Bounding ℓ-torsion in class groups of families of number fields of arbitrary degree

Caroline Turnage-Butterbaugh
Duke University

Connections for Women Workshop
Analytic Number Theory
MSRI
February 3, 2017

Binary Quadratic Forms

A binary quadratic form is a homogenous polynomial of degree 2 in two variables:

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

Binary Quadratic Forms

A binary quadratic form is a homogenous polynomial of degree 2 in two variables:

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

Equivalent Forms

Two binary quadratic forms (a,b,c) and (a',b',c') are said to be equivalent if there exists a matrix $A \in \mathrm{SL}_2(\mathbb{Z})$ such that if we make the linear change of variables

$$A \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x' \\ y' \end{pmatrix}$$

we have

$$ax'^2 + bx'y' + cy'^2 = a'x^2 + b'xy + c'y^2.$$

GAUSS AND BINARY QUADRATIC FORMS

In *Disquisitiones Arithmeticae*, Gauss

- classified the binary quadratic forms with a given discriminant

$$D := b^2 - 4ac, \qquad D \equiv 0,1 \pmod 4$$

Note that equivalent forms have the same discriminant;

Gauss and binary quadratic forms

In *Disquisitiones Arithmeticae*, Gauss

- classified the binary quadratic forms with a given discriminant

  $$D := b^2 - 4ac, \qquad D \equiv 0, 1 \pmod 4$$

  Note that equivalent forms have the same discriminant;

- formed the *class group*, the group of equivalence classes of binary quadratic forms of a given D with group action Gauss composition;

Gauss and binary quadratic forms

In *Disquisitiones Arithmeticae*, Gauss

- classified the binary quadratic forms with a given discriminant

$$D := b^2 - 4ac, \qquad D \equiv 0,1 \pmod 4)$$

  Note that equivalent forms have the same discriminant;

- 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.

Binary quadratic forms and quadratic number fields

Let $K = \mathbb{Q}(\sqrt{D})$. Two nonzero ideals $I, J \subset \mathcal{O}_K$ are said to be *equivalent* if there exists $r, s \in \mathcal{O}_K$ such that $(r)I = (s)J$.

Binary quadratic forms and quadratic number fields

Let $K = \mathbb{Q}(\sqrt{D})$. Two nonzero ideals $I, J \subset \mathcal{O}_K$ are said to be *equivalent* if there exists $r, s \in \mathcal{O}_K$ such that $(r)I = (s)J$.

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

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

Binary quadratic forms and quadratic number fields

Equivalent binary quadratic forms	$\longleftrightarrow$	equivalent ideals
composition of equivalence classes of forms	$\longleftrightarrow$	multiplication of equivalence classes of ideals

Binary quadratic forms and quadratic number fields

Equivalent binary quadratic forms	$\longleftrightarrow$	equivalent ideals
composition of equivalence classes of forms	$\longleftrightarrow$	multiplication of equivalence classes of ideals

Ideal class group

We denote by Cl_K the ideal class group of K. The class number of K is defined by

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

From the correspondence to binary quadratic fields, we see that $h(K)$ is finite.

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

Ideal class group

The ideal class group of K is defined to be

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

where J_K denotes the group of fractional ideals of K and P_K denotes the subgroup of principal ideals of K.

The class number of K is defined by

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

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

Ideal class group

The ideal class group of K is defined to be

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

where J_K denotes the group of fractional ideals of K and P_K denotes the subgroup of principal ideals of K.

The class number of K is defined by

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

Note:

$$h(K) = 1 \quad \Longleftrightarrow \quad \mathcal{O}_K \text{ is a PID} \quad \Longrightarrow \quad \mathcal{O}_K \text{ is a UFD}$$

Size of the class group

Landau observed (using Minkowski's Bound) that

$$|\mathrm{Cl}_K| \le \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2} D_K^{1/2}(\log D_K)^{n-1}$$

where $D_K = |\mathrm{Disc}\, K/Q|$ and r_2 denotes the number of pairs of conjugate complex embeddings of K.

ℓ-TORSION SUBGROUP

Definition

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

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

ℓ-TORSION SUBGROUP

Definition

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?

Trivial Bound

The trivial bound on the ℓ-torsion subgroup is simply the size of Cl_K:

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

for any integer $\ell \geq 1$ and $\varepsilon > 0$ arbitrarily small.

