Soundararajan, 2000)

Let ℓ be prime. For all but a possible zero-density exceptional family of imaginary quadratic fields $K/\mathbb{Q}$, we have

$$|\mathrm{Cl}_K[\ell]| \ll_{\ell,\varepsilon} D_K^{\frac{1}{2}-\frac{1}{2\ell}+\varepsilon}.$$

Nontrivial bounds on $|\mathrm{Cl}_K[\ell]|$ ... in families

Theorem (Soundararajan, 2000)

Let ℓ be prime. For all but a possible zero-density exceptional family of imaginary quadratic fields $K/\mathbb{Q}$, we have

$$|\mathrm{Cl}_K[\ell]| \ll_{\ell,\varepsilon} D_K^{\frac{1}{2}-\frac{1}{2\ell}+\varepsilon}.$$

Theorem (Heath-Brown & Pierce, 2014)

Let $\ell \geq 5$ be prime. For all but a possible zero-density exceptional family of imaginary quadratic fields $K/\mathbb{Q}$, we have

$$|\mathrm{Cl}_K[\ell]| \ll_{\ell,\varepsilon} D_K^{\frac{1}{2}-\frac{3}{2\ell+2}+\varepsilon}.$$

NONTRIVIAL BOUNDS ON $|\mathrm{Cl}_K[\ell]|$ ... IN FAMILIES

Theorem (Ellenberg, Pierce, & Wood, 2016)

Let $\ell \geq 1$, and let $[K : Q] = 2, 3$ or 5. For all but a possible zero-density exceptional family of fields $K/\mathbb{Q}$, we have

$$|\mathrm{Cl}_K[\ell]| \ll_{n,\ell,\varepsilon} D_K^{\frac{1}{2} - \frac{1}{2\ell(n-1)} + \varepsilon}.$$

If $[K : \mathbb{Q}] = 4$, then the same bound applies for K non-D_4.

Nontrivial bounds on $|\mathrm{Cl}_K[\ell]|$ . . . in families

Theorem (Ellenberg, Pierce, & Wood, 2016)

Let $\ell \geq 1$, and let $[K : Q] = 2, 3$ or 5. For all but a possible zero-density exceptional family of fields $K/\mathbb{Q}$, we have

$$|\mathrm{Cl}_K[\ell]| \ll_{n,\ell,\varepsilon} D_K^{\frac{1}{2} - \frac{1}{2\ell(n-1)} + \varepsilon}.$$

If $[K : \mathbb{Q}] = 4$, then the same bound applies for K non-D_4.

- Note that the bound is as strong as on GRH.

NONTRIVIAL BOUNDS ON $|\mathrm{Cl}_K[\ell]|$ ... IN FAMILIES

Theorem (Ellenberg, Pierce, & Wood, 2016)

Let $\ell \geq 1$, and let $[K : Q] = 2, 3$ or 5. For all but a possible zero-density exceptional family of fields $K/\mathbb{Q}$, we have

$$|\mathrm{Cl}_K[\ell]| \ll_{n,\ell,\varepsilon} D_K^{\frac{1}{2} - \frac{1}{2\ell(n-1)} + \varepsilon}.$$

If $[K : \mathbb{Q}] = 4$, then the same bound applies for K non-D_4.

- Note that the bound is as strong as on GRH.

Pierce, T., and Wood, (2017 preprint)
Under certain conditions (but never under GRH), we extend this result to different families in which $[K : \mathbb{Q}] \geq 2$.

Starting point

Theorem (Ellenberg & Venkatesh, 2007)

Suppose that there are M rational primes

$$p_1, p_2, \ldots, p_M$$

that split completely in K, where $p_j \leq D_K^{\delta}$ *and* $\delta < \frac{1}{2\ell(n-1)}$. *Then for any* $\varepsilon > 0$,

$$|\mathrm{Cl}_K[\ell]| \ll_{n,\ell,\varepsilon} D_K^{\frac{1}{2}+\varepsilon} M^{-1}.$$

Starting point

Theorem (Ellenberg & Venkatesh, 2007)

Suppose that there are M rational primes

$$p_1, p_2, \ldots, p_M$$

that split completely in K, where $p_j \leq D_K^{\delta}$ and $\delta < \frac{1}{2\ell(n-1)}$. Then for any $\varepsilon > 0$,

$$|\mathrm{Cl}_K[\ell]| \ll_{n,\ell,\varepsilon} D_K^{\frac{1}{2}+\varepsilon} M^{-1}.$$

Starting point

Theorem (Ellenberg & Venkatesh, 2007)

Suppose that there are M rational primes

$$p_1, p_2, \ldots, p_M$$

that split completely in K, where $p_j \le D_K^{\delta}$ *and* $\delta < \frac{1}{2\ell(n-1)}$*. Then for any* $\varepsilon > 0$*,*

$$|\mathrm{Cl}_K[\ell]| \ll_{n,\ell,\varepsilon} D_K^{\frac{1}{2}+\varepsilon} M^{-1}.$$

Question: How might one go about finding small primes that split completely in K?

Starting point

Theorem (Ellenberg & Venkatesh, 2007)

Suppose that there are M rational primes

$$p_1, p_2, \ldots, p_M$$

that split completely in K, where $p_j \leq D_K^{\delta}$ and $\delta < \frac{1}{2\ell(n-1)}$. Then for any $\varepsilon > 0$,

$$|\mathrm{Cl}_K[\ell]| \ll_{n,\ell,\varepsilon} D_K^{\frac{1}{2}+\varepsilon} M^{-1}.$$

Question: How might one go about finding small primes that split completely in K?

Answer: via a Chebotarev Density Theorem

An Effective Chebotarev Density Theorem

$$K \;\Big|\; n \quad \mathrm{Gal}(K/\mathbb{Q}) \cong G \;\Big|\; \mathbb{Q}$$

Theorem (Lagarias-Odlyzko*, 1975)

If GRH holds for $\zeta_K(s)$, then

$$\left| \#\{p \le x \text{ that split completely in } K\} - \frac{\mathrm{Li}(x)}{|G|} \right| \le \frac{C_0}{|G|} x^{1/2} \log(D_K x^{n_K})$$

for every $x \geq 2$ and C_0 is effectively computable.

An Effective Chebotarev Density Theorem

$$K \quad \Big| \; n \quad \mathrm{Gal}(K/\mathbb{Q}) \cong G \quad \mathbb{Q}$$

Theorem (Lagarias-Odlyzko*, 1975)

If GRH holds for $\zeta_K(s)$, then

$$\left| \#\{p \le x \text{ that split completely in } K\} - \frac{\mathrm{Li}(x)}{|G|} \right| \le \frac{C_0}{|G|} x^{1/2} \log(D_K x^{n_K})$$

for every $x \ge 2$ and C_0 is effectively computable.

**This is a special case of their theorem.*

An Effective Chebotarev Density Theorem

$$K \overset{n}{\Big|}\, \mathbb{Q} \quad \mathrm{Gal}(K/\mathbb{Q}) \cong G$$

Theorem (Lagarias-Odlyzko*, 1975)

If GRH holds for $\zeta_K(s)$, then

$$\left| \#\{p \le x \text{ that split completely in } K\} - \frac{\mathrm{Li}(x)}{|G|} \right| \le \frac{C_0}{|G|} x^{1/2} \log(D_K x^{n_K})$$

for every $x \ge 2$ and C_0 is effectively computable.

**This is a special case of their theorem.*

An Effective Chebotarev Density Theorem

$$\begin{array}{c} K \\ n \Big| \Big) \mathrm{Gal}(K/\mathbb{Q}) \cong G \\ \mathbb{Q} \end{array}$$

Theorem (Lagarias-Odlyzko*, 1975)

If GRH holds for $\zeta_K(s)$, then

$$\left| \#\{p \leq x \text{ that split completely in } K\} - \frac{\mathrm{Li}(x)}{|G|} \right| \leq \frac{C_0}{|G|} x^{1/2} \log(D_K x^{n_K})$$

for every $x \geq 2$ and C_0 is effectively computable.

**This is a special case of their theorem.*

- We may take $x = D_K^{\delta - \epsilon_0}$, with $\delta = \dfrac{1}{2\ell(n-1)}$.

An Effective Chebotarev Density Theorem

$$\begin{array}{c} K \\ n \Big| \Big) \mathrm{Gal}(K/\mathbb{Q}) \cong G \\ \mathbb{Q} \end{array}$$

Theorem (Lagarias-Odlyzko*, 1975)

If GRH holds for $\zeta_K(s)$, then

$$\left| \#\{p \le x \text{ that split completely in } K\} - \frac{\mathrm{Li}(x)}{|G|} \right| \le \frac{C_0}{|G|} x^{1/2} \log(D_K x^{n_K})$$

for every $x \ge 2$ and C_0 is effectively computable.

**This is a special case of their theorem.*

- We may take $x = D_K^{\delta - \epsilon_0}$, with $\delta = \dfrac{1}{2\ell(n-1)}$.
- Obtain at least $M \gg D_K^{1/(2\ell(n-1)) - \varepsilon_0}$ sufficiently small primes that split completely in K.