What do we think is true?

Conjecture

Let $K/\mathbb{Q}$ be a number field of degree n. Then for every integer $\ell \geq 1$,

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

Recorded by

- Brumer-Silverman, 1996
- Duke, 1998
- Zhang, 2005

What do we know is true?

Conjecture

Let $K/\mathbb{Q}$ be a number field of degree n. Then for every integer $\ell \geq 1$,

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

Theorem (Gauss)

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

What do we know is true?

Theorem (Ellenberg & Venkatesh, 2007)

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

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

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

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

What do we know is true?

Theorem (Ellenberg & Venkatesh, 2007)

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

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

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

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

Theorem (Bhargava *et. al.*, 2017)

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

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

What do we know is true?

Theorem (Ellenberg & Venkatesh, 2007)

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

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

What do we know is true?

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

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

What do we know is true?

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

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

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

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

What do we know is true?

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.

Bounding ℓ-torsion for higher degree fields

Here is the shape of theorem we aim to prove:

General shape of end result

Let G be a transitive subgroup of S_n of order $n \geq 2$. Let $\mathscr{F}(X)$ be the family of extensions $K/\mathbb{Q}$

Here is the shape of theorem we aim to prove:

General shape of end result

Let G be a transitive subgroup of S_n of order $n \geq 2$. Let $\mathscr{F}(X)$ be the family of extensions $K/\mathbb{Q}$ with $\mathrm{Gal}(\widetilde{K}/\mathbb{Q}) \cong G$ as a permutation group and with $D_K \in (0, X]$ and such that all tamely ramified primes in K have a fixed ramification type.

Bounding ℓ-torsion for higher degree fields

Here is the shape of theorem we aim to prove:

General shape of end result

Let G be a transitive subgroup of S_n of order $n \geq 2$. Let $\mathscr{F}(X)$ be the family of extensions $K/\mathbb{Q}$ with $\mathrm{Gal}(\widetilde{K}/\mathbb{Q}) \cong G$ as a permutation group and with $D_K \in (0, X]$ and such that all tamely ramified primes in K have a fixed ramification type. Then for all but a possible zero-density exceptional family of fields in $\mathscr{F}(X)$, each $K \in \mathscr{F}(X)$ satisfies for every integer $\ell \geq 1$ the bound

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

as long as certain conditions on G and conjectures (but never GRH) are met.

Unconditional Result

Theorem (Pierce, T. & Wood, 2017)

Let G be a cyclic group of order $n \geq 2$. Let $\mathscr{F}(X)$ be the family of Galois extensions $K/\mathbb{Q}$

Unconditional Result

Theorem (Pierce, T. & Wood, 2017)

Let G be a cyclic group of order $n \geq 2$. Let $\mathscr{F}(X)$ be the family of Galois extensions $K/\mathbb{Q}$ with $\mathrm{Gal}(K/\mathbb{Q}) \cong G$ as a permutation group and with $D_K \in (0, X]$ and such that all rational primes ramifying in K are totally ramified.

Unconditional Result

Theorem (Pierce, T. & Wood, 2017)

Let G be a cyclic group of order $n \geq 2$. Let $\mathscr{F}(X)$ be the family of Galois extensions $K/\mathbb{Q}$ with $\mathrm{Gal}(K/\mathbb{Q}) \cong G$ as a permutation group and with $D_K \in (0, X]$ and such that all rational primes ramifying in K are totally ramified. Then for all but a possible zero-density exceptional family of fields in $\mathscr{F}(X)$, each $K \in \mathscr{F}(X)$ satisfies for every integer $\ell \geq 1$ the bound

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

Unconditional Result

Theorem (Pierce, T. & Wood, 2017)

Let G be a cyclic group of order $n \geq 2$. Let $\mathscr{F}(X)$ be the family of Galois extensions $K/\mathbb{Q}$ with $\mathrm{Gal}(K/\mathbb{Q}) \cong G$ as a permutation group and with $D_K \in (0, X]$ and such that all rational primes ramifying in K are totally ramified. Then for all but a possible zero-density exceptional family of fields in $\mathscr{F}(X)$, each $K \in \mathscr{F}(X)$ satisfies for every integer $\ell \geq 1$ the bound

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

If in addition n is prime, then all fields in $\mathscr{F}(X)$ satisfy the bound without exception.