BOUNDING ℓ-TORSION ASSUMING GRH

Ellenberg-Venkatesh (2007)

$$|\mathrm{Cl}_K[\ell]| \quad \ll_{\ell,n,\varepsilon} \quad D_K^{\frac{1}{2}+\varepsilon} M^{-1}$$

Bounding ℓ-torsion assuming GRH

Ellenberg-Venkatesh (2007)

$$|\mathrm{Cl}_K[\ell]| \quad \ll_{\ell,n,\varepsilon} \quad D_K^{\frac{1}{2}+\varepsilon} M^{-1}$$

↓

Lagarias-Odlyzko (1975)

Conditional Effective Chebotarev Density Theorem

$$M \quad \gg \quad D_K^{1/(2\ell(n-1))-\varepsilon_0}$$

Bounding ℓ-torsion assuming GRH

Ellenberg-Venkatesh (2007)

$$|\mathrm{Cl}_K[\ell]| \quad \ll_{\ell,n,\varepsilon} \quad D_K^{\frac{1}{2}+\varepsilon} M^{-1}$$

↓

Lagarias-Odlyzko (1975)

Conditional Effective Chebotarev Density Theorem

$$M \quad \gg \quad D_K^{1/(2\ell(n-1))-\varepsilon_0}$$

↓

Ellenberg-Venkatesh (2007)

Assuming GRH, we have $|\mathrm{Cl}_K[\ell]| \ll_{\ell,n,\varepsilon} D_K^{\frac{1}{2}-\frac{1}{2\ell(n-1)}+\varepsilon}$

Bounding ℓ-torsion assuming GRH

Ellenberg-Venkatesh (2007)

$$|\mathrm{Cl}_K[\ell]| \quad \ll_{\ell,n,\varepsilon} \quad D_K^{\frac{1}{2}+\varepsilon} M^{-1}$$

↓

Lagarias-Odlyzko (1975)

Conditional Effective Chebotarev Density Theorem

$$M \quad \gg \quad D_K^{1/(2\ell(n-1))-\varepsilon_0}$$

↓

Ellenberg-Venkatesh (2007)

Assuming GRH, we have $|\mathrm{Cl}_K[\ell]| \ll_{\ell,n,\varepsilon} D_K^{\frac{1}{2}-\frac{1}{2\ell(n-1)}+\varepsilon}$

Goal: Remove GRH and obtain the same ℓ-torsion bound.

Bounding ℓ-torsion assuming GRH

Ellenberg-Venkatesh (2007)

$$|\mathrm{Cl}_K[\ell]| \quad \ll_{\ell,n,\varepsilon} \quad D_K^{\frac{1}{2}+\varepsilon} M^{-1}$$

↓

Lagarias-Odlyzko (1975)

Conditional Effective Chebotarev Density Theorem

$$M \quad \gg \quad D_K^{1/(2\ell(n-1))-\varepsilon_0}$$

↓

Ellenberg-Venkatesh (2007)

Assuming GRH, we have $|\mathrm{Cl}_K[\ell]| \ll_{\ell,n,\varepsilon} D_K^{\frac{1}{2}-\frac{1}{2\ell(n-1)}+\varepsilon}$

Goal: Remove GRH and obtain the same ℓ-torsion bound.

– We can do this at the cost of proving the result for all but a possible zero-density family of fields.

Same starting point as before

Theorem (Ellenberg & Venkatesh, 2007)

Suppose that there are M rational primes

$$p_1, p_2, \ldots, p_M$$

that split completely in K, where $p_j \leq D_K^{\delta}$ *and* $\delta < \frac{1}{2\ell(n-1)}$. *Then for any* $\varepsilon > 0$*,*

$$|\mathrm{Cl}_K[\ell]| \ll_{n,\ell,\varepsilon} D_K^{\frac{1}{2}+\varepsilon} M^{-1}.$$

Same starting point as before

Theorem (Ellenberg & Venkatesh, 2007)

Suppose that there are M rational primes

$$p_1, p_2, \ldots, p_M$$

that split completely in K, where $p_j \leq D_K^{\delta}$ *and* $\delta < \frac{1}{2\ell(n-1)}$. *Then for any* $\varepsilon > 0$,

$$|\mathrm{Cl}_K[\ell]| \ll_{n,\ell,\varepsilon} D_K^{\frac{1}{2}+\varepsilon} M^{-1}.$$

We need an effective Chebotarev density theorem for a family of fields K

- that does not assume GRH, and

SAME STARTING POINT AS BEFORE

Theorem (Ellenberg & Venkatesh, 2007)

Suppose that there are M rational primes

$$p_1, p_2, \dots, p_M$$

that split completely in K, where $p_j \leq D_K^{\delta}$ *and* $\delta < \frac{1}{2\ell(n-1)}$. *Then for any* $\varepsilon > 0$,

$$|\mathrm{Cl}_K[\ell]| \ll_{n,\ell,\varepsilon} D_K^{\frac{1}{2}+\varepsilon} M^{-1}.$$

We need an effective Chebotarev density theorem for a family of fields K

- that does not assume GRH, and
- has a low threshold on x.

Same starting point as before

Theorem (Ellenberg & Venkatesh, 2007)

Suppose that there are M rational primes

$$p_1, p_2, \ldots, p_M$$

that split completely in K, where $p_j \leq D_K^{\delta}$ *and* $\delta < \frac{1}{2\ell(n-1)}$. *Then for any* $\varepsilon > 0$,

$$|\mathrm{Cl}_K[\ell]| \ll_{n,\ell,\varepsilon} D_K^{\frac{1}{2}+\varepsilon} M^{-1}.$$

We need an effective Chebotarev density theorem for a family of fields K

- that does not assume GRH, and
- has a low threshold on x.

Let us first recall how to count primes.

Counting Primes

Motivating Question

Given a large number x, how many primes are there less than or equal to x?

Counting Primes

Motivating Question

Given a large number x, how many primes are there less than or equal to x?

That is, if we let

$$\pi(x) := \sum_{p \leq x} 1,$$

Counting Primes

Motivating Question

Given a large number x, how many primes are there less than or equal to x?

That is, if we let

$$\pi(x) := \sum_{p \leq x} 1,$$

how does $\pi(x)$ behave as $x \to \infty$?

Prime Number Theorem (Hadamard, de la Vallée Poussin 1896)

$$\pi(x) \sim \mathrm{Li}(x), \qquad x \to \infty$$

Prime Number Theorem (Hadamard, de la Vallée Poussin 1896)

$$\pi(x) \sim \mathrm{Li}(x), \qquad x \to \infty$$

Count primes with a weight:

$$\psi(x) := \sum_{n \leq x} \Lambda(n),$$

Prime Number Theorem (Hadamard, de la Vallée Poussin 1896)

$$\pi(x) \sim \mathrm{Li}(x), \qquad x \to \infty$$

Count primes with a weight:

$$\psi(x) := \sum_{n \le x} \Lambda(n), \qquad \Lambda(n) = \begin{cases} \log p, & \text{if } n = p^k, k \ge 1, \\ 0, & \text{else.} \end{cases}$$

Prime Number Theorem (Hadamard, de la Vallée Poussin 1896)

$$\pi(x) \sim \mathrm{Li}(x), \qquad x \to \infty$$

Count primes with a weight:

$$\psi(x) := \sum_{n \leq x} \Lambda(n), \qquad \Lambda(n) = \begin{cases} \log p, & \text{if } n = p^k, k \geq 1, \\ 0, & \text{else.} \end{cases}$$

Heuristic:

$$\psi(x) = \sum_{n \leq x} \Lambda(n)$$

Prime Number Theorem (Hadamard, de la Vallée Poussin 1896)

$$\pi(x) \sim \mathrm{Li}(x), \qquad x \to \infty$$

Count primes with a weight:

$$\psi(x) := \sum_{n \le x} \Lambda(n), \qquad \Lambda(n) = \begin{cases} \log p, & \text{if } n = p^k, k \ge 1, \\ 0, & \text{else.} \end{cases}$$

Heuristic:

$$\psi(x) = \sum_{n \le x} \Lambda(n) \approx \sum_{p \le x} \log p$$

Prime Number Theorem (Hadamard, de la Vallée Poussin 1896)

$$\pi(x) \sim \mathrm{Li}(x), \qquad x \to \infty$$

Count primes with a weight:

$$\psi(x) := \sum_{n \le x} \Lambda(n), \qquad \Lambda(n) = \begin{cases} \log p, & \text{if } n = p^k, k \ge 1, \\ 0, & \text{else.} \end{cases}$$

Heuristic:

$$\psi(x) = \sum_{n \le x} \Lambda(n) \approx \sum_{p \le x} \log p \approx \pi(x) \log x$$

Prime Number Theorem (Hadamard, de la Vallée Poussin 1896)

$$\pi(x) \sim \mathrm{Li}(x), \qquad x \to \infty$$

Count primes with a weight:

$$\psi(x) := \sum_{n \le x} \Lambda(n), \qquad \Lambda(n) = \begin{cases} \log p, & \text{if } n = p^k, k \ge 1, \\ 0, & \text{else.} \end{cases}$$

Heuristic:

$$\psi(x) = \sum_{n \le x} \Lambda(n) \approx \sum_{p \le x} \log p \approx \pi(x) \log x$$

$$\psi(x) \sim x \iff \pi(x) \sim \frac{x}{\log x}$$

PROVING $\psi(x) \sim x$

PROVING $\psi(x) \sim x$

Explicit Formula (truncated version)

We have

$$\psi(x) = x - \sum_{|\gamma| \leq x} \frac{x^\rho}{\rho} + O\left(\log^2 x\right)$$

where the sum is over the nontrivial zeros of $\zeta(s)$.

PROVING $\psi(x) \sim x$

Explicit Formula (truncated version)

We have

$$\psi(x) = x - \sum_{|\gamma| \le x} \frac{x^\rho}{\rho} + O\left(\log^2 x\right)$$

where the sum is over the nontrivial zeros of $\zeta(s)$.

$\rho = \beta + i\gamma$ is a nontrivial zero of $\zeta(s)$:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ prime}} \left(1 - \frac{1}{p^s}\right)^{-1}, \quad \Re(s) > 1$$

PROVING $\psi(x) \sim x$

Explicit Formula (truncated version)

We have

$$\psi(x) = x - \sum_{|\gamma| \le x} \frac{x^\rho}{\rho} + O\left(\log^2 x\right)$$

where the sum is over the nontrivial zeros of $\zeta(s)$.

$\rho = \beta + i\gamma$ is a nontrivial zero of $\zeta(s)$:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ prime}} \left(1 - \frac{1}{p^s}\right)^{-1}, \quad \Re(s) > 1$$

- Since $|x^\rho| = x^\beta$, if $\beta < 1$, then the contribution from the nontrivial zeros is not too big.

PROVING $\psi(x) \sim x$

Explicit Formula (truncated version)

We have

$$\psi(x) = x - \sum_{|\gamma| \le x} \frac{x^\rho}{\rho} + O\left(\log^2 x\right)$$

where the sum is over the nontrivial zeros of $\zeta(s)$.

$\rho = \beta + i\gamma$ is a nontrivial zero of $\zeta(s)$:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ prime}} \left(1 - \frac{1}{p^s}\right)^{-1}, \quad \Re(s) > 1$$

- Since $|x^\rho| = x^\beta$, if $\beta < 1$, then the contribution from the nontrivial zeros is not too big.
- Key to proof of the Prime Number Theorem:

$$\zeta(s) \neq 0 \text{ for } \Re(s) = 1$$

Counting primes in arithmetic progressions

Siegel-Walfisz Theorem (1935)

If $n \geq 2$ and a is coprime to q then as $x \to \infty$,

$$\pi(x; a, q) := \sum_{\substack{p \leq x \\ p \equiv a \pmod{q}}} 1 = \frac{1}{\varphi(q)} \mathrm{Li}(x) + \text{"error term"}.$$

Counting primes in arithmetic progressions

Siegel-Walfisz Theorem (1935)

If $n \geq 2$ and a is coprime to q then as $x \to \infty$,

$$\pi(x; a, q) := \sum_{\substack{p \leq x \\ p \equiv a \pmod{q}}} 1 = \frac{1}{\varphi(q)} \mathrm{Li}(x) + \text{"error term"}.$$

- The error term depends on the zero-free region of the Dirichlet L-function:

$$L(s, \chi_q) := \sum_{n=1}^{\infty} \frac{\chi_q(n)}{n^s}, \quad \Re(s) > 1$$

Counting prime ideals in number fields

$$\begin{array}{ccc} \mathcal{O}_k & \quad & k \\ | & & | \\ \mathbb{Z} & & \mathbb{Q} \end{array}$$

Prime Ideal Theorem (Landau 1918)
As $x \to \infty$,

$$\pi(x; k) := \sum_{\substack{\mathfrak{p} \subset \mathcal{O}_k \\ \mathrm{Nm}_{k/\mathbb{Q}}\mathfrak{p} \leq x}} 1 \; = \; \mathrm{Li}(x) + \text{"error term"}.$$

Counting prime ideals in number fields

$$\begin{array}{ccc} \mathcal{O}_k & & k \\ | & & | \\ \mathbb{Z} & & \mathbb{Q} \end{array}$$

Prime Ideal Theorem (Landau 1918)
As $x \to \infty$,

$$\pi(x; k) := \sum_{\substack{\mathfrak{p} \subset \mathcal{O}_k \\ \mathrm{Nm}_{k/\mathbb{Q}}\mathfrak{p} \leq x}} 1 = \mathrm{Li}(x) + \text{"error term"}.$$

The error term depends on the zero-free region of the Dedekind zeta-function of k:

Counting prime ideals in number fields

$$\begin{array}{ccc} \mathcal{O}_k & & k \\ | & & | \\ \mathbb{Z} & & \mathbb{Q} \end{array}$$

Prime Ideal Theorem (Landau 1918)
As $x \to \infty$,

$$\pi(x; k) := \sum_{\substack{\mathfrak{p} \subset \mathcal{O}_k \\ \mathrm{Nm}_{k/\mathbb{Q}}\mathfrak{p} \leq x}} 1 \;=\; \mathrm{Li}(x) \,+\, \text{"error term"}.$$

The error term depends on the zero-free region of the Dedekind zeta-function of k:

$$\zeta_k(s) := \sum_{I \subset \mathcal{O}_k} \frac{1}{(\mathrm{Nm}_{k/\mathbb{Q}} I)^s} = \prod_{\mathfrak{p} \subset \mathcal{O}_k} \left(1 - \frac{1}{(\mathrm{Nm}_{k/\mathbb{Q}}\mathfrak{p})^s}\right)^{-1}, \quad \Re(s) > 1$$

Counting prime ideals in number fields

$$\begin{array}{ccc} \mathcal{O}_k & & k \\ | & & | \\ \mathbb{Z} & & \mathbb{Q} \end{array}$$

Prime Ideal Theorem (Landau 1918)
As $x \to \infty$,

$$\pi(x;k) := \sum_{\substack{\mathfrak{p} \subset \mathcal{O}_k \\ \mathrm{Nm}_{k/\mathbb{Q}}\mathfrak{p} \le x}} 1 = \mathrm{Li}(x) + \text{"error term"}.$$

The error term depends on the zero-free region of the Dedekind zeta-function of k:

$$\zeta_k(s) := \sum_{I \subset \mathcal{O}_k} \frac{1}{(\mathrm{Nm}_{k/\mathbb{Q}} I)^s} = \prod_{\mathfrak{p} \subset \mathcal{O}_k} \left(1 - \frac{1}{(\mathrm{Nm}_{k/\mathbb{Q}}\mathfrak{p})^s}\right)^{-1}, \quad \Re(s) > 1$$

Example 1: When $k = \mathbb{Q}$, we have $\zeta_k(s) = \zeta(s)$.

Counting prime ideals in number fields

$$\begin{array}{ccc} \mathcal{O}_k & & k \\ | & & | \\ \mathbb{Z} & & \mathbb{Q} \end{array}$$

Prime Ideal Theorem (Landau 1918)
As $x \to \infty$,

$$\pi(x; k) := \sum_{\substack{\mathfrak{p} \subset \mathcal{O}_k \\ \mathrm{Nm}_{k/\mathbb{Q}}\mathfrak{p} \leq x}} 1 \;=\; \mathrm{Li}(x) + \text{"error term"}.$$

The error term depends on the zero-free region of the Dedekind zeta-function of k:

$$\zeta_k(s) := \sum_{I \subset \mathcal{O}_k} \frac{1}{(\mathrm{Nm}_{k/\mathbb{Q}} I)^s} = \prod_{\mathfrak{p} \subset \mathcal{O}_k} \left(1 - \frac{1}{(\mathrm{Nm}_{k/\mathbb{Q}}\mathfrak{p})^s}\right)^{-1}, \quad \Re(s) > 1$$

Example 1: When $k = \mathbb{Q}$, we have $\zeta_k(s) = \zeta(s)$.
Example 2: When $k = \mathbb{Q}(\sqrt{q})$, one can show $\zeta_k(s) = \zeta(s)L(s, \chi_q)$.

Counting prime ideals in number fields

$$\begin{array}{c} \mathcal{O}_k \\ | \\ \mathbb{Z} \end{array} \qquad \begin{array}{c} k \\ | \\ \mathbb{Q} \end{array}$$

Prime Ideal Theorem (Landau 1918)
As $x \to \infty$,

$$\pi(x;k) := \sum_{\substack{\mathfrak{p} \subset \mathcal{O}_k \\ \mathrm{Nm}_{k/\mathbb{Q}}\mathfrak{p} \leq x}} 1 = \mathrm{Li}(x) + \text{"error term"}.$$

The error term depends on the zero-free region of the Dedekind zeta-function of k:

$$\zeta_k(s) := \sum_{I \subset \mathcal{O}_k} \frac{1}{(\mathrm{Nm}_{k/\mathbb{Q}} I)^s} = \prod_{\mathfrak{p} \subset \mathcal{O}_k} \left(1 - \frac{1}{(\mathrm{Nm}_{k/\mathbb{Q}}\mathfrak{p})^s}\right)^{-1}, \quad \Re(s) > 1$$

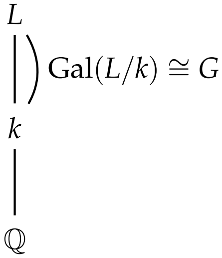
Generalized Riemann Hypothesis: Nontrivial zeros of $\zeta_K(s)$ have real part equal to $1/2$.

Counting prime ideals in conjugacy classes

Let L/k be a normal extension with Galois group $G = \mathrm{Gal}(L/k)$.

Counting prime ideals in conjugacy classes

Let L/k be a normal extension with Galois group $G = \mathrm{Gal}(L/k)$.



Counting prime ideals in conjugacy classes

Let L/k be a normal extension with Galois group $G = \mathrm{Gal}(L/k)$.

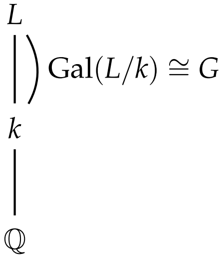
$$\pi_{\mathcal{C}}(x, L/k) := \#\left\{\mathfrak{p} \subset \mathcal{O}_k : \mathfrak{p} \text{ unramified in } L, \left[\frac{L/k}{\mathfrak{p}}\right] = \mathcal{C}, \mathrm{Nm}_{k/\mathbb{Q}}\mathfrak{p} \leq x\right\}$$

$$\begin{array}{l} L \\ \Big| \Big) \ \mathrm{Gal}(L/k) \cong G \\ k \\ \Big| \\ \mathbb{Q} \end{array}$$

Counting prime ideals in conjugacy classes

Let L/k be a normal extension with Galois group $G = \mathrm{Gal}(L/k)$.

$$\pi_{\mathcal{C}}(x, L/k) := \#\left\{\mathfrak{p} \subset \mathcal{O}_k : \mathfrak{p} \text{ unramified in } L, \left[\frac{L/k}{\mathfrak{p}}\right] = \mathcal{C}, \mathrm{Nm}_{k/\mathbb{Q}}\mathfrak{p} \le x\right\}$$



- $\mathfrak{p}$ is a prime ideal in $\mathcal{O}_k$ which is unramified in L.