$G = \mathrm{Gal}(\widetilde{K}/\mathbb{Q}) \cong S_n, n \geq 2$

Theorem (Pierce, T. & Wood, 2017)

Let $n \geq 2$ be fixed and let $\mathscr{F}(X)$ be the family of degree n extensions $K/\mathbb{Q}$ with square-free discriminant $D_K \in (0, X]$ and $\mathrm{Gal}(\widetilde{K}/\mathbb{Q}) \cong S_n$ as a permutation group. Then assuming the strong Artin conjecture and the Discriminant Multiplicity conjecture, for all a possible zero-density exceptional family of fields in $\mathscr{F}(X)$, each $K \in \mathscr{F}(X)$ satisfy for every integer $\ell \geq 1$ the bound

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

$G = \mathrm{Gal}(\widetilde{K}/\mathbb{Q}) \cong S_n, n \geq 2$

Theorem (Pierce, T. & Wood, 2017)

Let $n \geq 2$ be fixed and let $\mathscr{F}(X)$ be the family of degree n extensions $K/\mathbb{Q}$ with square-free discriminant $D_K \in (0, X]$ and $\mathrm{Gal}(\widetilde{K}/\mathbb{Q}) \cong S_n$ as a permutation group. Then assuming the strong Artin conjecture and the Discriminant Multiplicity conjecture, for all a possible zero-density exceptional family of fields in $\mathscr{F}(X)$, each $K \in \mathscr{F}(X)$ satisfy for every integer $\ell \geq 1$ the bound

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

The condition that D_K is square-free

- includes a positive proportion of possible discriminants;
- is equivalent to a condition on the ramification type of the tamely ramified primes in K.

Other cases

In addition to the cyclic and symmetric cases described, we have theorems for G simple and $G = D_p$ for p an odd prime.

Our method uses ideas from algebraic number theory, analytic number theory, and class field theory.

Goals for the rest of this talk:

- describe how to bound $|\mathrm{Cl}_K[\ell]|$ assuming GRH;
- describe the overall structure of our method which allows us to circumvent assuming GRH;
- introduce the necessary conjectures and notions as they appear in the course of the argument.

Starting point

Theorem (Ellenberg & Venkatesh, 2007)

Suppose K/k is an extension of number fields of degree n_K, and let ℓ be a positive integer. Set $\delta < \frac{1}{2\ell(n-1)}$ and suppose that

$$\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_M$$

are primes in $\mathcal{O}_k$ with $\mathrm{Nm}_{k/\mathbb{Q}}\mathfrak{p}_j \ll (\mathrm{Nm}_{K/k}\mathrm{Disc}\,(K/k))^{\delta}$ that split completely in K. 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 K/k is an extension of number fields of degree n_K, and let ℓ be a positive integer. Set $\delta < \frac{1}{2\ell(n-1)}$ and suppose that

$$\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_M$$

are primes in $\mathcal{O}_k$ with $\mathrm{Nm}_{k/\mathbb{Q}}\mathfrak{p}_j \ll (\mathrm{Nm}_{K/k}\mathrm{Disc}\,(K/k))^{\delta}$ that split completely in K. 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 in k that split completely in K?

Starting point

Theorem (Ellenberg & Venkatesh, 2007)

Suppose K/k is an extension of number fields of degree n_K, and let ℓ be a positive integer. Set $\delta < \frac{1}{2\ell(n-1)}$ and suppose that

$$\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_M$$

are primes in $\mathcal{O}_k$ with $\mathrm{Nm}_{k/\mathbb{Q}}\mathfrak{p}_j \ll (\mathrm{Nm}_{K/k}\mathrm{Disc}(K/k))^{\delta}$ that split completely in K. 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 in k that split completely in K?

Answer: via a Chebotarev Density Theorem

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

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

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

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

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

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

The Chebotarev Density Theorem shows that prime ideals are equidistributed among the conjugacy classes in G.

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

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

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

The Chebotarev Density Theorem shows that prime ideals are equidistributed among the conjugacy classes in G.

To count completely split primes, take $\mathscr{C}$ to be the trivial class.