Counting prime ideals in conjugacy classes

Let L/k be a normal extension with Galois group $G = \mathrm{Gal}(L/k)$.

$$\pi_{\mathcal{C}}(x, L/k) := \#\left\{\mathfrak{p} \subset \mathcal{O}_k : \mathfrak{p} \text{ unramified in } L, \left[\frac{L/k}{\mathfrak{p}}\right] = \mathcal{C}, \mathrm{Nm}_{k/\mathbb{Q}}\mathfrak{p} \leq x\right\}$$

L

$\big|\big)\ \mathrm{Gal}(L/k) \cong G$

k

$\big|$

$\mathbb{Q}$

- $\mathfrak{p}$ is a prime ideal in $\mathcal{O}_k$ which is unramified in L.
- $\left[\frac{L/k}{\mathfrak{p}}\right]$ is the Artin symbol, which denotes the fixed, targeted conjugacy class $\mathcal{C}$ within G.

Counting prime ideals in conjugacy classes

Chebotarev Density Theorem (1922)

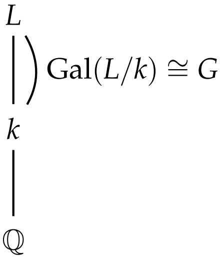
$$\pi_{\mathcal{C}}(x; L/k) \sim \frac{|\mathcal{C}|}{|G|}\mathrm{Li}(x), \quad x \to \infty$$

$$\begin{array}{c} L \\ \Big| \; \Big) \, \mathrm{Gal}(L/k) \cong G \\ k \\ \Big| \\ \mathbb{Q} \end{array}$$

Counting prime ideals in conjugacy classes

Effective **Chebotarev Density Theorem**

(Lagarias & Odlyzko 1975)

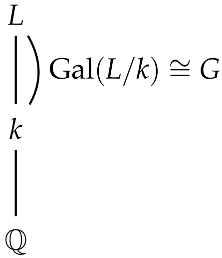


Counting prime ideals in conjugacy classes

Effective **Chebotarev Density Theorem**
(Lagarias & Odlyzko 1975)

$$\pi_{\mathcal{C}}(x; L/k) = \frac{|\mathcal{C}|}{|G|}\mathrm{Li}(x) + \text{"error term"}, \quad x \to \infty$$

The error term depends on the zero-free region of the Dedekind zeta-function of L.



COUNTING PRIME IDEALS IN CONJUGACY CLASSES

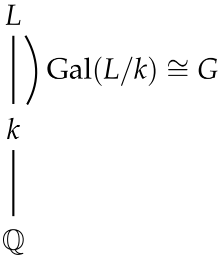
Effective **Chebotarev Density Theorem**

(Lagarias & Odlyzko 1975)

$$\pi_{\mathcal{C}}(x; L/k) = \frac{|\mathcal{C}|}{|G|}\mathrm{Li}(x) + \text{"error term"}, \quad x \to \infty$$

The error term depends on the zero-free region of the Dedekind zeta-function of L.

$$\zeta_L(s) := \zeta_k(s) \prod_{\substack{\rho \in \hat{G} \\ \rho \neq \rho_0}} L(s, \rho, L/k)^{\dim \rho}$$



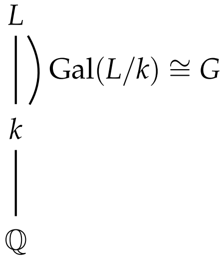
Counting prime ideals in conjugacy classes

Effective **Chebotarev Density Theorem**
(Lagarias & Odlyzko 1975)

$$\pi_{\mathcal{C}}(x; L/k) = \frac{|\mathcal{C}|}{|G|}\mathrm{Li}(x) + \text{"error term"}, \quad x \to \infty$$

The error term depends on the zero-free region of the Dedekind zeta-function of L.

$$\zeta_L(s) := \zeta_k(s) \prod_{\substack{\rho \in \hat{G} \\ \rho \neq \rho_0}} L(s, \rho, L/k)^{\dim \rho}$$



- Each $L(s, \rho, L/k)$ is an Artin L-function.

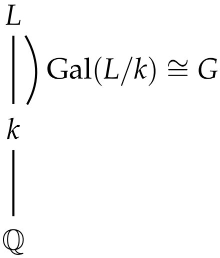
Counting prime ideals in conjugacy classes

Effective **Chebotarev Density Theorem**
(Lagarias & Odlyzko 1975)

$$\pi_{\mathcal{C}}(x; L/k) = \frac{|\mathcal{C}|}{|G|}\mathrm{Li}(x) + \text{"error term"}, \quad x \to \infty$$

The error term depends on the zero-free region of the Dedekind zeta-function of L.

$$\zeta_L(s) := \zeta_k(s) \prod_{\substack{\rho \in \hat{G} \\ \rho \neq \rho_0}} L(s, \rho, L/k)^{\dim \rho}$$



- Each $L(s, \rho, L/k)$ is an Artin L-function.
- The product is over the nontrivial irreducible representations of G.

Example of a Dedekind zeta-function $\zeta_L(s)$

Let $k = \mathbb{Q}$ and $G = \mathrm{Gal}(L/\mathbb{Q}) \cong S_3$.

$$\zeta_L(s) =$$

Example of a Dedekind zeta-function $\zeta_L(s)$

Let $k = \mathbb{Q}$ and $G = \mathrm{Gal}(L/\mathbb{Q}) \cong S_3$.

S_3 has the following Galois representations:

$$\zeta_L(s) =$$

Example of a Dedekind zeta-function $\zeta_L(s)$

Let $k = \mathbb{Q}$ and $G = \mathrm{Gal}(L/\mathbb{Q}) \cong S_3$.

S_3 has the following Galois representations:

- ρ_0 – trivial representation, 1-dimensional

$$\zeta_L(s) = \zeta(s)$$

Example of a Dedekind zeta-function $\zeta_L(s)$

Let $k = \mathbb{Q}$ and $G = \mathrm{Gal}(L/\mathbb{Q}) \cong S_3$.

S_3 has the following Galois representations:

- ρ_0 – trivial representation, 1-dimensional
- ρ_1 – sign representation, 1-dimensional

$$\zeta_L(s) = \zeta(s)\, L(s, \rho_1)$$

Example of a Dedekind zeta-function $\zeta_L(s)$

Let $k = \mathbb{Q}$ and $G = \mathrm{Gal}(L/\mathbb{Q}) \cong S_3$.

S_3 has the following Galois representations:

- ρ_0 – trivial representation, 1-dimensional
- ρ_1 – sign representation, 1-dimensional
- ρ_2 – standard representation, 2-dimensional

$$\zeta_L(s) = \zeta(s)\, L(s, \rho_1)\, L(s, \rho_2)^2$$

An Effective Chebotarev Density Theorem

Let L/k be a normal extension with Galois group $G = \mathrm{Gal}(L/k)$, $D_L = |\mathrm{Disc}\, L/\mathbb{Q}|$, and $n_L = [L : \mathbb{Q}]$.

An Effective Chebotarev Density Theorem

Let L/k be a normal extension with Galois group $G = \mathrm{Gal}(L/k)$, $D_L = |\mathrm{Disc}\, L/\mathbb{Q}|$, and $n_L = [L : \mathbb{Q}]$.

Theorem (Lagarias-Odlyzko, 1975)

For any fixed conjugacy class $\mathcal{C} \subset G$,

$$\left| \pi_{\mathcal{C}}(x, L/k) - \frac{|\mathcal{C}|}{|G|}\mathrm{Li}(x) \right| \leq \underbrace{\frac{|\mathcal{C}|}{|G|}\mathrm{Li}(x^{\beta_0}) + c_1 x \exp\left(-c_2 n_L^{1/2} (\log x)^{1/2}\right)}_{\text{Error term depends on zero-free region of } \zeta_L(s).}$$

for $x \geq \exp(10 n_L (\log D_L)^2)$, where

- *β_0 is a real, simple exceptional zero of $\zeta_L(s)$;*
- *c_1, c_2 are effectively computable constants.*

A *Conditional* Effective Chebotarev Density Theorem

Let L/k be a normal extension with Galois group $G = \mathrm{Gal}(L/k)$, $D_L = |\mathrm{Disc}\, L/\mathbb{Q}|$, and $n_L = [L : \mathbb{Q}]$.

A *Conditional* Effective Chebotarev Density Theorem

Let L/k be a normal extension with Galois group $G = \mathrm{Gal}(L/k)$, $D_L = |\mathrm{Disc}\, L/\mathbb{Q}|$, and $n_L = [L : \mathbb{Q}]$.

Theorem (Lagarias-Odlyzko, 1975)

If the **generalized Riemann hypothesis** *holds for the Dedekind zeta-function $\zeta_L(s)$, then for any fixed conjugacy class $\mathcal{C} \subset G$*

$$\left| \pi_{\mathcal{C}}(x, L/k) - \frac{|\mathcal{C}|}{|G|}\mathrm{Li}(x) \right| \leq \underbrace{C_0 \frac{|\mathcal{C}|}{|G|} x^{1/2} \log(D_L x^{n_L})}_{\text{Error term relies on GRH for } \zeta_L(s).}$$

for every $x \geq 2$, where

- *C_0 is an effectively computable constant.*

Comparing the theorems (Lagarias-Odlyzko, 1975)

Theorem (Unconditional)

For any fixed conjugacy class $\mathcal{C} \subset G$,

$$\left|\pi_{\mathcal{C}}(x, L/k) - \frac{|\mathcal{C}|}{|G|}\mathrm{Li}(x)\right| \le \frac{|\mathcal{C}|}{|G|}\mathrm{Li}(x^{\beta_0}) + c_1 x \exp\left(-c_2 n_L^{1/2} (\log x)^{1/2}\right)$$

for $x \ge \exp(10 n_L (\log D_L)^2$.

Comparing the theorems (Lagarias-Odlyzko, 1975)

Theorem (Unconditional)

For any fixed conjugacy class $\mathcal{C} \subset G$,

$$\left| \pi_{\mathcal{C}}(x, L/k) - \frac{|\mathcal{C}|}{|G|} \mathrm{Li}(x) \right| \leq \frac{|\mathcal{C}|}{|G|} \mathrm{Li}(x^{\beta_0}) + c_1 x \exp\left(-c_2 n_L^{1/2} (\log x)^{1/2} \right)$$

for $x \geq \exp(10 n_L (\log D_L)^2$.