An Effective Chebotarev Density Theorem

Theorem (Lagarias-Odlyzko, 1975)

Let L/k be a normal extension with Galois group $G = \mathrm{Gal}(L/k)$, $D_L = |\mathrm{Disc}\, L/\mathbb{Q}|$, and $n_L = [L:\mathbb{Q}]$. There exists an effectively computable constant C_0 such that if GRH holds for the Dedekind zeta function $\zeta_L(s)$, then for any fixed conjugacy class $\mathscr{C} \subset G$ and every $x \geq 2$

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

An Effective Chebotarev Density Theorem

Theorem (Lagarias-Odlyzko, 1975)

Let L/k be a normal extension with Galois group $G = \mathrm{Gal}(L/k)$, $D_L = |\mathrm{Disc}\, L/\mathbb{Q}|$, and $n_L = [L:\mathbb{Q}]$. There exists an effectively computable constant C_0 such that if GRH holds for the Dedekind zeta function $\zeta_L(s)$, then for any fixed conjugacy class $\mathscr{C} \subset G$ and every $x \geq 2$

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

Take $x = (\mathrm{Nm}_{k/\mathbb{Q}} \mathrm{Disc}\, K/k)^{1/(2\ell(n-1))}$.

Obtain at least $M \gg (\mathrm{Nm}_{k/\mathbb{Q}} \mathrm{Disc}\, K/k)^{1/(2\ell(n-1)) - \varepsilon_0}$ sufficiently small primes $\mathfrak{p} \subset \mathcal{O}_k$ that split completely in K.

Bounding ℓ-torsion assuming GRH

Ellenberg-Venkatesh

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

Bounding ℓ-torsion assuming GRH

Ellenberg-Venkatesh

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

↓

Effective Chebotarev Density Theorem
Lagarias-Odlyzko (conditional on GRH)

$$M \gg (\mathrm{Nm}_{k/\mathbb{Q}} \mathrm{Disc}\, K/k)^{1/(2\ell(n-1))-\varepsilon_0}$$

Bounding ℓ-torsion assuming GRH

Ellenberg-Venkatesh

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

↓

Effective Chebotarev Density Theorem
Lagarias-Odlyzko (conditional on GRH)

$$M \gg (\mathrm{Nm}_{k/\mathbb{Q}} \mathrm{Disc}\, K/k)^{1/(2\ell(n-1))-\varepsilon_0}$$

↓

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

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

↓

Effective Chebotarev Density Theorem
Lagarias-Odlyzko (conditional on GRH)

$$M \gg (\mathrm{Nm}_{k/\mathbb{Q}} \mathrm{Disc}\, K/k)^{1/(2\ell(n-1))-\varepsilon_0}$$

↓

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

We will remove the assumption on GRH, at the cost of proving the result for all but a zero-density family of fields.

Bounding ℓ-torsion without assuming GRH

Ellenberg-Venkatesh

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

Bounding ℓ-torsion without assuming GRH

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

Bounding ℓ-torsion without assuming GRH

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

Bounding ℓ-torsion without assuming GRH

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

Bounding ℓ-torsion without assuming GRH

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

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

Bounding ℓ-torsion without assuming GRH

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

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

Bounding ℓ-torsion without assuming GRH

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

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

Dedekind zeta function

Let L be a Galois extension over k.

The Dedekind zeta-function attached to L is defined by

$$\zeta_L(s) = \sum_{I \subset \mathcal{O}_L} \frac{1}{N(I)^s} = \prod_{\mathfrak{p} \subset \mathcal{O}_L} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1}, \quad \Re(s) > 1.$$

Dedekind zeta function

Let L be a Galois extension over k.

The Dedekind zeta-function attached to L is defined by

$$\zeta_L(s) = \sum_{I \subset \mathcal{O}_L} \frac{1}{N(I)^s} = \prod_{\mathfrak{p} \subset \mathcal{O}_L} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1}, \quad \Re(s) > 1.$$

The Dedekind zeta-function $\zeta_L(s)$ factors as a product of Artin L-functions:

$$\zeta_L(s) = \zeta_k(s) \prod_{\substack{\rho \in G \\ \rho \neq \rho_0 \text{ irreducible}}} L(s, \rho, L/k)^{\deg \rho}$$

- ρ is an irreducible, nontrivial representation of $G = \mathrm{Gal}(L/k)$.

FACTORIZATION OF $\zeta_L(s)$ FOR $G = \mathrm{Gal}(L/\mathbb{Q}) \cong S_5$

S_5 has the following Galois representations:

- ρ_0 – trivial representation, 1-dimensional
- ρ_1 – sign representation, 1-dimensional
- ρ_2 – standard representation, 4-dimensional
- ρ_3 – product of standard and sign representation, 4-dimensional
- ρ_4 – irreducible, 5-dimensional representation
- ρ_5 – irreducible, 5-dimensional representation
- ρ_6 – exterior square of standard representation, 6-dimensional

$$\zeta_L(s) = \zeta(s)L(s,\rho_1)L(s,\rho_2)^4L(s,\rho_3)^4L(s,\rho_4)^5L(s,\rho_5)^5L(s,\rho_6)^6$$

Assumed zero-free region for $\zeta_L(s)$

$$\zeta_L(s) = \zeta_k(s) \prod_{\substack{\rho \in G \\ \rho \neq \rho_0 \text{ irreducible}}} L(s, \rho, L/k)^{\deg \rho}$$

Zero-free region for $\zeta_k(s)$:

- We assume $\zeta_k(s)$ has no exceptional zero.
- Then for $\zeta_k(s)$, it is known that there exists an absolute constant c_k such that $\zeta_k(s)$ is zero-free in the region

$$\sigma > 1 - \frac{c_k}{n_k^2 \log D_k (|t| + 3)^{n_k}}.$$

Assumed zero-free region for $\zeta_L(s)$

$$\zeta_L(s) = \zeta_k(s) \prod_{\substack{\rho \in G \\ \rho \neq \rho_0 \text{ irreducible}}} L(s, \rho, L/k)^{\deg \rho}$$

Zero-free region for $\zeta_k(s)$:

- We assume $\zeta_k(s)$ has no exceptional zero.
- Then for $\zeta_k(s)$, it is known that there exists an absolute constant c_k such that $\zeta_k(s)$ is zero-free in the region

$$\sigma > 1 - \frac{c_k}{n_k^2 \log D_k (|t|+3)^{n_k}}.$$

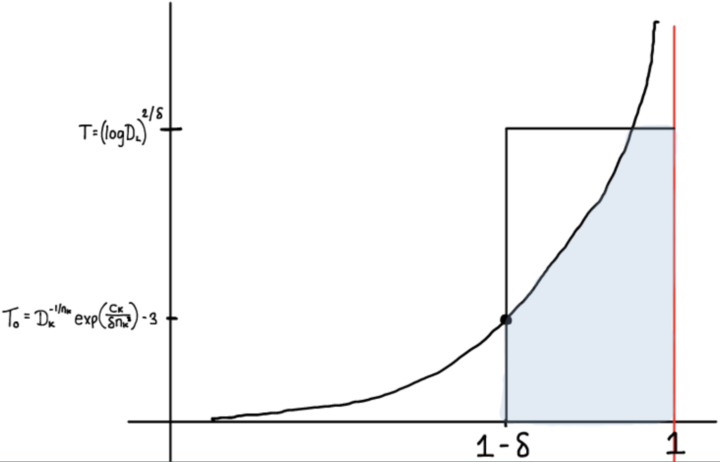
Zero-free region for $\zeta_L(s)/\zeta_k(s) = L(s, \rho)$:

- We assume that there exists a positive $\delta \leq 1/4$ such that $L(s, \rho)$ is zero-free in the region

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

ASSUMED ZERO-FREE REGION FOR $\zeta_L(s)$

$$\zeta_L(s) = \zeta_k(s) \prod_{\substack{\rho \in G \\ \rho \neq \rho_0 \text{ irreducible}}} L(s, \rho, L/k)^{\deg \rho}$$



An Effective Chebotarev Density Theorem

Theorem (Pierce, T. & Wood, 2017)

Let $0 < \delta \leq 1/4$ be a fixed positive constant. For any normal extension of number fields L/k with $[L:\mathbb{Q}] = n_L$ such that D_L is sufficiently large, $\zeta_L(s)$ obeys the assumed zero-free region, and $\zeta_k(s)$ has no exceptional zero, we have that for any conjugacy class $\mathscr{C} \subset G = \mathrm{Gal}(L/k)$

$$\left|\pi_{\mathscr{C}}(x, L/k) - \frac{|\mathscr{C}|}{|G|}\mathrm{Li}(x)\right| \leq C\frac{|\mathscr{C}|}{|G|}\frac{x}{(\log x)^2},$$

for all

$$x \geq c_1 \exp\left\{c_2(\log\log(D_L^{c_3}))^2\right\},$$

where C is an absolute constant and c_1, c_2, c_3 are explicit parameters depending on δ, n_k, n_L, D_k, and $|G|$.