Theorem (Conditional)

If GRH holds for $\zeta_L(s)$, then for any fixed conjugacy class $\mathcal{C} \subset G$

$$\left| \pi_{\mathcal{C}}(x, L/k) - \frac{|\mathcal{C}|}{|G|} \mathrm{Li}(x) \right| \leq C_0 \frac{|\mathcal{C}|}{|G|} x^{1/2} \log(D_L x^{n_L}).$$

for every $x \geq 2$.

Comparing the theorems (Lagarias-Odlyzko, 1975)

Theorem (Unconditional)

For any fixed conjugacy class $\mathcal{C} \subset G$,

$$\left|\pi_{\mathcal{C}}(x, L/k) - \frac{|\mathcal{C}|}{|G|}\mathrm{Li}(x)\right| \leq \frac{|\mathcal{C}|}{|G|}\mathrm{Li}(x^{\beta_0}) + c_1 x \exp\left(-c_2 n_L^{1/2}(\log x)^{1/2}\right)$$

for $x \geq \exp(10 n_L (\log D_L)^2$.

Theorem (Conditional)

If GRH holds for $\zeta_L(s)$, then for any fixed conjugacy class $\mathcal{C} \subset G$

$$\left|\pi_{\mathcal{C}}(x, L/k) - \frac{|\mathcal{C}|}{|G|}\mathrm{Li}(x)\right| \leq C_0 \frac{|\mathcal{C}|}{|G|} x^{1/2} \log(D_L x^{n_L}).$$

for every $x \geq 2$.

Comparing the theorems (Lagarias-Odlyzko, 1975)

Theorem (Unconditional)

For any fixed conjugacy class $\mathcal{C} \subset G$,

$$\left|\pi_{\mathcal{C}}(x, L/k) - \frac{|\mathcal{C}|}{|G|}\mathrm{Li}(x)\right| \leq \frac{|\mathcal{C}|}{|G|}\mathrm{Li}(x^{\beta_0}) + c_1 x \exp\left(-c_2 n_L^{1/2}(\log x)^{1/2}\right)$$

for $x \geq \exp(10 n_L (\log D_L)^2$.

Theorem (Conditional)

If GRH holds for $\zeta_L(s)$, then for any fixed conjugacy class $\mathcal{C} \subset G$

$$\left|\pi_{\mathcal{C}}(x, L/k) - \frac{|\mathcal{C}|}{|G|}\mathrm{Li}(x)\right| \leq C_0 \frac{|\mathcal{C}|}{|G|} x^{1/2} \log(D_L x^{n_L}).$$

for every $x \geq 2$.

COMPARING THE THEOREMS (LAGARIAS-ODLYZKO, 1975)

Theorem (Unconditional)

For any fixed conjugacy class $\mathcal{C} \subset G$,

$$\left| \pi_{\mathcal{C}}(x, L/k) - \frac{|\mathcal{C}|}{|G|}\mathrm{Li}(x) \right| \leq \frac{|\mathcal{C}|}{|G|}\mathrm{Li}(x^{\beta_0}) + c_1 x \exp\left(-c_2 n_L^{1/2} (\log x)^{1/2} \right)$$

for $x \geq \exp(10 n_L (\log D_L)^2 \geq D_L^{10 n_L}$.

Theorem (Conditional)

If GRH holds for $\zeta_L(s)$, then for any fixed conjugacy class $\mathcal{C} \subset G$

$$\left| \pi_{\mathcal{C}}(x, L/k) - \frac{|\mathcal{C}|}{|G|}\mathrm{Li}(x) \right| \leq C_0 \frac{|\mathcal{C}|}{|G|} x^{1/2} \log(D_L x^{n_L}).$$

for every $x \geq 2$.

Comparing the theorems (Lagarias-Odlyzko, 1975)

Theorem (Unconditional)

For any fixed conjugacy class $\mathcal{C} \subset G$,

$$\left|\pi_{\mathcal{C}}(x, L/k) - \frac{|\mathcal{C}|}{|G|}\mathrm{Li}(x)\right| \leq \frac{|\mathcal{C}|}{|G|}\mathrm{Li}(x^{\beta_0}) + c_1 x \exp\left(-c_2 n_L^{1/2}(\log x)^{1/2}\right)$$

for $x \geq \exp(10 n_L (\log D_L)^2 \geq D_L^{10 n_L}$.

Theorem (Conditional)

If GRH holds for $\zeta_L(s)$, then for any fixed conjugacy class $\mathcal{C} \subset G$

$$\left|\pi_{\mathcal{C}}(x, L/k) - \frac{|\mathcal{C}|}{|G|}\mathrm{Li}(x)\right| \leq C_0 \frac{|\mathcal{C}|}{|G|} x^{1/2} \log(D_L x^{n_L}).$$

for every $x \geq 2$.

Want: An *unconditional* effective CDT with a low threshold on x, no β_0 term, and an acceptable error term.

Skeleton of Theorem (Pierce, T., Wood)

Let $\mathcal{F}(X)$ be a family of fields, where $K \in \mathcal{F}(X)$ have

Skeleton of Theorem (Pierce, T., Wood)

Let $\mathcal{F}(X)$ be a family of fields, where $K \in \mathcal{F}(X)$ have

- *fixed degree n over $\mathbb{Q}$*

Skeleton of Theorem (Pierce, T., Wood)

Let $\mathcal{F}(X)$ be a family of fields, where $K \in \mathcal{F}(X)$ have

- *fixed degree n over $\mathbb{Q}$*
- *fixed Galois Group $G = \mathrm{Gal}(\widetilde{K}/\mathbb{Q})$*

Skeleton of Theorem (Pierce, T., Wood)

Let $\mathcal{F}(X)$ be a family of fields, where $K \in \mathcal{F}(X)$ have

- *fixed degree n over $\mathbb{Q}$*
- *fixed Galois Group $G = \mathrm{Gal}(\widetilde{K}/\mathbb{Q})$*
- $D_K \leq X$

Skeleton of Theorem (Pierce, T., Wood)

Let $\mathcal{F}(X)$ be a family of fields, where $K \in \mathcal{F}(X)$ have

- *fixed degree n over $\mathbb{Q}$*
- *fixed Galois Group $G = \mathrm{Gal}(\widetilde{K}/\mathbb{Q})$*
- $D_K \leq X$
- *a possible ramification restriction on tamely ramified primes;*

Skeleton of Theorem (Pierce, T., Wood)

Let $\mathcal{F}(X)$ be a family of fields, where $K \in \mathcal{F}(X)$ have

- *fixed degree n over $\mathbb{Q}$*
- *fixed Galois Group $G = \mathrm{Gal}(\widetilde{K}/\mathbb{Q})$*
- $D_K \leq X$
- *a possible ramification restriction on tamely ramified primes;*

Suppose it is known that $|\mathcal{F}(X)| \gg X^a$ for some $a > 0$.

Skeleton of Theorem (Pierce, T., Wood)

Let $\mathcal{F}(X)$ be a family of fields, where $K \in \mathcal{F}(X)$ have

- *fixed degree n over $\mathbb{Q}$*
- *fixed Galois Group $G = \mathrm{Gal}(\widetilde{K}/\mathbb{Q})$*
- $D_K \leq X$
- *a possible ramification restriction on tamely ramified primes;*

Suppose it is known that $|\mathcal{F}(X)| \gg X^a$ for some $a > 0$. Then for at most $O(X^b)$ exceptions, with $b < a$, for fixed $A \geq 2$, we have

$$\left| \pi_{\mathcal{C}}(x, \widetilde{K}/\mathbb{Q}) - \frac{|\mathcal{C}|}{|G|} \mathrm{Li}(x) \right| \leq \frac{|\mathcal{C}|}{|G|} \frac{x}{(\log x)^A}$$

Skeleton of Theorem (Pierce, T., Wood)

Let $\mathcal{F}(X)$ be a family of fields, where $K \in \mathcal{F}(X)$ have

- *fixed degree n over $\mathbb{Q}$*
- *fixed Galois Group $G = \mathrm{Gal}(\widetilde{K}/\mathbb{Q})$*
- $D_K \leq X$
- *a possible ramification restriction on tamely ramified primes;*

Suppose it is known that $|\mathcal{F}(X)| \gg X^a$ for some $a > 0$. Then for at most $O(X^b)$ exceptions, with $b < a$, for fixed $A \geq 2$, we have

$$\left| \pi_{\mathcal{C}}(x, \widetilde{K}/\mathbb{Q}) - \frac{|\mathcal{C}|}{|G|} \mathrm{Li}(x) \right| \leq \frac{|\mathcal{C}|}{|G|} \frac{x}{(\log x)^A}$$

where $x \geq \kappa_1 \exp\{\kappa_2 (\log \log D_{\widetilde{K}}^{\kappa_3})^2\}$, and the κ_i depend on $n, |G|, D_{\widetilde{K}}, a, b,$ and A.

Skeleton of Theorem (Pierce, T., Wood)

Let $\mathcal{F}(X)$ be a family of fields, where $K \in \mathcal{F}(X)$ have

- *fixed degree n over $\mathbb{Q}$*
- *fixed Galois Group $G = \mathrm{Gal}(\widetilde{K}/\mathbb{Q})$*
- $D_K \leq X$
- *a possible ramification restriction on tamely ramified primes;*

Suppose it is known that $|\mathcal{F}(X)| \gg X^a$ for some $a > 0$. Then for at most $O(X^b)$ exceptions, with $b < a$, for fixed $A \geq 2$, we have

$$\left| \pi_{\mathcal{C}}(x, \widetilde{K}/\mathbb{Q}) - \frac{|\mathcal{C}|}{|G|}\mathrm{Li}(x) \right| \leq \frac{|\mathcal{C}|}{|G|} \frac{x}{(\log x)^A}$$

where $x \geq \kappa_1 \exp\{\kappa_2(\log\log D_{\widetilde{K}}^{\kappa_3})^2\}$, and the κ_i depend on $n, |G|, D_{\widetilde{K}}, a, b,$ and A.