Bounding ℓ-torsion without assuming GRH

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

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

Bounding ℓ-torsion without assuming GRH

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

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

Bounding ℓ-torsion without assuming GRH

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

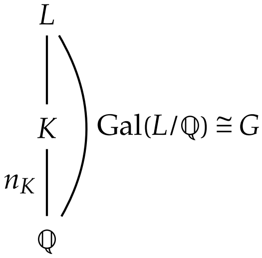
$$|\mathrm{Cl}_K[\ell]| \ll_{\ell,n,\varepsilon} D_K^{\frac{1}{2}-\frac{1}{2\ell(n-1)}+\varepsilon}.$$

Constructing a family of number fields

For the rest of the talk, we take $k = \mathbb{Q}$.

We define a family $\mathscr{F}$ of fields $K/\mathbb{Q}$ by fixing:

- the degree $[K:\mathbb{Q}] = n_K$
- the Galois group G of the Galois closure L of K
- a ramification type for all tamely ramified primes in K



Counting number fields

We assume that we can find an appropriate bound on the cardinality of the collection

$$\mathscr{F}(X) := \left\{K \in \mathscr{F} : D_K \in (0, X]\right\}.$$

Counting number fields

We assume that we can find an appropriate bound on the cardinality of the collection

$$\mathscr{F}(X) := \left\{ K \in \mathscr{F} : D_K \in (0, X] \right\}.$$

For certain families $\mathscr{F}$, this is known. For example:

$\mathrm{Gal}(\widetilde{K}/\mathbb{Q}) \cong G \cong S_3$	Davenport and Heibronn, 1971
$\mathrm{Gal}(\widetilde{K}/\mathbb{Q}) \cong G \cong S_4$	Bhargava, 2005
$\mathrm{Gal}(\widetilde{K}/\mathbb{Q}) \cong G \cong S_5$	Bhargava, 2010

Counting number fields

For G cyclic, we can compute a sufficient lower bound on $|\mathscr{F}(X)|$.

Counting number fields

For G cyclic, we can compute a sufficient lower bound on $|\mathscr{F}(X)|$.

For $G \cong S_n$ for $n \geq 2$, known lower bounds $|\mathscr{F}(X)|$ suffice.

Counting number fields

For G cyclic, we can compute a sufficient lower bound on $|\mathscr{F}(X)|$.

For $G \cong S_n$ for $n \geq 2$, known lower bounds $|\mathscr{F}(X)|$ suffice.

In other cases, one might need to assume a weak form of Malle's Conjecture:

Conjecture (Malle – weak form)

Let $K/\mathbb{Q}$ be a number field of degree n_K, and $G = \mathrm{Gal}(\widetilde{K}/\mathbb{Q})$ a transitive subgroup of S_n. For all $\varepsilon > 0$, there exist constants $\mu_1 = \mu_1(G)$ and $\mu_2 = \mu_2(G, \varepsilon) > 0$ such that for all $X \geq 1$,

$$\mu_1 X^{a(G)} \leq |\mathscr{F}(X)| \leq \mu_2 X^{a(G)+\varepsilon}$$

where $a(G)$ is a number depending on the index of G and satisfies $1/(n-1) \leq a(G) \leq 1$.

Checking in

We have defined a family $\mathscr{F}$ of fields and a collection

$$\mathscr{F}(X) := \left\{K \in \mathscr{F} : D_K \in (0, X]\right\}.$$

In some cases, we can compute appropriate bounds of $|\mathscr{F}(X)|$, in other cases we must assume a weak form of Malle's Conjecture.

Show assumed zero-free region is obeyed
by "most" number fields in $\mathscr{F}(X)$.

We must introduce automorphic L-functions.