- No β_0 term.

Skeleton of Theorem (Pierce, T., Wood)

Let $\mathcal{F}(X)$ be a family of fields, where $K \in \mathcal{F}(X)$ have

- *fixed degree n over $\mathbb{Q}$*
- *fixed Galois Group $G = \mathrm{Gal}(\widetilde{K}/\mathbb{Q})$*
- $D_K \le X$
- *a possible ramification restriction on tamely ramified primes;*

Suppose it is known that $|\mathcal{F}(X)| \gg X^a$ for some $a > 0$. Then for at most $O(X^b)$ exceptions, with $b < a$, for fixed $A \ge 2$, we have

$$\left| \pi_{\mathcal{C}}(x, \widetilde{K}/\mathbb{Q}) - \frac{|\mathcal{C}|}{|G|}\mathrm{Li}(x) \right| \le \frac{|\mathcal{C}|}{|G|} \frac{x}{(\log x)^A}$$

where $x \ge \kappa_1 \exp\{\kappa_2(\log\log D_{\widetilde{K}}^{\kappa_3})^2\}$, and the κ_i depend on $n, |G|, D_{\widetilde{K}}, a, b$, and A.

- No β_0 term. Can take $x = D_{\widetilde{K}}^{\eta}$ for η small.

Skeleton of Theorem (Pierce, T., Wood)

Let $\mathcal{F}(X)$ be a family of fields, where $K \in \mathcal{F}(X)$ have

- *fixed degree n over $\mathbb{Q}$*
- *fixed Galois Group $G = \mathrm{Gal}(\widetilde{K}/\mathbb{Q})$*
- $D_K \leq X$
- *a possible ramification restriction on tamely ramified primes;*

Suppose it is known that $|\mathcal{F}(X)| \gg X^a$ for some $a > 0$. Then for at most $O(X^b)$ exceptions, with $b < a$, for fixed $A \geq 2$, we have

$$\left| \pi_{\mathcal{C}}(x, \widetilde{K}/\mathbb{Q}) - \frac{|\mathcal{C}|}{|G|}\mathrm{Li}(x) \right| \leq \frac{|\mathcal{C}|}{|G|} \frac{x}{(\log x)^A}$$

where $x \geq \kappa_1 \exp\{\kappa_2(\log\log D_{\widetilde{K}}^{\kappa_3})^2\}$, and the κ_i depend on $n, |G|, D_{\widetilde{K}}, a, b,$ and A.

- No β_0 term. Can take $x = D_{\widetilde{K}}^{\eta}$ for η small.

We prove *most* Dedekind zeta-functions in the family satisfy a certain zero-free region.

Application to bounding ℓ-torsion

Skeleton of Corollary (Pierce, T., Wood)

Let $\mathcal{F}(X)$ be a family of fields for which the previous Chebotarev Density Theorem holds. For the nonexceptional fields $K \in \mathcal{F}(X)$, we have

$$|\mathrm{Cl}_K[\ell]| \ll_{n,\ell,\varepsilon} D_K^{\frac{1}{2}-\frac{1}{2\ell(n-1)}+\varepsilon}.$$

Application to bounding ℓ-torsion

Skeleton of Corollary (Pierce, T., Wood)

Let $\mathcal{F}(X)$ be a family of fields for which the previous Chebotarev Density Theorem holds. For the nonexceptional fields $K \in \mathcal{F}(X)$, we have

$$|\mathrm{Cl}_K[\ell]| \ll_{n,\ell,\varepsilon} D_K^{\frac{1}{2}-\frac{1}{2\ell(n-1)}+\varepsilon}.$$

Question:
To which families does our Chebotarev Density Theorem apply?

$[K : \mathbb{Q}]$	$\mathrm{Gal}(\widetilde{K}/\mathbb{Q})$	restriction on tamely ramified primes	size of exceptional family	size of total family

$[K:\mathbb{Q}]$	$\mathrm{Gal}(\widetilde{K}/\mathbb{Q})$	restriction on tamely ramified primes	size of exceptional family	size of total family
$n \geq 2$	C_n	totally ramified	$\ll X^{\varepsilon}, \varepsilon > 0$	$\sim cX^{1/(n-1)}$

$[K:\mathbb{Q}]$	$\mathrm{Gal}(\widetilde{K}/\mathbb{Q})$	restriction on tamely ramified primes	size of exceptional family	size of total family
$n \geq 2$	C_n	totally ramified	$\ll X^{\varepsilon}, \varepsilon > 0$	$\sim cX^{1/(n-1)}$
3	S_3	transposition	$\ll X^{1/3}$ Ellenberg-Venkatesh	$\sim cX$ Bhargava

$[K:\mathbb{Q}]$	$\mathrm{Gal}(\widetilde{K}/\mathbb{Q})$	restriction on tamely ramified primes	size of exceptional family	size of total family
$n \geq 2$	C_n	totally ramified	$\ll X^{\varepsilon}, \varepsilon > 0$	$\sim cX^{1/(n-1)}$
3	S_3	transposition	$\ll X^{1/3}$ Ellenberg-Venkatesh	$\sim cX$ Bhargava
4	S_4	transposition	$\ll X^{1/2+\varepsilon}, \varepsilon > 0$ Klüners	$\sim cX$ Bhargava

$[K:\mathbb{Q}]$	$\mathrm{Gal}(\widetilde{K}/\mathbb{Q})$	restriction on tamely ramified primes	size of exceptional family	size of total family
$n \geq 2$	C_n	totally ramified	$\ll X^{\varepsilon}, \varepsilon > 0$	$\sim cX^{1/(n-1)}$
3	S_3	transposition	$\ll X^{1/3}$ Ellenberg-Venkatesh	$\sim cX$ Bhargava
4	S_4	transposition	$\ll X^{1/2+\varepsilon}, \varepsilon > 0$ Klüners	$\sim cX$ Bhargava
4	A_4	K_4 subgroup	$\ll X^{0.27}$	$\gg X^{1/2}$

$[K:\mathbb{Q}]$	$\mathrm{Gal}(\widetilde{K}/\mathbb{Q})$	restriction on tamely ramified primes	size of exceptional family	size of total family
$n \geq 2$	C_n	totally ramified	$\ll X^{\varepsilon}, \varepsilon > 0$	$\sim cX^{1/(n-1)}$
3	S_3	transposition	$\ll X^{1/3}$ Ellenberg-Venkatesh	$\sim cX$ Bhargava
4	S_4	transposition	$\ll X^{1/2+\varepsilon}, \varepsilon > 0$ Klüners	$\sim cX$ Bhargava
4	A_4	K_4 subgroup	$\ll X^{0.27}$	$\gg X^{1/2}$
$p \geq 5$	D_p order $2p$	reflection	$\ll X^{1/(p-1)}$	$\gg X^{2/(p-1)}$

CONDITIONAL ON THE STRONG ARTIN CONJECTURE

$[K:\mathbb{Q}]$	$\mathrm{Gal}(\widetilde{K}/\mathbb{Q})$	restriction on tamely ramified primes	size of exceptional family	size of total family

CONDITIONAL ON THE STRONG ARTIN CONJECTURE

$[K:\mathbb{Q}]$	$\mathrm{Gal}(\widetilde{K}/\mathbb{Q})$	restriction on tamely ramified primes	size of exceptional family	size of total family
5	S_5	transposition	$\ll X^{199/200}$	$\gg X$ Bhargava

Conditional on the Strong Artin Conjecture

$[K:\mathbb{Q}]$	$\mathrm{Gal}(\widetilde{K}/\mathbb{Q})$	restriction on tamely ramified primes	size of exceptional family	size of total family
5	S_5	transposition	$\ll X^{199/200}$	$\gg X$ Bhargava
$n \geq 6$	S_n	transposition	$\ll X^{\Delta}$ if there exists $\ll D^{\Delta}$ degree n fields such that $D_K = D$.	$\gg X^{1/2+1/n}$ Bhargava, Shankur Wang

CONDITIONAL ON THE STRONG ARTIN CONJECTURE

$[K:\mathbb{Q}]$	$\mathrm{Gal}(\widetilde{K}/\mathbb{Q})$	restriction on tamely ramified primes	size of exceptional family	size of total family
5	S_5	transposition	$\ll X^{199/200}$	$\gg X$ Bhargava
$n \geq 6$	S_n	transposition	$\ll X^{\Delta}$ if there exists $\ll D^{\Delta}$ degree n fields such that $D_K = D$.	$\gg X^{1/2+1/n}$ Bhargava, Shankur Wang
$n \geq 5$	A_n	none	$\ll X^{\varepsilon}, \varepsilon > 0$	$\gg X^{\beta_n - \varepsilon}$ $\beta_n = \frac{1-2/n!}{4n-4}$

Overview of argument

Ellenberg-Venkatesh

$$|\mathrm{Cl}_K[\ell]| \quad \ll_{\ell,n,\varepsilon} \quad D_K^{\frac{1}{2}+\varepsilon} M^{-1}$$

Overview of argument

Ellenberg-Venkatesh

$$|\mathrm{Cl}_K[\ell]| \quad \ll_{\ell,n,\varepsilon} \quad D_K^{\frac{1}{2}+\varepsilon} M^{-1}$$

↓

Effective Chebotarev Density Theorem
assuming non-GRH zero-free region

Overview of argument

Ellenberg-Venkatesh

$$|\mathrm{Cl}_K[\ell]| \quad \ll_{\ell,n,\varepsilon} \quad D_K^{\frac{1}{2}+\varepsilon} M^{-1}$$

↓

Effective Chebotarev Density Theorem
assuming non-GRH zero-free region

↓

Show assumed zero-free region is obeyed
by "most" number fields in an appropriate family

Overview of argument

Ellenberg-Venkatesh

$$|\mathrm{Cl}_K[\ell]| \quad \ll_{\ell,n,\varepsilon} \quad D_K^{\frac{1}{2}+\varepsilon} M^{-1}$$

↓

Effective Chebotarev Density Theorem
assuming non-GRH zero-free region

↓

Show assumed zero-free region is obeyed
by ″most″ number fields in an appropriate family

↓

Control the propagation of ″bad″ fields within the family

Overview of argument

Ellenberg-Venkatesh

$$|\mathrm{Cl}_K[\ell]| \ll_{\ell,n,\varepsilon} D_K^{\frac{1}{2}+\varepsilon} M^{-1}$$

↓

Effective Chebotarev Density Theorem
assuming non-GRH zero-free region

↓

Show assumed zero-free region is obeyed
by "most" number fields in an appropriate family

↓

Control the propagation of "bad" fields within the family

↓

Without assuming GRH, conclude

$|\mathrm{Cl}_K[\ell]| \ll_{\ell,n,\varepsilon} D_K^{\frac{1}{2}-\frac{1}{2\ell(n-1)}+\varepsilon}$ for non-exceptional K.