Counting zeros of automorphic L-functions

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

Let $s = \beta + i\gamma$ denote a zero of the corresponding automorphic L-function, $L(s, \pi)$.

Counting zeros of automorphic L-functions

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

Let $s = \beta + i\gamma$ denote a zero of the corresponding automorphic L-function, $L(s, \pi)$.

Define

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

Counting zeros of automorphic L-functions

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

Let $s = \beta + i\gamma$ denote a zero of the corresponding automorphic L-function, $L(s, \pi)$.

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.

Zero-free region for a family of automorphic L-functions

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.

ZERO-FREE REGION FOR A FAMILY OF AUTOMORPHIC L-FUNCTIONS

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 for all but a possible zero-density subfamily of L-functions

A couple of issues:

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

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

A couple of issues:

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

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

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

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

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

A couple of issues:

$$\frac{\zeta_L(s)}{\zeta(s)} = \prod_{\substack{\pi \neq \pi_0 \\ \pi \text{ cuspidal}}} L(s,\pi)^{d_j}$$

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.

Applying Kowalski-Michel

Let L denote the Galois closure of K over $\mathbb{Q}$.

$$\frac{\zeta_L(s)}{\zeta(s)} = L(s,\pi_1)^{d_1} \cdots L(s,\pi_j)^{d_j} \cdots L(s,\pi_r)^{d_r}$$

Applying Kowalski-Michel

Let L denote the Galois closure of K over $\mathbb{Q}$.

$$\frac{\zeta_L(s)}{\zeta(s)} = L(s,\pi_1)^{d_1} \cdots L(s,\pi_j)^{d_j} \cdots L(s,\pi_r)^{d_r}$$

For each j,

- let $\mathscr{L}_j$ denote the subfamily of $L(s,\pi_j)^{d_j}$ as K varies over the family $\mathscr{F}$;

Applying Kowalski-Michel

Let L denote the Galois closure of K over $\mathbb{Q}$.

$$\frac{\zeta_L(s)}{\zeta(s)} = L(s,\pi_1)^{d_1} \cdots L(s,\pi_j)^{d_j} \cdots L(s,\pi_r)^{d_r}$$

For each j,

- let $\mathscr{L}_j$ denote the subfamily of $L(s,\pi_j)^{d_j}$ as K varies over the family $\mathscr{F}$;
- apply Kowalski & Michel's zero-density result for cuspidal automorphic L-functions to the subfamily $\mathscr{L}_j$;

Applying Kowalski-Michel

Let L denote the Galois closure of K over $\mathbb{Q}$.

$$\frac{\zeta_L(s)}{\zeta(s)} = L(s,\pi_1)^{d_1} \cdots L(s,\pi_j)^{d_j} \cdots L(s,\pi_r)^{d_r}$$

For each j,

- let $\mathscr{L}_j$ denote the subfamily of $L(s,\pi_j)^{d_j}$ as K varies over the family $\mathscr{F}$;
- apply Kowalski & Michel's zero-density result for cuspidal automorphic L-functions to the subfamily $\mathscr{L}_j$;
- conclude a zero-density set of exceptional L-functions in $\mathscr{L}_j$ can potentially fail to have the desired zero-free region.

Applying Kowalski-Michel

Let L denote the Galois closure of K over $\mathbb{Q}$.

$$\frac{\zeta_L(s)}{\zeta(s)} = L(s,\pi_1)^{d_1} \cdots L(s,\pi_j)^{d_j} \cdots L(s,\pi_r)^{d_r}$$

For each j,

- let $\mathscr{L}_j$ denote the subfamily of $L(s,\pi_j)^{d_j}$ as K varies over the family $\mathscr{F}$;
- apply Kowalski & Michel's zero-density result for cuspidal automorphic L-functions to the subfamily $\mathscr{L}_j$;
- conclude a zero-density set of exceptional L-functions in $\mathscr{L}_j$ can potentially fail to have the desired zero-free region.

Key technical point: for each j, we must quantify how many fields L in the family of Galois closures could contain any given exceptional L-function in $\mathscr{L}_j$.