Overview of argument

Ellenberg-Venkatesh

$$|\mathrm{Cl}_K[\ell]| \ll_{\ell,n,\varepsilon} D_K^{\frac{1}{2}+\varepsilon} M^{-1}$$

↓

Effective Chebotarev Density Theorem
assuming non-GRH zero-free region

↓

Show assumed zero-free region is obeyed
by "most" number fields in an appropriate family

↓

Control the propagation of "bad" fields within the family

↓

Without assuming GRH, conclude

$|\mathrm{Cl}_K[\ell]| \ll_{\ell,n,\varepsilon} D_K^{\frac{1}{2}-\frac{1}{2\ell(n-1)}+\varepsilon}$ for non-exceptional K.

Overview of argument

Ellenberg-Venkatesh

$$|\mathrm{Cl}_K[\ell]| \quad \ll_{\ell,n,\varepsilon} \quad D_K^{\frac{1}{2}+\varepsilon} M^{-1}$$

↓

Effective Chebotarev Density Theorem
assuming non-GRH zero-free region

↓

Show assumed zero-free region is obeyed
by "most" number fields in an appropriate family

↓

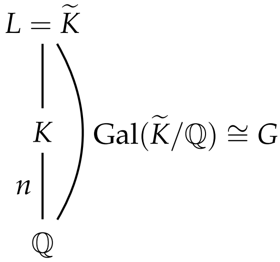
Control the propagation of "bad" fields within the family

↓

Without assuming GRH, conclude

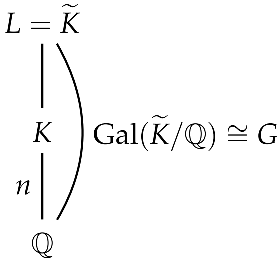
$|\mathrm{Cl}_K[\ell]| \ll_{\ell,n,\varepsilon} D_K^{\frac{1}{2}-\frac{1}{2\ell(n-1)}+\varepsilon}$ for non-exceptional K.

The zero-free region



$$\zeta_{\widetilde{K}}(s) = \zeta(s) \prod_{\substack{\rho \in \hat{G} \\ \rho \neq \rho_0 \text{ irreducible}}} L(s, \rho, \widetilde{K}/\mathbb{Q})^{\dim \rho}$$

The zero-free region

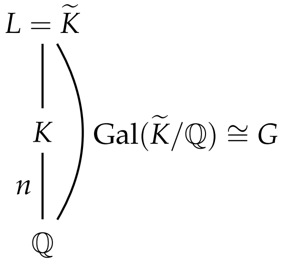


$$\zeta_{\widetilde{K}}(s) = \zeta(s) \prod_{\substack{\rho \in \hat{G} \\ \rho \neq \rho_0 \text{ irreducible}}} L(s, \rho, \widetilde{K}/\mathbb{Q})^{\dim \rho}$$

Known zero-free region for $\zeta(s)$:

$$\sigma > 1 - \frac{c}{\log^{2/3}(|t| + 2) \log\log^{1/3}(|t| + 3)}.$$

The zero-free region



$$\zeta_{\widetilde{K}}(s) = \zeta(s) \prod_{\substack{\rho \in \hat{G} \\ \rho \neq \rho_0 \text{ irreducible}}} L(s, \rho, \widetilde{K}/\mathbb{Q})^{\dim \rho}$$

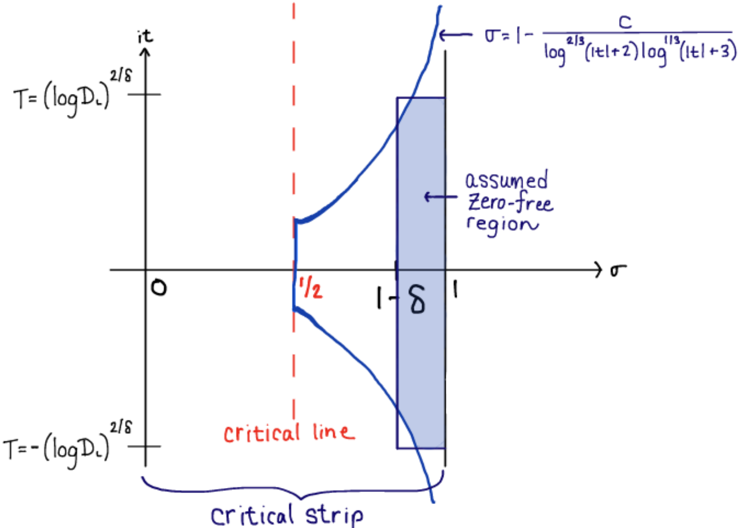
Known zero-free region for $\zeta(s)$:

$$\sigma > 1 - \frac{c}{\log^{2/3}(|t|+2) \log \log^{1/3}(|t|+3)}.$$

Assumed zero-free region for $\zeta_{\widetilde{K}}(s)/\zeta(s)$:

$$[1-\delta, 1] \times [-(\log D_{\widetilde{K}})^{2/\delta}, (\log D_{\widetilde{K}})^{2/\delta}].$$

$$\zeta_{\widetilde{K}}(s) = \zeta(s) \prod_{\substack{\rho \in \hat{G} \\ \rho \neq \rho_0 \text{ irreducible}}} L(s, \rho, \widetilde{K}/\mathbb{Q})^{\dim \rho}$$



Proving the Chebotarev Density Theorem

Idea of the proof

- We return to the method of Lagarias-Odlyzko.

Proving the Chebotarev Density Theorem

Idea of the proof

- We return to the method of Lagarias-Odlyzko.

- We insert our *assumed* zero-free region for $\zeta_L(s)/\zeta(s)$ at a key point.

Proving the Chebotarev Density Theorem

Idea of the proof

- We return to the method of Lagarias-Odlyzko.
- We insert our *assumed* zero-free region for $\zeta_L(s)/\zeta(s)$ at a key point.
- We work delicately to provide both an acceptable effective error term, and a sufficiently small threshold for x depending on D_L.

Theorem (Pierce, T., Wood)

Let $0 < \delta \leq 1/4$ be a fixed positive constant. For any normal extension of number fields $L/\mathbb{Q}$ with $[L:\mathbb{Q}] = n_L$ such that D_L is sufficiently large and $\zeta_L(s)$ obeys the assumed zero-free region, we have that for any $A \geq 2$ and any conjugacy class $\mathcal{C} \subset G = \mathrm{Gal}(L/\mathbb{Q})$

$$\left|\pi_{\mathcal{C}}(x, L/\mathbb{Q}) - \frac{|\mathcal{C}|}{|G|}\mathrm{Li}(x)\right| \leq \underbrace{\frac{|\mathcal{C}|}{|G|}\frac{x}{(\log x)^A}}_{\text{error term depends on assumed zero-free region}}$$

for all

$$x \geq \underbrace{c_1 \exp\left\{c_2(\log\log(D_L^{c_3})^{3/2} \log\log\log(D_L^{c_4}))^{1/2}\right\}}_{\geq (\log D_L)^{\text{small power}}},$$

where all the constants can be written explicitly.

Bounding ℓ-torsion without assuming GRH

Ellenberg-Venkatesh

$$|\mathrm{Cl}_K[\ell]| \ll_{\ell,n,\varepsilon} D_K^{\frac{1}{2}+\varepsilon} M^{-1}$$

↓

Prove an effective Chebotarev Density Theorem assuming non-GRH zero-free region

↓

Show that within an appropriate family of fields K, most $\zeta_{\widetilde{K}}(s)$ obey the zero-free region

↓

Control the propagation of ”bad” fields within the family

↓

Without assuming GRH, conclude

$|\mathrm{Cl}_K[\ell]| \ll_{\ell,n,\varepsilon} D_K^{\frac{1}{2}-\frac{1}{2\ell(n-1)}+\varepsilon}$ for non-exceptional K.

BOUNDING ℓ-TORSION WITHOUT ASSUMING GRH

Ellenberg-Venkatesh

$$|\mathrm{Cl}_K[\ell]| \quad \ll_{\ell,n,\varepsilon} \quad D_K^{\frac{1}{2}+\varepsilon} M^{-1}$$

↓

Prove an effective Chebotarev Density Theorem assuming non-GRH zero-free region

↓

Show that within an appropriate family of fields K, most $\zeta_{\widetilde{K}}(s)$ obey the zero-free region

↓

Control the propagation of "bad" fields within the family

↓

Without assuming GRH, conclude

$|\mathrm{Cl}_K[\ell]| \ll_{\ell,n,\varepsilon} D_K^{\frac{1}{2}-\frac{1}{2\ell(n-1)}+\varepsilon}$ for non-exceptional K.

Key Tool - zeros of automorphic L-functions

Let π be a cuspidal automorphic representation on $\mathrm{GL}_m(\mathbb{Q})$.

Consider the corresponding automorphic L-function $L(s, \pi)$.

Key Tool - zeros of automorphic L-functions

Let π be a cuspidal automorphic representation on $\mathrm{GL}_m(\mathbb{Q})$.