Bounding ℓ-torsion without assuming GRH

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

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

Bounding ℓ-torsion without assuming GRH

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

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

Controlling Propagation

Theorem (Klüners & Nicolae, 2016)

Let $L_1/\mathbb{Q}$ and $L_2/\mathbb{Q}$ be finite Galois extensions. For $j = 1,2$ let G_j denote the Galois group of $L_j/\mathbb{Q}$ and χ_j a faithful character of G_j. If

$$L(s, \chi_1, L_1/\mathbb{Q}) = L(s, \chi_2, L_2/\mathbb{Q})$$

then

$$L_1 = L_2 \quad \text{and } \chi_1 = \chi_2.$$

Controlling Propagation

Theorem (Klüners & Nicolae, 2016)

Let $L_1/\mathbb{Q}$ and $L_2/\mathbb{Q}$ be finite Galois extensions. For $j = 1, 2$ let G_j denote the Galois group of $L_j/\mathbb{Q}$ and χ_j a faithful character of G_j. If

$$L(s, \chi_1, L_1/\mathbb{Q}) = L(s, \chi_2, L_2/\mathbb{Q})$$

then

$$L_1 = L_2 \quad \text{and } \chi_1 = \chi_2.$$

For relative extensions L/k, with $k \neq \mathbb{Q}$, the authors show that the Artin L-function need not detect the identity of fields.

Counting number fields

We reduce the problem to counting the number of appropriate distinct subfields

$$\mathbb{Q} \subset F \subset L$$

that arise as K varies.

Counting number fields

We reduce the problem to counting the number of appropriate distinct subfields

$$\mathbb{Q} \subset F \subset L$$

that arise as K varies.

We must control what primes can divide D_K, and thus we restrict to inertia types that

- generate all of G and
- control the propagation of bad fields;

Counting number fiels

In certain cases we also assume the Discriminant Multiplicity Conjecture:

Conjecture (Discriminant Multiplicity Conjecture)

Let $M_d(D)$ be the number of degree d number fields $K/\mathbb{Q}$ with $D_K = D$. Then for each $d \geq 1$

$$M_d(D) \ll_{d,\varepsilon} D^{\varepsilon}$$

for every $D \geq 1$.

Counting number fiels

In certain cases we also assume the Discriminant Multiplicity Conjecture:

Conjecture (Discriminant Multiplicity Conjecture)

Let $M_d(D)$ be the number of degree d number fields $K/\mathbb{Q}$ with $D_K = D$. Then for each $d \geq 1$

$$M_d(D) \ll_{d,\varepsilon} D^{\varepsilon}$$

for every $D \geq 1$.

- Assuming the Discriminant Multiplicity Conjecture for all degrees d gives the full ℓ-torsion conjecture.
- We assume it only for $d = n$ (fixed) and get a bound on ℓ-torsion for all ℓ.

COUNTING NUMBER FIELS

In certain cases we also assume the Discriminant Multiplicity Conjecture:

Conjecture (Discriminant Multiplicity Conjecture)

Let $M_d(D)$ be the number of degree d number fields $K/\mathbb{Q}$ with $D_K = D$. Then for each $d \geq 1$

$$M_d(D) \ll_{d,\varepsilon} D^{\varepsilon}$$

for every $D \geq 1$.

- Assuming the Discriminant Multiplicity Conjecture for all degrees d gives the full ℓ-torsion conjecture.
- We assume it only for $d = n$ (fixed) and get a bound on ℓ-torsion for all ℓ.
- We do not need to assume this conjecture for cyclic fields.

Bounding ℓ-torsion without assuming GRH

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

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

Bounding ℓ-torsion without assuming GRH

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

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

$G = \mathrm{Gal}(\widetilde{K}/\mathbb{Q}) \cong S_n, n \geq 2$

Theorem (Pierce, T. & Wood, 2017)

Let $n \geq 2$ be fixed and let $\mathscr{F}(X)$ be the family of degree n extensions $K/\mathbb{Q}$ with square-free discriminant $D_K \in (0, X]$ and $\mathrm{Gal}(\widetilde{K}/\mathbb{Q}) \cong S_n$ as a permutation group. Then assuming the strong Artin conjecture and the Discriminant Multiplicity conjecture, for all a possible zero-density exceptional family of fields in $\mathscr{F}(X)$, each $K \in \mathscr{F}(X)$ satisfy for every integer $\ell \geq 1$ the bound

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

Thank you