Consider the corresponding automorphic L-function $L(s, \pi)$.

Let $s = \beta + i\gamma$ denote a zero of $L(s, \pi)$.

KEY TOOL - ZEROS OF AUTOMORPHIC L-FUNCTIONS

Let π be a cuspidal automorphic representation on $\mathrm{GL}_m(\mathbb{Q})$.

Consider the corresponding automorphic L-function $L(s, \pi)$.

Let $s = \beta + i\gamma$ denote a zero of $L(s, \pi)$.

Define

$$N(\pi; \alpha, T) := \# \text{ of zeros of } L(s, \pi) \text{ such that } \beta > \alpha \text{ and } |\gamma| \leq T.$$

KEY TOOL - ZEROS OF AUTOMORPHIC L-FUNCTIONS

Let π be a cuspidal automorphic representation on $\mathrm{GL}_m(\mathbb{Q})$.

Consider the corresponding automorphic L-function $L(s, \pi)$.

Let $s = \beta + i\gamma$ denote a zero of $L(s, \pi)$.

Define

$$N(\pi; \alpha, T) := \# \text{ of zeros of } L(s, \pi) \text{ such that } \beta > \alpha \text{ and } |\gamma| \leq T.$$

Kowalski and Michel have given a bound for $N(\pi; \alpha, T)$ that holds on average for an appropriately defined family of cuspidal automorphic representations.

Theorem (Kowalski & Michel, 2002)

Let $S(q)$, $q \geq 1$ be a family of cuspidal automorphic representations satisfying a prescribed set of conditions. Let $\alpha \geq 3/4$ and $T \geq 2$. Then there exists $c_0 > 0$, depending on the family, such that

$$\sum_{\pi \in S(q)} N(\pi; \alpha, T) \ll T^B q^{c_0 \frac{1-\alpha}{2\alpha-1}}$$

for all $q \geq 1$ and some $B \geq 0$ that depends on the family. The implied constant only depends on the choice of c_0.

Theorem (Kowalski & Michel, 2002)

Let $S(q)$, $q \geq 1$ be a family of cuspidal automorphic representations satisfying a prescribed set of conditions. Let $\alpha \geq 3/4$ and $T \geq 2$. Then there exists $c_0 > 0$, depending on the family, such that

$$\sum_{\pi \in S(q)} N(\pi; \alpha, T) \ll T^B q^{c_0 \frac{1-\alpha}{2\alpha - 1}}$$

for all $q \geq 1$ and some $B \geq 0$ that depends on the family. The implied constant only depends on the choice of c_0.

Applied to $L(s, \pi)$ for $\pi \in S(q)$ $\implies$ a zero-free region of the desired shape that holds for all but a possible zero-density sub-family of L-functions

We wish to apply Kowalski-Michel to $\dfrac{\zeta_{\tilde{K}}(s)}{\zeta(s)}$ as K varies over $\mathcal{F}(X)$.

A couple of issues:

We wish to apply Kowalski-Michel to $\frac{\zeta_{\tilde{K}}(s)}{\zeta(s)}$ as K varies over $\mathcal{F}(X)$.

A couple of issues:

1. We are working with Artin L-functions, which in general are not known to be automorphic.

We wish to apply Kowalski-Michel to $\frac{\zeta_{\tilde{K}}(s)}{\zeta(s)}$ as K varies over $\mathcal{F}(X)$.

A couple of issues:

1. We are working with Artin L-functions, which in general are not known to be automorphic.

2. Kowalski & Michel's result applies to family of cuspidal automorphic representations. We would like to apply it to a family of *isobaric* automorphic representations.

$$\frac{\zeta_{\widetilde{K}}(s)}{\zeta(s)} = \prod_{\substack{\rho \in \hat{G} \\ \rho \neq \rho_0 \text{ irreducible}}} L(s, \rho, \widetilde{K}/\mathbb{Q})^{d_j}, \quad d_j = \deg(\rho_j).$$

Issue # 1 – We are working with Artin L-functions, which in general are not known to be automorphic.

$$\frac{\zeta_{\widetilde{K}}(s)}{\zeta(s)} = \prod_{\substack{\rho \in \hat{G} \\ \rho \neq \rho_0 \text{ irreducible}}} L(s, \rho, \widetilde{K}/\mathbb{Q})^{d_j}, \quad d_j = \deg(\rho_j).$$

Issue # 1 – We are working with Artin L-functions, which in general are not known to be automorphic.

Assuming the strong Artin conjecture, we have that each $L(s, \rho, \widetilde{K}/\mathbb{Q})$ is automorphic, i.e. we can write

$$L(s, \rho, \widetilde{K}/\mathbb{Q}) = L(s, \pi)$$

for each $L(s, \rho, \widetilde{K}/\mathbb{Q})$ in our product.

$$\frac{\zeta_{\widetilde{K}}(s)}{\zeta(s)} = \prod_{\substack{\rho \in \hat{G} \\ \rho \neq \rho_0 \text{ irreducible}}} L(s, \rho, \widetilde{K}/\mathbb{Q})^{d_j}, \quad d_j = \deg(\rho_j).$$

Issue # 2 – Kowalski & Michel applies to families of cuspidal automorphic representations, but we are working with families of isobaric automorphic representations.

$$\frac{\zeta_{\widetilde{K}}(s)}{\zeta(s)} = \prod_{\substack{\rho \in \hat{G} \\ \rho \neq \rho_0 \text{ irreducible}}} L(s, \rho, \widetilde{K}/\mathbb{Q})^{d_j}, \quad d_j = \deg(\rho_j).$$

Issue # 2 – Kowalski & Michel applies to families of cuspidal automorphic representations, but we are working with families of isobaric automorphic representations.

- We decompose each Dedekind zeta function into a product of cuspidal automorphic L-functions.

$$\frac{\zeta_{\widetilde{K}}(s)}{\zeta(s)} = \prod_{\substack{\rho\in\hat{G} \\ \rho\neq\rho_0 \text{ irreducible}}} L(s,\rho,\widetilde{K}/\mathbb{Q})^{d_j}, \quad d_j = \deg(\rho_j).$$

Issue # 2 – Kowalski & Michel applies to families of cuspidal automorphic representations, but we are working with families of isobaric automorphic representations.

- We decompose each Dedekind zeta function into a product of cuspidal automorphic L-functions.
- We apply the Kowalski-Michel result to the sub-family generated by each factor.

A new obstacle:

In generalizing Kowalski-Michel, we uncover a technical barrier:

– *a priori*, each sub-family could lead to many bad fields for which our Chebotarev Density Theorem does not apply.

A new obstacle:

In generalizing Kowalski-Michel, we uncover a technical barrier:

– *a priori*, each sub-family could lead to many bad fields for which our Chebotarev Density Theorem does not apply.

Must define our families of fields to avoid this situation – where potential "bad" elements in each sub-family propagate to create a "large" family of "bad" Dedekind zeta-functions $\zeta_{\widetilde{K}}(s)$.

Bounding ℓ-torsion without assuming GRH

Ellenberg-Venkatesh

$$|\mathrm{Cl}_K[\ell]| \ll_{\ell,n,\varepsilon} D_K^{\frac{1}{2}+\varepsilon} M^{-1}$$

↓

Prove an effective Chebotarev Density Theorem assuming non-GRH zero-free region

↓

Show that within an appropriate family of fields K, most $\zeta_{\widetilde{K}}(s)$ obey the zero-free region

↓

Control the propagation of "bad" fields within the family

↓

Without assuming GRH, conclude

$|\mathrm{Cl}_K[\ell]| \ll_{\ell,n,\varepsilon} D_K^{\frac{1}{2}-\frac{1}{2\ell(n-1)}+\varepsilon}$ for non-exceptional K.

Controlling propagation of bad fields

Sketch of new idea

- We transform the problem to counting how often $\widetilde{K}_1$ and $\widetilde{K}_2$ both contain a particular subfield F. This relies on work of Klüners and Nicolae (2016).

Controlling propagation of bad fields

Sketch of new idea

- We transform the problem to counting how often $\widetilde{K}_1$ and $\widetilde{K}_2$ both contain a particular subfield F. This relies on work of Klüners and Nicolae (2016).

- To handle this counting problem, we make ramification type restrictions and derive a precise relationship between the D_F, D_K, $D_{\widetilde{K}}$.

Controlling propagation of bad fields

Sketch of new idea

- We transform the problem to counting how often $\widetilde{K}_1$ and $\widetilde{K}_2$ both contain a particular subfield F. This relies on work of Klüners and Nicolae (2016).

- To handle this counting problem, we make ramification type restrictions and derive a precise relationship between the D_F, D_K, $D_{\widetilde{K}}$.
  – Here, we must handle the issue for each type of G individually.

Controlling propagation of bad fields

Sketch of new idea

- We transform the problem to counting how often $\widetilde{K}_1$ and $\widetilde{K}_2$ both contain a particular subfield F. This relies on work of Klüners and Nicolae (2016).

- To handle this counting problem, we make ramification type restrictions and derive a precise relationship between the D_F, D_K, $D_{\widetilde{K}}$.
  – Here, we must handle the issue for each type of G individually.

- Then we quantify how many K can have a particular discriminant.

Bounding ℓ-torsion without assuming GRH

Ellenberg-Venkatesh

$$|\mathrm{Cl}_K[\ell]| \quad \ll_{\ell,n,\varepsilon} \quad D_K^{\frac{1}{2}+\varepsilon} M^{-1}$$

↓

Prove an effective Chebotarev Density Theorem assuming non-GRH zero-free region

↓

Show that within an appropriate family of fields K, most $\zeta_{\widetilde{K}}(s)$ obey the zero-free region

↓

Control the propagation of "bad" fields within the family

↓

Without assuming GRH, conclude

$|\mathrm{Cl}_K[\ell]| \ll_{\ell,n,\varepsilon} D_K^{\frac{1}{2}-\frac{1}{2\ell(n-1)}+\varepsilon}$ for non-exceptional K.

Thanks for y’all’s attention!